

# The Effective Shafarevich Conjecture

by

**Robin Visser**

**Thesis**

Submitted to the University of Warwick

for the degree of

**Doctor of Philosophy**

**Mathematics Institute**

September 2024

THE UNIVERSITY OF  
**WARWICK**

# Contents

<b>List of Tables</b>	<b>v</b>
<b>List of Algorithms</b>	<b>viii</b>
<b>List of Figures</b>	<b>ix</b>
<b>Acknowledgments</b>	<b>x</b>
<b>Declarations</b>	<b>xii</b>
<b>Abstract</b>	<b>xiii</b>
<b>List of Notation</b>	<b>xiv</b>
<b>Chapter 1 Introduction</b>	<b>1</b>
1.1 History . . . . .	6
1.1.1 Elliptic Curves . . . . .	6
1.1.2 Higher genus curves . . . . .	11
1.1.3 Higher dimension abelian varieties . . . . .	12
1.2 Hyperelliptic Curves . . . . .	13
1.2.1 Affine models . . . . .	15
1.2.2 Good reduction and minimal discriminants . . . . .	16
1.2.3 Rosenhain normal form . . . . .	17
1.3 Jacobians . . . . .	19
1.3.1 Primes of almost good reduction . . . . .	22
1.3.2 Computing with the Jacobian . . . . .	23
1.3.3 Fields of $n$ -torsion on the Jacobian . . . . .	24
1.4 Cluster pictures . . . . .	27
1.5 Invariants of hyperelliptic curves . . . . .	31
1.5.1 Invariants for genus 2 curves . . . . .	32

1.6	$L$ -functions . . . . .	33
1.6.1	Primes $\mathfrak{p}$ of good reduction for $C$ . . . . .	35
1.6.2	Primes $\mathfrak{p}$ of bad reduction for $C$ . . . . .	36
1.6.3	Genus 2 case . . . . .	37
1.7	Modularity results and conjectures . . . . .	37
1.7.1	Elliptic curves . . . . .	38
1.7.2	Higher dimensions . . . . .	40
<b>Chapter 2 Potential good reduction of hyperelliptic curves</b>		<b>43</b>
2.1	Preliminaries . . . . .	45
2.1.1	Potential good reduction for hyperelliptic curves $C$ . . . . .	45
2.1.2	Potential good reduction for $\text{Jac}(C)$ . . . . .	47
2.2	Potential good reduction of hyperelliptic curves . . . . .	53
2.3	Hyperelliptic curves with rational Weierstrass points . . . . .	59
2.4	Upper bounds for $c_K(g)$ . . . . .	62
<b>Chapter 3 Elliptic and hyperelliptic curves over <math>\mathbb{Z}_\ell</math>-cyclotomic extensions</b>		<b>67</b>
3.1	Units and $S$ -units of $\mathbb{Q}(\zeta)$ . . . . .	72
3.1.1	Cyclotomic units and $S$ -units . . . . .	74
3.1.2	Units and $S$ -units from cyclotomic polynomials . . . . .	76
3.2	The $S$ -unit equation over $\mathbb{Q}(\zeta_{\ell^n})^+$ . . . . .	77
3.2.1	Proof of Theorem 3.2 for $\ell = 2$ and $3$ . . . . .	81
3.2.2	Proof of Theorem 3.1 for $\ell = 2$ . . . . .	81
3.3	The unit equation over $\mathbb{Q}(\zeta_{\ell^n})^+$ . . . . .	81
3.4	The $S$ -unit equation over $\mathbb{Q}_{\infty,5}$ . . . . .	82
3.5	The $S$ -unit equation over $\mathbb{Q}_{\infty,7}$ . . . . .	85
3.6	Isogeny classes of elliptic curves over $\mathbb{Q}_{\infty,\ell}$ . . . . .	87
3.7	From $S$ -unit equations to elliptic curves . . . . .	89
3.8	Hyperelliptic curves over $\mathbb{Q}_{\infty,\ell}$ with few bad primes . . . . .	92
3.9	Isogeny classes of hyperelliptic curves over $\mathbb{Q}_{\infty,\ell}$ . . . . .	98
3.10	Endomorphism rings . . . . .	104
<b>Chapter 4 Abelian surfaces <math>A/\mathbb{Q}</math> with full rational 2-torsion</b>		<b>106</b>
4.1	Fields of 2-power torsion . . . . .	108
4.2	The Faltings–Serre method . . . . .	112
4.2.1	Deviation groups . . . . .	113
4.2.2	The case where $\bar{\rho}_i$ is trivial . . . . .	116

4.2.3	Livné's criterion . . . . .	118
4.2.4	Grenié's criterion . . . . .	120
4.3	Computational results . . . . .	124
4.3.1	Elliptic curves . . . . .	125
4.3.2	Abelian surfaces . . . . .	126
4.3.3	Solving the conjugacy problem for $\mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ . . . . .	132
4.3.4	Computing the possible Galois groups $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ . . . . .	134
4.3.5	Searching for rank 2 subgroups of $\mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ . . . . .	135

**Chapter 5 Computing abelian surfaces  $A/\mathbb{Q}$  with good reduction outside 2** **139**

5.1	Computing $L$ -functions of 2-power conductor . . . . .	141
5.1.1	Computing $L$ -functions of 2-power conductor . . . . .	145
5.1.2	Results . . . . .	149
5.1.3	Further constraining the Jacobian 2-torsion . . . . .	150
5.2	Computing genus 2 curves with good reduction outside $S$ . . . . .	153
5.2.1	Number fields unramified away from 2 . . . . .	155
5.2.2	Solving the $S$ -unit equations . . . . .	156
5.2.3	$S$ -unit Galois constraints . . . . .	159
5.2.4	Equivalence classes of polynomials . . . . .	160
5.2.5	Initialising the linear system . . . . .	162
5.2.6	Closest Vector Problem . . . . .	165
5.2.7	Integer Linear Programming . . . . .	168
5.3	Gluing elliptic curves . . . . .	170
5.3.1	Gluing elliptic curves $E/\mathbb{Q}$ with good reduction away from 2 . . . . .	172

**Chapter 6 List of abelian surfaces  $A/\mathbb{Q}$  with good reduction outside 2** **175**

6.1	Computational results and Statistics . . . . .	176
6.1.1	Minimal Weierstrass model . . . . .	176
6.1.2	Automorphism group . . . . .	177
6.1.3	Torsion subgroup . . . . .	177
6.1.4	Conductor . . . . .	178
6.1.5	Mordell-Weil group and Rank . . . . .	179
6.1.6	Endomorphisms of the Jacobian . . . . .	180
6.1.7	Sato-Tate group . . . . .	181
6.1.8	Jacobian decomposition . . . . .	183
6.1.9	Isogenies . . . . .	183

6.1.10	Rational points . . . . .	186
6.1.11	$L$ -function and BSD invariants . . . . .	188
6.1.12	Mod- $\ell$ Galois images . . . . .	190
6.2	List of $\mathbb{Q}$ -isogeny classes of abelian surfaces $A/\mathbb{Q}$ . . . . .	191
6.3	List of genus 2 curves $C/\mathbb{Q}$ . . . . .	209
6.4	List of $\overline{\mathbb{Q}}$ -isomorphism classes of genus 2 curves . . . . .	251
<b>Appendix A Field systems of genus 2 curves</b>		<b>260</b>
<b>Appendix B Mod-<math>\ell</math> Galois images</b>		<b>263</b>
B.1	Mod 2 Galois images . . . . .	263
B.2	Mod 3 Galois images . . . . .	265
<b>Bibliography</b>		<b>271</b>

# List of Tables

1.1	Elliptic curves $E/\mathbb{Q}$ with good reduction outside $S$ . . . . .	7
1.2	Elliptic curves $E$ over quadratic fields $K$ with good reduction outside $S$ . . . . .	7
1.3	Factorisation of the ideals $(\alpha_i - \alpha_j)$ (i.e. up to units) . . . . .	30
4.1	A list of the possible values for $\text{tr}(M)$ , where $M \in \text{GL}_2(\mathbb{Z}/2^{10}\mathbb{Z})$ such that $M \equiv I \pmod{2}$ , $\det(M) = p$ , and $ \text{tr}(M)  \leq 2\sqrt{p}$ . . . . .	125
4.2	For each odd prime $p = 3, 5, \dots, 31$ , we tabulate the number of good Euler factors $L_p(T)$ for dimension 2 abelian varieties $A/\mathbb{Q}$ . . . . .	127
4.3	For each odd prime $p$ , we tabulate the number of possible Euler factors $L_p(T)$ of good reduction which correspond to some matrix $M \in \text{GSp}_4(\mathbb{Z}/2^n\mathbb{Z})$ such that $M \equiv I \pmod{2}$ and $\det(M) \equiv p^2 \pmod{2^n}$ . . . . .	127
4.4	For each $n \leq 6$ , we tabulate the possibilities for the $2^n$ -torsion field $\mathbb{Q}(A[2^n])$ (if known), its Galois group $\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ , and the corresponding number of valid Euler factors obtained for $L_p(T)$ obtained from $\text{GSp}_4(\mathbb{Z}/2^n\mathbb{Z})$ using Algorithm 6. . . . .	131
4.5	A summary of the Euler factors $L_p(T)$ for the three isogeny classes of principally polarised abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2 and with $\mathbb{Q}(A[2]) = \mathbb{Q}$ . . . . .	131
5.1	List of all 234 known degree 4 rational motivic weight 1 $L$ -functions of conductor $2^n$ , each corresponding to an isogeny class of abelian surfaces $A/\mathbb{Q}$ of conductor $2^n$ . The set of $L$ -functions for $N \leq 2^9$ is conditionally complete, assuming the paramodular conjecture. . . . .	145
5.2	Number of Euler factors $L_p(T)$ such that both $L_p(1)$ and $L_p(-1)$ are divisible by $\#\text{Jac}(C)(\mathbb{Q})[2]$ . . . . .	152

5.3	For each odd prime $p \leq 31$ , we tabulate the number of possible degree 4 Euler factors $L_p(T)$ of good reduction which are the characteristic polynomial of some matrix $M \in \mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$ such that $M$ fixes at least 8 points (mod 2). . . . .	153
5.4	Summary of the number fields of degree at most 6 unramified away from 2 . . . . .	156
5.5	List of possible types of field systems for genus 2 curves $C : y^2 = f(x)$ with $\mathbb{Q}(\mathcal{R})$ unramified outside 2. Here $K_*$ (resp. $L_*$ ) denotes an arbitrary number field of degree 2 (resp. 4) unramified away from 2. The number of rational 2-torsion points on $\mathrm{Jac}(C)$ corresponding to each field system is also tabulated. . . . .	157
5.6	Summary of the three possible octic fields which contain $\mathbb{Q}(\mathcal{R})$ . . . .	157
5.7	Number of $S$ -unit solutions to $\tau_1 + \tau_2 = 1$ where $\tau_i \in \mathcal{O}_S^\times$ over the field $K$ . All computations were run by Matschke [307]. For each $S$ -unit equation, the total CPU time in seconds (rounded to the nearest second) is also given. . . . .	158
5.8	Summary of all possible values of $\sigma(\lambda)$ for the cross ratio $\lambda = (\alpha_i - \alpha_j)(\alpha_k - \alpha_\ell)/((\alpha_i - \alpha_k)(\alpha_j - \alpha_\ell))$ for all 24 possible permutations $\sigma \in S_4$	160
5.9	Number of solutions to $\tau_1 + \tau_2 = 1$ where $\tau_i \in \mathcal{O}_S^\times$ such that $\sigma(\tau_1) = 1 - \tau_1$ for an order 2 automorphism $\sigma \in \mathrm{Aut}(M/\mathbb{Q})$ . . . . .	161
5.10	The system of linear constraints corresponding to each possible cluster picture $\Sigma_p$ of an odd prime $p$ of almost good reduction for a genus 2 curve $C : y^2 = f(x)$ where $\deg(f) = 6$ . Here $\psi_{i_p}$ denotes an $S$ -unit generator lying above the prime $p$ . . . . .	165
5.11	The $\mathbb{Q}$ -isogeny classes of elliptic curves $E/\mathbb{Q}$ with good reduction outside 2 . . . . .	172
5.12	Table of all 55 isogeny classes of abelian surfaces $A$ which split over $\mathbb{Q}$ , i.e. where $A$ is $\mathbb{Q}$ -isogenous to $E_1 \times E_2$ for some two elliptic curves $E_1, E_2$ over $\mathbb{Q}$ with good reduction outside 2. Each cell in the table gives the number of known genus 2 curves $C/\mathbb{Q}$ whose Jacobian is isogenous to $E_1 \times E_2$ (with the rows (resp. columns) denoting the Cremona label of the isogeny class of $E_1$ (resp. $E_2$ )). . . . .	174
6.1	Primes of (geometric) bad reduction for $C/\mathbb{Q}$ . . . . .	176
6.2	Possible types of field systems for our genus 2 curves $C/\mathbb{Q}$ . . . . .	176
6.3	Automorphism groups for $C$ over $\mathbb{Q}$ . . . . .	177
6.4	Automorphism groups for $C$ over $\overline{\mathbb{Q}}$ . . . . .	177

6.5	Torsion subgroup $J(\mathbb{Q})_{\text{tors}}$ of the Jacobian $J$ of $C/\mathbb{Q}$ . . . . .	178
6.6	Conductor $N$ of the Jacobian $\text{Jac}(C)$ for each curve $C$ . . . . .	179
6.7	Two-Selmer groups $\text{Sel}^{(2)}(J)$ of $J = \text{Jac}(C)$ . . . . .	179
6.8	Endomorphism algebra $\text{End}(J) \otimes \mathbb{Q}$ of $J = \text{Jac}(C)$ . . . . .	180
6.9	Geometric endomorphism algebra $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ of $J = \text{Jac}(C)$ . . . .	181
6.10	The endomorphism field $J_{\text{endo}}$ of $J = \text{Jac}(C)$ . . . . .	181
6.11	Identity component $\text{ST}^0(J)$ of the Sato-Tate group $\text{ST}(J)$ , and the corresponding real geometric endomorphism algebra $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$ .	182
6.12	Sato-Tate group $\text{ST}(J)$ of the Jacobian $J$ of $C$ . . . . .	183
6.13	Minimal degree of a number field $E$ such that $\text{Jac}(C)$ splits over $E$ .	183
6.14	Pairs of non-isomorphic curves $(C_1, C_2)$ whose Jacobians are $\mathbb{Q}$ -isogenous of odd degree. . . . .	185
6.15	Number of isogeny classes in Table 6.20 containing $n$ known Jacobians.	186
6.16	Number of known rational points $\#C(\mathbb{Q})$ found on $C$ . . . . .	187
6.17	Analytic order $ \text{III}_{\text{an}} $ of the Tate-Shafarevich group (for curves $C/\mathbb{Q}$ where $ \text{III}_{\text{an}} $ could be computed) . . . . .	190
6.18	Image of the mod 2 Galois representation $\bar{\rho}_{C,2} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GSp}_4(\mathbb{F}_2)$	191
6.19	Index of the image of the mod 3 Galois representation $\bar{\rho}_{C,3} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow$ $\text{GSp}_4(\mathbb{F}_3)$ . . . . .	192
6.20	A list of the 234 known isogeny classes of abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2. . . . .	194
6.21	A list of 512 known genus 2 curves $C/\mathbb{Q}$ whose Jacobian has good reduction away from 2. . . . .	211
6.22	The 67 known $\overline{\mathbb{Q}}$ -isomorphism classes of genus 2 curves $C/\mathbb{Q}$ whose Jacobian has good reduction away from 2. . . . .	252
A.1	The 48 possible field systems $[M_1, M_2, \dots, M_m]$ of genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2. . . . .	260
B.1	The 15 possible mod 2 Galois images $\text{Im}(\bar{\rho}_{C,2})$ in $\text{GSp}_4(\mathbb{F}_2)$ for the known 512 genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2 . . . . .	263
B.2	The 33 possible mod 3 Galois images $\text{Im}(\bar{\rho}_{C,3})$ in $\text{GSp}_4(\mathbb{F}_3)$ for the known 512 genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2 . . . . .	266



# List of Algorithms

1	Probabilistic algorithm to compute whether $A, B \in \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ are conjugate . . . . .	133
2	Probabilistic algorithm to compute a set of conjugacy class representatives in $\mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ . . . . .	134
3	Computing all central $C_2^k$ -extensions $H$ of a finite group $G$ such that $H$ is a quotient of $\langle a, b \mid a^2 = 1 \rangle$ . . . . .	135
4	Probabilistic algorithm to compute whether two matrices $A, B \in \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ are $C$ -stable conjugate. . . . .	136
5	Probabilistic algorithm to compute $C$ -stable conjugacy class representatives in $\mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ . . . . .	137
6	Compute the possible Euler factors $L_p(T)$ at an odd prime $p$ for a dimension $d$ abelian variety $A/\mathbb{Q}$ with good reduction away from 2 (using $\mathrm{GSp}_{2d}(\mathbb{Z}/2^n\mathbb{Z})$ ) . . . . .	138
7	Compute all possible rational degree $2g$ good Euler factors at $p$ . . .	149
8	Compute all possible rational degree $2g$ bad Euler factors at $p$ . . .	150
9	A breadth-first search algorithm to compute all possible tuples of the first few Dirichlet coefficients $(a_1, a_2, \dots, a_{p_k})$ of a rational degree 4 motivic weight 1 $L$ -function of conductor $N$ and sign $\varepsilon$ . . . . .	151
10	Algorithm to compute all genus 2 curves $C/\mathbb{Q}$ with good reduction outside $S$ and such that $\mathrm{Jac}(C)$ has good reduction outside 2 (using the Closest Vector approach) . . . . .	167
11	Algorithm to compute all genus 2 curves $C/\mathbb{Q}$ with good reduction outside $S$ and such that $\mathrm{Jac}(C)$ has good reduction outside 2 (using the integer linear programming (ILP) method) . . . . .	169

# List of Figures

1.1	Cluster picture $\Sigma_3$ for the genus 2 curve $C$ given in (1.17). . . . .	30
2.1	A chain of clusters $\mathfrak{s} \subsetneq C_1 \subsetneq C_2 \subsetneq \cdots \subsetneq C_n$ . . . . .	49
2.2	The four possible cluster pictures $\Sigma_{\mathfrak{p}}$ for a prime $\mathfrak{p}$ of bad reduction for $C$ but good reduction for $\text{Jac}(C)$ for a genus 2 curve $C/K$ . . . .	49
2.3	Cluster picture $\Sigma_p$ for primes $p$ dividing $2^r + 1$ . . . . .	50
2.4	Cluster picture $\Sigma_p$ for primes $p$ dividing $2^r - 1$ . . . . .	50
2.5	Cluster picture $\Sigma_p$ for primes $p$ dividing $k$ . . . . .	51
2.6	One of the four possible cluster pictures $\Sigma_p$ for primes $p$ dividing $k^2 - \ell^2$ . . . . .	52
4.1	Field diagram of various 2-extensions of $\mathbb{Q}$ unramified away from 2. In the case of Theorem 4.6, we have that $\mathbb{Q}(A[4]) = \mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(A[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$ . . . . .	111

# Acknowledgments

Oh boy, where do I begin. It goes without saying that my deepest gratitude goes to my supervisor, Professor Samir Siksek. I've been sitting here for ages trying to come up with exactly the right words to express my thanks, but this seems like a near-impossible task. I think I'll just keep this short and simply thank Samir for his tremendous support, endless patience, countless ideas, brilliant sense of humour, and unwavering encouragement throughout the past four years! Almost every week I would come to his office with some particular problem — often trivial in hindsight — and he always knew exactly how to tackle it with fresh insights and new avenues to explore. This thesis owes more to Samir than I could possibly express in words, and I've been incredibly fortunate to have had the opportunity to learn from him.

Let me also express my deep thanks to my PhD examiners, Damiano Testa and Martin Bright, for their meticulous reading of an earlier draft of this thesis and for a very enjoyable viva. Their many valuable comments, feedback, and suggestions have greatly improved this work, and I am especially grateful to them for catching many of my typos!

Many people have played an essential role in contributing ideas and discussions to this thesis. While it would be impossible to mention everyone who has contributed in one way or another, I'd particularly like to thank Raymond van Bommel, Armand Brumer, Noam Elkies, David Farmer, David Loeffler, Davide Lombardo, Benjamin Matschke, Pieter Moree, Ariel Pacetti, Ignasi Sánchez Rodríguez, Jeroen Sijsling, Andrew Sutherland, Damiano Testa, and John Voight for their many valuable discussions, feedback, and helpful emails. If I haven't mentioned you, and you think I should have - my sincerest apologies!

I am also grateful to the anonymous referees for their useful feedback on Chapters 2 and 3 of this thesis.

A big thank you to the organisers of all the conferences and workshops I attended during my time at Warwick, for giving me the opportunity to present my research. I would also like to thank the entire Number Theory group at Warwick for their wonderful support, lovely lunch discussions, and for the beautiful long walks from Leamington Spa to the Maths Institute.

I am also very grateful to the UK Engineering and Physical Sciences Research Council and the Warwick Mathematics Institute for funding this opportunity to pursue my PhD.

Finally, I want to thank all the teachers, mentors, and supervisors who have guided me on my path to Warwick. In particular, Dirk Basson, Phil Labuschagne, Vanessa October, Angela Roberts, Juana Sanchez-Ortega, and Stephan Wagner — thank you.

And last, but certainly not least, a huge amount of gratitude goes to my family. Writing this thesis would not have been possible without their endless love, encouragement, and support (not to mention the wonderful company of all their cats)!

This thesis was typeset with L<sup>A</sup>T<sub>E</sub>X 2<sub>ε</sub><sup>1</sup> by the author.

---

<sup>1</sup>L<sup>A</sup>T<sub>E</sub>X 2<sub>ε</sub> is an extension of L<sup>A</sup>T<sub>E</sub>X. L<sup>A</sup>T<sub>E</sub>X is a collection of macros for T<sub>E</sub>X. T<sub>E</sub>X is a trademark of the American Mathematical Society. The style package *warwickthesis* was used.

# Declarations

This thesis is submitted to the University of Warwick in support of my application for the degree of Doctor of Philosophy. It has been composed by myself and has not been submitted in any previous application for any degree. The work presented was carried out by the author except in the cases outlined below.

Chapter 1 introduces the effective Shafarevich conjecture and defines the relevant concepts used in this thesis. It contains no original research and is purely expository in nature.

Chapter 2 presents new results regarding the potential good reduction of hyperelliptic curves and their Jacobians, and has been submitted for publication [465]. Chapter 3 investigates the Shafarevich conjecture over  $\mathbb{Z}_\ell$ -cyclotomic extensions, and was written jointly with Samir Siksek and has been published in *Algebra & Number Theory* [413]. At the start of each of these chapters, we have indicated how its content in this thesis differs in any significant way from the preprint versions.

Chapters 4, 5, and 6 present, unless otherwise stated, new unpublished work giving various theoretical and computational techniques for computing abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2.

# Abstract

Let  $K$  be a number field,  $d$  a positive integer, and  $S$  a finite set of primes of  $K$ . One of the crowning achievements of 20th-century arithmetic geometry was Faltings' proof that there are only finitely many isomorphism classes of dimension  $d$  abelian varieties  $A/K$  with good reduction away from  $S$ . While many effective algorithms have been developed to explicitly classify elliptic curves  $E/K$  with good reduction outside a finite set of primes  $S$ , effectively solving this problem in higher dimensions remains a challenge. Developing an algorithm that can effectively output a set of all such dimension  $d$  abelian varieties  $A/K$  with good reduction away from  $S$  is known as the *effective Shafarevich problem*, which remains unsolved.

In this thesis, we begin by giving an introduction and survey on some known methods for classifying abelian varieties  $A/K$  with good reduction away from a finite set of primes, starting with the case of elliptic curves for which a wealth of known algorithms exist.

In Chapter 2, we investigate the existence of infinitely many genus  $g$  hyperelliptic curves  $C/K$  with potential good reduction outside a fixed number of primes in  $K$ , and give explicit lower and upper bounds on the number of such primes that can occur. In Chapter 3, we show that the analogous Shafarevich conjecture over  $\mathbb{Z}_\ell$ -cyclotomic extensions of number fields fails to hold by exhibiting numerous examples of infinite families of elliptic curves  $E/\mathbb{Q}_{\infty,\ell}$  and hyperelliptic curves  $C/\mathbb{Q}_{\infty,\ell}$  with good reduction outside a fixed small number of primes  $S$  in  $\mathbb{Q}_{\infty,\ell}$ .

Chapters 4 through 6 present new theoretical and computational methods for computing abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2, making substantial progress toward resolving the effective Shafarevich conjecture for  $K = \mathbb{Q}$ ,  $d = 2$ , and  $S = \{2\}$ . In Chapter 4, we prove that there exist exactly three isogeny classes of principally polarized abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 which contain surfaces with full rational 2-torsion. In Chapter 5, we develop new methods to classify hyperelliptic curves  $C/K$  with good reduction outside  $S$ , extending Smart's method by using the closest vector method (CVP) and integer linear programming (ILP). Finally, Chapter 6 concludes this thesis with our *pièce de résistance*: a detailed set of tables describing the 234 known isogeny classes of abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2, including the 512 known genus 2 curves  $C/\mathbb{Q}$  whose Jacobians have good reduction outside 2.

# List of Notation

$\mathbb{Q}$	The rational field
$\mathbb{A}^n$	Affine $n$ -space
$\mathbb{P}^n$	Projective $n$ -space
$\mathbb{P}_{d_1, d_2, d_3}^2$	Weighted projective plane (of weights $d_1$ , $d_2$ , and $d_3$ )
$\mathcal{O}_K$	The ring of algebraic integers in $K$ .
$\mathcal{O}_K^\times$	The group of units in $K$ .
$\mathcal{O}_{K,S}$	The ring of $S$ -integers in $K$ .
$\mathcal{O}_{K,S}^\times$	The group of $S$ -units of $K$ .
$\overline{K}$	An algebraic closure of $K$ ,
$G_K$	The absolute Galois group of $K$ , i.e. the Galois group of $\overline{K}/K$ .
$A(K)$	The group of $K$ -rational points on an abelian variety $A/K$ .
$A[m]$	The $m$ -torsion subgroup of an abelian variety $A$ .
$\widehat{A}$	The dual abelian variety of $A$ .
$\text{III}_{A/K}$	The Tate-Shafarevich group of an abelian variety $A/K$ .
$R_{A/K}$	The regulator of an abelian variety $A/K$ .
$(g_1, g_2, g_3)$	The G2-invariants of a genus 2 curve $C/K$ .
$\text{Hom}(A_1, A_2)$	The group of isogenies from $A_1$ to $A_2$ .
$N(\mathfrak{p})$	The norm of the prime ideal $\mathfrak{p}$ .
$\text{Pic}^0(C)$	The degree zero divisor classes of the Picard group of $C$ .
$\mathbb{A}_F$	The ring of adeles of a global field $F$ .
$\Sigma_{\mathfrak{p}}$	The cluster picture of a hyperelliptic curve at the prime $\mathfrak{p}$ .
$d_{\mathfrak{s}}$	The depth of a cluster $\mathfrak{s}$ ; i.e. $\min_{r, r' \in \mathfrak{s}} v_{\mathfrak{p}}(r - r')$ .
$r \wedge \mathfrak{s}$	The smallest cluster containing both $r$ and $\mathfrak{s}$ .
$\pi_{K, \text{odd}}(n)$	The number of odd primes in $K$ with norm $\leq n$ .
$\mathcal{B}_{\text{odd}}(C/K)$	The set of odd primes $\mathfrak{p}$ in $K$ for which $C/K$ does not have potential good reduction at $\mathfrak{p}$ .

- $\mathfrak{f}_K$  The conductor of an abelian number field  $K$ .
- $\Phi_m$  The  $m$ -th cyclotomic polynomial.
- $\mathbb{Z}_\ell$  The  $\ell$ -adic integers.
- $\mu_n$  The set of  $\ell^n$ -th roots of unity.
- $\mathbb{Q}_{n,\ell}$  The unique degree  $\ell^n$  totally real subfield of  $\cup_{r=1}^\infty \mathbb{Q}(\mu_r)$ .
- $\mathbb{Q}_{\infty,\ell}$  The  $\mathbb{Z}_\ell$ -cyclotomic extension of  $\mathbb{Q}$ ; i.e.  $\cup_{r=1}^\infty \mathbb{Q}_{r,\ell}$ .
- $K_{n,\ell}$  The compositum  $K \cdot \mathbb{Q}_{n,\ell}$ .
- $K_{\infty,\ell}$  The  $\mathbb{Z}_\ell$ -cyclotomic extension of  $K$ ; the compositum  $K \cdot \mathbb{Q}_{\infty,\ell}$ .
- $K_\infty$  An abbreviation for  $K_{\infty,\ell}$ .
- $\mathcal{O}_{\infty,\ell}$  The ring of integers in  $K_{\infty,\ell}$ ; the integral closure of  $\mathbb{Z}$  in  $K_{\infty,\ell}$ .
- $\mathcal{O}_\infty$  An abbreviation for  $\mathcal{O}_{\infty,\ell}$ .
- $v_\ell$  The totally ramified prime of  $\mathbb{Q}_{\infty,\ell}$  above  $\ell$ .
- $\mathbb{G}_m$  The (algebraic) multiplicative group.
- $\text{ord}_{\mathfrak{p}}(\alpha)$  The  $\mathfrak{p}$ -adic valuation of  $\alpha$ .
- $\zeta_n$  A primitive  $n$ -th root of unity.
- $\Omega_{n,\ell}$  An abbreviation for the cyclotomic field  $\mathbb{Q}(\zeta_{\ell^n})$ .
- $\Omega_{\infty,\ell}$  An abbreviation for  $\cup_{n=1}^\infty \Omega_{n,\ell}$ .
- $\lambda_n$  The unique prime ideal of  $\mathbb{Q}(\zeta_{\ell^n})$  above  $\ell$ .
- $C_n$  The group of cyclotomic units in  $\Omega_{n,\ell}$ ; i.e.  $V_n \cap \mathcal{O}(\Omega_{n,\ell})^\times$ .
- $V_n$  The subgroup of  $\mathcal{O}(\Omega_{n,\ell}, \{v_\ell\})^\times$  generated by  $\{\pm \zeta_{\ell^n}, 1 - \zeta_{\ell^n}^k : 1 \leq k < \ell^n\}$ .
- $\mu$  The Möbius function.
- $\Omega_{n,\ell}^+$  An abbreviation for  $\mathbb{Q}(\zeta_{\ell^n} + 1/\zeta_{\ell^n})$ ; the unique index 2 totally real subfield of  $\Omega_{n,\ell}$ .
- $\Omega_{\infty,\ell}^+$  The unique index 2 totally real subfield of  $\Omega_{\infty,\ell}$ ; i.e.  $\cup_{n=1}^\infty \Omega_{n,\ell}^+$ .
- $\mathcal{Z}_n$  The set of primitive  $\ell^n$ -th roots of unity.
- $\mathcal{Z}_n^+$  The set  $\{\zeta + \zeta^{-1} : \zeta \in \mathcal{Z}_n\}$ .
- $G_n$  The Galois group of  $\Omega_{n,\ell}^+/\mathbb{Q}_{n-1,\ell}$  (of order  $(\ell - 1)/2$ ).
- $H_n$  The Galois group of  $\Omega_{n,\ell}^+/\Omega_{n-1,\ell}^+$  (of order  $\ell$ ).
- $G_\infty$  The Galois group of  $\Omega_{\infty,\ell}^+/\mathbb{Q}_{\infty,\ell}$  (of order  $(\ell - 1)/2$ ).
- $\varphi(n)$  The Euler totient function; the number of positive integers less than  $n$  coprime to  $n$ .
- $\Psi_m$  The homogenisation  $Y^{\varphi(m)}\Phi_m(X/Y)$  of the  $m$ -th cyclotomic polynomial  $\Phi_m$ .
- $\eta_i$  An abbreviation for  $\zeta_{\ell^n}^{1+\ell^{n-1}(i-1)} + \zeta_{\ell^n}^{-1-\ell^{n-1}(i-1)}$ .
- $h_n$  The class number of the cyclotomic field  $\Omega_{n,\ell} = \mathbb{Q}(\zeta_{\ell^n})$ .



- $h_n^+$  The class number of  $\Omega_{n,\ell}^+ = \mathbb{Q}(\zeta_{\ell^n} + 1/\zeta_{\ell^n})$
- $T_\ell(A)$  The  $\ell$ -adic Tate module of an abelian variety  $A/K$ .
- $\rho_{A,\ell}$  The  $\ell$ -adic Galois representation of  $G_K$  on  $T_\ell(A)$ .
- $\bar{\rho}_{A,\ell}$  The mod- $\ell$  Galois representation of  $G_K$  on  $T_\ell(A)$ .
- $\Gamma_{\mathbb{R}}(s)$  An abbreviation for  $\pi^{-s/2}\Gamma(s/2)$ .
- $\Gamma_{\mathbb{C}}(s)$  An abbreviation for  $2(2\pi)^{-s}\Gamma(s)$ .
- $\Delta_{\min}$  The discriminant of a minimal Weierstrass model for a hyperelliptic curve  $C/K$ .
- $K_1$  An abbreviation for the imaginary quadratic field  $\mathbb{Q}(\sqrt{-1})$ .
- $K_2$  An abbreviation for the imaginary quadratic field  $\mathbb{Q}(\sqrt{-2})$ .
- $K_3$  An abbreviation for the real quadratic field  $\mathbb{Q}(\sqrt{2})$ .
- $L_1$  An abbreviation for the quartic field  $\mathbb{Q}(\sqrt[4]{-1})$ .
- $L_2$  An abbreviation for the quartic field  $\mathbb{Q}(\sqrt[4]{2})$ .
- $L_3$  An abbreviation for the quartic field  $\mathbb{Q}(\sqrt[4]{-2})$ .
- $L_4$  An abbreviation for the quartic field  $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ .
- $L_5$  An abbreviation for the quartic field  $\mathbb{Q}(\sqrt{-2-\sqrt{2}})$ .
- $L_6$  An abbreviation for the quartic field  $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ .
- $L_7$  An abbreviation for the quartic field  $\mathbb{Q}(\sqrt{1+\sqrt{-1}})$ .
- $M_1$  An abbreviation for the octic field  $\mathbb{Q}(\sqrt[8]{-1})$ .
- $M_2$  An abbreviation for the octic field  $\mathbb{Q}(\zeta_8, \sqrt[4]{2})$ .
- $M_3$  An abbreviation for the octic field  $\mathbb{Q}(\sqrt[4]{2\sqrt{2}-3})$ .
- $\text{Aut}(C)$  The automorphism group of a curve  $C/K$ .
- $\text{Aut}(C_{\overline{K}})$  The geometric automorphism group of a curve  $C$  over  $\overline{K}$ .
- $\text{End}(A)$  The endomorphism ring of an abelian variety  $A/K$ .
- $\text{End}(A_{\overline{K}})$  The geometric endomorphism ring of an abelian variety  $A/K$ .
- $A_{\text{endo}}$  The endomorphism field of an abelian variety  $A/K$ ; i.e. the smallest field  $L$  extending  $K$  over which all geometric endomorphisms of  $A/K$  are defined.
- $C_n$  The cyclic group of order  $n$ .
- $D_n$  The dihedral group of order  $2n$ .
- $M_n(R)$  The ring of  $n \times n$  matrices over  $R$ .
- $\mathbb{H}$  The quaternions.
- $\text{Res}_{K/\mathbb{Q}}(E)$  The Weil restriction of an elliptic curve  $E/K$  to  $\mathbb{Q}$ .
- $X_1(N)$  The modular curve for the congruence subgroup  $\Gamma_1(N)$ .
- $J_1(N)$  The Jacobian of the modular curve  $X_1(N)$ .

- $\mathrm{ST}(A)$  The Sato-Tate group of an abelian variety  $A$ .
- $\mathrm{ST}^0(A)$  The identity component of the Sato-Tate group of an abelian variety  $A$ .
- $K_v$  The completion of the number field  $K$  at a place  $v$ .
- $\mathrm{Sel}^{(2)}(A/K)$  The 2-Selmer group of the abelian variety  $A/K$ .
- $H^1(G, M)$  The 1st cohomology group of the  $G$ -module  $M$ .
- $A \circ B$  A central product of the groups  $A$  and  $B$ .
- $A \rtimes B$  A semidirect product of the groups  $A$  and  $B$ , with normal subgroup  $A$ .
- $\mathrm{SD}_n$  The semidihedral (or quasidihedral) group of order  $n$ .
- $Q_n$  The (generalised) quaternion group of order  $n$ .
- $\mathrm{OD}_n$  The modular maximal-cyclic group of order  $n$ .
- $S_n$  The symmetric group of order  $n!$ .

*“When you see someone putting on his Big Boots, you can be pretty sure that an  
Adventure is going to happen.” - A.A. Milne, Winnie-the-Pooh*

# Chapter 1

## Introduction

I rather ambitiously titled this thesis “*The Effective Shafarevich Conjecture*”. As I started writing this introductory chapter, it became immediately clear that to give a full history of the Shafarevich conjecture would result in this thesis being far longer than even Tolstoy’s *War and Peace*. So I unfortunately cannot claim that this will be an exhaustive overview to all the amazing work that’s been done towards the effective Shafarevich conjecture, and have referenced other excellent expository texts on the subject wherever possible. However, whilst I’ll be as brief as I can, I’ll aim to include all the necessary details and background relevant to the scope of this thesis!

In the early 20th century, Louis J. Mordell [320] posed several conjectures regarding the finiteness of rational solutions to Diophantine equations. Having proven his famous theorem that  $E(\mathbb{Q})$  is finitely generated for elliptic curves  $E/\mathbb{Q}$ , in the same paper he posed several further conjectures; some examples include whether smooth curves of the form  $y^2 = ax^4 + bx^3 + cx^2 + dx + e$  have finitely many integer solutions, or whether the equation  $z^2 = ax^6 + bx^5y + \cdots + fxy^5 + gy^6$  has finitely many rational solutions. More generally, he stated the following now famous conjecture:

**Conjecture 1.1** (Mordell 1922 [320]). *Any smooth curve  $C/\mathbb{Q}$  of genus  $g > 1$  has only finitely many rational points.*

At the time, this was quite a bold proposition!<sup>1</sup> This was an open problem for many decades, with the only significant progress at first being Chabauty’s proof [99] in the case of genus  $g$  curves  $C/\mathbb{Q}$  satisfying the property that the rank of its Jacobian is strictly less than  $g$ .

---

<sup>1</sup>Even more than 40 years after Mordell stated his conjecture, André Weil famously remarked that “*there is no evidence for or against*” the Mordell conjecture [480, p. 454]!

At the 1962 International Congress of Mathematicians in Stockholm, Igor R. Shafarevich proposed another finiteness conjecture which further generalised the Mordell conjecture.<sup>2</sup>

**Conjecture 1.2** (Shafarevich 1962 [473]). *Let  $K$  be a number field,  $g \geq 2$  a positive integer, and  $S$  a finite set of places in  $K$ . Then there exist only finitely many smooth genus  $g$  curves  $C/K$  with good reduction outside  $S$ .*<sup>3</sup>

A classical theorem of Torelli [450] states that a curve  $C/K$  of genus  $\geq 2$  is uniquely determined by its Jacobian  $\text{Jac}(C)$  considered as a principally polarised abelian variety (a proof for perfect fields  $K$  is given in [118, Cor 12.2], and also given in the appendix of [279] for arbitrary fields  $K$ ). Thus, we have that the above conjecture is in fact implied by the following more general conjecture on finiteness of abelian varieties:

**Conjecture 1.3** (Shafarevich 1962 [473]). *Let  $K$  be a number field,  $d$  a positive integer, and  $S$  a finite set of places in  $K$ . Then there exist only finitely many principally polarised abelian varieties  $A/K$  of dimension  $d$  with good reduction outside  $S$ .*

Shafarevich himself proved Conjecture 1.3 for elliptic curves ( $d = 1$ ), as well as sketching the proof for hyperelliptic curves (see [339, 344]), and it was shown by Parshin [343] that Conjecture 1.2 implies the Mordell conjecture, thus reducing the problem of proving the Mordell conjecture to proving Conjecture 1.3.

Conjecture 1.3 (along with the Tate conjecture for abelian varieties over number fields [451, Section 4]) was eventually proven by Gerd Faltings in 1983 [164], therefore proving the Mordell conjecture! This proof got Faltings the 1986 Fields medal and is considered one of the crowning achievements in 20th century arithmetic geometry. Excellent overviews of the ideas behind Faltings' proof are given by Bloch [47] and Mazur [311].

**Theorem** (Faltings 1983 [164, p. 363]). *Let  $K$  be a number field,  $d$  and  $g$  positive integers, and  $S$  a finite set of places of  $K$ . Then there exist only finitely many*

<sup>2</sup>It seems Shafarevich himself only conjectured the statement on finiteness of genus  $g$  curves  $C/K$  with good reduction outside a given set  $S$  of primes, although the latter more general conjecture on finiteness of abelian varieties is nowadays also commonly referred to as the Shafarevich conjecture.

<sup>3</sup>We remark that the statement of this conjecture for genus 0 curves (smooth plane conics) follows from some classical results in class field theory (e.g. see [463]). However, regarding genus 1 curves, there do exist pairs  $(K, S)$  with  $S$  nonempty, such that there are infinitely many genus 1 curves  $C/K$  with good reduction outside  $S$  [311, p. 241]. In particular, the Shafarevich conjecture for genus 1 curves  $C/K$  with everywhere good reduction would imply that the Tate-Shafarevich group  $\text{III}_{E/K}$  for elliptic curves  $E/K$  is finite [351, p. 2], which is still an open problem!

*isomorphism classes of polarised abelian varieties  $A/K$  of dimension  $g$ , polarisation degree  $d$ , and good reduction outside  $S$ .*

A theorem of Zarhin [488] proved that, for any abelian variety  $A/K$ , the abelian variety  $A^4 \times \widehat{A}^4$  is principally polarised. Combined with Faltings theorem above, this proves the Shafarevich conjecture without the need to have any polarisation assumption:

**Theorem** (Faltings–Zarhin). *Let  $K$  be a number field,  $d$  a positive integer, and  $S$  a finite set of places in  $K$ . Then there exist only finitely many abelian varieties  $A/K$  of dimension  $d$  with good reduction outside  $S$ .*

Some further proofs of Faltings’ theorem were given by Vojta [467] using diophantine approximation techniques, which was further simplified by Faltings [165] and Bombieri [50]. There’s an excellent book recently published by Ikoma–Kawaguchi–Moriwaki [231] which gives a fully self-contained and detailed proof of the Mordell conjecture following the approach by Bombieri and Vojta. There is also a more recent proof by Lawrence and Venkatesh [280] using  $p$ -adic Hodge theory (see also Liu’s recent notes [283]).

Nowadays, both the polarised and unpolarised versions of the Shafarevich conjecture have been proven for many other families of varieties: e.g. for K3 surfaces [15, 404], hyper-Kähler varieties [187], flag varieties [237], del Pezzo surfaces [381], certain canonically polarised surfaces [236], Enriques surfaces [439], and certain Fano threefolds [238].

This introduction would not be complete without also mentioning that analogous versions of the Mordell conjecture and Shafarevich conjecture have also been posed over function fields, with their proofs being given before Faltings’ proof over number fields.<sup>4</sup> In the 1960s, the Mordell conjecture over characteristic zero function fields was proven independently by Manin [300] and Grauert [198] (with Coleman [111] correcting an error in Manin’s proof), and was proven by Samuel [374] in the positive characteristic case. Similarly, the Shafarevich conjecture for function fields was resolved by Arakelov [17], Parshin [343], and Szpiro [436].

## Effective Conjectures

One could more generally ask if effective algorithms exist for the Mordell and Shafarevich conjectures. Whilst we do have effectivity results for function fields [487],

---

<sup>4</sup>When stating the Mordell conjecture for curves  $C$  over function fields  $K/k$ , one must exclude isotrivial curves (i.e. curves  $C/K$  which are  $L$ -isomorphic to a curve  $C_0/k$ , over a finite extension  $L/K$ ).

Faltings' proof for number fields is not fully effective. Whilst Parshin [437] recognised that his proof can be used to give an effective bound on the cardinality of  $C(K)$ , neither his proof nor the other proofs of Vojta–Faltings–Bombieri or Lawrence–Venkatesh can be used to (even in principle) give a fully effective algorithm to compute  $C(K)$  in all cases. Indeed, even effectively determining whether  $C(\mathbb{Q}) \neq \emptyset$  is still an open problem.<sup>5</sup>

We thus pose the following effective version of the Mordell conjecture:

**Conjecture** (Effective Mordell). *There exists an effective algorithm that accepts as input a number field  $K$  and a smooth curve  $C/K$  of genus  $g > 1$ , and outputs all  $K$ -rational points on the curve  $C(K)$  (or equivalently, outputs a constant  $h_{C/K}$  such that all points in  $C(K)$  have height at most  $h_{C/K}$ ).*

This conjecture has been stated in many different ways with various different generalisations (e.g. see modified Szpiro conjecture [438], the ABC conjecture [303, 336], or Vojta's height inequality [466]; effective versions of any of these would imply the effective Mordell conjecture [155]).

Whilst the effective Mordell conjecture is still open in general, many approaches have been published to study this in certain cases. These include local methods, descent, constructing quotients, Chabauty–Coleman [99, 111] (also quadratic Chabauty, non-abelian Chabauty [265]). An excellent review of these methods, in particular those of Chabauty and the Mordell–Weil sieve is given by McCallum–Poonen [313] and by Siksek [411], whilst a more comprehensive overview of Kim's non-abelian Chabauty is given by Corwin [119].

A thorough survey of the two methods of Lawrence–Venkatesh and Kim is given by Balakrishnan–Best–Bianchi–Lawrence–Müller–Triantafyllou–Vonk [25], describing possible approaches towards a proof of the effective Mordell conjecture. Recently, Kim's non-abelian Chabauty has had the most success in practically determining the set  $C(\mathbb{Q})$  for many curves  $C/\mathbb{Q}$  for which Chabauty on its own doesn't work. A recent famous example was determining all rational points on the split Cartan modular curve  $X_{\text{sp}}^+(13)$  (the *cursed curve*) done by Balakrishnan–Dogra–Müller–Tuitman–Vonk [24].<sup>6</sup> Kim's methods have also been applied to compute the rational points on the modular curves  $X_0^+(N)$  for  $N = 67, 73$ , and  $103$ , done by

<sup>5</sup>It's perhaps worth mentioning that it's not obvious whether such an algorithm should even exist, as it was shown by David–Putnam–Robinson–Matiyasevich [130, 305] that there in fact does not exist any algorithm to determine whether an arbitrary system of Diophantine equations has solutions over  $\mathbb{Z}$  (Hilbert's 10th problem).

<sup>6</sup>Bilu, Parent, and Rebolledo [40, 41] had already determined all rational points on  $X_{\text{sp}}^+(p)$  for all primes  $p \geq 11$  with the exception of  $p = 13$ . They refer to level 13 as the *cursed level* (e.g. see [41, Remark 5.11]) as their methods break down for  $p = 13$ .

Balakrishnan–Best–Bianchi–Lawrence–Müller–Triantafillou–Vonk [25] with various other genus 2 and 3 modular curves  $X_0^+(N)$  for prime levels  $N$  from 107 to 239 recently being resolved by Balakrishnan–Dogra–Müller–Tuitman–Vonk [26].

We shall also pose the analogous effective conjecture for Shafarevich, both for curves of genus  $> 1$  and for abelian varieties.

**Conjecture 1.4** (Effective Shafarevich I). *There exists an effective algorithm that accepts as input, a number field  $K$ , a positive integer  $g \geq 2$ , and a finite set  $S$  of places in  $K$ , and outputs a list of all smooth genus  $g$  curves  $C/K$  with good reduction outside  $S$  (or equivalently, outputs a constant  $c_{K,g,S}$  such that all such curves satisfy  $h_F(C) \leq c_{K,g,S}$ , where  $h_F(C)$  denotes the Faltings height<sup>7</sup> of  $C$ , as defined in [319, p. 153]).*

**Conjecture 1.5** (Effective Shafarevich II). *There exists an effective algorithm that accepts as input, a number field  $K$ , a positive integer  $d \geq 1$ , and a finite set  $S$  of places in  $K$ , and outputs a list of all dimension  $d$  abelian varieties  $A/K$  with good reduction outside  $S$  (or equivalently, outputs a constant  $c_{K,d,S}$  such that all such abelian varieties satisfy  $h_F(A) \leq c_{K,d,S}$ ).*

Rémond [361] noted that the construction of Kodaira–Parshin can be made effective, thus showing that Effective Shafarevich I implies Effective Mordell. Furthermore, as noted in [470, Proposition 6.1], Effective Shafarevich II implies Effective Shafarevich I.

While effective approaches to Mordell’s conjecture have been developed in many cases, both versions of the effective Shafarevich conjecture have been resolved in far fewer cases. For this thesis, we shall focus on providing methods to solve these two effective versions of the Shafarevich conjecture. We begin this chapter by giving a brief overview of several well-known methods to solve the effective Shafarevich conjecture for elliptic curves, followed by an overview of some cases which have been resolved for higher genus curves and higher dimensional abelian varieties. Chapters 4 through 6 will then focus on our attempts to solve Effective Shafarevich II for  $K = \mathbb{Q}$ ,  $d = 2$ , and  $S = \{2\}$ .

---

<sup>7</sup>Instead of the Faltings height  $h_F(C)$ , any height function  $h(C)$  which satisfies the effective Northcott property would work equivalently (i.e. a function  $h$  such that, for all  $B \in \mathbb{R}$ , the set  $\{\text{curves } C/K \mid h(C/K) \leq B\}$  is finite and can effectively be computed).



## 1.1 History

### 1.1.1 Elliptic Curves

We first consider the simplest case: the theory of elliptic curves. The study of elliptic curves had their origins as far back as Diophantus [29] in the 2nd century AD, with their study truly being at the forefront of modern number theory over the last 150 years. More recently, the use of elliptic curves in cryptography has truly cemented its importance both in pure number theory as well as applications in computer science. Excellent references regarding the theory of elliptic curves are given by Cassels [97] and Silverman [415, 414].

There is an extensive amount of literature available on classifying elliptic curves  $E/K$  with good reduction outside  $S$ , and thus the following is certainly not an exhaustive overview by any means.

Firstly, we note that the case  $K = \mathbb{Q}$  and  $S = \emptyset$  simply corresponds to showing that there are no elliptic curves over  $\mathbb{Q}$  with everywhere good reduction. This can be handled by an elementary Diophantine argument, first stated by Tate, with a proof published by Ogg [337, p. 144] in the 1960s. In the same paper, Ogg [337] also classified all 24 elliptic curves over  $\mathbb{Q}$  with good reduction outside  $S = \{2\}$ . Coghlan [108] and Stephens [424] independently computed all 752 elliptic curves  $E/\mathbb{Q}$  with good reduction away from  $S = \{2, 3\}$  (see also Ogg [338] and Neumann [331] for some partial results). Several authors also considered the classification of elliptic curves with good reduction outside one prime  $p$ , and the related subproblem of computing all elliptic curves  $E/\mathbb{Q}$  with prime conductor  $p$ . The  $S = \{3\}$  case was done by Hadano [210], with various results for larger primes  $p$  shown by Setzer [398], Neumann [332, 333], Hadano [211], and Bölling [49].

Many other papers then followed, giving a full classification of elliptic curves  $E/\mathbb{Q}$  with good reduction outside of various sets of primes  $S$ . An overview of some of these results are given in Table 1.1.

Beyond the case  $K = \mathbb{Q}$ , the next natural step would be to classify elliptic curves  $E$  over various quadratic fields  $K$  with good reduction outside  $S$ . Indeed, as with the rational case, this has similarly been extensively studied by many authors [278, 347, 348, 349, 432, 123], with the specific case of  $S = \emptyset$  receiving much attention over the last few decades by Setzer [399, 400], Ishii [232, 233], Rohrlich [366], Comalada, Nart [112, 113, 114], Zhao [492] and Kida, Kagawa [244, 246, 259, 260, 261,

---

<sup>8</sup>We note that Coghlan's original paper lists a total of 760 models of elliptic curves, however 8 of these curves are actually  $\mathbb{Q}$ -isomorphic to previously listed elliptic curves.

<sup>9</sup>This computation was originally done heuristically, but has since been verified unconditionally.

Table 1.1: Summary of total number of elliptic curves  $E/\mathbb{Q}$  with good reduction outside  $S$ , for various sets  $S$ . We denote  $|E(S)|$  as the total number of such elliptic curves.

Set $S$	$ E(S) $	Authors	Year
$\emptyset$	0	Tate, proof published by Ogg [337]	1965
$\{2\}$	24	Ogg [337]	1965
$\{2, 3\}$	752	Coghlán <sup>8</sup> [108], Stephens [424]	1967, 1965
$\{11\}$	12	Agrawal-Coates-Hunt-Van der Poorten [8]	1980
$\{2, p\}, p \leq 23$	280, 288, ...	Cremona, Lingham [127]	2007
$\{2, 3, 23\}$	5520	Koutsianas [270]	2015
$\{2, 3, 5, 7, 11\}$	592 192	von Känel, Matschke [471]	2016
$\{2, 3, 5, 7, 11, 13\}$	4 576 128	Best, Matschke <sup>9</sup> [36]	2020
$\{2, 3, \dots, 19\}$	217 923 072	Matschke [306, 308]	2021

262, 263, 264]. A (partially complete) database of elliptic curves with everywhere good reduction over real quadratic fields of discriminant  $\leq 10^6$  is given by Elkies [156].

We shall simply give a brief table summarising some of the above results, extending the tables of Laska [278, p. 93] given in Table 1.2.

Table 1.2: Summary of the total number of elliptic curves over quadratic fields  $K$  with good reduction outside  $S$  for  $S = \emptyset, \{2\}, \{3\}$ , or  $\{2, 3\}$ . An asterisk indicates that completeness is conditional on GRH. Values which haven't been verified (even conditionally) are only given as a lower bound.

Set $S$	Field $K$						
	$\mathbb{Q}(\sqrt{-5})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}(\sqrt{5})$
$\emptyset$	0	0	0	0	0	0	0
$\{2\}$	32*	48	40	64	400	288*	384
$\{3\}$	$\geq 40$	18	$\geq 32$	8	76*	$\geq 34$	56
$\{2, 3\}$	$\geq 8464$	1776	$\geq 12288$	1280	9536*	$\geq 10304$	9920

Nowadays, effective algorithms to classify all elliptic curves over  $K$  with good reduction outside any finite set  $S$  have been well-studied, with early effective algorithms given by Coates [107] to modern implementations of Cremona–Lingham [127] being implemented in Sage and Magma, with many practical optimisations having being well-developed in the elliptic case.

We provide a summary of some of the most well-known methods for solving the Shafarevich problem for elliptic curves below, noting that the techniques

involved are not strictly disjoint. While it is impossible to delve into the specifics of each method in detail, we offer numerous references that apply or implement these methods for the interested reader.

1. **Elementary (ad hoc) methods:** Let  $E/\mathbb{Q}$  be an elliptic curve with global minimal model  $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ . If  $E/\mathbb{Q}$  has good reduction away from  $S$ , then its minimal discriminant  $\Delta_{\min}$  given by

$$\Delta_{\min} = b_2^2b_8 - 8b_3^4 - 27b_6^2 + 9b_2b_4b_6,$$

is an  $S$ -smooth integer, where  $b_2 = a_1^2 - 4a_2$ ,  $b_4 = 2a_4 - a_1a_3$ ,  $b_6 = a_3^2 - 4a_6$ , and  $b_8 = a_4^2 - a_1a_3a_4 + a_1^2a_6 + a_2a_3^2 - 4a_2a_6$  (see [415, p. 42]). As  $\text{ord}_p(\Delta_{\min})$  can be uniformly bounded for all primes  $p$ , this gives an explicit finite set of Diophantine equations, which can be solved directly via elementary arguments if  $S$  is small enough, as Ogg [337] did in the case of  $S = \emptyset$  and  $S = \{2\}$ .

For larger degree number fields  $K$ , and larger sets of primes  $S$ , this approach quickly becomes infeasible to do in practice, requiring more advanced techniques.

2. **Mordell curves:** Given an elliptic curve  $E/K$ , we have that the minimal discriminant  $\Delta_{\min}$  satisfies  $c_6^2 = c_4^3 - 1728\Delta_{\min}$  where  $c_4 = b_2^2 - 24b_4$  and  $c_6 = b_2^3 - 36b_2b_4 + 216b_6$ . Thus, one approach to compute such  $E/K$  with good reduction away from  $S$  is by computing the possible values for  $c_4$  and  $c_6$  by computing all  $S$ -integral points on the Mordell curves  $Y^2 = X^3 + k$  for finitely many values of  $k$ .

Whilst it's a classical result of Siegel and Mahler [409, 296] that there are only finitely such  $S$ -integral points, explicit bounds on the heights of such points were given by Baker and Coates [22, 21, 107], giving an algorithm to effectively compute all such  $S$ -integral points assuming knowledge of the full set of Mordell-Weil generators for  $Y^2 = X^3 + k$ .

This method was successfully implemented by Cremona–Lingham [127] to compute all elliptic curves  $E/\mathbb{Q}$  with good reduction outside  $\{2, p\}$  and  $\{2, 3, p\}$  for various odd primes  $p$ . The Cremona–Lingham algorithm has also been implemented in Sage [373] over  $\mathbb{Q}$  as

`EllipticCurves_with_good_reduction_outside_S.`

3. **Thue–Mahler equations.** Let  $E/K$  be an elliptic curve with good reduction away from  $S$ . It has been shown by Bennett–Gherga–Rechnitzer [32, Theo-

rem 1] that  $E/K$  can be uniquely determined (up to twisting) by the triple  $(F, u, v)$ , where  $F(x, y) \in \mathbb{Z}[x, y]$  is a binary cubic form whose discriminant is an  $S \cup \{2, 3\}$ -smooth integer, and  $(u, v)$  is a pair of integers such that

$$F(u, v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 u v^2 + \omega_3 v^3 = C, \quad (1.1)$$

for some  $S \cup \{2, 3\}$ -smooth integer  $C$ . In particular, they show that some twist of  $E/K$  has a simplified Weierstrass model of the form  $y^2 = x^3 - 27H_F(u, v)x + 27G_F(u, v)$  where  $H_F \in \mathbb{Z}[x, y]$  is the Hessian of  $F$ , and  $G_F \in \mathbb{Z}[x, y]$  is the Jacobian determinant of  $F$  and  $H$  (see [32, p. 1345]). By thus computing all cubic binary forms  $F(x, y)$  of a given discriminant (e.g. using Cremona's algorithm [125, p. 71]) up to equivalence, and then computing all integer solutions  $(u, v)$  to the relevant Thue-Mahler equations (1.1), this yields an effective algorithm to compute all elliptic curves  $E/K$  with good reduction outside  $S$ .

It's known that there are finitely many such solutions by Mahler [295], extending work of Thue [448]. Methods to effectively solve such Thue-Mahler equations were developed by Vinogradov-Sprindžuk [464], Coates [106], Bugeaud-Györy [84], Evertse [159], with practical implementations given by Tzanakis-De Weger [453, 454] and most recently also by Gherga and Siksek [191].

This method was first implemented by Agrawal, Coates, Hunt, and van der Poorten [8] to compute all elliptic curves  $E/\mathbb{Q}$  with conductor 11 with some recent computations being done Bennett-Gherga-Rechnitzer [32, 33] to compute all elliptic curves  $E/\mathbb{Q}$  with good reduction away from  $\{2, 3, 23\}$  and  $\{2, 3, 5, 7, 11\}$ .

4. **Modular symbols:** If  $E/K$  is a modular elliptic curve of conductor  $\mathcal{N}$  over some totally real field  $K$ , then there exists some suitable Hilbert newform  $f$  of parallel weight 2 and level  $\mathcal{N}$  whose  $L$ -function coincides with that of  $E/K$ . This gives a method to compute all modular elliptic curves with good reduction outside  $S$  by computing the space of  $\Gamma_0(N)$  modular symbols (and the corresponding action of the Hecke algebra) for finitely many levels  $N$ .

If  $K = \mathbb{Q}$  or a totally real quadratic or cubic field, then it is known that all such elliptic curves are modular [68, 136, 185], and thus this method gives an unconditional computation of all such elliptic curves.

Modular symbols were first introduced by Birch [43]. One of the first implementations of the modular symbol method to compute elliptic curves was by Tingley [449], who extended famous tables of Birch-Kuyk [44] by computing

all modular elliptic curves over  $\mathbb{Q}$  of conductor  $N \leq 300$ . This was then furthermore extended by Cremona [124] who published a list of all elliptic curves of conductor  $N \leq 1000$  over  $\mathbb{Q}$ , with recent online tables going far beyond 1000.

An excellent overview of the modular symbol method is given by Cremona [124] and a more computational source is also given by Stein [422].

5.  **$S$ -unit equations:** Given an elliptic curve  $E/K : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$  with good reduction away from  $S$ , we have that  $\lambda := (\alpha_3 - \alpha_1)/(\alpha_2 - \alpha_1)$  is an  $S \cup \{2\}$ -unit in  $K(E[2])$ , and similarly  $1 - \lambda = (\alpha_2 - \alpha_3)/(\alpha_2 - \alpha_1)$  is also an  $S \cup \{2\}$ -unit in  $K(E[2])$ .

This therefore gives an algorithm to classify all such  $\lambda$  by first classifying all possible 2-division fields  $K(E[2])$  (e.g. by doing a Hunter search [109, p. 445]), and then finding all solutions to the  $S$ -unit equation  $x + y = 1$  in  $K(E[2])$ .

Such equations were shown to have finitely many solutions by Siegel [409] for  $S = \emptyset$ , Mahler [295] for  $K = \mathbb{Q}$ , and Parry [342] for general  $S$ -units over number fields  $K$ . By using the theory of logarithmic forms by Baker [20], Györy [207, 208] gave some of the first effective height bounds for solutions to  $S$ -unit equations, with further optimal bounds given recently by Györy and Yu [209]. Nowadays there are numerous practical implementations of  $S$ -unit solvers, e.g. see von Känel–Matschke [471], Alvarado-Koutsianas-Malmskog-Rasmussen-Vincent-West [13], and Matschke [306], giving a fully general implementation of this in Sage.

This method has been the most successful in solving effective Shafarevich for elliptic curves for large sets  $S$  in recent years, with Benjamin Matschke using an optimised  $S$ -unit equation solver to compute all 217 923 072 elliptic curves  $E/\mathbb{Q}$  with good reduction away from the first eight rational primes [306, 308] (a computation that took almost one CPU-month).

Nowadays, computations of all elliptic curves of conductor  $N$  for large  $N$  ranges over many databases. Since the original 1972 Antwerp tables [44] listing elliptic curves of conductor  $N \leq 200$ , an enormous amount of computations over many CPU-decades have been run, with the LMFDB listing computations of Cremona giving all elliptic curves of conductor  $N \leq 500\,000$ . We must also mention the Stein–Watkins [423] database of elliptic curves extending Brumer and McGuinness original database [82]. Recently, a database of elliptic curves ordered by height was also given by Balakrishnan, Ho, Kaplan, Spicer, Stein, and Weigandt [27].

### 1.1.2 Higher genus curves

Beyond elliptic curves, the next natural problem is to classify genus 2 curves  $C/K$  with good reduction away from a finite set of primes  $S$ . Whilst effective methods are also known in the genus 2 case, far fewer cases have been practically computed compared to the computation of elliptic curves.

One of the first classifications of genus 2 curves was Merriman–Smart’s [314, 315] list of 164 genus 2 curves  $C/\mathbb{Q}$  containing at least one rational Weierstrass point and with good reduction away from 2. This was extended by Smart [418] who gave a full classification of all 366 genus 2 curves over  $\mathbb{Q}$  with good reduction outside  $\{2\}$ , using finiteness results from Evertse and Györy [160].<sup>10</sup> A recent project by Rowan [370] has also studied the case of classifying genus 2 curves  $C/\mathbb{Q}$  with good reduction outside  $\{3\}$ .

Recently, Dąbrowski–Sadek [144] have considered the case of classifying genus 2 curves  $C/\mathbb{Q}$  with good reduction outside one odd prime, under the assumption that  $C$  has at least two rational Weierstrass points. They have also recently constructed infinitely many examples of genus 2 curves  $C/K$  over quadratic fields  $K$  with everywhere good reduction [143].

Finally, we mention the works of Malmskog–Rasmussen [299] as well as Bouw–Koutsianas–Sijlsing–Wewers [62] who gave a classification of Picard curves (i.e. genus 3 curves with affine equation  $y^3 = f(x)$  for some quartic  $f$ ) with good reduction outside  $\{3\}$  and  $\{2, 3\}$  respectively.

Nowadays, effective algorithms to classify all genus  $g$  hyperelliptic curves  $C/K$  with good reduction away from  $S$  are well-known, with an explicit algorithm sketched in Chapter 2. Effective height bounds on genus  $g$  hyperelliptic curves  $C/K$  with good reduction outside  $S$  were recently given by von Känel [468].

Beyond the hyperelliptic (and certain superelliptic) cases, not much seems to be known regarding effective Shafarevich algorithms for curves at present. Even just formulating an effective algorithm to compute genus 3 plane quartic curves  $C/\mathbb{Q} : f(x, y, z) = 0$  with good reduction outside some small set of primes  $S$  appears to be intractable with current methods, with no obvious way to reduce the problem to that of solving  $S$ -unit equations or Thue–Mahler equations.

---

<sup>10</sup>Similarly to some early tables of elliptic curves, we remark that their paper listed 427 such models of genus 2 curves, although many models were  $\mathbb{Q}$ -isomorphic to each other, as noted by van Wamelen [461, p. 1690].

### 1.1.3 Higher dimension abelian varieties

Compared to the elliptic case, the effective Shafarevich conjecture for abelian varieties has been solved in far fewer cases in higher dimensions. Nonetheless, a lot of work has particularly been invested in the case  $S = \emptyset$ , i.e. classifying abelian varieties  $A/K$  with good reduction everywhere.

In the case of good reduction everywhere over  $\mathbb{Q}$ , Abrashkin first proved that there are no such abelian varieties of dimension 2 and 3 [3, 4]. and then Abrashkin and Fontaine [180] independently showed that there are no such nontrivial abelian varieties (of any positive dimension) over  $\mathbb{Q}$ . The same result was also shown by Fontaine for everywhere good reduction over  $K = \mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3}),$  or  $\mathbb{Q}(\sqrt{5})$ . Some further results were also shown by Abrashkin where he also showed the nonexistence of such solutions for  $K = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-7})$  and the cyclotomic field  $\mathbb{Q}(\zeta_7)$  [2].

Schoof classified all such abelian varieties (up to isogeny) with everywhere good reduction over  $\mathbb{Q}(\sqrt{6})$  [382] as well as for certain cyclotomic fields  $\mathbb{Q}(\zeta_f)$  [383]. Recently, Schoof has extended a similar classification to all real quadratic fields of discriminant at most 37 [387]. We also mention the recent work of Demb  le [134] giving a classification of all abelian varieties over  $\mathbb{Q}(\sqrt{53}), \mathbb{Q}(\sqrt{61}),$  and  $\mathbb{Q}(\sqrt{73})$  with everywhere good reduction, assuming GRH.

For semistable abelian varieties over  $\mathbb{Q}$  having good reduction outside one prime, Brumer–Kramer [78] showed that there’s no such abelian variety having good reduction outside  $p$  for any prime  $p \in \{2, 3, 5, 7\}$ . Schoof [384] extended this classification to good reduction outside 11 or 13. Calegari [88], extending the above results of Schoof and Brumer–Kramer showed that, for  $N$  squarefree, there exists a nontrivial semistable abelian variety  $A/\mathbb{Q}$  with good reduction outside the primes dividing  $N$  if and only if  $N \notin \{1, 2, 3, 5, 6, 7, 10, 13\}$ , thus settling the question of the existence of such abelian varieties over  $\mathbb{Q}$ .

Schoof also showed a similar classification for  $N = 15$  and  $23$  [385, 386], showing that any simple semistable abelian variety  $A/\mathbb{Q}$  with good reduction outside some prime  $N$  with  $N \leq 23$  must be isogenous to  $J_0(N)$ . Brumer–Kramer gave some extensions to this result for certain semistable abelian varieties  $A/K$  under some conditions on the 2-torsion group  $A[2]$  [80].

Effective algorithms to compute all abelian varieties  $A/K$  of  $\text{GL}_2$ -type with good reduction outside  $S$  have been published by von K  nel [470]. In particular, examples for constructing abelian varieties of  $\text{GL}_2$ -type with everywhere good reduction are also given by Demb  le and Kumar [135], with examples of abelian surfaces given in [194, 193].



We remark that the assumption of semistability here is essential! Indeed, without this assumption, one can find many examples of (non-semistable) abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2; in particular we know of at least 234 such isogeny classes of abelian surfaces with conductors ranging from  $2^8$  to  $2^{20}$  (shown in Table 6.20).

Finally, we should mention an effective algorithm developed by Levent Alpöge and Brian Lawrence [11], which provides a general algorithm to solve the effective Shafarevich conjecture, assuming some standard motivic conjectures (see also Alpöge’s thesis [12, Chapter 7]). Inspired by the results given by Patrikis–Volocho–Zarhin [345], they proved the following theorem:

**Theorem** (Alpöge–Lawrence 2020). [11] *There exists an effective algorithm  $T$  that takes as input a positive integer  $d$ , a number field  $K$  and a finite set of places  $S$  of  $K$ , and outputs (if  $T$  terminates) the finite set of all principally polarised dimension  $d$  abelian varieties over  $K$  with good reduction outside  $S$ , along with an unconditional certificate of correctness of the output. The Fontaine–Mazur, Grothendieck–Serre, absolute Hodge, and Tate conjectures together imply that  $T$  always terminates.*

In particular, their algorithm terminates if given any  $\ell$ -adic Galois representation  $\rho : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_{2g}(\mathbb{Q}_\ell)$  satisfying a set of reasonable constraints, there exists an abelian variety  $A/K$  of dimension  $d$  such that its  $\ell$ -adic Galois representation  $\rho_{A,\ell}$  is isomorphic to  $\rho^{\oplus(d/g)}$ . This conjecture is in particular implied by the conjectures of Fontaine–Mazur, Grothendieck–Serre, absolute Hodge, and Tate, where formal statements of these conjectures can be found in [345, Section 3].

We shall present a very simplified version of a similar algorithm to that given by Alpöge–Lawrence in Chapter 4.<sup>11</sup>

Giving a provably complete list of abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 is still an open problem. Attempts at solving this problem will be the focus of Chapters 4, 5 and 6.

## 1.2 Hyperelliptic Curves

We’ll start by stating some preliminary definitions and results required for the rest of the thesis. First, we give a formal definition of hyperelliptic curves, closely following

---

<sup>11</sup>Whilst this algorithm is (conjecturally) effective, a very rough back-of-the-envelope computation suggests that the current age of the universe ( $\approx 13.7$  billion years) would be a *very weak* lower bound on the length of time it would take for  $T$  to provably compute all principally polarised abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 (although we remark this is excluding any attempts to optimise their algorithm)!



the definitions given by Stoll [431] (see also Galbraith [188, Chapter 10]). In order to define hyperelliptic curves, we first need to define a suitable ambient space.

**Definition 1.2.** [431, p. 5] Let  $K$  be a field, and let  $d_1, d_2, d_3$  be fixed positive integers. We define the **weighted projective space**  $\mathbb{P}_{d_1, d_2, d_3}^2$  as the ambient space whose points over  $K$  are weighted equivalence classes of  $K^3 \setminus \{0, 0, 0\}$ . In other words, we define

$$\mathbb{P}_{d_1, d_2, d_3}^2 := K^3 \setminus \{0, 0, 0\} / \sim$$

where  $\sim$  denotes an equivalence relation on  $K^3 \setminus \{0, 0, 0\}$ , where for  $(X, Y, Z), (X', Y', Z') \in K^3 \setminus \{0, 0, 0\}$ , we have

$$(X, Y, Z) \sim (X', Y', Z') \quad \text{if and only if} \quad (X, Y, Z) = (\lambda^{d_1} X', \lambda^{d_2} Y', \lambda^{d_3} Z')$$

for some  $\lambda \in \overline{K}^\times$ .<sup>12</sup> We write the corresponding point in  $\mathbb{P}_{d_1, d_2, d_3}^2$  as  $(X : Y : Z)$ .

We do note that there are various equivalent ways of defining hyperelliptic curves in the literature. One elegant definition is to define such a curve  $C/K$  as a complete non-singular curve of genus  $g \geq 2$  which admits a map  $x : C \rightarrow \mathbb{P}^1$  of degree 2. Now by picking some function  $y \in k(C)$  such that  $y \notin k(x)$ , one can show that this is equivalent to the following more explicit definition:

**Definition 1.3.** [431, p. 5] Let  $K$  be a field, and let  $g \geq 2$  be a fixed positive integer.<sup>13</sup> If  $\text{char}(K) \neq 2$ , then a **hyperelliptic curve of genus  $g$**  is a subvariety of  $\mathbb{P}_{1, g+1, 1}^2$  defined by an equation of the form

$$Y^2 = F(X, Z) \tag{1.4}$$

where  $F \in K[X, Z]$  is homogeneous of degree  $2g + 2$  and is squarefree. Otherwise, if  $\text{char}(K) = 2$ , then a **hyperelliptic curve of genus  $g$**  is a smooth subvariety of  $\mathbb{P}_{1, g+1, 1}^2$  defined by an equation of the form

$$Y^2 + H(X, Z)Y = F(X, Z) \tag{1.5}$$

where  $H, F \in K[X, Z]$  are homogeneous polynomials of degrees  $g + 1$  and  $2g + 2$  respectively.

---

<sup>12</sup>We require  $\lambda$  to be in the algebraic closure  $\overline{K}$  (as opposed to just  $K$ ) to ensure, for example, that all points of the form  $(0 : X : 0)$  are equivalent (otherwise,  $\mathbb{P}_{d_1, d_2, d_3}^2$  would not be a well-defined variety)!

<sup>13</sup>Whilst some authors include  $g = 1$  in the definition of hyperelliptic curves, we'll adopt the safer convention of assuming  $g \geq 2$  (even though some of our later results for hyperelliptic curves will still remain true if  $g = 1$ ).

We note in the above definition that, if  $\text{char}(K) \neq 2$ , then if some curve  $C$  is given in the form (1.5), then one can complete the square on the left hand side to obtain a curve in the form (1.4).

It's also worth noting that one can define hyperelliptic curves without needing weighted projective space, however it's not as simple as taking the projective closure of the affine curve  $y^2 = f(x)$  (otherwise, this introduces singular points). Indeed, an alternative definition using ordinary projective space is to first consider an affine curve  $C_0 : y^2 = f(x)$  for some degree  $d$  squarefree polynomial  $f(x) \in K[x]$ , and then define the hyperelliptic curve  $C$  as the closure of the image of the map  $[1, x, x^2, \dots, x^{g+1}, y] : C_0 \longrightarrow \mathbb{P}^{g+2}$ , where  $g = \lfloor (d-1)/2 \rfloor$  (e.g. see Silverman [415, Exercise 2.14, p. 40]).

For convenience, we shall often only refer to affine models  $y^2 = f(x)$  of hyperelliptic curves for the remainder of this thesis (and will thus not explicitly refer to weighted projective space very often).

### 1.2.1 Affine models

For a given hyperelliptic curve  $C/K$ , any point  $(X : Y : Z) \in C$  must have either  $X \neq 0$  or  $Z \neq 0$ . Therefore, we can cover  $C$  with two affine charts, given by  $\psi_1$  and  $\psi_2$ :

$$\begin{aligned} \psi_1 : \mathbb{A}^2 &\longrightarrow \mathbb{P}_{1,g+1,1}^2 & \text{and} & & \psi_2 : \mathbb{A}^2 &\longrightarrow \mathbb{P}_{1,g+1,1}^2 \\ (x, y) &\longmapsto (x : y : 1) & & & (y, z) &\longmapsto (1 : y : z) \end{aligned}$$

We note that almost all points of  $C$  lie in the affine patch  $\psi_1(\mathbb{A}^2)$ . Indeed, let  $c'$  be the coefficient of  $X^{2g+2}$  in  $F(X, Z)$ . Then note that, if  $(1 : Y : 0) \in C$ , then  $Y^2 = c'$ , which yields exactly one additional solution  $(1 : 0 : 0)$  if  $c' = 0$ , otherwise, two distinct solutions if  $c' \neq 0$ . We denote these points as the *points at infinity* of  $C$ .

Therefore, one can easily study  $C$  by simply restricting to the affine patch  $\psi_1(\mathbb{A}^2)$  and defining  $f(x) = F(X, 1)$ , whilst keeping in mind the additional one (resp. two) points at infinity if  $\deg f(x)$  is odd (resp. even). We simply notate the unique point at infinity as  $\infty$  if  $\deg f(x)$  is odd, or as the two points  $\infty_1$  and  $\infty_2$  if  $\deg f(x)$  is even.

We shall therefore study hyperelliptic curves as non-singular projective models of the affine curve

$$y^2 + h(x)y = f(x) \tag{1.6}$$

where  $\deg h(x) < g + 2$  and  $\deg f(x) \in \{2g + 1, 2g + 2\}$  with  $f(x)$  having distinct roots. Such an equation (1.6) is called a **Weierstrass equation** for the curve  $C/K$ . If furthermore we have  $f(x), h(x) \in \mathcal{O}_K[x]$ , then such an equation is called **integral**. If we assume that  $K$  doesn't have characteristic 2, then as before we can complete the square on the left hand side of (1.6) which allows us to assume  $h = 0$ , and thus obtain an affine model for  $C$  as

$$y^2 = f(x) \tag{1.7}$$

where  $\deg f(x) \in \{2g + 1, 2g + 2\}$ . Such an equation is called a **simplified Weierstrass equation** for  $C/K$ .

Given any genus  $g$  hyperelliptic curve  $C/K$ , we denote the ramification points of the degree-2 cover  $C \rightarrow \mathbb{P}^1$  as the **Weierstrass points** of  $C$ . If  $C/K$  has a simplified model  $y^2 = f(x)$ , then these are equivalently the points  $(\alpha_i, 0)$  where  $\alpha_i$  is a root of  $f(x)$ .

### 1.2.2 Good reduction and minimal discriminants

We can now introduce the notion of reduction at a prime  $\mathfrak{p}$ . One can give a formal definition using scheme-theoretic language: given any smooth curve  $C/K$ , one can say that  $C$  has good reduction at  $\mathfrak{p}$  if and only if  $C$  is the generic fiber of a smooth proper scheme over  $\text{Spec}(\mathcal{O}_{\mathfrak{p}})$ , where  $\mathcal{O}_{\mathfrak{p}}$  is the completion of  $\mathcal{O}_K$  with respect to the prime  $\mathfrak{p}$  (see e.g. Hindry–Silverman [222, p. 158], Liu [287, p. 462] or Serrà [391, p. 16]). In the particular case of hyperelliptic curves  $C/K$ , for this thesis we can instead give the following more explicit definition using integral Weierstrass equations:

**Definition 1.8** (Good/bad reduction [431, p. 14]). Let  $C/K$  be a hyperelliptic curve. Let  $\mathfrak{p}$  be a prime of  $\mathcal{O}_K$ . We say that  $C/K$  has **good reduction** at the prime  $\mathfrak{p}$  if there exists an integral Weierstrass model  $y^2 + h(x)y = f(x)$  for  $C/K$ , such that the Weierstrass equation  $y^2 + \tilde{h}(x)y = \tilde{f}(x)$ , obtained by reducing the coefficients of  $f(x)$  and  $h(x) \bmod \mathfrak{p}$ , defines a smooth curve  $\tilde{C}$  over  $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$ . Otherwise we say that  $C/K$  has **bad reduction** at  $\mathfrak{p}$ .

More generally, given any finite set of primes  $S$ , we say that a curve  $C/K$  has **good reduction outside  $S$**  if  $C/K$  has good reduction at all primes  $\mathfrak{p} \notin S$ .

One of the most important invariants of a hyperelliptic curve  $C/K$  which encodes the primes of bad reduction for  $C/K$  is the (minimal) discriminant.

**Definition 1.9** (Minimal discriminant [286, p. 4581]). Let  $C/K$  be a hyperelliptic curve of genus  $g$ . For a particular integral Weierstrass equation  $y^2 + h(x)y = f(x)$

of  $C/K$ , we define the **discriminant**  $\Delta_{f,h}$  of this Weierstrass equation as

$$\Delta_{f,h} := \begin{cases} 2^{4g} c^2 \cdot \text{Disc}\left(f(x) + \frac{1}{4}h(x)^2\right) & \text{if } \deg(f + h^2/4) \text{ is odd,} \\ 2^{4g} \cdot \text{Disc}\left(f(x) + \frac{1}{4}h(x)^2\right) & \text{if } \deg(f + h^2/4) \text{ is even,} \end{cases}$$

where  $c$  denotes the leading coefficient of  $f + h^2/4$ . We say that such a Weierstrass equation is **minimal at the prime  $\mathfrak{p}$**  if  $\text{ord}_{\mathfrak{p}}(\Delta_{f,h})$  is minimal among the discriminants  $\Delta_{f,h}$  of all integral Weierstrass equations  $y^2 + h(x)y = f(x)$  for  $C/K$ . We say that a Weierstrass equation  $y^2 + h(x)y = f(x)$  for  $C/K$  is **globally minimal** if it is minimal for all primes  $\mathfrak{p}$  in  $\mathcal{O}_K$ .

The **minimal discriminant** of  $C/K$  is thus the discriminant  $\Delta_{f,h}$  of a globally minimal Weierstrass equation for  $C/K$ . We denote the minimal discriminant as  $\Delta_{\min}$ .

We note that a globally minimal Weierstrass model may not necessarily exist for a hyperelliptic curve  $C$  over an arbitrary number field  $K$ . However, if  $K$  has class number 1 (e.g. for  $K = \mathbb{Q}$ ), then every hyperelliptic curve  $C/K$  has a globally minimal Weierstrass model (and hence a well-defined minimal discriminant  $\Delta_{\min}$ ); see e.g. [291, p. 737] or [286, Remarque 6]. We also note that any hyperelliptic curve  $C$  over a number field  $K$  of class number 1 has a simplified Weierstrass model  $y^2 = f(x)$  which is minimal at every odd prime  $\mathfrak{p}$  (see e.g. [144, Lemma 3.1]).

By Definition 1.8, we note that a hyperelliptic curve  $C/K$  has good reduction at a prime  $\mathfrak{p}$  if and only if there exists an integral Weierstrass equation  $y^2 + h(x)y = f(x)$  for  $C/K$  whose discriminant  $\Delta$  satisfies  $\text{ord}_{\mathfrak{p}}(\Delta) = 0$ . Thus, the primes  $\mathfrak{p}$  of bad reduction for a hyperelliptic curve  $C/K$  are precisely the primes  $\mathfrak{p}$  dividing  $\Delta_{\min}$ .

See also Liu [288] for an algorithm to explicitly compute minimal Weierstrass equations (and thus minimal discriminants) of hyperelliptic curves  $C$  over number fields  $K$  of class number 1.

### 1.2.3 Rosenhain normal form

Given a hyperelliptic curve  $C/K$ , for many of our arguments, it will be most convenient to assume some particular structure on the Weierstrass points of  $C$ , such as assuming that all Weierstrass points are integral, or alternatively that  $(0, 0)$  and  $(1, 0)$  are both Weierstrass points for  $C$ . With this aim, we can prove the following well-known result:

**Proposition 1.6.** *Let  $C/K$  be a smooth genus  $g$  hyperelliptic curve over some field  $K$  with  $\text{char}(K) \neq 2$ . Then  $C/K$  is isomorphic over  $\overline{K}$  to a curve with a Weierstrass*

model of the form

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_{2g-1})$$

for some  $\lambda_1, \dots, \lambda_{2g-1} \in \overline{K}^\times$ .

We first consider the case for elliptic curves (i.e. genus  $g = 1$ ). We recall that any elliptic curve  $E/K$  is isomorphic over  $\overline{K}$  to an elliptic curve given in Legendre form:  $y^2 = x(x-1)(x-\lambda)$ , for some  $\lambda \in \overline{K}$  with  $\lambda \neq 0, 1$  [415, p. 49]. This allows us to study the  $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves by simply specifying  $\lambda$ . We now consider the generalisation of this argument to hyperelliptic curves:

Let  $C/K$  be a hyperelliptic curve over some field  $K$ , with  $\text{char}(K) \neq 2$ . We assume that a simplified model for  $C$  is given by  $y^2 = f(x)$ . First consider the case where  $\deg f = 2g + 2$ . We thus have that

$$y^2 = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{2g+2})$$

for some  $c \in K$  and distinct roots  $\alpha_i \in \overline{K}$ .

Now we consider the Möbius transformations sending the roots  $\alpha_1, \alpha_2, \alpha_3$  to  $0, 1$  and  $\infty$  respectively, given by

$$x = \frac{\alpha_3(\alpha_2 - \alpha_1)x' + \alpha_1(\alpha_3 - \alpha_2)}{(\alpha_2 - \alpha_1)x' + (\alpha_3 - \alpha_2)} \quad \text{and} \quad y = \frac{Ay'}{((\alpha_2 - \alpha_1)x' + (\alpha_3 - \alpha_2))^{g+1}}$$

where we have  $A \in \overline{K}$  given by

$$A = \sqrt{c} \cdot (\alpha_3 - \alpha_2)(\alpha_3 - \alpha_1)(\alpha_2 - \alpha_1)^g \cdot \sqrt{\alpha_1 - \alpha_2} \cdot \prod_{i=4}^{2g+2} \sqrt{\alpha_3 - \alpha_i}.$$

We therefore have that  $C$  is isomorphic over  $\overline{K}$  to a non-singular projective curve with affine model

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_{2g-1}) \tag{1.10}$$

where  $\lambda_1, \dots, \lambda_{2g-1}$  are distinct roots given by

$$\lambda_i = \frac{(\alpha_3 - \alpha_2)(\alpha_{i+3} - \alpha_1)}{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_{i+3})} \tag{1.11}$$

for all  $i \in \{1, \dots, 2g-1\}$ . Similarly, in the case where  $\deg f = 2g + 1$ , then we

obtain a similar result by considering the simpler transformations

$$x = (\alpha_2 - \alpha_1)x' + \alpha_1 \quad \text{and} \quad y = \sqrt{c} \cdot (\alpha_2 - \alpha_1)^{(2g+1)/2} y'$$

which again yields that  $C$  is isomorphic over  $\overline{K}$  to a non-singular projective curve with affine model

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2) \cdots (x-\lambda_{2g-1})$$

where  $\lambda_1, \dots, \lambda_{2g-1}$  are distinct roots given by

$$\lambda_i = \frac{\alpha_{i+2} - \alpha_1}{\alpha_2 - \alpha_1}$$

for all  $i \in \{1, \dots, 2g-1\}$ .

Transforming a hyperelliptic curve  $C$  into the above form is known as transforming into *Rosenhain normal form* [368].

Whilst the above isomorphism allows us to represent any hyperelliptic curve as one with Weierstrass points including 0, 1, and  $\infty$ , we note that this only yields an isomorphic curve over some quadratic extension of  $K(\alpha_1, \dots, \alpha_n)$ . To instead consider isomorphisms only over  $K(\alpha_1, \dots, \alpha_n)$ , we can instead adjust the constant  $A$  to be in  $K(\alpha_1, \dots, \alpha_n)$ . This therefore yields an isomorphism of  $C$  over  $K(\alpha_1, \dots, \alpha_n)$  to an equation of the form:

$$y^2 = c'x(x-1)(x-\lambda_1) \cdots (x-\lambda_{2g-1})$$

where  $\lambda_i$  is given as before in (1.11), and  $c' \in K(\alpha_1, \dots, \alpha_n)$ .

We also note that we are free to choose any three of the roots  $\alpha_1, \dots, \alpha_{2g+2}$  to send to 0, 1,  $\infty$ , and not necessarily just  $\alpha_1, \alpha_2, \alpha_3$ . Thus, for a given hyperelliptic curve of genus  $g$ , there may be several possible representations given in the form (1.10), however there will always be only finitely many (specifically, at most  $(2g+2)!$ ) possible representations in the form (1.10). We note that this agrees with the fact that the moduli space of genus  $g$  hyperelliptic curves  $\mathcal{H}_g$  has dimension  $2g-1$ , e.g. see [173, p. 75].

### 1.3 Jacobians

As with hyperelliptic curves, there are various ways one can define and work with Jacobian varieties. We shall not dive too deeply into the formal definition of the

Jacobian here; for the purposes of this thesis, it suffices to know simply that the Jacobian  $\text{Jac}(C)$  of a smooth genus  $g$  curve  $C/K$  is a dimension  $g$  abelian variety over  $K$ , whose  $K$ -rational points are naturally isomorphic to the  $K$ -rational degree 0 divisor classes in the Picard group  $\text{Pic}^0(C)$ .

For completeness, we shall give a definition of the Jacobian first over  $\mathbb{C}$  (the *analytic Jacobian*), then for arbitrary fields  $K$  (the *algebraic Jacobian*) in the case where  $C(K) \neq \emptyset$ . A good introductory reference for Jacobians over  $\mathbb{C}$  is Griffiths [202], whereas good general discussions for Jacobians in general are given by Milne [319] and Mumford [324].

**Definition 1.12** (Analytic Jacobian). [202, p. 153] Let  $C$  be a smooth curve of genus  $g$  over  $\mathbb{C}$ . Let  $\omega_1, \omega_2, \dots, \omega_g$  be a basis for the space of regular differentials  $\Omega_{\mathbb{C}}^1(C)$  over  $\mathbb{C}$ . Define the lattice  $\Lambda \subset \mathbb{C}^g$  as

$$\Lambda := \left\{ \left( \int_{\gamma} \omega_1, \int_{\gamma} \omega_2, \dots, \int_{\gamma} \omega_g \right) \mid \gamma \in H_1(C, \mathbb{Z}) \right\} \subset \mathbb{C}^g.$$

where  $H_1(C, \mathbb{Z})$  is the first homology group of  $C$ . We define the complex torus  $\mathbb{C}^g/\Lambda$  as the **analytic Jacobian** of  $C$ .

Even for curves  $C$  defined over number fields  $K$ , we'll still call the above definition (considering  $C$  as a curve over  $\mathbb{C}$ ) the *analytic Jacobian* of  $C/K$ . One can show that the analytic Jacobian is canonically a principally polarised abelian variety, with a natural isomorphism to  $\text{Pic}^0(C)$ ; e.g. see [202, p. 156].

To define the Jacobian over arbitrary fields  $K$ , we wish to give the Picard group  $\text{Pic}^0(C)$  some algebraic structure, however doing this explicitly is far more non-trivial in the general case; there are some subtleties to consider. In the case where  $C(K) \neq \emptyset$ , we can give the following (non-constructive) definition, following the definition given in Milne [319]:

**Definition 1.13** (Algebraic Jacobian). [319, p. 85] Let  $C/K$  be a smooth projective curve such that  $C(K) \neq \emptyset$ . Let  $\mathbf{Var}_K$  denote the category of varieties over  $K$  and let  $\mathbf{Set}$  denote the category of sets. For any variety  $T$  in  $\mathbf{Var}_K$ , we denote  $\text{Pic}^0(T)$  as the *degree 0 Picard group* of  $T$  (see [319, p. 35] for a formal definition).

We define the Picard functor  $P_C^0$  as the contravariant functor between  $\mathbf{Var}_K$  and  $\mathbf{Set}$  given by

$$P_C^0 : \mathbf{Var}_K \longrightarrow \mathbf{Set}, \quad T \longmapsto \frac{\text{Pic}^0(C \times T)}{q^* \text{Pic}^0(T)}.$$

In other words,  $P_C^0(T)$  are the families of invertible sheaves of degree zero on  $C$

parametrised by  $T$ , modulo trivial families (here,  $q^*$  denotes the pullback of the standard projection map  $q : C \times T \rightarrow T$ ).

Furthermore, for any variety  $X$ , we define the contravariant functor  $h_X$  given by

$$h_X : \mathbf{Var}_K \longrightarrow \mathbf{Set}, \quad T \longmapsto \mathrm{Hom}(T, X).$$

We thus define the **Jacobian**  $\mathrm{Jac}(C)$  of  $C$  as the variety  $J$  such that the functor  $P_C^0$  is isomorphic to  $h_J$ .<sup>14</sup> Such a variety always exists if  $C(K) \neq \emptyset$ , and is furthermore unique (up to isomorphism) by Yoneda's lemma. An explicit construction of  $\mathrm{Jac}(C)$  as a variety birational to the  $g$ -th symmetric power of  $C$  is given by Weil [476].

Whilst this gives a satisfactory definition of  $\mathrm{Jac}(C)$  in the case where  $C(K) \neq \emptyset$ , we would still like to work with  $\mathrm{Jac}(C)$  even if  $C(K) = \emptyset$ . Unfortunately in this case, the above functor  $P_C^0$  is not always representable, and so a general definition requires more care; see e.g. [319, p. 86]. In particular, one requirement for representability is that the natural map  $\mathrm{Pic}(C) \rightarrow \mathrm{Pic}(C_L)^{\mathrm{Gal}(L/K)}$  be a bijection, for a Galois extension  $L/K$ . Indeed, for any Galois extension  $L/K$ , we have an exact sequence

$$0 \rightarrow \mathrm{Pic}(C) \rightarrow \mathrm{Pic}(C_L)^{\mathrm{Gal}(L/K)} \rightarrow \mathrm{Br}(K)$$

where  $\mathrm{Br}(K)$  is the Brauer group of the field  $K$ . i.e. given an element in  $\mathrm{Pic}(C_L)^{\mathrm{Gal}(L/K)}$ , there is a Brauer group obstruction to having it arise from an element in  $\mathrm{Pic}(C)$ .<sup>15</sup> Fortunately these issues can be dealt with, and a formal definition of the Jacobian for arbitrary curves  $C/K$  can be given essentially by replacing  $P_C^0$  with its *sheafification*, the details of which we omit here; see Bosch–Lütkebohmert–Raynaud [57, Chapter 8], Milne [319, Chapter 3], or Urbanik [456] for a full formal definition.

One corollary of the above definition is that the functorial definition of the Jacobian  $J(C)$  is isomorphic to  $\mathrm{Pic}^0(C)$  and thus  $J(C)$  is naturally an abelian variety. However, we note that this definition does not give any explicit model for  $J(C)$ .

In general, providing an explicit model of the Jacobian in terms of a set of defining polynomials is a highly non-trivial task. For elliptic curves ( $g = 1$ )  $E$ , we simply have that  $\mathrm{Jac}(E)$  is isomorphic to  $E$ , since  $E$  is isomorphic to  $\mathrm{Pic}^0(E)$  by the map  $P \mapsto P - (\infty)$ . Already in the genus 2 case, things become a lot more complicated. Indeed, Cassels and Flynn [98] gave an explicit construction for the Jacobian of an arbitrary genus 2 curve over  $K$  as a smooth projective curve in  $\mathbb{P}^{15}$

<sup>14</sup>We remark that this definition is also simply the statement that  $P_C^0$  is *represented* by  $\mathrm{Jac}(C)$ .

<sup>15</sup>We refer to Snowden's lecture notes [419] for a further discussion on the obstructions to representability of the Jacobian in the general case.



defined by 72 quadratic forms over  $K$ . It is thus best left for computers to use these equations!

Giving a detailed overview of Jacobian varieties is well beyond the scope of this thesis, so we shall not go into much further detail regarding Jacobians, as most of our calculations will simply use results from cluster pictures [148] (as described in Section 1.4) and so we'll not need to work directly with the geometry of the Jacobian. For the most part, it suffices to know that the **Jacobian** of a genus  $g$  curve  $C/K$  is some dimension  $g$  abelian variety  $A/K$  whose  $K$ -rational points  $A(K)$  is finitely generated (by the Mordell-Weil theorem [431, p. 20]) and which naturally represents the Picard group  $\text{Pic}^0(C)$ .

### 1.3.1 Primes of almost good reduction

One key property of Jacobians which is central to our thesis is that, if  $C/K$  has good reduction at some prime  $\mathfrak{p}$ , then  $\text{Jac}(C)$  will have good reduction at  $\mathfrak{p}$  (this follows by functoriality). But crucially the converse is not true! A prime  $\mathfrak{p}$  of bad reduction for  $C$  but good reduction for  $\text{Jac}(C)$  is sometimes called a prime of *almost good reduction* or *mild bad reduction* for  $C$ .

The primary invariant of Jacobians  $\text{Jac}(C)$  (and more generally abelian varieties) which encodes the primes of bad reduction for  $\text{Jac}(C)$ , is the **conductor**  $N$ . This is a positive integer with the property that, for each prime  $\mathfrak{p}$  in  $\mathcal{O}_K$ , we have  $\text{ord}_{\mathfrak{p}}(N) > 0$  if and only if  $\text{Jac}(C)$  has bad reduction at  $\mathfrak{p}$ . By a slight abuse of terminology, we define the conductor of a curve  $C/K$  as the conductor of its Jacobian  $\text{Jac}(C)$ .<sup>16</sup> For elliptic curves  $E/K$  and genus 2 curves  $C/K$  with conductor  $N$  and minimal discriminant  $\Delta_{\min}$ , it's known that  $\text{ord}_{\mathfrak{p}}(N) \leq \text{ord}_{\mathfrak{p}}(\Delta_{\min})$  for all primes  $\mathfrak{p}$  in  $\mathcal{O}_K$ ; in particular this implies that  $N$  divides the minimal discriminant  $\Delta_{\min}$  [285]. Similar conductor-discriminant inequalities have also been shown by Srinivasan [420, 421] and Obus–Srinivasan [334] for hyperelliptic curves, and Kohls [268, Chapter 5] for superelliptic curves. For a full definition of the conductor and further background, see Brumer–Kramer [77], Liu [285], or Lockhart–Rosen–Silverman [292].

A rather trivial example demonstrating the existence of primes of almost good reduction can be seen by noting that the Jacobian of any genus 0 curve is a dimension 0 abelian variety (a point) which trivially has good reduction everywhere.

<sup>16</sup>It's worth remarking that this is not quite the same as the definition of the conductor  $N_C$  of a curve  $C$  given in [469, p. 4461].

A far more interesting example by Armand Brumer [76] is given by the following genus 2 curve  $C/\mathbb{Q}$ :

$$C/\mathbb{Q} : y^2 = (x^2 + 4)(14008x^4 - 6548x^3 - 10807372x^2 + 15298348x - 597161415)$$

The conductor is  $N = 47891 = 83 \cdot 577$ , however the minimal discriminant is  $\Delta_{\min} = 31^{12} \cdot 83 \cdot 577 \cdot 23549^{12}$  (a 76-digit number!); here both the primes 31 and 23549 are primes of almost good reduction for  $C/\mathbb{Q}$ .

Proving an effective bound on the possible primes of almost good reduction for  $C$  given a bound on the bad primes for  $\text{Jac}(C)$  would give an effective solution to the Shafarevich conjecture for Jacobians of hyperelliptic curves. Unfortunately, this is still a very open problem; as the above example illustrates, such primes of mild bad reduction can be very big!

Whilst we won't make much use of the following observation in our thesis, one can give the following rather neat necessary and sufficient criterion for a prime  $\mathfrak{p}$  to be a prime of almost good reduction for  $C$ :

First recall that a criterion of Neron-Ogg-Shafarevich [397, p. 493] states that, for an abelian variety  $A/K$ ,  $A$  has good reduction at a prime  $\mathfrak{p}$  if and only if the action of the inertia subgroup  $I_{\mathfrak{p}} \subset \text{Gal}(\overline{K}/K)$  acts trivially on the  $\ell$ -adic Tate module  $T_{\ell}(A)$  (for any prime  $\ell$  coprime to the residue characteristic of  $\mathfrak{p}$ ). An analogous criterion for smooth proper curves  $C/K$  is given by Oda [335, Theorem 3.2], stating that a curve  $C/K$  has good reduction at  $\mathfrak{p}$  if and only if the action of  $I_{\mathfrak{p}}$  acts trivially on the pro- $\ell$  completion of its geometric fundamental group  $\pi_1(C \otimes \overline{K})_{\ell}$ .

Now noting that  $T_{\ell}(A) \cong \pi_1(A \otimes \overline{K})_{\ell}$  (e.g. see [133, p. 15]), and using that the fundamental group of  $\text{Jac}(C)$  is simply the abelianisation of the fundamental group of  $C$  (e.g. see [427, Proposition 68]), one can characterise primes  $\mathfrak{p}$  of almost good reduction as the primes  $\mathfrak{p}$  for which  $I_{\mathfrak{p}}$  has a non-trivial action on  $\pi_1(C \otimes \overline{K})_{\ell}$  but acts trivially on its abelianisation  $\pi_1(C \otimes \overline{K})_{\ell}^{\text{ab}}$ .

A detailed description of the action of inertia  $I_{\mathfrak{p}}$  on  $\pi_1(C \otimes \overline{K})_{\ell}$  for primes  $\mathfrak{p}$  of almost good reduction is given by Oda [335]. Whilst this criterion gives a geometric explanation for primes  $\mathfrak{p}$  of almost good reduction, in order to run explicit computations with such primes for Jacobians of hyperelliptic curves, it's far simpler for us to use the machinery of cluster pictures, which we shall introduce in Section 1.4!

### 1.3.2 Computing with the Jacobian

For our purposes, we won't need to know the algebraic structure of the Jacobian, and instead perform computations on  $\text{Jac}(C)$  by working explicitly with divisor classes

$[D] \in \text{Pic}^0(C)$ . Given a curve  $C/K$  of genus  $g$ , recall that one can represent a degree 0 divisor  $D$  in  $\text{Div}^0(C)$  as a formal sum of points

$$D = n_1(P_1) + n_2(P_2) + \cdots + n_k(P_k),$$

where  $P_i \in C(\overline{K})$  and  $n_i \in \mathbb{Z}$  such that  $n_1 + \cdots + n_k = 0$ . For a subfield  $L \subset \overline{K}$ , we say that the divisor  $D \in \text{Div}^0(C)$  is  $L$ -rational if  $D$  is fixed by the action of  $\text{Gal}(\overline{K}/L)$ . The degree 0 Picard group  $\text{Pic}^0(C)$  is simply the quotient of  $\text{Div}^0(C)$  by the set of principal divisors  $\text{Princ}(C) := \{\text{div}(f) : f \in \overline{K}(C)^\times\}$ .

We state the following theorem which allows us to uniquely represent elements of  $\text{Pic}^0(C)$  as certain unordered tuples of points:

**Theorem 1.7.** [90, p. 96] *Let  $C/K$  be a genus  $g$  hyperelliptic curve with a fixed point  $P_\infty \in C(K)$ . Then each divisor class  $[D]$  in  $\text{Pic}^0(C)$  has a unique representative of the form*

$$(P_1) + (P_2) + \cdots + (P_k) - k(P_\infty)$$

for some  $k \leq g$ , where  $P_i \neq -P_j$  for  $i \neq j$  and such that no  $P_i$  satisfying  $P_i = -P_i$  appears more than once.<sup>17</sup> Such divisors are called *reduced divisors*.

For hyperelliptic curves  $C/K$  with an odd degree model, one can always take  $P_\infty$  to be the unique point at infinity. Otherwise, for hyperelliptic curves with an even degree model, we can take divisors of the form  $(P_1) + (P_2) + \cdots + (P_k) - (k/2)(P_{+\infty} + P_{-\infty})$  with  $k$  even.

The way Jacobians are handled computationally, particularly in Magma, is usually via the *Mumford representation* [325], i.e. the reduced divisor  $D = (P_1) + (P_2) + \cdots + (P_k) - k(P_0)$  is stored as a pair of two polynomials  $(a(x), b(x))$  where  $a = (x - x_1)(x - x_2) \cdots (x - x_k)$  and  $b(x)$  is the unique polynomial of degree  $< k$  such that  $b(x_i) = y_i$ , where  $P_i = (x_i, y_i)$ . Cantor [90] gave an algorithm to perform arithmetic on these pairs, giving a computational method to work with Jacobians of hyperelliptic curves without requiring an explicit model for  $\text{Jac}(C)$  as a variety.

### 1.3.3 Fields of $n$ -torsion on the Jacobian

Finally, we shall give some results about torsion points over the Jacobian  $\text{Jac}(C)$  of a hyperelliptic curve  $C/K$ . If the context of the hyperelliptic curve  $C$  is clear, we abbreviate  $\text{Jac}(C)$  simply by  $J$ . As with elliptic curves, we also denote the set of  $n$ -torsion points on  $J$  (over  $\overline{K}$ ) by  $J[n]$ , and we let  $K(J[n])$  denote the smallest finite algebraic extension of  $K$  containing all coordinates of the points of the  $n$ -torsion

<sup>17</sup>Here, for a point  $P = (x, y)$  on  $C$ , we define  $-P$  as  $(x, -y)$ .

points  $J[n]$ . It's well-known that  $J[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$  if  $\text{char}(K)$  does not divide  $n$ . Otherwise, if  $\text{char}(K) = p$ , then there exists some integer  $i \in \{0, \dots, g\}$  such that for all  $m \geq 1$ , we have  $J[p^m] \cong (\mathbb{Z}/p^m\mathbb{Z})^i$  [324, p. 64].

We now give a sketch proof of the field in which the 2-torsion  $J[2]$  lies.

**Theorem 1.8.** [485, p. 5] *Let  $C/K$  be a hyperelliptic curve with affine model  $C : y^2 = c(x - \alpha_1) \cdots (x - \alpha_n)$ . Then the field of 2-torsion  $K(J[2])$  is  $K(\alpha_1, \dots, \alpha_n)$ .*

*Proof.* [485, p. 5] We shall first give an explicit description of the elements of  $J[2]$ . Indeed, let  $\mathcal{W}$  denote the Weierstrass points of  $C$ . Then for any subset  $U \subset \mathcal{W}$  of even cardinality, we define the divisor  $e_U \in \text{Div}^0(C)$  as

$$e_U := \begin{cases} \sum_{P \in U} P - |U| \cdot (\infty) & \text{if } n \text{ odd,} \\ \sum_{P \in U} P - \frac{|U|}{2} \cdot ((\infty_1) + (\infty_2)) & \text{if } n \text{ even.} \end{cases}$$

We claim that the set of all  $e_U$  over all subsets  $U \subseteq \mathcal{W}$  of even cardinality cover all elements in  $J[2]$ . Indeed, we first note that, for any  $\alpha_i$ , we have that the divisor of the function  $x - \alpha_i \in K(C)^\times$  is

$$\text{Div}(x - \alpha_i) = \begin{cases} 2(\alpha_i, 0) - 2(\infty) & \text{if } n \text{ odd,} \\ 2(\alpha_i, 0) - ((\infty_1) + (\infty_2)) & \text{if } n \text{ even.} \end{cases}$$

Therefore, by taking the appropriate product of functions  $(x - \alpha_i)$ , we have that  $2e_U$  is principal, and thus each  $e_U$  is an element of  $J[2]$ .

Next, we aim to show which elements  $e_U$  are equivalent in  $\text{Pic}^0(C)$ . We first note that  $e_{U_1} + e_{U_2}$  is equivalent to  $e_{U_1 \ominus U_2}$  where  $U_1 \ominus U_2 = (U_1 \cup U_2) \setminus (U_1 \cap U_2)$  is the symmetric difference of  $U_1$  and  $U_2$ . Since  $\text{div}(y) = e_{\mathcal{W}}$ , we have that  $e_{\mathcal{W}}$  is principal, and furthermore that  $e_U$  is principal if and only if  $e_{\mathcal{W} \setminus U}$  is principal. Thus it suffices to classify when  $e_U$  is principal for subsets  $U \subset \mathcal{W}$  where  $|U| \leq g$ .

Now let  $U \subset \mathcal{W}$  be non-empty and  $|U| \leq g$ . Assume for contradiction that  $e_U = \text{div}(h)$  for some function  $h \in K(C)^\times$ . By definition of  $e_U$ ,  $h$  cannot have any poles at any affine (i.e. non-infinite) point in  $C$ , thus  $h$  is some polynomial in  $x$  and  $y$ . Furthermore, noting that the divisor of poles of  $y$  has degree  $n$ , and the divisors of poles of  $h$  has degree  $|U| \leq g = \lfloor \frac{n-1}{2} \rfloor$ , this implies  $h$  must be a polynomial only in  $x$ . As  $U$  non-empty, we have for some  $(\alpha_i, 0) \in U$ , that  $h(\alpha_i) = 0$  and so  $(x - \alpha_i)$  divides  $h$ . However, since  $\text{ord}_{(\alpha_i, 0)}(x - \alpha_i) = 2$ , this implies that  $h/(x - \alpha_i)$  must have some pole on the affine part of  $C$ , which yields a contradiction.

By the above argument, this proves that we have a unique distinct divisor  $e_U$  in  $\text{Pic}^0(C)$  for every partition of  $\mathcal{W}$  into two even subsets. As there are  $2^{2g}$  such partitions, and  $|J[2]| = 2^{2g}$ , this finally implies that all elements of  $J[2]$  are represented by divisors of the form  $e_U$ . Therefore,  $K(J[2]) \subseteq K(\alpha_1, \dots, \alpha_n)$ .

For the other inclusion, one can show that the only permutation in the Galois group  $\text{Gal}(K(\alpha_1, \dots, \alpha_n)/K)$  which fixes every partition of  $\mathcal{W}$  into two even subsets is the identity [485, p. 6], assuming  $n \neq 4$ . This therefore proves the other inclusion, and thus the claim holds.  $\square$

We shall also state an analogous result for the field of 4-torsion  $K(J[4])$ . A proof in the case where  $J$  is the Jacobian of an odd degree hyperelliptic curve is given later in Lemma 3.34.

**Theorem 1.9.** [485, p. 7] *Let  $C/K$  be a hyperelliptic curve with affine model  $C : y^2 = c(x - \alpha_1) \cdots (x - \alpha_n)$ . Then the field of 4-torsion  $K(J[4])$  is*

$$K(J[4]) = \begin{cases} K(J[2])\left(\zeta_4, \{\sqrt{\alpha_i - \alpha_j}\}_{1 \leq i, j \leq n}\right) & \text{if } n \text{ odd,} \\ K(J[2])\left(\zeta_4, \{\sqrt{\alpha_i - \alpha_j}\}_{1 \leq i, j \leq n}, \prod_{\substack{1 \leq \ell \leq n-1 \\ \ell \neq i, j}} \sqrt{\alpha_\ell - \alpha_n}\right) & \text{if } n \text{ even.} \end{cases}$$

Before moving on to cluster pictures, it's worth mentioning the following definition, which will allow us to classify the various Jacobians seen in a later section:

**Definition 1.14.** Let  $C/K$  be a hyperelliptic curve of genus  $g$  with its associated Jacobian  $\text{Jac}(C)$ . Then we say that  $\text{Jac}(C)$  is **split** (over  $K$ ) if there exist abelian varieties  $A_1$  and  $A_2$  over  $K$  of lower dimension than  $g$ , such that  $\text{Jac}(C)$  is isogenous (over  $K$ ) to  $A_1 \times A_2$ .

Otherwise, we say the Jacobian is **simple** (over  $K$ ). Furthermore, if there do not exist abelian varieties  $A_1, A_2$  over  $\overline{K}$  such that  $\text{Jac}(C)$  is isogenous (over  $\overline{K}$ ) to  $A_1 \times A_2$ , then we say that the Jacobian is **geometrically simple**.

Specifically, if  $C/K$  is a genus 2 curve, then  $\text{Jac}(C)$  splits exactly when it's isogenous to  $E_1 \times E_2$  for some two elliptic curves  $E_1, E_2$  over  $K$ .

It's worth also mentioning the following theorem, which in some cases allows us to easily identify when the Jacobian of a genus 2 curve  $C$  is split:

**Theorem 1.10.** [98, p. 155] *Let  $C/K$  be a smooth bielliptic genus 2 curve with Weierstrass model of the form*

$$y^2 = ax^6 + bx^4 + cx^2 + d.$$

*Then the Jacobian  $\text{Jac}(C)$  is isogenous to the product of the two elliptic curves  $E_1/K$  and  $E_2/K$  given by*

$$E_1 : y^2 = ax^3 + bx^2 + cx + d, \quad \text{and} \quad E_2 : y^2 = dx^3 + cx^2 + bx + a.$$

We further note that this also gives an alternative way to calculate the rank, since we have that  $\text{rank}(\text{Jac}(C)) = \text{rank}(E_1) + \text{rank}(E_2)$ . A proof of this theorem can be found in Cassels-Flynn [98, p. 155].

## 1.4 Cluster pictures

We shall finally introduce the main machinery which we'll use to study the reduction of hyperelliptic curves. For a given hyperelliptic curve  $C$  over  $K$ , we consider the notion of *cluster pictures*, first introduced by Dokchitser, Dokchitser, Maistret, and Morgan [147], where its power to compute many arithmetic invariants of hyperelliptic curves is described in [148].

**Definition 1.15.** [148, p. 1215] Let  $g \geq 2$ , and let  $C$  be a hyperelliptic curve over a number field  $K$  of genus  $g$  given with a simplified model

$$y^2 = f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where  $n \in \{2g + 1, 2g + 2\}$  and where  $\alpha_1, \dots, \alpha_n \in \overline{K}$  are the  $n$  complex roots of  $f(x)$ . Let  $\mathcal{R} = \{\alpha_1, \dots, \alpha_n\}$  and let  $\mathcal{P}(\mathcal{R})$  be the power set of  $\mathcal{R}$ . Let  $\mathfrak{p}$  be an odd prime in  $K$ , and let  $v_{\mathfrak{p}}$  denote the discrete normalised  $p$ -adic valuation induced by  $\mathfrak{p}$ . We define the **cluster picture**  $\Sigma_{\mathfrak{p}} \subset \mathcal{P}(\mathcal{R})$  associated to  $C$  (with respect to  $\mathfrak{p}$ ) as the following set:

$$\Sigma_{\mathfrak{p}} := \{\mathfrak{s} \in \mathcal{P}(\mathcal{R}) \mid \mathfrak{s} = D_{z,d} \cap \mathcal{R} \text{ for some } z \in \overline{K}, d \in \mathbb{Q}\}$$

where  $D_{z,d} := \{x \in \overline{K} \mid v_{\mathfrak{p}}(x - z) \geq d\}$ . I.e. these are simply the subsets of  $\mathcal{R}$  which are cut out by bounded  $p$ -adic discs in  $K$ .<sup>18</sup>

<sup>18</sup>We note that the extension of the  $p$ -adic valuation from  $K$  to  $K(J[2])$  is not uniquely determined

Before we state the theorems, we must first introduce some cluster picture terminology:

**Definition 1.16.** Elements  $\mathfrak{s}$  of  $\Sigma_{\mathfrak{p}}$  are called *clusters*. The *depth*  $d_{\mathfrak{s}}$  of a cluster  $\mathfrak{s}$  is

$$d_{\mathfrak{s}} := \min_{r, r' \in \mathfrak{s}} v_{\mathfrak{p}}(r - r')$$

(i.e. the maximal valuation which cuts out  $\mathfrak{s}$ ). For any cluster  $\mathfrak{s} \in \Sigma_{\mathfrak{p}}$  we also define the *leading depth*  $\nu_{\mathfrak{s}}$  as

$$\nu_{\mathfrak{s}} := v_{\mathfrak{p}}(c) + \sum_{r \in \mathcal{R}} d_{r \wedge \mathfrak{s}}$$

where  $r \wedge \mathfrak{s}$  denotes the smallest cluster containing both  $r$  and  $\mathfrak{s}$ .

We easily note that  $\Sigma_{\mathfrak{p}}$  will always contain all the singleton elements  $\{r_i\}$  for all  $r_i \in \mathcal{R}$ , as well as the entire set of roots  $\mathcal{R}$ . If  $\Sigma_{\mathfrak{p}}$  consists of only these elements, we say that the cluster picture at  $\mathfrak{p}$  is *trivial*.

We call a cluster  $\mathfrak{s}$  *odd* (resp. *even*) if  $|\mathfrak{s}|$  is odd (resp. even). If  $\mathfrak{s}' \subsetneq \mathfrak{s}$  is a maximal subcluster, we say that  $\mathfrak{s}'$  is a *child* of  $\mathfrak{s}$  and that  $\mathfrak{s}$  is the *parent* of  $\mathfrak{s}'$ . We call a cluster  $\mathfrak{s}$  *principal* if  $|\mathfrak{s}| \geq 3$  except if either  $\mathfrak{s} = \mathcal{R}$  is even and has exactly two children, or if  $\mathfrak{s}$  has a child of size  $2g$ .

The remarkable property of cluster pictures (and why it's so useful) is that, for any hyperelliptic curve  $C/K$ , it provides a very simple way of easily reading off the reduction type of  $C$  as well as  $\text{Jac}(C)$  at any odd prime  $\mathfrak{p}$ .

We now partially restate the main theorem given by Dokchitser–Dokchitser–Maistret–Morgan [148]. We first recall that a variety  $X$  over some number field  $K$  has *potentially good reduction* at  $\mathfrak{p}$  if there exists a finite extension  $K'/K$  such that  $X/K'$  has good reduction at a prime above  $\mathfrak{p}$ .

**Theorem 1.11.** [148, p. 1218] *Let  $C/K$  be a hyperelliptic curve of genus  $g$ , and let  $\mathfrak{p}$  be an odd prime in  $K$ . Then we can read off the reduction type of  $C$  at  $\mathfrak{p}$  using  $\Sigma_{\mathfrak{p}}$  as follows:*

- (i)  *$C$  has potentially good reduction at  $\mathfrak{p}$  if and only if  $\Sigma_{\mathfrak{p}}$  has no proper clusters of size  $< 2g + 1$  (i.e.  $\Sigma_{\mathfrak{p}}$  is either trivial, or consists of a single non-trivial cluster of size  $2g + 1$ )*
- (ii) *Assuming  $C$  has potentially good reduction at  $\mathfrak{p}$ , it then furthermore has good reduction at  $\mathfrak{p}$ , if  $K(\mathcal{R})/K$  is unramified at  $\mathfrak{p}$  and  $v_{\mathfrak{s}} \in 2\mathbb{Z}$  for the unique principal cluster  $\mathfrak{s}$ .*

---

if multiple primes in  $K(J[2])$  lie above  $\mathfrak{p}$ , however choosing a different valuation simply corresponds to constructing  $\Sigma_{\mathfrak{p}}$  over  $\sigma(\mathcal{R})$  for some  $\sigma \in \text{Gal}(K(\mathcal{R})/K)$ , and thus yields an isomorphic cluster picture.

- (iii)  $\text{Jac}(C)$  has potentially good reduction at  $\mathfrak{p}$  if and only if all clusters  $\mathfrak{s} \neq \mathcal{R}$  in  $\Sigma_{\mathfrak{p}}$  are odd.
- (iv) Furthermore,  $\text{Jac}(C)$  has good reduction at  $\mathfrak{p}$  if and only if  $K(\mathcal{R})/K$  is unramified at  $\mathfrak{p}$  and  $v_{\mathfrak{s}} \in 2\mathbb{Z}$  for all principal clusters  $\mathfrak{s}$ .

A beautiful overview of everything that cluster pictures can do is given in [35]. We note that cluster pictures have recently been used very successfully in a wide variety of computations and theorems, e.g. see [150, 16, 272, 323, 38, 74, 199]. We also remark that a Sage implementation to compute cluster pictures has been given by Best and van Bommel [37].

We now illustrate applying this theorem to the following example of a genus 2 curve over  $\mathbb{Q}$ .

**Example 1.12.** Let  $C/\mathbb{Q}$  be a genus 2 curve given by the simplified model,

$$C/\mathbb{Q} : y^2 = 6x^6 - 13x^5 + 27x^4 - 28x^3 + 27x^2 - 13x + 6. \quad (1.17)$$

We remark that this is the genus 2 curve with LMFDB label 2880.c.368640.1 [290, Genus 2 curve 2880.c.368640.1]. By factorising the right hand side of (1.17), we obtain  $y^2 = (x^2 - x + 1)(2x^2 - x + 2)(3x^2 - 2x + 3)$ , and therefore the Weierstrass points of  $C$  can be presented as

$$y^2 = 6(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)(x - \alpha_5)(x - \alpha_6)$$

where

$$\alpha_1 = \frac{1+i\sqrt{3}}{2}, \quad \alpha_2 = \frac{1-i\sqrt{3}}{2}, \quad \alpha_3 = \frac{1+i\sqrt{15}}{4}, \quad \alpha_4 = \frac{1-i\sqrt{15}}{4}, \quad \alpha_5 = \frac{1+2i\sqrt{2}}{3}, \quad \alpha_6 = \frac{1-2i\sqrt{2}}{3}.$$

Therefore, a splitting field can be obtained as the degree 8 extension  $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-3}, \sqrt{5})$ . We note that the ideals (2), (3), (5) ramify over  $K$  into two prime factors each:

$$(2) = \mathfrak{p}_2^2 \cdot \mathfrak{q}_2^2, \quad (3) = \mathfrak{p}_3^2 \cdot \mathfrak{q}_3^2, \quad (5) = \mathfrak{p}_5^2 \cdot \mathfrak{q}_5^2.$$

Let's now consider calculating the cluster picture at the prime  $p = 3$ . We can therefore without loss of generality extend the 3-adic valuation to  $K$  using  $\mathfrak{q}_3$ . We therefore notice the following valuations between the roots  $\alpha_i$ : note that  $(\alpha_1 - \alpha_2) = (i\sqrt{3}) = \mathfrak{p}_3\mathfrak{q}_3$ , and thus  $v_3(\alpha_1 - \alpha_2) = \frac{1}{2}$ .

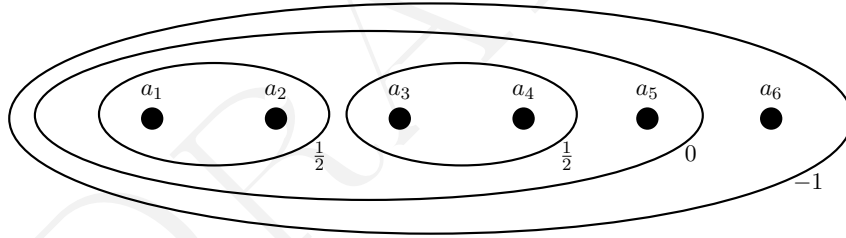
Similarly, we note  $(\alpha_3 - \alpha_4) = (\frac{i\sqrt{15}}{2})$ , which also has 3-adic valuation of  $1/2$ . Indeed, we can tabulate the differences between each of the roots  $\alpha_1, \dots, \alpha_6$ :



Table 1.3: Factorisation of the ideals  $(\alpha_i - \alpha_j)$  (i.e. up to units)

	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\alpha_4$	$\alpha_5$	$\alpha_6$
$\alpha_1$	0	$\mathfrak{p}_3 \mathfrak{q}_3$	$\mathfrak{p}_2^{-2}$	$\mathfrak{q}_2^{-2}$	$\mathfrak{p}_3^{-2}$	$\mathfrak{q}_3^{-2}$
$\alpha_2$		0	$\mathfrak{p}_2^{-2}$	$\mathfrak{q}_2^{-2}$	$\mathfrak{p}_3^{-2}$	$\mathfrak{q}_3^{-2}$
$\alpha_3$			0	$\mathfrak{p}_2^{-2} \mathfrak{q}_2^{-2} \mathfrak{p}_3 \mathfrak{q}_3 \mathfrak{p}_5 \mathfrak{q}_5$	$\mathfrak{p}_2^{-2} \mathfrak{p}_3^{-2}$	$\mathfrak{p}_2^{-2} \mathfrak{q}_3^{-2}$
$\alpha_4$				0	$\mathfrak{q}_2^{-2} \mathfrak{p}_3^{-2}$	$\mathfrak{q}_2^{-2} \mathfrak{q}_3^{-2}$
$\alpha_5$					0	$\mathfrak{p}_2^5 \mathfrak{q}_2^5 \mathfrak{p}_3^{-2} \mathfrak{q}_3^{-2}$
$\alpha_6$						0

From the above table, we note that 3-adic valuation, is at least  $-1$  for any difference  $\alpha_i - \alpha_j$ , thus the depth of the cluster around all roots is  $-1$ . Furthermore, we'll have a cluster of size 5 around all the roots except  $\alpha_6$ , and finally we'll have two twin clusters around  $\{\alpha_1, \alpha_2\}$ , and  $\{\alpha_3, \alpha_4\}$  of depth  $1/2$ . This yields the following cluster picture  $\Sigma_3$ :

Figure 1.1: Cluster picture  $\Sigma_3$  for the genus 2 curve  $C$  given in (1.17).

Note that, if we chose to extend the 3-adic valuation to  $\mathfrak{p}_3$  instead of  $\mathfrak{q}_3$ , this would yield an isomorphic cluster with  $\alpha_5$  and  $\alpha_6$  swapped.

One limitation of cluster pictures is that they only apply to odd primes  $\mathfrak{p}$ . In particular, there's no easy criterion to determine whether a genus  $g \geq 3$  hyperelliptic curve  $C/\mathbb{Q}$  or its Jacobian has (potential) good reduction at  $p = 2$ . However, we do mention some recent progress on extending these methods to even primes  $\mathfrak{p}$  by Dokchitser–Morgan [151], Fiore–Yelton [172], and Gehrunger–Pink [190]. It's also worth mentioning that analogous definitions of cluster pictures also exist for superelliptic curves (e.g. see [340, Section 2] or [273]).

## 1.5 Invariants of hyperelliptic curves

When characterising hyperelliptic curves  $C$  over number fields  $K$ , it is often useful to work with a set of invariants corresponding to the  $\overline{K}$ -isomorphism class of  $C$ . This area of study has its roots in 19th century mathematics, where a good treatment of some results from that time can be found in Elliott [157] and Hilbert [221].

Let  $K$  be a field with  $\text{char}(K) \neq 2$  and let  $C/K$  be a genus  $g$  hyperelliptic curve with an even degree simplified Weierstrass model  $y^2 = c(x - \alpha_1) \cdots (x - \alpha_n)$  where  $n = 2g + 2$ . Let  $m$  be a positive even integer. For our purposes, we shall consider degree  $m$  invariants of the form

$$I_m(C) := (4c)^m \sum_{\sigma \in S_n / \sim} \prod_{(i,j) \in \mathcal{S}} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}), \quad (1.18)$$

where  $\mathcal{S}$  is a finite set of distinct pairs  $(i, j)$ ,  $i \neq j$ , such that each  $i \in \{1, \dots, n\}$  appears in exactly  $m$  pairs in  $\mathcal{S}$ . Here, the sum runs over all permutations  $\sigma \in S_n$  of the index set  $\{1, \dots, n\}$  which yield distinct expressions for the product  $\prod_{(i,j) \in \mathcal{S}} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$ ; i.e.  $\sigma$  runs over all  $S_n$ -Galois orbits, where  $\sigma_1 \sim \sigma_2$  if and only if we have equality between the two sets,  $\{(\sigma_1(i), \sigma_1(j)) \mid (i, j) \in \mathcal{S}\}$  and  $\{(\sigma_2(i), \sigma_2(j)) \mid (i, j) \in \mathcal{S}\}$ ; e.g. see Igusa [230, p. 620] or Smart [418, p. 282].

These invariants have the crucial property that, for any  $k$ -tuple of even integers  $(m_1, m_2, \dots, m_k)$ , if two genus  $g$  hyperelliptic curves  $C$  and  $D$  are isomorphic over  $\overline{K}$ , then we have the equality

$$(I_{m_1}(C) : I_{m_2}(C) : \cdots : I_{m_k}(C)) = (I_{m_1}(D) : I_{m_2}(D) : \cdots : I_{m_k}(D))$$

as elements in the weighted projective space  $\mathbb{P}_{m_1, m_2, \dots, m_k}^{k-1}$ .

In particular, by considering all such invariants  $I_m(C)$ , we can thus uniquely characterise  $\overline{K}$ -isomorphism classes of hyperelliptic curves by the following proposition:

**Proposition 1.13** ([281, Proposition 1.3]). *Let  $C, D$  be two hyperelliptic curves of genus  $g$  over a field  $K$  with  $\text{char}(K) \neq 2$ . Then  $C$  is isomorphic to  $D$  over  $\overline{K}$  if and only if there exists some  $\lambda \in \overline{K}^\times$  such that*

$$I_m(C) = \lambda^m I_m(D)$$

*for all positive  $m$ .*

Naively, it seems a priori that we would need to evaluate infinitely many

invariants  $I_m(C)$  and  $I_m(D)$  in order to determine whether two hyperelliptic curves  $C, D$  are  $\overline{K}$ -isomorphic via Proposition 1.13. However, in practice, one need only compute finitely many of the invariants  $I_m$  by a famous result of Gordan [197] and Hilbert [221] which states that the dimension of the space of such invariants is finite. Although we remark that an explicit basis for this space is known only for degrees  $n \leq 10$  (e.g. see [71, 70, 408, 31]).

### 1.5.1 Invariants for genus 2 curves

In our case, we shall be interested in the invariants characterising the  $\overline{K}$ -isomorphism classes for genus 2 curves. Let  $K$  be a field with  $\text{char}(K) \neq 2$ , and let  $C/K : y^2 = c(x - \alpha_1) \cdots (x - \alpha_6)$  be a genus 2 hyperelliptic curve. Using (1.18) for the degrees  $m \in \{2, 4, 6, 10\}$ , we can therefore explicitly define the following set of **Igusa-Clebsch invariants** [230, p. 620]:

$$\begin{aligned} I_2 &:= (4c)^2 \sum_{\sigma \in S_6/\sim} (\alpha_{\sigma(1)} - \alpha_{\sigma(2)})^2 (\alpha_{\sigma(3)} - \alpha_{\sigma(4)})^2 (\alpha_{\sigma(5)} - \alpha_{\sigma(6)})^2, \\ I_4 &:= (4c)^4 \sum_{\sigma \in S_6/\sim} \left( (\alpha_{\sigma(1)} - \alpha_{\sigma(2)})^2 (\alpha_{\sigma(2)} - \alpha_{\sigma(3)})^2 (\alpha_{\sigma(3)} - \alpha_{\sigma(1)})^2 (\alpha_{\sigma(4)} - \alpha_{\sigma(5)})^2 \right. \\ &\quad \cdot (\alpha_{\sigma(5)} - \alpha_{\sigma(6)})^2 (\alpha_{\sigma(6)} - \alpha_{\sigma(4)})^2 \Big), \\ I_6 &:= (4c)^6 \sum_{\sigma \in S_6/\sim} \left( (\alpha_{\sigma(1)} - \alpha_{\sigma(2)})^2 (\alpha_{\sigma(2)} - \alpha_{\sigma(3)})^2 (\alpha_{\sigma(3)} - \alpha_{\sigma(1)})^2 (\alpha_{\sigma(4)} - \alpha_{\sigma(5)})^2 \right. \\ &\quad \cdot (\alpha_{\sigma(5)} - \alpha_{\sigma(6)})^2 (\alpha_{\sigma(6)} - \alpha_{\sigma(4)})^2 (\alpha_{\sigma(1)} - \alpha_{\sigma(4)})^2 (\alpha_{\sigma(2)} - \alpha_{\sigma(5)})^2 \\ &\quad \cdot (\alpha_{\sigma(3)} - \alpha_{\sigma(6)})^2 \Big), \\ I_{10} &:= (4c)^{10} \prod_{1 \leq i < j \leq 6} (\alpha_i - \alpha_j)^2, \end{aligned}$$

where, as stated before, each sum and product runs over the permutations  $\sigma$  of  $\{1, \dots, 6\}$  which yield distinct expressions. By the previous discussion, the weighted projective element  $(I_2 : I_4 : I_6 : I_{10}) \in \mathbb{P}_{2,4,6,10}^3$  is invariant under  $\overline{K}$ -isomorphisms, and in particular uniquely determines the  $\overline{K}$ -isomorphism class of  $C$ ; see Clebsch [103].

To work in addition to the case where  $\text{char}(K) = 2$ , we can furthermore define the **Igusa invariants** [230, p. 621-622] (or  $J$ -invariants), as follows:

$$J_2 := I_2/8,$$

$$\begin{aligned}
J_4 &:= (4J_2^2 - I_4)/96, \\
J_6 &:= (8J_2^3 - 160J_2J_4 - I_6)/576, \\
J_8 &:= (J_2J_6 - J_4^2)/4, \\
J_{10} &:= I_{10}/4096,
\end{aligned}$$

whereby it can similarly be proven that, for any two genus 2 curves  $C/K$  and  $D/K$ , then  $C$  is isomorphic to  $D$  over  $\overline{K}$  if and only if there exists some  $\lambda \in \overline{K}^\times$  such that  $J_m(C) = \lambda^m J_m(D)$  for all  $m \in \{2, 4, 6, 8, 10\}$ .

One advantage of the Igusa invariants is that we can read off when a curve  $C$  has potential good reduction at any prime  $p$  (including at  $p = 2$ ).

**Theorem 1.14.** [284, Theorem 1] *Let  $C/\mathbb{Q}$  be a smooth genus 2 curve with Igusa invariants  $(J_2, J_4, J_6, J_8, J_{10})$  defined above. Then  $C$  has potential good reduction at a prime  $p$  if and only if  $J_{2i}^5/J_{10}^i \in \mathbb{Z}_p$  for all  $i = 1, \dots, 5$ .*

To give a simpler description of the  $\overline{K}$ -isomorphism classes of genus 2 curves, we also consider the **G2 invariants**, defined by Cardona–Quer–Nart–Pujolàs [94, 95], defined in terms of the Igusa invariants  $J_i$ , as follows:

$$(g_1, g_2, g_3) = \begin{cases} (J_2^5/J_{10}, J_2^3J_4/J_{10}, J_2^2J_6/J_{10}), & \text{if } J_2 \neq 0, \\ (0, J_4^5/J_{10}^2, J_4J_6/J_{10}) & \text{if } J_2 = 0, J_4 \neq 0, \\ (0, 0, J_6^5/J_{10}^3), & \text{otherwise.} \end{cases} \quad (1.19)$$

This time, we have that two genus 2 curves  $C, D$  are  $\overline{K}$ -isomorphic if and only if their G2-invariants are the same. We also remark that Theorem 1.14 implies that if any prime  $p$  divides any of the denominators of  $g_1, g_2, g_3$ , then  $C$  will not have potentially good reduction at  $p$  (however, the converse is not true).

For completeness, we note that a set of explicit formulae for the Igusa–Clebsch invariants  $I_2, I_4, I_6$  and  $I_{10}$  in terms of  $\lambda_1, \lambda_2, \lambda_3$  for a genus 2 curve  $C/K$  in Rosenhain normal form  $C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$  is given in the appendix of Malmendier–Shaska [298, p. 303–304].

## 1.6 $L$ -functions

One of the most important isogeny invariants of abelian varieties  $A/K$  is its  $L$ -function  $L(A/K, s)$ .

**Definition 1.20** ( $L$ -function of an abelian variety [247]). Let  $A$  be an abelian variety over some number field  $K$ . The  $L$ -function of  $A/K$  is given by the following Euler

product:

$$L(A/K, s) := \prod_{\mathfrak{p} \in \mathcal{O}_K} L_{\mathfrak{p}}(N(\mathfrak{p})^{-s})^{-1}$$

where  $N(\mathfrak{p})$  denotes the norm (over  $\mathbb{Q}$ ) of  $\mathfrak{p}$ , and where the product is taken over all prime ideals  $\mathfrak{p}$  of  $\mathcal{O}_K$  (or equivalently finite places of  $K$ ).

Each of the local Euler factors  $L_{\mathfrak{p}}(T)$  essentially depends on the reduction type of  $A$  at  $\mathfrak{p}$ . It can be defined generally in terms of the geometric Frobenius in a decomposition group at  $\mathfrak{p}$ , as follows: [63] Let  $D_{\mathfrak{p}} \subset \text{Gal}(\overline{K}/K)$  be a decomposition group at  $\mathfrak{p}$ , and let  $I_{\mathfrak{p}} \subset D_{\mathfrak{p}}$  denote the inertia group at  $\mathfrak{p}$ . We pick an arithmetic Frobenius element  $\sigma_{\mathfrak{p}} \in D_{\mathfrak{p}}$  (i.e.  $\sigma_{\mathfrak{p}}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{p}}$ ).

Then we define the local Euler factor  $L_{\mathfrak{p}}(T)$  at  $\mathfrak{p}$  as

$$L_{\mathfrak{p}}(T) := \det(1 - T\sigma_{\mathfrak{p}}^{-1} | V^{I_{\mathfrak{p}}})$$

where  $V := H_{\text{ét}}^1(A \otimes_K \overline{K}, \mathbb{Q}_{\ell})$  is the first étale cohomology group of  $A$ , for some prime  $\ell$  different from the residue characteristic of  $\mathfrak{p}$ .<sup>19</sup> It's known that  $L(A/K, s)$  converges on  $\text{Re}(s) > \frac{3}{2}$  and that each of the local Euler factors  $L_{\mathfrak{p}}(T)$  is a polynomial with integer coefficients and is independent from the choice of  $\ell$  [318, Theorem 19.1].

Given that we have the isomorphism  $H_{\text{ét}}^1(C \otimes_K \overline{K}, \mathbb{Q}_{\ell}) \cong H_{\text{ét}}^1(\text{Jac}(C) \otimes_K \overline{K}, \mathbb{Q}_{\ell})$ , we can define the  $L$ -function of a smooth projective curve  $C/K$  simply as the  $L$ -function of its Jacobian, i.e.  $L(C/K, s) := L(\text{Jac}(C)/K, s)$ . Note that by Faltings isogeny theorem [164], two abelian varieties  $A/K$  and  $B/K$  are  $K$ -isogenous if and only if  $L(A/K, s) = L(B/K, s)$ .

In order to do full justice to a section on  $L$ -functions, we must mention one of the most notable conjectures on the subject: the Birch and Swinnerton-Dyer conjecture. First conjectured for elliptic curves in [46], this was generalised by Tate [442] to abelian varieties, and quite miraculously predicts how global information about  $A/K$  can be read off from  $L(A/K, s)$ !

**Conjecture** (Birch–Swinnerton-Dyer). [206, p. 224] *Let  $A$  be a dimension  $d$  abelian variety over a number field  $K$  of discriminant  $\Delta_K$ , and assume that  $L(A/K, s)$  has an analytic continuation to  $\mathbb{C}$ . Then*

- (i) (Weak BSD) *The order of vanishing  $r$  of  $L(A/K, s)$  at  $s = 1$  is equal to the rank of  $A/K$ .*

---

<sup>19</sup>We note the Galois equivariant isomorphism  $H_{\text{ét}}^1(A \otimes_K \overline{K}, \mathbb{Q}_{\ell}) \cong V_{\ell}(A)^{\vee}$ , hence some authors choose to replace  $H_{\text{ét}}^1(A \otimes_K \overline{K}, \mathbb{Q}_{\ell})$  in the definition with  $V_{\ell}(A)^{\vee}$ , i.e. the dual of  $T_{\ell}(A) \otimes_{\mathbb{Z}_{\ell}} \mathbb{Q}_{\ell}$ , where  $T_{\ell}(A)$  is the  $\ell$ -adic Tate module of  $A$  (e.g. see Commelin [115, p. 13] or Morgan [321, p. 4]).

(ii) (Strong BSD) Let  $\text{III}_{A/K}$  be the Tate-Shafarevich group of  $A/K$ . Then  $\text{III}_{A/K}$  is finite and

$$\lim_{s \rightarrow 1} \frac{L(A/K, s)}{(s-1)^r} = \frac{\Omega_{A/K} \cdot |\text{III}_{A/K}| \cdot R_{A/K} \cdot \prod_{\mathfrak{p}} c_{\mathfrak{p}}}{|A(K)_{\text{tors}}| \cdot |\widehat{A}(K)_{\text{tors}}| \cdot |\Delta_K|^{d/2}},$$

where  $\widehat{A}$  is the dual of  $A$ ,  $A(K)_{\text{tors}}$  (resp.  $\widehat{A}(K)_{\text{tors}}$ ) is the torsion subgroup of  $A(K)$  (resp.  $\widehat{A}(K)$ ),  $R_{A/K}$  is the regulator,  $\Omega_{A/K}$  is the product of its real and complex periods, and  $c_{\mathfrak{p}}$  is the Tamagawa number of  $A$  at  $\mathfrak{p}$ .

Whilst the BSD conjecture has been proven in some cases (e.g. for elliptic curves  $E/\mathbb{Q}$  of analytic rank at most 1 [269], and certain abelian surfaces of analytic rank 0 [293]), this is still a highly open problem in general!<sup>20</sup>

### 1.6.1 Primes $\mathfrak{p}$ of good reduction for $C$

Whilst Definition 1.20 gives a fully general definition of the local Euler factors for any prime  $\mathfrak{p}$ , it's not as easy to explicitly compute  $L_{\mathfrak{p}}(T)$  directly from the definition.

Indeed, if  $\mathfrak{p}$  is a prime of good reduction for a genus  $g$  curve  $C/K$ , then we can compute  $L_{\mathfrak{p}}(T)$  in a simpler way than given above. Here, the local Euler factor  $L_{\mathfrak{p}}(T)$  is simply given by the zeta function:

$$L_{\mathfrak{p}}(T) = Z_{\mathfrak{p}}(T)(1-T)(1-N(\mathfrak{p})T) \quad (1.21)$$

In order to define  $Z_{\mathfrak{p}}(T)$ , we let  $\#C(\mathbb{F}_{\mathfrak{p}^k})$  denote the number of points in the reduction of  $C$  to the residue field  $\mathbb{F}_{\mathfrak{p}^k}$ , where  $\mathbb{F}_{\mathfrak{p}^k}$  is a finite degree  $k$  extension of  $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$ . We can then give  $Z_{\mathfrak{p}}(T)$  as

$$Z_{\mathfrak{p}}(T) = \exp \left( \sum_{k=1}^{\infty} \frac{\#C(\mathbb{F}_{\mathfrak{p}^k})}{k} T^k \right)$$

where the above is interpreted as a formal power series with coefficients in  $\mathbb{Q}$ . Whilst it might seem that we need to evaluate  $\#C(\mathbb{F}_{\mathfrak{p}^k})$  for infinitely many  $k$  to evaluate  $L_{\mathfrak{p}}(T)$ , it has been shown by Weil [477] that  $Z_{\mathfrak{p}}(T)$  is a rational function and that  $L_{\mathfrak{p}}(T)$  is a degree  $2g$  polynomial. If we let  $L_{\mathfrak{p}}(T) = \prod_{i=1}^{2g} (1 - \alpha_i T)$  for some  $\alpha_i \in \mathbb{C}$ ,

<sup>20</sup>At this point, it also seems customary nowadays that any text introducing the BSD conjecture also gives the following quote from John Tate in 1974: “*This remarkable conjecture relates the behavior of a function  $L$  at a point where it is not at present known to be defined to the order of a group  $\text{III}$  which is not known to be finite!*” [443, p. 198]. We do remark that  $L(E/\mathbb{Q}, s)$  has been proven to be defined at  $s = 1$  for elliptic curves  $E/\mathbb{Q}$ , although the finiteness of  $\text{III}$  is still an open problem in general.

then we can evaluate  $L_{\mathfrak{p}}(T)$  by taking logarithms of (1.21) and subsequently using the power series for log, to obtain

$$\#C(\mathbb{F}_{\mathfrak{p}^k}) = N(\mathfrak{p})^k + 1 - \sum_{i=1}^{2g} \alpha_i^k \quad (1.22)$$

for all positive  $k$  [110, p. 135]. Therefore, by utilising Newton's relations between the roots and coefficients of  $L_{\mathfrak{p}}(T)$ , we can calculate any good Euler factor by simply counting points on  $C(\mathbb{F}_{\mathfrak{p}^k})$  for  $k = 1, \dots, g$ .

It's worth also mentioning that an alternative method to computing  $L_{\mathfrak{p}}(T)$  for hyperelliptic curves directly from  $\text{Jac}(C)$  if  $g \leq 3$  involves first calculating  $\#\text{Jac}(C)(\mathbb{F}_{\mathfrak{p}}) = L_{\mathfrak{p}}(1)$ , and  $\#\text{Jac}(\tilde{C})(\mathbb{F}_{\mathfrak{p}}) = L_{\mathfrak{p}}(-1)$ , where  $\tilde{C}$  denotes a non-isomorphic quadratic twist of  $C \bmod \mathfrak{p}$ .<sup>21</sup> We can then use Lemma 4 from [433] to compute  $L_{\mathfrak{p}}(T)$  for sufficiently large  $\mathfrak{p}$ . Kedlaya and Sutherland [256] gives a nice overview of computing  $L$ -functions of hyperelliptic curves in the genus  $g \leq 3$  case.

### 1.6.2 Primes $\mathfrak{p}$ of bad reduction for $C$

If  $\mathfrak{p}$  is a prime of bad reduction of  $C$ , then it's usually not as simple to calculate the Euler factor  $L_{\mathfrak{p}}(T)$ . In general, the standard way to compute such Euler factors is to construct a regular model for  $C$  at  $\mathfrak{p}$ , which is the default implementation given in Magma [58]. Bouw and Wewers [63] give an alternate way to compute  $L_{\mathfrak{p}}(T)$  by computing the semistable reduction of  $C$  at  $\mathfrak{p}$ .

For most of our curves, particularly for even primes  $\mathfrak{p}$ , usually the simplest and quickest way to compute such Euler factors is to just make a guess for the local factor  $L_{\mathfrak{p}}(T)$ , and then verify whether the  $L$ -function  $L(C/K, s)$  satisfies its conjectural Hasse-Weil functional equation, given in (1.24). As for each  $\mathfrak{p}$ , there are only finitely many possible bad Euler factors  $L_{\mathfrak{p}}(T)$ , and only finitely many primes  $\mathfrak{p}$  of bad reduction, this yields an effective procedure to heuristically calculate both the conductor  $N$  and all the Euler factors  $L_{\mathfrak{p}}(T)$  at all primes.

Finally, we should remark that some recent results of Maistret and Sutherland [297] uses cluster pictures to give a fast approach to compute Euler factors  $L_{\mathfrak{p}}(T)$  for primes  $\mathfrak{p}$  where  $C$  has bad reduction, but where  $\text{Jac}(C)$  has good reduction.

---

<sup>21</sup>Given a hyperelliptic curve  $C : y^2 = f(x)$ , the unique non-isomorphic quadratic twist can be given by  $\tilde{C} : \alpha y^2 = f(x)$  where  $\alpha \in \mathbb{F}_{\mathfrak{p}}$  is any quadratic non-residue.

### 1.6.3 Genus 2 case

To make some computations explicit, let's consider the genus 2 case: Let  $C/K$  be a genus 2 curve with good reduction at  $\mathfrak{p}$ . We define the trace at  $\mathfrak{p}$  as  $a_{\mathfrak{p}} := N(\mathfrak{p}) + 1 - \#C(\mathbb{F}_{\mathfrak{p}})$ , and similarly define  $a_{\mathfrak{p}^2} := N(\mathfrak{p})^2 + 1 - \#C(\mathbb{F}_{\mathfrak{p}^2})$ .

Now, by using (1.22) and Newton relations between the roots and coefficients of  $L_{\mathfrak{p}}(T)$ , we obtain the following formula for all good Euler factors

$$L_{\mathfrak{p}}(T) = 1 - a_{\mathfrak{p}}T + (a_{\mathfrak{p}}^2 - a_{\mathfrak{p}^2})T^2 - a_{\mathfrak{p}}N(\mathfrak{p})T^3 + N(\mathfrak{p})^2T^4. \quad (1.23)$$

For primes  $\mathfrak{p}$  of bad reduction for  $\text{Jac}(C)$ , we can simply make a guess of the Euler factor  $L_{\mathfrak{p}}(T)$ , which we know will be of the form

$$L_{\mathfrak{p}}(T) = 1 + A_1T + A_2T^2 + A_3T^3$$

for some  $A_i \in \mathbb{Z}$ . Now, using that the roots of  $L_{\mathfrak{p}}(T)$  must have absolute value  $N(\mathfrak{p})^{k/2}$  for some  $k \in \{-1, 0, 1, 2\}$  (e.g. see [166, p. 366]), this yields a bound on the coefficients  $A_i$ ; namely that  $|A_1| \leq 3\sqrt{N(\mathfrak{p})}$ ,  $|A_2| \leq 6N(\mathfrak{p})$ , and  $|A_3| \leq 4N(\mathfrak{p})^{3/2}$ . This therefore implies there are only finitely many possible bad Euler factors to check. For example, if  $C/\mathbb{Q}$  is a genus 2 curve whose Jacobian has bad reduction at  $p = 2$ , then there are only at most 27 possible bad Euler factors for  $L_2(T)$ , given below:

$$\begin{aligned} &1, 1 - T, 1 + T, 1 - 2T^2, (1 - T)(1 + T), (1 - T)^2, 1 - T + T^2, 1 + T^2, \\ &1 + T + T^2, (1 + T)^2, 1 - 2T + 2T^2, 1 - T + 2T^2, 1 + 2T^2, 1 + T + 2T^2, \\ &1 + 2T + 2T^2, (1 + T)(1 - 2T^2), (1 - T)(1 + 2T + 2T^2), (1 - T)(1 + T + 2T^2), \\ &(1 - T)(1 + 2T^2), (1 - T)(1 - T + 2T^2), (1 - T)(1 - 2T + 2T^2), \\ &(1 - T)(1 - 2T^2), (1 + T)(1 - 2T + 2T^2), (1 + T)(1 - T + 2T^2), \\ &(1 + T)(1 + 2T^2), (1 + T)(1 + T + 2T^2), (1 + T)(1 + 2T + 2T^2). \end{aligned}$$

## 1.7 Modularity results and conjectures

We'll conclude our introduction by giving a very brief overview on what has been proven regarding the modularity of abelian varieties. One primary motivation for proving such results is that it allows us to classify abelian varieties  $A/K$  with good reduction outside  $S$  by computing suitable modular forms (or more generally automorphic forms) of level  $N$ , for finitely many  $N$ .

Another motivation for these modularity results is to prove the Hasse-Weil



conjecture [218, 478] for a wide family of abelian varieties:

**Conjecture 1.15** (Hasse-Weil conjecture). *Let  $K$  be a number field of conductor  $\mathfrak{f}_K$  and discriminant  $\Delta_K$ . Let  $A/K$  be an abelian variety of dimension  $d$ . Then  $L(A/K, s)$  has an analytic continuation to all of  $\mathbb{C}$  and the completed  $L$ -function (e.g. see [56, p. 396])*

$$\Lambda(A/K, s) := (N(\mathfrak{f}_K) \Delta_K^{2d})^{s/2} ((2\pi)^{-s} \Gamma(s))^{d[K:\mathbb{Q}]} L(A/K, s) \quad (1.24)$$

satisfies the functional equation

$$\Lambda(A/K, s) = w_{A/K} \cdot \Lambda(A/K, 2 - s)$$

where  $w_{A/K} \in \{-1, +1\}$  is the global root number of  $A/K$ .

Whilst the case of dimension  $d = 0$  was proven classically by Riemann [365] (equivalent to proving the functional equation for the usual zeta function  $\zeta_{\mathbb{Q}}(s)$ ), proving this conjecture for higher dimensions is far more challenging! Usually, the main strategy involves establishing some modularity (or potential modularity) result, which we give a very brief discussion of below.

### 1.7.1 Elliptic curves

Thorne [447] has given an excellent recent survey on the modularity of elliptic curves, although we'll present a short summary here of what's been proven to date. In the 1950s, Taniyama first proposed some problems which suggested connections between rational elliptic curves  $E/\mathbb{Q}$  and modular forms, with a more precise conjecture formulated by Shimura. Weil [479] then provided further evidence for this conjecture in the 1960s. Thus the conjecture that all rational elliptic curves are modular became known as the Taniyama-Shimura-Weil conjecture for the latter half of the 20th century.<sup>22</sup> This was eventually proven for semistable elliptic curves by Wiles [482] and Taylor–Wiles [445] and finally for all elliptic curves  $E/\mathbb{Q}$  by Breuil–Conrad–Diamond–Taylor [68].

**Theorem 1.16** (Modularity for elliptic curves  $E/\mathbb{Q}$  [444, 445, 68]). *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  of conductor  $N$ . Then there exists a cusp form  $f \in S_2(\Gamma_0(N))$  such that  $L(E, s) = L(f, s)$ .*

---

<sup>22</sup>An excellent summary of the history of the Taniyama-Shimura-Weil conjecture is given by Lang [275].

There are various equivalent statements of this theorem. This theorem is equivalent to the statement that the associated Galois representation  $\rho_{E,p} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Q}_p)$  for a suitable prime  $p$ , is isomorphic to the Galois representation  $\rho_f$  associated to a cusp form  $f \in S_2(\Gamma_0(N))$ , as defined by Eichler and Shimura [137], or that there exists a nonconstant morphism from  $X_0(N) \rightarrow E$  (see Carayol [92] for proofs of their equivalence). The modularity of elliptic curves over  $\mathbb{Q}$  (together with a theorem of Ribet [363]) was most famously used to prove Fermat's Last Theorem; a problem which requires no introduction given the immense wealth of literature on the topic [7, 129, 154, 267, 362, 416, 426]!

As modularity relates the  $L$ -function  $L(E, s)$  of an elliptic curve  $E/\mathbb{Q}$  to that of a weight 2 cusp form  $f \in S_2(\Gamma_0(N))$ , this therefore implies the Hasse-Weil conjecture for  $E/\mathbb{Q}$ .

Proving analogous modularity theorems for elliptic curves over arbitrary number fields  $F$  is still a very open problem. Generally speaking, we say that an elliptic curve  $E$  over some number field  $F$  is *modular* either if  $E$  has complex multiplication (CM) or if there exists some regular algebraic automorphic representation  $\pi$  of  $\text{GL}_2(\mathbb{A}_F)$  whose  $L$ -function coincides with  $L(E/F, s)$  (e.g. see [91, p. 2]). However giving an explicit description of such a  $\pi$  is far from trivial for arbitrary number fields  $F$ , indeed for most non totally-real number fields  $F$ , we don't even have an adequate construction for attaching an elliptic curve  $E/F$  to modular forms for  $F$ !

In the case of totally real fields  $K$ , we have the following conjectured correspondence between  $E/K$  and Hilbert newforms.

**Conjecture.** *Let  $E$  be an elliptic curve over a totally real number field  $K$  of conductor  $\mathcal{N}$ . Then there exists a Hilbert newform  $f$  of parallel weight 2 and level  $\mathcal{N}$  such that  $L(E, s) = L(f, s)$*

Whilst this conjecture is still open in general for all totally real number fields  $K$ , it has been proven in many particular cases, starting with the case of semistable elliptic curves over  $\mathbb{Q}(\sqrt{2})$  and  $\mathbb{Q}(\sqrt{17})$  being done by Jarvis and Manoharmayum [235]. Subsequently, modularity for all elliptic curves over real quadratic fields was proven by Freitas, Le Hung, and Siksek [185], for totally real cubic fields by Derickx, Najman, and Siksek [136], for certain totally real quartic fields by Box [64], and for all but finitely many totally real quintic fields by Ishitsuka, Ito, and Yoshikawa [234]. Thorne [446] also proved modularity for elliptic curves over  $\mathbb{Z}_p$ -cyclotomic extensions of  $\mathbb{Q}$ .

Often if one cannot prove modularity, it's easier to prove potential modularity, originally proven by Taylor for all elliptic curves  $E$  over totally real fields  $K$ .

**Theorem** (Potential modularity of elliptic curves). [444] *Let  $E$  be an elliptic curve over a totally real number field  $K$ . Then  $E/K$  is potentially modular, i.e. there exists a finite extension  $L/K$  of number fields such that  $E/L$  is modular. In particular  $L(E/K, s)$  has meromorphic continuation to  $\mathbb{C}$  and satisfies its conjectured functional equation given by the Hasse-Weil conjecture.*

Buzzard [86] gives an excellent survey on some of the main ideas behind proving (potential) modularity. Recently, potential modularity has also been proven for elliptic curves over all CM fields [9], and arbitrary quadratic extensions of totally real fields [66].

Establishing modularity for elliptic curves over fields which are not totally real has been far more challenging. For elliptic curves  $E$  over imaginary quadratic fields  $K$ , it is conjectured that  $L(E/K, s) = L(f, s)$  for some Bianchi modular form  $f$ . We should mention some early computations by Cremona [121, 122] investigating such correspondences between elliptic curves and Bianchi modular forms.

Nonetheless, significant progress has been made recently, with Allan, Khare, Thorne [10] have proven that a positive proportion of elliptic curves over certain CM fields are modular, Very recently, Caraiani and Newton have established modularity (under some technical assumptions) for elliptic curves over imaginary quadratic fields [91], and Whitmore [481] proving modularity for a positive proportion of elliptic curves over arbitrary quadratic extensions of totally real fields.

### 1.7.2 Higher dimensions

For abelian varieties  $A/K$  of higher dimensions, giving a modularity statement is somewhat more non-trivial, where stating an explicit modularity conjecture depends heavily on the dimension of  $A$ , the number field  $K$ , and the structure of the endomorphism ring  $\text{End}_K(A)$ .

For abelian varieties over  $\mathbb{Q}$  of  $\text{GL}_2$ -type (i.e. where  $\text{End}_{\mathbb{Q}}(A)$  is a number field of degree  $\dim(A)$ ), Ribet [364] showed that Serre's modularity conjecture [395] would imply that all such abelian varieties of  $\text{GL}_2$ -type occur as a quotient of  $J_1(N)$  for some  $N$ . This has since been proven by Khare, Wintenberger, and Kisin [257, 258, 266], thus proving Ribet's result unconditionally. In particular, for atypical abelian surfaces  $A/\mathbb{Q}$  of  $\text{GL}_2$ -type, one can relate their  $L$ -function to those of classical, Hilbert, or Bianchi modular forms [53].

For abelian varieties not of  $\text{GL}_2$ -type, far less is known. Yoshida [486] first conjectured that for any abelian surface  $A/\mathbb{Q}$ , there exists a weight 2 Siegel modular form  $f$  such that  $L(A, s) = L(f, s)$ .

This conjecture was made precise by Brumer and Kramer, proposing an explicit 1-to-1 correspondence between isogeny classes of abelian surfaces  $A/\mathbb{Q}$  with  $\text{End}_{\mathbb{Q}}(A) = \mathbb{Z}$  and suitable paramodular newforms. By defining a suitable paramodular group  $K(N) \subset \text{Sp}_4(\mathbb{Q})$  of level  $N$ , we denote  $S_2^{(2)}(K(N))$  as the space of weight 2 degree 2 Siegel modular cusp forms with respect to  $K(N)$ . Gritsenko [203, 204] gave a map  $\text{Grit} : J_{2,N}^{\text{cusp}} \rightarrow S_2^{(2)}(K(N))$  which constructs level  $N$  paramodular forms from Jacobi forms of level  $N$ . Such forms are excluded from the conjecture by Brumer–Kramer. Brumer–Kramer then define a *nonlift weight two paramodular cuspidal newform*  $f \in S_2^{(2)}(\Gamma^{\text{para}}(N))$  as an element of  $S_2^{(2)}(K(N))$  which is perpendicular to the space of Gritsenko lifts  $\text{Grit}(J_{2,N}^{\text{cusp}})$ .

**Conjecture** (Paramodular conjecture). [79] *Let  $A$  be an abelian surface over  $\mathbb{Q}$  of conductor  $N$  such that  $\text{End}_{\mathbb{Q}} A = \mathbb{Z}$ . Then there exists a cuspidal nonlift Siegel paramodular newform  $f \in S_2^{(2)}(\Gamma^{\text{para}}(N))$  of degree 2 and weight 2, such that  $L(A, s) = L(f, s, \text{spin})$ .*

Brumer and Kramer further conjecture (including a correction from Calegari [89]) that the union of all isogeny classes of abelian surfaces  $A/\mathbb{Q}$  of conductor  $N$  with  $\text{End}_{\mathbb{Q}} A = \mathbb{Z}$  and all QM abelian fourfolds  $B/\mathbb{Q}$  of conductor  $N^2$ , are in bijection with the set of suitable paramodular forms of level  $N$  (up to scaling) [81].

Strong evidence for this conjecture was shown by Poor, Shurman, and Yuen [357, 355, 356] and Brumer–Kramer [79] who explicitly computed the dimension of the space  $S_2^{(2)}(\Gamma^{\text{para}}(N))$  for small levels  $N$ . However a provably complete list of paramodular forms of level  $N$  is only known for  $N \leq 353$ ; indeed, the set  $S_2^{(2)}(\Gamma^{\text{para}}(N))$  is trivial for all  $N \leq 353$  unless  $N$  is 249, 277, 295, 349, or 353. Some recent tables of Poor and Yuen [358] give a heuristic computation of the dimension of level  $N$  paramodular newforms  $S_2^{(2)}(\Gamma^{\text{para}}(N))$  for  $N \leq 1000$  (which include computations from [356, 205, 434]).

Proving the paramodular conjecture would provide one method to effectively classify abelian surfaces of small conductor  $N$ ; indeed we should mention the following provisional result by Booker and Sutherland [55]:

**Theorem** (Booker–Sutherland WIP [55]). *Assume the paramodular conjecture. Then there are 456  $L$ -functions of abelian surfaces  $A/\mathbb{Q}$  with conductor  $N \leq 1000$ .*

The main theorem which will be the most useful to us in Chapter 5 is the proof by Boxer, Calegari, Gee, and Pilloni of potential modularity for abelian surfaces:

**Theorem.** [66] *Let  $A$  be an abelian surface over a totally real field  $K$ . Then  $A$  is potentially automorphic. In particular,  $L(A/K, s)$  has meromorphic continuation to  $\mathbb{C}$  and satisfies its conjectured functional equation given by the Hasse–Weil conjecture.*

Whilst proving the full modularity of all abelian surfaces  $A/\mathbb{Q}$  is still out of reach, we must briefly mention some very recent work by Boxer, Calegari, Gee, and Pilloni [67] proving the modularity of a positive proportion of abelian surfaces over  $\mathbb{Q}$ . In particular, their main theorem implies that any genus 2 curve  $C/\mathbb{Q}$  which contains a rational Weierstrass point, has maximal mod-3 Galois image, and has good ordinary reduction at the primes 2 and 3, is modular.

DRAFT

# Chapter 2

## Potential good reduction of hyperelliptic curves

In this chapter, we shall be interested in the reduction of hyperelliptic curves  $C/K$  with all of its Weierstrass points defined over  $K$ , and shall prove various results regarding the existence of infinitely many genus  $g$  hyperelliptic curves with potential good reduction outside a fixed number of primes in  $K$ . An earlier draft of this chapter is publicly available as a preprint [465] and is currently under review.

Compared to the preprint version, we have rewritten and adapted most of the introduction, have added Section 2.1.2 consisting of three new theorems (Theorems 2.10, 2.12, and 2.13), and added a new Corollary 2.21 to Section 2.3.

We first recall that a prime  $\mathfrak{p}$  in  $K$  is considered *odd* if it lies above an odd rational prime (or equivalently has odd absolute norm  $N_{K/\mathbb{Q}}(\mathfrak{p})$ ), and define  $\pi_{K,\text{odd}}(n)$  as the number of odd primes in  $K$  with norm no greater than  $n$ . We also define  $\mathcal{B}_{\text{odd}}(C/K)$  as the set of odd primes  $\mathfrak{p}$  in  $K$  for which a curve  $C/K$  does not have potential good reduction at  $\mathfrak{p}$ , sometimes denoted as primes of *geometric bad reduction*.

A summary of the main results of this chapter is the following:

**Theorem 2.1.** (*Theorem 2.14, Theorem 2.15*) *Let  $K$  be a number field, and let  $C/K$  be a genus  $g$  hyperelliptic curve  $C/K$  with all its Weierstrass points in  $K$ . Then  $\mathfrak{p} \in \mathcal{B}_{\text{odd}}(C/K)$  for all odd primes  $\mathfrak{p}$  satisfying  $N_{K/\mathbb{Q}}(\mathfrak{p}) < 2g$ . Furthermore, there are only finitely many  $\overline{K}$ -isomorphism classes of genus  $g$  hyperelliptic curves  $C/K$  with all Weierstrass points in  $K$  satisfying  $\#\mathcal{B}_{\text{odd}}(C/K) \leq \pi_{K,\text{odd}}(2g) + 1$ .*

This gives us the lower bound  $c_K(g) > \pi_{K,\text{odd}}(2g) + 1$ , where  $c_K(g)$  denotes the smallest positive integer such that there exist infinitely many  $\overline{K}$ -isomorphism

classes of genus  $g$  hyperelliptic curves  $C/K$  with all Weierstrass points in  $K$  having potentially good reduction outside  $c_K(g)$  primes in  $K$ . Applying Theorem 2.1 to  $K = \mathbb{Q}$  gives the following corollaries:

**Corollary 2.2.** (Corollary 2.19) *Let  $C/\mathbb{Q}$  be a genus  $g$  hyperelliptic curve with rational Weierstrass points. Then  $C$  cannot have potentially good reduction at any odd prime  $p \leq 2g$ .*

This allows us to prove the following extension of a theorem of Box and Le Fourn [65, Corollary 2]:

**Theorem 2.3.** (Corollary 2.20, Corollary 2.21) *There are no genus 2 hyperelliptic curves  $C/\mathbb{Q}$  with all rational Weierstrass points and with potential good reduction outside one prime. Furthermore, there are no genus 3 hyperelliptic curves  $C/\mathbb{Q}$  with all rational Weierstrass points and with potential good reduction outside two primes.*

Finally, in Section 2.4, we also prove the following various conditional and unconditional upper bounds for  $c_K(g)$ .

**Theorem 2.4.** (Theorem 2.22, Theorem 2.23, Theorem 2.24) *Let  $K$  be a number field of degree  $n$ . Then  $c_K(g) \leq (\frac{2}{\log 2} + o(1))ng \log g$  as  $g \rightarrow \infty$ . Furthermore, under the assumption of the Hardy-Littlewood prime  $k$ -tuples conjecture for  $K$ , we have  $c_K(g) \leq 2g - 1 + n\pi(2g)$ , and under the assumption of Schinzel's hypothesis H for  $K$ , we have moreover that*

$$c_K(g) \leq \sum_{\substack{1 \leq d < g, \text{ or} \\ d < 2g, d \text{ even}}} \frac{n}{[K(\zeta_d) : \mathbb{Q}(\zeta_d)]} + 1 + n\pi(2g).$$

Precise statements of the Hardy-Littlewood prime  $k$ -tuples conjecture and the Schinzel hypothesis H are provided in Section 2.4. This hence gives rise to the following corollaries:

**Corollary 2.5.** (Corollary 2.25, Corollary 2.26) *Let  $K$  be a number field of degree  $n$  with no non-trivial abelian subfields, and suppose that Schinzel's hypothesis H holds for  $K$ . Then if  $K$  is abelian (and hence of prime degree) with conductor  $\mathfrak{f}_K$ , then*

$$c_K(g) \leq \begin{cases} \frac{3}{2}g(1 + \frac{n-1}{\mathfrak{f}_K}) + 1 + n\pi(2g) & \text{if } \mathfrak{f}_K \text{ odd,} \\ \frac{3}{2}g(1 + \frac{4(n-1)}{3\mathfrak{f}_K}) + 1 + n\pi(2g) & \text{if } \mathfrak{f}_K \text{ even,} \end{cases}$$

*otherwise  $c_K(g) \leq \frac{3}{2}g + n\pi(2g)$  if  $K$  is non-abelian.*

## 2.1 Preliminaries

We'll begin by recalling a few standard results regarding the reduction of hyperelliptic curves. Whilst these results are certainly not new, they can be proven very easily using the machinery of cluster pictures. To illustrate the versatility of this approach, we'll provide brief proofs.

### 2.1.1 Potential good reduction for hyperelliptic curves $C$

**Proposition 2.6.** *Let  $K$  be a number field, and let  $C/K$  be a genus  $g$  hyperelliptic curve with Weierstrass points in  $K$ , given in Rosenhain normal form*

$$y^2 = cx(x-1)(x-\lambda_1)\dots(x-\lambda_{2g-1}), \quad c, \lambda_i \in K.$$

*Let  $\mathfrak{p}$  be an odd prime of  $K$ . Then  $C$  has potentially good reduction at  $\mathfrak{p}$  if and only if we have  $v_{\mathfrak{p}}(\lambda_i) = v_{\mathfrak{p}}(\lambda_i - 1) = 0$  for all  $i \in 1, \dots, 2g-1$ , and  $v_{\mathfrak{p}}(\lambda_i - \lambda_j) = 0$  for all distinct  $i, j \in \{1, \dots, 2g-1\}$ . (i.e. the values  $\lambda_i, \lambda_i - 1, \lambda_i - \lambda_j$  are all  $\mathfrak{p}$ -units)*

*Proof.* Let  $C/K$  be given in the above form, and let  $\mathcal{R}$  denote the Weierstrass points, i.e.  $\mathcal{R} := \{0, 1, \lambda_1, \dots, \lambda_{2g-1}\}$ . Then by Theorem 1.11, since  $|\mathcal{R}| = 2g+1$ , we have that  $C$  has potentially good reduction at  $\mathfrak{p}$  if and only if  $\Sigma_{\mathfrak{p}}$  is trivial.

Note that  $\Sigma_{\mathfrak{p}}$  is trivial if and only if  $v_{\mathfrak{p}}(r_i - r_j)$  is constant over all distinct pairs  $r_i, r_j \in \mathcal{R}$ . However, since  $v_{\mathfrak{p}}(1 - 0) = 0$ , this implies that  $v_{\mathfrak{p}}(\lambda_i) = v_{\mathfrak{p}}(\lambda_i - 1) = 0$  for all  $i$ , and that  $v_{\mathfrak{p}}(\lambda_i - \lambda_j) = 0$  for all  $i, j$ , which yields the result.  $\square$

This immediately implies the following corollary:

**Corollary 2.7.** *Let  $K$  be a number field, and let  $S$  be a finite set of primes of  $K$ , and assume that  $S$  contains all even primes of  $K$ . Let  $\mathcal{O}_S^{\times}$  denote the set of  $S$ -units in  $K$ . Then for a given hyperelliptic curve  $C/K$  of the above form,  $C$  has potentially good reduction outside  $S$  if and only if  $\lambda_i, \lambda_i - 1$  and  $\lambda_i - \lambda_j$  are in  $\mathcal{O}_S^{\times}$  for all  $i, j$ .*

This therefore gives us an effective procedure to list the Rosenhain normal forms of all hyperelliptic curves  $C$  over a given number field  $K$ , with potentially good reduction outside a finite set of primes  $S$ . It relies purely on (i) determining all number fields having bounded degree and discriminant, as well as (ii) solving  $S$ -unit equations over these fields:

1. Compute a list  $\mathcal{F}$  of all fields  $L/K$  which are unramified outside  $S$ , with degree  $d = [L : K]$  at most  $(2g+1)!$  as follows:



- (a) Use [330, p. 203] to show that any such field  $L/K$  must have discriminant  $\mathfrak{d}_{L/K}$  dividing the ideal  $\prod_{\mathfrak{p} \in S} \mathfrak{p}^{d(d+1)}$ . This yields a finite number of possible discriminants for  $L/K$ .
- (b) For each possible discriminant  $\mathfrak{d}_{L/K}$ , perform a Hunter search [109, p. 445] to compute all possible number fields  $L/K$  with degree  $d$  and discriminant  $\mathfrak{d}_{L/K}$ .

2. For each field  $L$  in  $\mathcal{F}$ , do the following:

- (a) Enumerate all solutions  $(\lambda_1, \dots, \lambda_{2g+1})$  to the  $2g-1$   $S$ -unit equations:

$$\lambda_1 + \mu_1 = 1, \quad \dots, \quad \lambda_{2g-1} + \mu_{2g+1} = 1, \quad \lambda_i, \mu_i \in \mathcal{O}_{L,S}^\times$$

such that  $\lambda_i - \lambda_j \in \mathcal{O}_{L,S}^\times$  for all  $i, j \in \{1, \dots, 2g-1\}$ .

- (b) For each solution  $(\lambda_1, \dots, \lambda_{2g+1})$ , construct the curve  $C/L$  of the form  $C : y^2 = x(x-1)(x-\lambda_1) \dots (x-\lambda_{2g-1})$ .<sup>1</sup>

This therefore gives an effective procedure to find all possible Rosenhain normal forms of hyperelliptic curves, and thus all possible  $\overline{K}$ -isomorphism classes. Given that there are only finitely many solutions to any given  $S$ -unit equation (see e.g. [161, p. 61]), this gives the following corollary:

**Corollary 2.8.** *For a given number field  $K$ , finite set of primes  $S$ , and genus  $g \geq 2$ , there are only finitely many  $\overline{K}$ -isomorphism classes of hyperelliptic curves  $C/K$  of genus  $g$  with potentially good reduction outside  $S$ . Moreover, these curves can be effectively computed, as given in the above algorithm.*

To translate these  $\overline{K}$ -isomorphism classes into a complete list of  $K$ -isomorphism classes, we can use the following identities of Evertse-Györy and Smart relating the cross-ratios  $\lambda_i$  to the roots  $\alpha_i$ .

Recall that, if  $y^2 = c(x-\alpha_1) \dots (x-\alpha_{2g+1})$ , then  $\lambda_i = (\alpha_{i+2} - \alpha_1)/(\alpha_2 - \alpha_1)$ . One can recover the roots  $\alpha_1, \dots, \alpha_{2g+1}$  from the cross-ratios  $\lambda_i$  via the identity

$$(\alpha_i - \alpha_j)^{2(g+1)(2g+1)} = \Delta \left( \prod_{1 \leq k < \ell \leq n} \frac{\lambda_i - \lambda_j}{\lambda_k - \lambda_\ell} \right)^2 \quad (2.1)$$

<sup>1</sup>We note that not all such curves  $C/L$  have a model over  $K$ . An obvious necessary condition is that  $C^\sigma$  is  $L$ -isomorphic to  $C$  for all  $\sigma \in \text{Gal}(L/K)$ , however this is not a sufficient condition in general, as noted by Shimura [407, Theorem 3]. See Mestre [317] for a necessary and sufficient criterion for genus 2 curves  $C/K$ .

where  $\Delta$  is the discriminant of  $C/K$  [162, p. 82]. Since  $\Delta$  can be effectively bounded (e.g. see [402, Lemma 2]), this gives finitely many possible values of  $\alpha_i - \alpha_j$  for each pair  $i, j$ .

Similarly, if  $\deg(f) = 2g + 2$ , then we have  $\lambda_i = (\alpha_3 - \alpha_2)(\alpha_{i+3} - \alpha_1)/((\alpha_2 - \alpha_1)(\alpha_3 - \alpha_{i+3}))$ . Again one can recover the roots  $\alpha_1, \dots, \alpha_{2g+2}$  from the expression

$$(\alpha_i - \alpha_j)^{2g(2g+1)} = \pm \frac{(\Omega_i \Omega_j)^{2g+1}}{\Omega_1 \Omega_2 \cdots \Omega_{2g+2}} \prod_{\substack{1 \leq k < \ell \leq n \\ k \neq i, \ell \neq j}} \frac{(\lambda_i - \lambda_j)(\lambda_k - \lambda_\ell)}{(\lambda_i - \lambda_k)(\lambda_j - \lambda_\ell)} \quad (2.2)$$

where  $\Omega_i := \prod_{i \neq k} (\alpha_i - \alpha_k)$  [418, p. 276]. As with the discriminant  $\Delta$ , one can also show that  $\Omega_i$  arise from an effectively computable finite set, as we will prove in Lemma 5.9 in Chapter 5. Thus, we have that the pairs  $\alpha_i - \alpha_j$  arise from an effectively computable finite set.

Finally, note that shifting  $x \mapsto x + \beta$  for some  $\beta \in \mathcal{O}_K$  changes  $\alpha_1 + \cdots + \alpha_n$  by  $n\beta$ . Thus, we can further assume that  $\alpha_1 + \cdots + \alpha_n$  arise from an effectively computable set  $\mathcal{O}_K/n\mathcal{O}_K$ . Finally, one can uniquely recover the roots  $\alpha_1, \dots, \alpha_n$  using the expression

$$\alpha_i = \frac{1}{n} \left( \sum_{k=1}^n \alpha_k + \sum_{j=1}^n (\alpha_i - \alpha_j) \right) \quad (2.3)$$

which thus yields a finite number of cases for the roots  $\alpha_1, \dots, \alpha_n$ .<sup>2</sup>

This proves the effective Shafarevich conjecture for hyperelliptic curves:

**Corollary 2.9.** *For a given number field  $K$ , finite set of primes  $S$ , and genus  $g \geq 2$ , there are only finitely many ( $K$ -isomorphism classes of) hyperelliptic curves  $C/K$  of genus  $g$  with good reduction outside  $S$ . Moreover, these curves can be effectively computed, as given in the above algorithm.*

We remark that an explicit bound on the height of Weierstrass models for genus  $g$  hyperelliptic curves  $C/K$  with good reduction outside  $S$  is given by von Känel [468].

### 2.1.2 Potential good reduction for $\text{Jac}(C)$

We now shift our attention to studying the Jacobian  $\text{Jac}(C)$  of hyperelliptic curves. We can prove the following condition for when the Jacobian itself has good reduction:

---

<sup>2</sup>Alternatively, we could assume that  $S$  contains all primes dividing  $n$ , thus allowing us to assume  $\alpha_1 + \cdots + \alpha_n = 0$ .

**Theorem 2.10.** *Let  $C/K$  be a genus  $g$  hyperelliptic curve with Weierstrass points in  $K$ , given in Rosenhain normal form*

$$y^2 = cx(x-1)(x-\lambda_1)\cdots(x-\lambda_{2g-1})$$

*Then  $\text{Jac}(C)$  has good reduction at an odd prime  $\mathfrak{p}$  if and only if  $\text{Jac}(C)$  has potentially good reduction at  $\mathfrak{p}$ , and if  $v_{\mathfrak{p}}(\lambda_i)$ ,  $v_{\mathfrak{p}}(\lambda_i - 1)$  and  $v_{\mathfrak{p}}(\lambda_i - \lambda_j)$  all have the same parity as  $v_{\mathfrak{p}}(c)$ .*

*Proof.* Let  $\Sigma_{\mathfrak{p}}$  be the cluster picture of  $C$  at  $\mathfrak{p}$ . First assume that  $v_{\mathfrak{p}}(\lambda_i)$ ,  $v_{\mathfrak{p}}(\lambda_i - 1)$  and  $v_{\mathfrak{p}}(\lambda_i - \lambda_j)$  all have the same parity as  $v_{\mathfrak{p}}(c)$ . By Theorem 1.11, to show that  $\text{Jac}(C)$  has good reduction at  $\mathfrak{p}$ , it suffices to show that  $\nu_{\mathfrak{s}}$  is even, for all principal clusters  $\mathfrak{s}$ .

Firstly, we note that since  $v_{\mathfrak{p}}(\lambda_i)$ ,  $v_{\mathfrak{p}}(\lambda_i - 1)$  and  $v_{\mathfrak{p}}(\lambda_i - \lambda_j)$  all have the same parity as  $v_{\mathfrak{p}}(c)$ , this implies the depths  $d_{\mathfrak{s}}$  of all principal clusters have the same parity as  $v_{\mathfrak{p}}(c)$ .

We can proceed by a standard inductive approach. Let  $\mathfrak{s}$  be a principal cluster of  $\Sigma_{\mathfrak{p}}$ . Let  $C_1$  denote the parent of  $\mathfrak{s}$ ,  $C_2$  denote the parent of  $C_1$ , and so on, until we have  $C_n = \mathcal{R}$ , as shown in Figure 2.1. This therefore yields the following chain of clusters:

$$\mathfrak{s} \subsetneq C_1 \subsetneq C_2 \subsetneq \cdots \subsetneq C_n = \mathcal{R}.$$

The calculation of  $\nu_{\mathfrak{s}}$  can therefore be given as

$$\nu_{\mathfrak{s}} = v_{\mathfrak{p}}(c) + \sum_{r \in \mathcal{R}} d_{r \wedge \mathfrak{s}} = v_{\mathfrak{p}}(c) + \sum_{r \in \mathfrak{s}} d_{\mathfrak{s}} + \sum_{\substack{r \in C_1 \\ r \notin \mathfrak{s}}} d_{C_1} + \sum_{\substack{r \in C_2 \\ r \notin C_1}} d_{C_2} + \cdots + \sum_{\substack{r \in C_n \\ r \notin C_{n-1}}} d_{C_n}$$

Now as  $\text{Jac}(C)$  has potentially good reduction at  $\mathfrak{p}$ , this implies that all clusters  $\mathfrak{s}$  have odd size. Therefore, we note that, except for the first  $v_{\mathfrak{p}}(c)$  and  $\sum_{r \in \mathfrak{s}} d_{\mathfrak{s}}$ , each of the remaining sums contains an even number of terms, and therefore has even parity.

Furthermore, as  $|\mathfrak{s}|$  is odd, this implies the parity of the first sum is simply  $d_{\mathfrak{s}}$ . Finally, as  $d_{\mathfrak{s}}$  has the same parity as  $v_{\mathfrak{p}}(c)$ , this gives us

$$\nu_{\mathfrak{s}} \equiv v_{\mathfrak{p}}(c) + d_{\mathfrak{s}} \equiv 0 \pmod{2}$$

which proves that  $\text{Jac}(C)$  has good reduction at  $\mathfrak{p}$ . Conversely, if  $\text{Jac}(C)$  has good reduction at  $\mathfrak{p}$ , then  $\nu_{\mathfrak{s}}$  is even for all clusters  $\mathfrak{s}$  (noting that every cluster  $\mathfrak{s}$  is principal as all clusters are odd). Given any pair  $i, j$ , let  $\mathfrak{s}$  be the smallest cluster containing

both  $\lambda_i$  and  $\lambda_j$ . Then  $v_{\mathfrak{p}}(\lambda_i - \lambda_j) = d_{\mathfrak{s}} \equiv v_{\mathfrak{p}}(c) \pmod{2}$ , where a similar argument also shows that  $v_{\mathfrak{p}}(\lambda_i) = v_{\mathfrak{p}}(\lambda_i - 1) \equiv v_{\mathfrak{p}}(c) \pmod{2}$ , thus concluding the proof.  $\square$

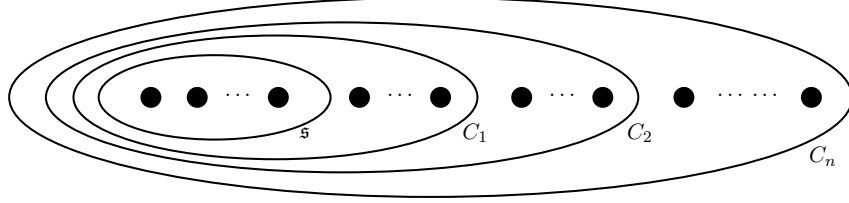


Figure 2.1: A chain of clusters  $\mathfrak{s} \subsetneq C_1 \subsetneq C_2 \subsetneq \cdots \subsetneq C_n$ .

Applying this to all odd primes  $p$ , we get the following immediate corollary:

**Corollary 2.11.** *Let  $C/K$  be a hyperelliptic curve given as above. Then  $\text{Jac}(C)$  has good reduction outside  $S$  if and only if  $\text{Jac}(C)$  has potentially good reduction outside  $S$ , and  $\lambda_i, \lambda_i - 1$  and  $\lambda_i - \lambda_j$  are in  $c\mathcal{O}_S^\times \cdot A$ , where  $A := \{\alpha \in K^\times : (\alpha) = \mathfrak{m}^2 \text{ for some fractional ideal } \mathfrak{m} \text{ in } K\}$ .*

In contrast to the effective Shafarevich problem for hyperelliptic curves, we remark that no known algorithm exists to effectively classify genus  $g$  hyperelliptic curves over  $K$  whose Jacobian has good reduction outside a finite set of primes  $S$ . If we were to attempt to prove this using the cluster picture criterion, then if we specialise to genus 2 curves, we remark that by [148], there are essentially four possible cluster pictures  $\Sigma_{\mathfrak{p}}$  for a prime  $\mathfrak{p}$  of almost good reduction for a genus 2 curve  $C/K$ , as shown in Figure 2.2.

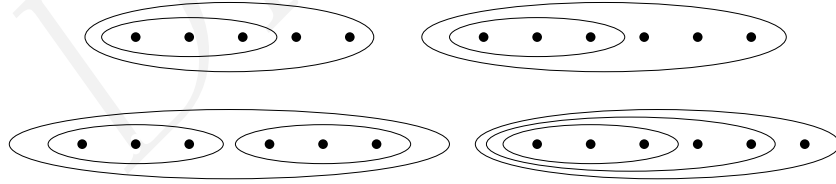


Figure 2.2: The four possible cluster pictures  $\Sigma_{\mathfrak{p}}$  for a prime  $\mathfrak{p}$  of bad reduction for  $C$  but good reduction for  $\text{Jac}(C)$  for a genus 2 curve  $C/K$

Thus, for a genus 2 curve  $C/K$  whose Jacobian  $\text{Jac}(C)$  has good reduction outside  $S$ , an a priori arbitrary number of primes  $\mathfrak{p}$  outside  $S$  could have any one of the four above cluster pictures, with different pictures for different primes  $\mathfrak{p}$  of almost good reduction. One of the fundamental difficulties of this problem is that there's no obvious way of reducing this problem to that of solving  $S$ -unit equations.

We now show that, in general, there are far more curves with Jacobian having potentially good reduction outside a given set  $S$ , than curves themselves having potentially good reduction outside  $S$ .

**Theorem 2.12.** *There are infinitely many (non-isomorphic over  $\overline{\mathbb{Q}}$ ) genus 2 hyperelliptic curves  $C$  over  $\mathbb{Q}$  with rational Weierstrass points with  $\text{Jac}(C)$  having potentially good reduction outside  $\{2\}$ .*

We note that this is in contrast to the elliptic case, where the above is not true.

*Proof.* Let  $r \geq 1$  be any positive integer, and consider the genus 2 curve  $C/\mathbb{Q}$  given by Rosenhain normal form  $\lambda_1 = 2^r + 1$ ,  $\lambda_2 = \frac{2^r+1}{2}$ , and  $\lambda_3 = 2^r$ , i.e.

$$C : y^2 = x(x-1)(x-2^r-1)(x-\frac{2^r+1}{2})(x-2^r).$$

We now consider a few cases depending on each odd prime  $p$ .

- **Case 1.**  $p$  divides  $2^r + 1$ . Let  $d := v_p(\lambda_1) \geq 1$ . We clearly note that  $v_p(\lambda_2) = d$  and  $v_p(\lambda_1 - \lambda_2) = v_p(2^r + 1) = d$ , with all other valuations being 0. (noting that  $2^r + 1$  doesn't have any odd primes in common with  $2^r - 1$ ).

Therefore, the only non-trivial cluster is the cluster of size 3 formed by  $\{0, \lambda_1, \lambda_2\}$ .

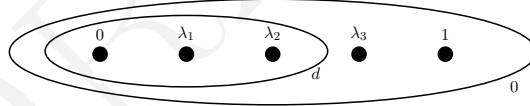


Figure 2.3: Cluster picture  $\Sigma_p$  for primes  $p$  dividing  $2^r + 1$ .

- **Case 2.**  $p$  divides  $2^r - 1$ . Similarly, we let  $d := v_p(2^r - 1) \geq 1$ . Note that  $v_p(\lambda_3 - 1) = v_p(2^r - 1) = d$  and  $v_p(\lambda_2 - \lambda_3) = d$ , with all other valuations being 0.

Therefore, the non-trivial cluster is the cluster of size 3 formed by  $\{1, \lambda_2, \lambda_3\}$ .

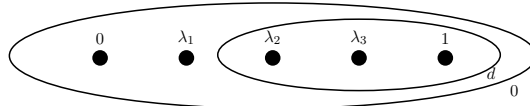


Figure 2.4: Cluster picture  $\Sigma_p$  for primes  $p$  dividing  $2^r - 1$ .

- **Case 3.** All other odd  $p$ . Clearly,  $v_p(\lambda_i) = v_p(\lambda_i - 1) = 0$ , and  $v_p(\lambda_i - \lambda_j) = 0$ , and thus the cluster picture  $\Sigma_p$  is trivial.

Therefore, in all cases, the cluster picture  $\Sigma_p$  only contains odd clusters, which proves that  $\text{Jac}(C)$  has potentially good reduction at all primes outside  $\{2\}$ . As  $r$  ranges over the positive integers, we obtain infinitely many genus 2 curves  $C/\mathbb{Q}$  with distinct Rosenhain normal forms and thus infinitely many distinct  $\overline{\mathbb{Q}}$ -isomorphism classes of genus 2 curves over  $\mathbb{Q}$ .  $\square$

We'll end this section by going one step further and giving an infinite family of genus 3 hyperelliptic curves  $C/\mathbb{Q}$  with rational Weierstrass points where  $\text{Jac}(C)$  has potential good reduction outside  $\{2\}$ .

**Theorem 2.13.** *There are infinitely many (non-isomorphic over  $\overline{\mathbb{Q}}$ ) genus 3 hyperelliptic curves  $C$  over  $\mathbb{Q}$  with rational Weierstrass points with  $\text{Jac}(C)$  having potentially good reduction outside  $\{2\}$ .*

*Proof.* Let  $k, \ell, m$  be three distinct pairwise coprime positive integers such that  $k^2 + \ell^2 = 2m^2$ . We consider the genus 3 hyperelliptic curve  $C/\mathbb{Q}$  given in Weierstrass form:

$$C : y^2 = x(x - k)(x + k)(x - \ell)(x + \ell)(x - m)(x + m).$$

As before, we check that  $\text{Jac}(C)$  has potential good reduction at every odd prime  $p$  using cluster pictures.

- **Case 1:**  $p$  divides  $k$ . As  $\ell$  and  $m$  are coprime to  $k$ , clearly  $p$  doesn't divide any of  $\pm\ell$ ,  $\pm m$ ,  $k \pm \ell$  or  $k \pm m$ . Now assume for contradiction  $p$  divides either  $\ell + m$  or  $\ell - m$ . Then  $p$  divides  $\ell^2 - m^2 = m^2 - k^2$  implying  $p$  divides  $m$ ; a contradiction. Therefore the cluster picture  $\Sigma_p$  has a single non-trivial cluster of size 3 formed by  $\{0, k, -k\}$ .

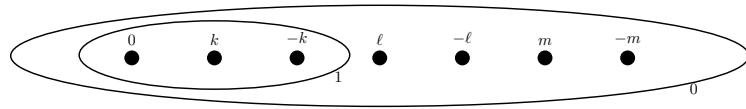


Figure 2.5: Cluster picture  $\Sigma_p$  for primes  $p$  dividing  $k$ .

- **Case 2:**  $p$  divides  $\ell$  or  $p$  divides  $m$ . This is done similarly to Case 1, where  $\Sigma_p$  consists of a single size 3 cluster formed either by  $\{0, \ell, -\ell\}$  or  $\{0, m, -m\}$  respectively.

- **Case 3:**  $p$  divides  $k^2 - \ell^2$ . Thus  $p$  divides either  $k + \ell$  or  $k - \ell$ , but not both, as then  $p = 2$ , a contradiction. Noting that  $k^2 - \ell^2 = 2(m^2 - \ell^2) = 2(k^2 - m^2)$ , this therefore implies  $p$  divides exactly one of  $m + \ell$  or  $m - \ell$ , and exactly one of  $k + m$  or  $k - m$ . Also, note that  $p$  cannot divide any of  $k, \ell$ , or  $m$  as that contradicts  $k, \ell, m$  being pairwise coprime. Thus, in all cases, we have that  $\Sigma_p$  consists of two distinct non-trivial clusters each of size 3. The four possibilities for the non-trivial clusters of  $\Sigma_\ell$  are

$$\begin{aligned} & \{\{k, \ell, m\}, \{-k, -\ell, -m\}\}, \quad \{\{k, \ell, -m\}, \{-k, -\ell, m\}\}, \\ & \{\{k, -\ell, m\}, \{-k, \ell, -m\}\}, \quad \{\{k, -\ell, -m\}, \{-k, \ell, m\}\} \end{aligned}$$

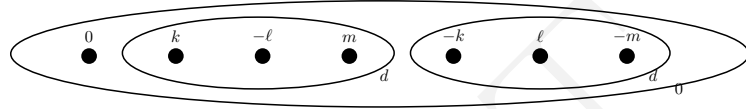


Figure 2.6: One of the four possible cluster pictures  $\Sigma_p$  for primes  $p$  dividing  $k^2 - \ell^2$ .

- **Case 4:** All other odd primes  $p$ . Clearly, the cluster picture  $\Sigma_p$  is trivial.

As before, in all cases, the cluster picture  $\Sigma_p$  only contains odd clusters, which proves that  $\text{Jac}(C)$  has potentially good reduction at all primes outside  $\{2\}$ .

It remains to note that there exist infinitely many such pairwise coprime  $k, \ell, m$  such that  $k^2 + \ell^2 = 2m^2$ . Indeed, one easily checks that the plane conic  $x^2 + y^2 = 2$  has infinitely many rational solutions, parametrised by  $(\frac{t^2-2t-1}{t^2+1}, \frac{t^2+2t-1}{t^2+1})$  for  $t \in \mathbb{Q}$ . In particular, one can take the infinite family  $(k, \ell, m) = (u^2 - 2u - 1, u^2 + 2u - 1, u^2 + 1)$  for any even integer  $u \geq 2$ .

To show that this gives us infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes of genus 3 curves, we note that a Rosenhain normal form for the family  $(k, \ell, m) = (u^2 - 2u - 1, u^2 + 2u - 1, u^2 + 1)$  can be given as

$$y^2 = x(x-1)(x+1)\left(x - \frac{u^2-2u-1}{u^2+1}\right)\left(x + \frac{u^2-2u-1}{u^2+1}\right)\left(x - \frac{u^2+2u-1}{u^2+1}\right)\left(x + \frac{u^2+2u-1}{u^2+1}\right).$$

It's clear that  $\frac{u^2-2u-1}{u^2+1}$  attains infinitely many distinct values as  $u$  ranges over the even integers (e.g. since  $\frac{u^2-2u-1}{u^2+1} = 1 - \frac{2u+2}{u^2+1}$ , this ratio is never 1 for any positive even integer  $u$  but tends to 1 as  $u \rightarrow \infty$ ). Thus, analogously to Theorem 2.12, we obtain infinitely many genus 3 curves  $C/\mathbb{Q}$  with distinct Rosenhain normal forms and thus infinitely many distinct  $\overline{\mathbb{Q}}$ -isomorphism classes of genus 3 curves over  $\mathbb{Q}$ .  $\square$

We remark that hyperelliptic curves also of genus 4 and 5 with potentially

good reduction outside  $\{2\}$  can easily be found, however we are still unsure if any such curves exist with genus  $\geq 6$ . It's possible that similar constructions to those given in Theorems 2.12 and 2.13 exist for genus  $g \geq 4$  hyperelliptic curves, however we have been unable to find any.

## 2.2 Potential good reduction of hyperelliptic curves

We can now begin to prove our main theorem. We start with the following observation, which easily follows from cluster pictures:

**Theorem 2.14.** *Let  $C/K$  be a hyperelliptic curve with Weierstrass points in  $K$ . Then  $C$  cannot have potentially good reduction at any odd prime  $\mathfrak{p}$  such that  $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq 2g$ .*

*Proof.* Let  $C$  be given by its Rosenhain normal form:

$$y^2 = cx(x-1)(x-\lambda_1)\cdots(x-\lambda_{2g-1})$$

and assume for contradiction that  $C$  has potentially good reduction at  $\mathfrak{p}$ , where  $\mathfrak{p}$  is an odd prime ideal of  $K$  such that  $N(\mathfrak{p}) \leq 2g$ .

We have by Theorem 2.6 that  $\lambda_1, \dots, \lambda_{2g-1}$  must all be  $\mathfrak{p}$ -units. Furthermore, note that each of the roots  $0, 1, \lambda_1, \dots, \lambda_{2g-1}$  must yield distinct values under the reduction map  $\mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}$ . However, this is a contradiction if  $2g+1 > N(\mathfrak{p})$ , noting that  $\#\mathcal{O}_K/\mathfrak{p} = N(\mathfrak{p})$ .  $\square$

We remark that the above inequality is tight, since given any odd prime  $\mathfrak{p}$  with  $N(\mathfrak{p}) > 2g$ , we can simply let  $0, 1, \lambda_1, \dots, \lambda_{2g-1}$  be some distinct representative elements in the residue field to yield an example of a curve  $C$  with good reduction at  $\mathfrak{p}$ .

This result immediately implies that there are only finitely many  $\overline{K}$ -isomorphism classes of genus  $g$  hyperelliptic curves  $C/K$  with Weierstrass points in  $K$  having potentially good reduction outside at most  $\pi_{K,\text{odd}}(2g)$  odd primes. However, remarkably we can go one step further:

**Theorem 2.15.** *There are only finitely many  $\overline{K}$ -isomorphism classes of genus  $g$  hyperelliptic curves  $C/K$  with rational Weierstrass points in  $K$  having potentially good reduction outside at most  $\pi_{K,\text{odd}}(2g) + 1$  primes.*

In order to prove the above theorem, we shall make use of the following elementary (albeit technical) lemma:



**Lemma 2.16.** *Let  $K$  be a number field and  $S$  a fixed finite set of primes of  $K$ . Then there exist only finitely many odd primes  $\mathfrak{p}$  such that there exist distinct  $T$ -units  $x, y, z \in \mathcal{O}_T^\times$  where  $T = S \cup \{\mathfrak{p}\}$  such that  $x - y$ ,  $x - z$ , and  $y - z$  are all  $T$ -units, and such that  $v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y), v_{\mathfrak{p}}(z), v_{\mathfrak{p}}(x - y), v_{\mathfrak{p}}(x - z), v_{\mathfrak{p}}(y - z)$  are not all equal.*

The proof of this lemma proceeds by analysing various three term  $S$ -unit equations, and thus we shall make essential use of the following finiteness result for general term  $S$ -unit equations, first conjectured by Mahler.

**Theorem.** [161, p. 131] *Let  $K$  be a number field and  $S$  a fixed finite set of primes of  $K$ . Let  $n \geq 2$  and  $a_1, \dots, a_n \in K$  be non-zero elements in  $K$ . Then there are only finitely many tuples  $(x_1, \dots, x_n)$ ,  $x_i \in \mathcal{O}_S^\times$  such that*

$$a_1x_1 + \dots + a_nx_n = 1$$

*and such that  $\sum_{i \in I} a_i x_i \neq 0$  for every non-empty subset  $I$  of  $\{1, \dots, n\}$ .*

This was first proven (under some stronger assumptions) in the case  $K = \mathbb{Q}$  independently by Dubois–Rhin [153] and Schlickewei [379], after which it was proven for arbitrary number fields  $K$  independently by Evertse [159] and van der Poorten and Schlickewei [460]. These proofs used the famous subspace theorem of Schmidt [380].<sup>3</sup> Unlike two term  $S$ -unit equations, we don't have an explicit algorithm to effectively compute all such non-degenerate solutions. However explicit bounds on the number of solutions can be derived (e.g. see Evertse–Schlickewei–Schmidt [163] or Amoroso–Viada [14]).

Restating the above theorem in the case  $n = 3$  and  $a_1 = a_2 = a_3 = 1$  yields the following theorem:

**Theorem 2.17.** [161, p. 131] *Let  $K$  be a number field and  $S$  a fixed finite set of primes of  $K$ . Then the equation  $u + v + w = 1$  has only finitely many solutions in  $u, v, w \in \mathcal{O}_S^\times$ , such that  $u, v, w \neq 1$  (i.e. only finitely many non-degenerate solutions).*

With the above theorem under our belt, we can now prove Lemma 2.16.

*Proof of Lemma 2.16.* Let  $\mathcal{P}$  be the set of odd primes  $\mathfrak{p}$  in  $K$  such that there exist distinct  $T$ -units  $x, y, z \in \mathcal{O}_T^\times$  where  $T = S \cup \{\mathfrak{p}\}$  such that  $x - y$ ,  $x - z$ , and  $y - z$  are all  $T$ -units, and such that  $v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y), v_{\mathfrak{p}}(z), v_{\mathfrak{p}}(x - y), v_{\mathfrak{p}}(x - z), v_{\mathfrak{p}}(y - z)$  are not all equal. In summary, we shall prove that  $\mathcal{P}$  is finite by following the procedure outlined below:

---

<sup>3</sup>Schmidt's subspace theorem is a higher-dimensional analogue of Roth's theorem [369], and has several rather surprising applications (see Bilu [42] for an excellent survey of the subspace theorem)!

1. Let  $\mathfrak{p} \in \mathcal{P}$  be such a prime, and let  $T = S \cup \{\mathfrak{p}\}$ .
2. By assumption, there exist distinct  $T$ -units  $x, y, z \in \mathcal{O}_T^\times$  satisfying the above conditions.
3. Let  $s := \frac{x}{z}$  and  $t := \frac{y}{z}$ . By then considering various cases depending on the signs of  $v_{\mathfrak{p}}(s)$  and  $v_{\mathfrak{p}}(t)$ , we show that  $s$  and  $t$  must arise explicitly from solutions to the three term  $S$ -unit equation  $u + v + w = 1$  (we crucially note here that  $S$ , and hence  $u, v, w$ , does *not* depend on  $T$ ).
4. For each case, we check the possible degenerate solutions. We then apply Theorem 2.17 to conclude that there exist only finitely many such  $u, v, w \in \mathcal{O}_S^\times$  and thus finitely many  $s, t \in \mathcal{O}_T^\times$ .
5. By the assumption that  $v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y), v_{\mathfrak{p}}(z), v_{\mathfrak{p}}(x-y), v_{\mathfrak{p}}(x-z), v_{\mathfrak{p}}(y-z)$  are not all equal, this implies at least one of  $s, t, s-1, t-1, s-t$  must have non-zero  $\mathfrak{p}$ -adic valuation. Therefore, the finiteness of the pairs  $(s, t)$  implies finitely many possible primes  $\mathfrak{p} \in \mathcal{P}$ .

We thus proceed by first letting  $\mathfrak{p} \in \mathcal{P}$ . We can assume without loss of generality that  $v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(y) \geq v_{\mathfrak{p}}(z)$ . For brevity we denote  $s := \frac{x}{z}$  and  $t := \frac{y}{z}$  and define  $a := v_{\mathfrak{p}}(s)$  and  $b := v_{\mathfrak{p}}(t)$ , noting that  $a, b$  are non-negative integers where  $a \geq b$ . We also define  $c := v_{\mathfrak{p}}(s-1)$ ,  $d := v_{\mathfrak{p}}(t-1)$  and  $e := v_{\mathfrak{p}}(s-t)$ , noting that  $s, t$  and  $s-t$  are all  $T$ -units.

The proof now proceeds by considering the various cases for  $a$  and  $b$ . In each case, the main idea is to obtain a three term  $S$ -unit equation from which we will obtain only finitely many solutions.

- **Case 1:**  $a, b > 0$  and  $a > b$ . This implies  $c = d = 0$  and  $e = b$ , and thus we have

$$s-1 = u, \quad \text{and} \quad t-1 = v,$$

for some  $u, v \in \mathcal{O}_S^\times$ . As  $v_{\mathfrak{p}}(u-v) = v_{\mathfrak{p}}(t)$ , we have that  $t/(u-v)$  is an  $S$ -unit, and thus by rearranging, we obtain the three term  $S$ -unit equation:

$$\frac{t}{u-v}u - \frac{t}{u-v}v - v = 1. \tag{2.4}$$

At this stage, we would like to apply Theorem 2.17 in order to conclude that there are only finitely many solutions to the above equation. We must therefore check that we do not obtain (or only obtain finitely many) degenerate solutions where one of the above terms equals 1:

- (i) If the first term of (2.4) is 1, then  $t = v - u$  which implies  $x = 0$ , contradiction.
- (ii) If the second term of (2.4) is 1, then  $tv = v - u$ , which implies  $s = t(1 - v)$  and hence  $1 - v$  has positive  $\mathfrak{p}$ -adic valuation. But  $v - 1 = t - 2$  which yields a contradiction, since  $\mathfrak{p}$  is odd.
- (iii) If the third term of (2.4) is 1, then  $t = 0$ , contradiction.

Therefore, we have a three term  $S$ -unit equation with no degenerate solutions. Thus, there are only finitely many solutions to (2.4), and thus only finitely many  $v$ , and thus clearly only finitely many  $\mathfrak{p}$ , noting that  $b$  is positive.

- **Case 2:**  $a, b > 0$  and  $a = b$ . As before, we have

$$s - 1 = u, \quad \text{and} \quad t - 1 = v$$

for some  $u, v \in \mathcal{O}_S^\times$ . Noting that  $v_{\mathfrak{p}}(t/s) = 0$ , by rearranging, we obtain the three term  $S$ -unit equation:

$$\frac{t}{s}u + \frac{t}{s} - v = 1. \tag{2.5}$$

Once again, we check the three cases:

- (i) If the first term of (2.5) is 1, then  $tu = s$  and  $t = vs$  which implies  $uv = 1$ . Now by multiplying the first two equations we get

$$st - (s + t) + 1 = (s - 1)(t - 1) = uv = 1,$$

which implies  $v_{\mathfrak{p}}(s + t) = v_{\mathfrak{p}}(st) = 2a > a$ , and thus  $v_{\mathfrak{p}}(s - t) = v_{\mathfrak{p}}(s + t - 2t) = a$  as  $\mathfrak{p}$  odd. This thus yields the following two term  $S$ -unit equation:

$$\frac{s}{t} - \frac{s - t}{t} = 1,$$

which implies finitely many values for  $\frac{s}{t}$  and thus for  $u$ , and so only finitely many values for  $\mathfrak{p}$ .

- (ii) If the second term of (2.5) is 1, then  $x = y$ , contradiction.
- (iii) If the third term of (2.5) is 1, then  $u = 1$  and thus  $x/z = 2$ , contradiction.

Therefore, as before, we obtain only finitely many solutions.

- **Case 3:**  $a > 0$  and  $b = 0$ . We therefore have  $c = 0$  and  $e = 0$ . This yields

$$s - 1 = u, \quad s - t = w$$

for some  $u, w \in \mathcal{O}_S^\times$ , which yields the three term  $S$ -unit equation:

$$w + t - u = 1. \quad (2.6)$$

- (i) If  $w = 1$ , then  $v_{\mathfrak{p}}(t - 1) = v_{\mathfrak{p}}(s - 2) = 0$ , as  $\mathfrak{p}$  odd. Therefore  $t - 1 = v$  for some  $v \in \mathcal{O}_S^\times$ . This yields a two term  $S$ -unit equation, of which there are only finitely many solutions for  $t, v$ , and thus for  $u$ , hence only finitely many for  $p$ .
  - (ii) If  $t = 1$ , then  $y = z$ , contradiction.
  - (iii) If  $u = -1$ , then  $x = 0$ , contradiction.
- **Case 4:**  $a = b = 0$  and  $c > d$ . This implies  $e = d$  which yields the three term  $S$ -unit equation:

$$\frac{t-1}{s-t}t - \frac{t-1}{s-t}s + t = 1. \quad (2.7)$$

Firstly, if  $d = 0$ , then  $v_{\mathfrak{p}}(t - 1) = 0$  which yields a two term  $S$ -unit equation of which there are only finitely many solutions. Thus, we may assume  $d > 0$ .

- (i) If the first term of (2.7) is 1, then  $s - t = t(t - 1)$  which implies  $s = t^2$ . This yields
 
$$s - 1 = (t - 1)(t + 1)$$
 which implies  $t + 1$  has positive  $\mathfrak{p}$ -adic valuation. But  $t + 1 = (t - 1) + 2$  which yields a contradiction as  $\mathfrak{p}$  odd.
  - (ii) If the second term of (2.7) is 1, then  $t - 1 = t - s$  and so  $s = 1$ , contradiction.
  - (iii) If the third term of (2.7) is 1, then  $y = z$ , contradiction.
- **Case 5:**  $a = b = 0$  and  $c = d$ . Again, note that if  $c = d = 0$ , then  $s$  and  $t$  satisfy two term  $S$ -unit equations, of which there are only finitely many solutions. This thus implies only finitely many  $p$ , since we'd then have  $v_{\mathfrak{p}}(s - t) > 0$  by assumption.

Now assume  $c, d \neq 0$ , and note that  $c, e$  must necessarily be positive. We

obtain the three term  $S$ -unit equation:

$$\frac{s-1}{t-1} - \frac{s-1}{t-1}t + s = 1. \quad (2.8)$$

- (i) If the first term of (2.8) is 1, then  $s = t$ , contradiction.
- (ii) If the second term of (2.8) is 1, then  $(s-1)t = -(t-1)$  and  $(s-1) = -s(t-1)$  which implies  $st = 1$ . By a similar argument to the above case 4(i), we have  $v_{\mathfrak{p}}(t+1) = 0$ . This implies

$$e = v_{\mathfrak{p}}(s-t) = v_{\mathfrak{p}}(1-t^2) = v_{\mathfrak{p}}(1-t) = c.$$

This implies that we have the following two term  $S$ -unit equation:

$$\frac{s-1}{t-1} - \frac{s-t}{t-1} = 1,$$

which implies only finitely many solutions for  $\frac{s-1}{t-1}$ . Therefore, this gives finitely many  $t$ , and thus finitely many  $\mathfrak{p}$ .

- (iii) If  $s = 1$ , then  $x = z$ , contradiction.

- **Case 6:**  $a = b = 0$  and  $c < d$ . Done analogously to Case 4.

Therefore, in each case, we obtain only finitely many valid primes  $\mathfrak{p}$ , which concludes the proof.  $\square$

We note that effectively obtaining a list of all possible primes  $\mathfrak{p}$  depends entirely on the effectiveness of solving the above three term  $S$ -unit equations. From the results of [161], no finite algorithm has been found to determine all possible solutions, however one can obtain an explicit bound on the number of possible  $\mathfrak{p}$ , which for a fixed number of terms, is exponential in  $|S|$  [161, p. 132].

We are now finally ready to prove Theorem 2.15:

*Proof of Theorem 2.15.* Let  $C/K$  be a hyperelliptic curve of genus  $g$  given in Rosenhain normal form  $C : y^2 = x(x-1)(x-\lambda_1) \cdots (x-\lambda_{2g-1})$  with Weierstrass points in  $K$ . By Theorem 2.14,  $C$  cannot have potentially good reduction at any odd primes with norm less than  $2g$ . Now assume  $C$  has potentially good reduction outside exactly  $\pi_{K,\text{odd}}(2g) + 1$  odd primes  $T$ .

Thus,  $T$  must consist of all  $\pi_{K,\text{odd}}(2g)$  odd primes with norm below  $2g$ , plus one additional prime  $\mathfrak{p}$ . Now by Corollary 2.7, we must have that  $\lambda_1, \lambda_2, \lambda_1 - 1, \lambda_2 - 1$  and  $\lambda_1 - \lambda_2$  are all  $T$ -units. Therefore, by Lemma 2.16, there are only finitely many

possible primes  $\mathfrak{p}$ , and thus by either applying Faltings' theorem [118, p. 25] or by the finiteness of solutions to  $T$ -unit equations, we obtain only finitely many  $\overline{K}$ -isomorphism classes of hyperelliptic curves with potentially good reduction outside  $T$ .  $\square$

It's worth mentioning that our proof of Theorem 2.15 above applied Lemma 2.16 using only the Weierstrass points  $0, 1, \lambda_1$ , and  $\lambda_2$ . However, by Corollary 2.7, we know that  $\lambda_i$ ,  $\lambda_i - 1$  and  $\lambda_i - \lambda_j$  must be  $T$ -units for all distinct  $i$  and  $j$ . Indeed, if we were to make use all the known constraints on the roots  $\lambda_i$ , it's reasonable to conjecture that we could expect to prove a significantly stronger lower bound for  $c_K(g)$ .

A heuristic argument suggests that if we generalise Lemma 2.16 where, instead of just adjoining one prime  $T := S \cup \{\mathfrak{p}\}$ , we adjoin an additional  $k$  primes  $T := S \cup \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$  for some  $k < g$ , then assuming we don't encounter any degenerate solutions, this could yield a potential linear lower bound of  $g + \pi_{K, \text{odd}}(2g)$  for  $c_K(g)$ . Motivated by this possible argument, we therefore make the following conjecture:

**Conjecture 2.18.** *Let  $K$  be a number field and  $g$  a positive integer. Then  $c_K(g) \geq g + \pi_{K, \text{odd}}(2g)$ .*

In principle, one could fix some small positive integer  $k < g$ , and then attempt to prove a suitable generalisation of Lemma 2.16 for  $T := S \cup \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$  where we similarly check all the necessary cases, and assuming no degeneracy occurs, prove Conjecture 2.18 for that value of  $k$ , as we did in Lemma 2.16 for  $k = 1$ . However, besides extending the case bash analysis for particular small values of  $k$ , we do not know at this stage how to produce such a proof for an arbitrary  $k$ .

We shall now restrict our attention to the specific case where  $C$  is a hyperelliptic curve over  $\mathbb{Q}$ , with all of its Weierstrass points in  $\mathbb{Q}$ .

### 2.3 Hyperelliptic curves with rational Weierstrass points

Firstly, although this is already well-known, it's worth stating the application of Theorem 2.14 to the case of rational Weierstrass points:

**Corollary 2.19.** *Let  $C/\mathbb{Q}$  be a genus  $g$  hyperelliptic curve with rational Weierstrass points. Then  $C$  cannot have potentially good reduction at any odd prime  $p \leq 2g$ .*

**Remarks.**

- We remark that the above is not true for genus 2 curves over  $\mathbb{Q}$  with non-rational Weierstrass points. For example the curve  $y^2 = x(x-1)(x+1)(x-i)(x+i)$  has minimal discriminant  $\Delta_{\min} = -2^{16}$  and so does have good reduction at  $p = 3$ .
- We note that  $p$  being odd is essential here, e.g. the genus 2 curve  $y^2 = x(x-3)(x-4)(x-16)(x-20)$  with all rational Weierstrass points has minimal model  $y^2 + (x^2+x)y = x^5 - 6x^4 + 3x^3 + 13x^2 + 3x$  with discriminant  $\Delta_{\min} = 3^4 5^2 13^2 17^2$  and so has good reduction at  $2$ <sup>4</sup>.
- We also note that this only applies to the curve  $C$  and not its Jacobian  $\text{Jac}(C)$ . For example, the genus 2 curve  $C/\mathbb{Q} : y^2 = x(x-1)(x-2)(x-9)(x-18)$  has bad reduction at 3, but its Jacobian has good reduction at 3.

Note that this clearly implies that no genus 2 hyperelliptic curve with rational Weierstrass points has potentially good reduction at 3. This corollary can be applied to give a short proof of the following result from Box and Le Fourn [65], which was originally proven using a two-dimensional analogue of Baker's and Runge's method applied to the Siegel variety  $A_2(2)$  (i.e. the moduli space of principally polarised abelian surfaces with full 2-torsion). We also remark that similar statements have been shown by Dąbrowski and Sadek (e.g. see [144, Theorem 4.1]).

**Corollary 2.20.** [65, Corollary 2] *There is no genus 2 hyperelliptic curve  $C$  over  $\mathbb{Q}$  such that all Weierstrass points of  $C$  are rational and  $C$  has potentially good reduction at all but one of the primes.*

*Proof.* As shown above, such a curve  $C$  cannot have potentially good reduction at 3. Now assume for contradiction such a curve has potentially good reduction outside 3. By applying Corollary 2.7, we can now effectively compute all genus 2 curves  $C/\mathbb{Q}$  with rational Weierstrass points having potentially good reduction outside  $S = \{2, 3\}$ .

By Corollary 2.7, we proceed by solving the  $S$ -unit equation  $x + y = 1$ , where  $x, y \in \mathcal{O}_S^\times$ . These solutions can be computed using existing algorithms, such as those described by von Känel and Matschke [471]. Using their Sage [373] implementation, we obtained the following 21 solutions for  $x \in \mathcal{O}_S^\times$ :

$$-8, -3, -2, -1, -\frac{1}{2}, -\frac{1}{3}, -\frac{1}{8}, \frac{1}{9}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{8}{9}, \frac{9}{8}, \frac{4}{3}, \frac{3}{2}, 2, 3, 4, 9,$$

---

<sup>4</sup>It's reasonable to conjecture that there might exist similar examples of higher genus hyperelliptic curves with all rational Weierstrass points and with good reduction at 2. Although a quick brute force computer search failed to find any such explicit examples for genus 3.

and can conclude that any such curve must be  $\overline{\mathbb{Q}}$ -isomorphic to one of the following two curves:

$$\begin{aligned} C_1 : y^2 &= x(x-1)(x-2)(x-3)(x-4), & \text{with } \Delta_{\min} &= 2^{18}3^4 \\ C_2 : y^2 &= x(x-2)(x-3)(x-4)(x-6), & \text{with } \Delta_{\min} &= 2^{14}3^6 \end{aligned}$$

We can use Theorem 1.14 to verify that neither of the two curves above have potential good reduction at 2. Indeed, computing  $(J_2^5/J_{10}, J_4^5/J_{10}^2, J_6^5/J_{10}^3, J_8^5/J_{10}^4)$  for each curve, we find that 2 divides at least one of the denominators, thus showing both  $C_1$  and  $C_2$  do not have potential good reduction at 2. This gives us our contradiction, and thus the result holds.  $\square$

We can go one step further and prove a similar result for genus 3 hyperelliptic curves:

**Corollary 2.21.** *There is no genus 3 hyperelliptic curve  $C$  over  $\mathbb{Q}$  such that all Weierstrass points of  $C$  are rational and  $C$  has potentially good reduction at all but two of the primes.*

*Proof.* Again, we have that  $C$  cannot have potential good reduction at 3 and 5. Assume for contradiction such a curve has potential good reduction outside  $\{3, 5\}$ . As before, we can effectively compute all such curves by solving the  $S$ -unit equation  $x + y = 1$ , where  $x, y \in \mathcal{O}_S^\times$  for  $S = \{2, 3, 5\}$ . This time, we obtain 99 solutions for  $x \in \mathcal{O}_S^\times$ , and can conclude that any such curve must be  $\overline{\mathbb{Q}}$ -isomorphic to one of the following ten curves:

$$\begin{aligned} C_1 : y^2 &= x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6), & \text{with } \Delta_{\min} &= 2^{36}3^{10}5^4 \\ C_2 : y^2 &= x(x-2)(x-3)(x-4)(x-5)(x-6)(x-8), & \text{with } \Delta_{\min} &= 2^{44}3^{12}5^4 \\ C_3 : y^2 &= x(x-1)(x-3)(x-4)(x-5)(x-6)(x-9), & \text{with } \Delta_{\min} &= 2^{40}3^{16}5^6 \\ C_4 : y^2 &= x(x-1)(x-2)(x-4)(x-5)(x-6)(x-10), & \text{with } \Delta_{\min} &= 2^{46}3^{12}5^8 \\ C_5 : y^2 &= x(x-2)(x-4)(x-5)(x-6)(x-8)(x-10), & \text{with } \Delta_{\min} &= 2^{30}3^{10}5^6 \\ C_6 : y^2 &= x(x-1)(x-4)(x-5)(x-6)(x-9)(x-10), & \text{with } \Delta_{\min} &= 2^{42}3^{16}5^{10} \\ C_7 : y^2 &= x(x-2)(x-3)(x-4)(x-6)(x-8)(x-12), & \text{with } \Delta_{\min} &= 2^{32}3^{16}5^4 \\ C_8 : y^2 &= x(x-2)(x-4)(x-5)(x-8)(x-10)(x-20), & \text{with } \Delta_{\min} &= 2^{36}3^{16}5^{12} \\ C_9 : y^2 &= x(x-6)(x-10)(x-12)(x-15)(x-18)(x-30), & \text{with } \Delta_{\min} &= 2^{32}3^85^{12} \\ C_{10} : y^2 &= x(x-4)(x-6)(x-9)(x-24)(x-36)(x-54), & \text{with } \Delta_{\min} &= 2^{40}3^{20}5^{16} \end{aligned}$$

Unlike genus 2 curves, we do not currently have a set of invariants analogous



to the Igusa invariants for genus 3 hyperelliptic curves from which potential good reduction at 2 can be read off.

However, in principle, one can directly check whether any particular curve  $C/K$  has (potential) good reduction at  $p$  by computing a stable reduction model  $\mathcal{C}$  for  $C/K$ , and counting the components of positive genus for  $\mathcal{C}$ . In principle, this can always be done for an arbitrary curve  $C/K$  by repeatedly applying a suitable sequence of blow-ups, normalisations, and blow-downs (and allowing ramified covers), although in practice this is often a highly non-trivial computation, e.g. see Harris–Morrison [217, Chapter 3.C] for an outline of such an algorithm.

For our purposes, we used the MCLF [372] Sage package to compute stable reduction models for each of the 10 curves  $C_i/\mathbb{Q}$  above.<sup>5</sup> In each case, we found that  $\mathcal{C}$  contained three positive genus components (each of genus 1), thus proving that  $C_i/\mathbb{Q}$  does not have potential good reduction at 2 for each  $i = 1, \dots, 10$ .<sup>6</sup>  $\square$

Finally, whilst we acknowledge no effective height bounds are known for solutions to general term  $S$ -unit equations, in principle one can give an effective bound on the number of possible primes  $p$  in Lemma 2.16. By nothing more than computational evidence, we make the following conjecture:

**Conjecture.** *Let  $C/\mathbb{Q}$  be a hyperelliptic curve with rational Weierstrass points.*

1. *If  $C$  has genus 2 and has geometric bad reduction exactly at  $\{2, 3, p\}$  for some prime  $p \geq 5$ , then  $p \in \{5, 7, 11, 13, 17, 73\}$ .*
2.  *$C$  has genus 3 and has geometric bad reduction exactly at  $\{2, 3, 5, p\}$  for some prime  $p \geq 7$ , then  $p \in \{7, 11, 13, 17, 19, 23, 29, 41, 43, 53\}$ .*

## 2.4 Upper bounds for $c_K(g)$

It's worth mentioning some of the results we can obtain regarding upper bounds for  $c_K(g)$ . Most of the more interesting results are conditional on various conjectures concerning the distribution of primes.

For a given number field  $K$ , we recall that a  $k$ -tuple  $(h_1, \dots, h_k)$  of distinct elements in  $\mathcal{O}_K$  is *admissible* if, for every prime  $\mathfrak{p}$  in  $K$ , the set  $\{h_1, \dots, h_k\}$  does not consist of all residues mod  $\mathfrak{p}$ . We also say that an element  $x \in \mathcal{O}_K$  is *prime* if the

<sup>5</sup>We note that similar functionality also exists in Magma, using the `RegularModel` function, however Magma was unable to compute regular models at  $p = 2$  for some of the above curves.

<sup>6</sup>We furthermore checked that the graph of components of  $\mathcal{C}$  contained a cycle for some of our curves  $C/\mathbb{Q}$ , thereby proving in these cases that  $\text{Jac}(C)$  does not have potential good reduction at 2 (e.g. see [61, Remark 1.4]).

principal ideal generated by  $x$  is prime. We now first recall the Hardy–Littlewood prime  $k$ -tuples conjecture for  $K$  [216]:

**Conjecture.** (*Hardy–Littlewood prime  $k$ -tuples conjecture for number fields*) Let  $K$  be a number field and  $(h_1, \dots, h_k)$  an admissible  $k$ -tuple in  $\mathcal{O}_K$ . Then there exist infinitely many  $x \in \mathcal{O}_K$  such that each of  $x + h_1, \dots, x + h_k$  is prime.

Notably, one can therefore prove the following result, conditional on the assumption of the above conjecture.

**Theorem 2.22.** *Let  $K$  be a number field of degree  $n$ . Under the assumption of the Hardy–Littlewood prime  $k$ -tuples conjecture for  $K$ , then  $c_K(g) \leq 2g - 1 + n\pi(2g)$ .*

*Proof.* For a given genus  $g \geq 2$ , we consider the following admissible prime  $2g - 1$  tuple  $(h_1, \dots, h_{2g-1})$ :

$$(0, (2g)!, 2 \cdot (2g)!, 3 \cdot (2g)!, \dots, (2g - 2) \cdot (2g)!)$$
 (2.9)

Now by the Hardy–Littlewood prime  $k$ -tuples conjecture, there exist infinitely many primes  $p$  in  $K$  such that  $p + h_1, \dots, p + h_{2g-1}$  are all prime. Thus, for each such prime  $p$ , we can construct the genus  $g$  hyperelliptic curve  $C_p/K$  as

$$C_p : y^2 = x(x - p - h_1)(x - p - h_2) \cdots (x - p - h_{2g-1})(x - 2p - 2g \cdot (2g)!).$$

As the only possible primes of bad reduction are those which divide the differences between Weierstrass points, it's clear that the only possible primes of bad reduction are either the primes  $p + h_1, \dots, p + h_{2g-1}$  or the primes dividing  $(2g)!$ , of which there are at most  $n\pi(2g)$ . Thus, the number of primes of geometric bad reduction for  $C_p$  is at most  $2g - 1 + n\pi(2g)$ .

This therefore yields the existence of infinitely many genus  $g$  hyperelliptic curves  $C/K$  satisfying  $\#\mathcal{B}_{\text{odd}}(C/K) \leq 2g - 1 + n\pi(2g)$ . Furthermore, as this construction yields infinitely many distinct sets of primes of geometric bad reduction  $\mathcal{B}_{\text{odd}}(C/K)$ , this gives rise to infinitely many  $\overline{K}$ -isomorphism classes of such curves.<sup>7</sup> This therefore yields the conditional bound  $c_K(g) \leq 2g - 1 + n\pi(2g)$ .  $\square$

Whilst the above result gives a conditional linear upper bound for  $c_K(g)$ , it's worth noting that we can also give an unconditional linearithmic bound for  $c_K(g)$ .

<sup>7</sup>Alternatively, one can note that the Rosenhain normal form of  $C_p$  can be given as  $y^2 = x(x - 1)(x - \frac{p-h_2}{p-h_1}) \cdots$ , and since the ratios  $\frac{p-h_2}{p-h_1}$  are pairwise distinct for different primes  $p$ , this yields infinitely many distinct  $\overline{K}$ -isomorphism classes.

**Theorem 2.23.** *Let  $K$  be a number field of degree  $n$ . We have  $c_K(g) \leq (\frac{2}{\log 2} + o(1))ng \log g$  as  $g \rightarrow \infty$ .*

*Proof.* Let  $(h_1, \dots, h_{2g-1})$  be the same admissible prime tuple as given in (2.9). We shall apply the result of Murty and Vatwani [327, p. 183], which asserts the existence of infinitely many integers  $k$  such that  $(k + h_1) \cdots (k + h_{2g-1})$  has at most  $(\frac{2}{\log 2} + o(1))g \log g$  prime divisors in  $\mathbb{Q}$  (here the  $o(1)$  term goes to 0 as  $g \rightarrow \infty$ ). By therefore considering the set of genus  $g$  hyperelliptic curves

$$C_k : y^2 = x(x - k - h_1) \cdots (x - k - h_{2g-1})(x - 2k - 2g \cdot (2g)!)$$

this yields the desired upper bound. By a similar argument to Theorem 2.22, we note that the curves  $C_k$  yield infinitely many distinct  $\overline{K}$ -isomorphism classes.  $\square$

It's tempting to ask how far we can push our conditional upper bounds. Whilst a sublinear bound is almost certainly out of reach, we can sharpen the above theorem if we furthermore assume the following generalisation to the Hardy-Littlewood prime  $k$ -tuples conjecture. This goes by various different names, often called Schinzel's hypothesis H [378], generalised Dickson's conjecture, or the generalised Bunyakovsky conjecture.

**Conjecture.** (*Schinzel's hypothesis H for number fields*) *Let  $K$  be a number field and  $(f_1, \dots, f_k)$  a collection of  $k$  distinct nonconstant irreducible polynomials in  $\mathcal{O}_K[x]$ , such that for all primes  $\mathfrak{p}$  in  $K$ , there exists an  $n \in \mathcal{O}_K$  where  $v_{\mathfrak{p}}(f_1(n)f_2(n) \cdots f_k(n)) = 0$ . Then there exist infinitely many  $x \in \mathcal{O}_K$  such that each of  $f_1(x), \dots, f_k(x)$  is prime.*

Under the assumption of the above conjecture, we can prove the following sharpened upper bound for  $c_K(g)$ .

**Theorem 2.24.** *Let  $K$  be a number field of degree  $n$ . Assuming Schinzel's hypothesis H for  $K$ , we have that*

$$c_K(g) \leq \sum_{\substack{1 \leq d < g, \text{ or} \\ d < 2g, d \text{ even}}} \frac{n}{[K(\zeta_d) : \mathbb{Q}(\zeta_d)]} + 1 + n\pi(2g) \quad (2.10)$$

*Proof.* For brevity, we shall denote  $\alpha := (2g)!$ . The idea is to consider, for infinitely many  $k$ , genus  $g$  hyperelliptic curves of the form

$$C_k : y^2 = x(x-1)(x+1)(x-\alpha k)(x+\alpha k)(x-(\alpha k)^2)(x+(\alpha k)^2) \cdots (x-(\alpha k)^{g-1})(x+(\alpha k)^{g-1})$$

We note that the only possible primes of bad reduction are those which divide  $2\alpha k$ ,  $(\alpha k)^d - 1$ , or  $(\alpha k)^d + 1$  for some  $d < g$ . Under the assumption of Schinzel's hypothesis H, it thus suffices to count the number of irreducible factors of  $(\alpha x)^d \pm 1$  over  $K$ .

It's well-known that  $(\alpha x)^d \pm 1$  factorises over  $\mathbb{Q}$  as a product of cyclotomic polynomials, i.e.

$$(\alpha x)^d - 1 = \prod_{i|d} \Phi_i(\alpha x), \quad \text{and} \quad (\alpha x)^d + 1 = \prod_{\substack{i|2d \\ i \nmid d}} \Phi_i(\alpha x),$$

where  $\Phi_i(x)$  denotes the  $i$ -th cyclotomic polynomial. Furthermore, the factorisation of  $\Phi_i(x)$  over  $K$  can be given as  $\Phi_i(\alpha x) = f_{i,1}(\alpha x) \cdots f_{i,\ell_i}(\alpha x)$  where each  $f_{i,j}(x)$  has degree  $[K(\zeta_i) : K]$ , and hence  $\ell_i = \frac{\varphi(i)}{[K(\zeta_i) : K]} = \frac{n}{[K(\zeta_d) : \mathbb{Q}(\zeta_d)]}$  by the tower law.

Now Schinzel's hypothesis H states that we can find infinitely many primes  $p$  in  $K$  such that  $f_{i,j}(\alpha p)$  are all prime, noting that the factor of  $\alpha$  ensures we have no local obstructions to primality. By thus counting the primes dividing  $(\alpha p)^d \pm 1$ , the prime  $p$ , and the primes dividing  $2\alpha$ , this therefore yields the conditional bound

$$c_K(g) \leq \sum_{\substack{1 \leq d < g, \text{ or} \\ d < 2g, d \text{ even}}} \frac{n}{[K(\zeta_d) : \mathbb{Q}(\zeta_d)]} + 1 + n\pi(2g)$$

which yields our result.  $\square$

Whilst the above construction does not necessarily improve upon the result given in Theorem 2.22 for all fields  $K$ , one can obtain the following two corollaries:

**Corollary 2.25.** *Let  $K$  be a primitive abelian number field of (necessarily prime) degree  $n$  and conductor  $\mathfrak{f}_K$ . Then assuming Schinzel's hypothesis H for  $K$ , we have*

$$c_K(g) \leq \begin{cases} \frac{3}{2}g\left(1 + \frac{n-1}{\mathfrak{f}_K}\right) + 1 + n\pi(2g) & \text{if } \mathfrak{f}_K \text{ odd,} \\ \frac{3}{2}g\left(1 + \frac{4(n-1)}{3\mathfrak{f}_K}\right) + 1 + n\pi(2g) & \text{if } \mathfrak{f}_K \text{ even.} \end{cases}$$

*Proof.* Since  $K$  has conductor  $\mathfrak{f}_K$ , this implies  $[K(\zeta_d) : \mathbb{Q}(\zeta_d)] = 1$  if  $\mathfrak{f}_K$  divides  $d$ , and  $[K(\zeta_d) : \mathbb{Q}(\zeta_d)] = n$  otherwise, noting that  $K$  is primitive. We can therefore easily evaluate the bound given in (2.10) as

$$c_K(g) \leq \sum_{\substack{1 \leq d < g, \text{ or} \\ d < 2g, d \text{ even} \\ \mathfrak{f}_K \nmid d}} n + \sum_{\substack{1 \leq d < g, \text{ or} \\ d < 2g, d \text{ even} \\ \mathfrak{f}_K \mid d}} 1 + 1 + n\pi(2g)$$

If  $\mathfrak{f}_K$  is odd, this evaluates to

$$c_K(g) \leq \frac{3gn}{2\mathfrak{f}_K} + \left(\frac{3}{2}g - \frac{3}{2}\frac{g}{\mathfrak{f}_K}\right) + 1 + n\pi(2g)$$

whilst if  $\mathfrak{f}_K$  is even, this yields

$$c_K(g) \leq \frac{2gn}{\mathfrak{f}_K} + \left(\frac{3}{2}g - \frac{2g}{\mathfrak{f}_K}\right) + 1 + n\pi(2g)$$

which proves the result.  $\square$

**Corollary 2.26.** *Let  $K$  be a number field such that its maximal abelian subfield is  $\mathbb{Q}$ . Then assuming Schinzel's hypothesis  $H$  for  $K$ , we have  $c_K(g) \leq \frac{3}{2}g + n\pi(2g)$ .*

*Proof.* The above condition implies that  $K \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$  for all  $d$ , and thus the bound given in (2.10) implies our result.  $\square$

Finally, it's worth mentioning that the bound given in (2.10) does not necessarily represent the optimal conditional bound for all genera  $g$ , even over  $\mathbb{Q}$ . For example, under the assumption of Schinzel's hypothesis  $H$ , there exist infinitely many integers  $k$  such that  $k, \alpha k - 1, \alpha k + 1, (\alpha k)^2 + 1, (\alpha k)^2 - 2(\alpha k) - 1$ , and  $(\alpha k)^2 - 2(\alpha k) + 1$  are all prime, where  $\alpha := 7!$ .

From this, one can therefore conditionally construct infinitely many genus 5 curves  $C/\mathbb{Q}$  of the form:

$$\begin{aligned} C_k : y^2 = & x \cdot (x - (\alpha k)^2(\alpha k - 1)(\alpha k + 1)) \cdot (x + (\alpha k)^2(\alpha k - 1)(\alpha k + 1)) \\ & \cdot (x - \alpha k(\alpha k - 1)(\alpha k + 1)) \cdot (x + \alpha k(\alpha k - 1)(\alpha k + 1)) \\ & \cdot (x - (\alpha k - 1)(\alpha k + 1)) \cdot (x + (\alpha k - 1)(\alpha k + 1)) \\ & \cdot (x - \alpha k(\alpha k - 1)^2) \cdot (x + \alpha k(\alpha k - 1)^2) \\ & \cdot (x - \alpha k(\alpha k + 1)^2) \cdot (x + \alpha k(\alpha k + 1)^2) \end{aligned}$$

which yields a conditional bound of  $c_{\mathbb{Q}}(5) \leq 10$ , and thus one better than the bound of 11 given by (2.10).

Besides the above example, we should mention however that we haven't found any better examples for higher genera over  $\mathbb{Q}$ , noting that a naive computational search quickly becomes unmanageable for large genus hyperelliptic curves.

# Chapter 3

## Elliptic and hyperelliptic curves over $\mathbb{Z}_\ell$ -cyclotomic extensions

Whilst Falting's proof laid the Shafarevich conjecture to rest for curves over number fields, one can ask whether Shafarevich holds over certain larger subfields of  $\overline{\mathbb{Q}}$ . In this chapter, we prove that an analogous version of the Shafarevich conjecture does not hold over  $\mathbb{Z}_\ell$ -cyclotomic extensions of number fields  $K$ . In particular, we show that the  $S$ -unit equation  $\varepsilon + \delta = 1$ , with  $\varepsilon, \delta \in \mathcal{O}_{\mathbb{Q}_{\infty, \ell}, S}^\times$  has infinitely many solutions for  $\ell \in \{2, 3, 5, 7\}$ , where  $S$  consists only of the totally ramified prime above  $\ell$ . We use this to give various explicit constructions of infinite families of elliptic and hyperelliptic curves defined over  $\mathbb{Q}_{\infty, \ell}$  with good reduction away from 2 and  $\ell$ .

This chapter was written jointly with Samir Siksek and has been published in *Algebra & Number Theory* [413]. Compared to both the preprint and published version, we have added some further remarks in Sections 3.4, 3.5 and 3.7, added a new Lemma 3.28 and added a new Section 3.10 investigating the possible endomorphism rings arising from our constructions.

Let  $\ell$  be a rational prime and  $r$  a positive integer. Write  $\mathbb{Q}_{r, \ell}$  for the unique degree  $\ell^r$  totally real subfield of  $\bigcup_{n=1}^\infty \mathbb{Q}(\mu_n)$ , where  $\mu_n$  denotes the set of  $\ell^n$ -th roots of 1. We let  $\mathbb{Q}_{\infty, \ell} = \bigcup_r \mathbb{Q}_{r, \ell}$ ; this is the  $\mathbb{Z}_\ell$ -cyclotomic extension of  $\mathbb{Q}$ , and  $\mathbb{Q}_{r, \ell}$  is called the  $r$ -th layer of  $\mathbb{Q}_{\infty, \ell}$ . Now let  $K$  be a number field, and write  $K_{\infty, \ell} = K \cdot \mathbb{Q}_{\infty, \ell}$  and  $K_{r, \ell} = K \cdot \mathbb{Q}_{r, \ell}$ . To ease notation we shall sometimes write  $K_\infty$  for  $K_{\infty, \ell}$ . We write  $\mathcal{O}_\infty$  (or  $\mathcal{O}_{\infty, \ell}$ ) for the integers in  $K_\infty$  (i.e. the integral closure of  $\mathbb{Z}$  in  $K_\infty$ ), and write  $\mathcal{O}_r$  (or  $\mathcal{O}_{r, \ell}$ ) for the integers of  $K_{r, \ell}$ . Clearly  $\mathcal{O}_{\infty, \ell} = \bigcup_r \mathcal{O}_{r, \ell}$ . The motivation for this chapter is a series of conjectures and theorems that suggest that the arithmetic of curves (respectively abelian varieties) over  $K_\infty$  is similar to the arithmetic of curves (respectively abelian varieties) over  $K$ . One of these is the following conjecture of

Mazur [309], which in essence says that the Mordell–Weil theorem continues to hold over  $K_\infty$ .

**Conjecture** (Mazur). *Let  $A/K_\infty$  be an abelian variety. Then  $A(K_\infty)$  is finitely generated.*

Another is a conjecture of Parshin and Zarhin [489, page 91] which is the analogue of Faltings’ theorem (Mordell conjecture) over  $K_\infty$ .

**Conjecture** (Parshin and Zarhin). *Let  $X/K_\infty$  be a curve of genus  $\geq 2$ . Then  $X(K_\infty)$  is finite.*

A third is the following theorem of Zarhin [490, Corollary 4.2], which asserts that the Tate homomorphism conjecture (also a theorem of Faltings [164] over number fields) continues to hold over  $K_\infty$ .

**Theorem** (Zarhin). *Let  $A, B$  be abelian varieties defined over  $K_{\infty,\ell}$ , and denote their respective  $\ell$ -adic Tate modules by  $T_\ell(A), T_\ell(B)$ . Then the natural embedding*

$$\mathrm{Hom}_{K_\infty}(A, B) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{K_\infty}/K_\infty)}(T_\ell(A), T_\ell(B))$$

*is a bijection.*

Mazur’s conjecture is now known to hold for certain elliptic curves. For example, if  $E$  is an elliptic curve defined over  $\mathbb{Q}$  then  $E(\mathbb{Q}_\infty)$  is finitely generated thanks to theorems of Kato, Ribet and Rohrlich [200, Theorem 1.5]. From this one can deduce [200, Theorem 1.24] that  $X(\mathbb{Q}_\infty)$  is finite for curves  $X/\mathbb{Q}$  of genus  $\geq 2$  equipped with a non-constant morphism to an elliptic curve  $X \rightarrow E$  defined over  $\mathbb{Q}$ . We also note that the conjecture of Parshin and Zarhin follows easily from Mazur’s conjecture and Faltings’ theorem. Indeed, using the Abel–Jacobi map we can deduce from Mazur’s conjecture that  $X(K_\infty) = X(K_r)$  for suitably large  $r$ , and we know that  $X(K_r)$  is finite by Faltings’ theorem.

It is natural to wonder whether other standard conjectures and theorems concerning the arithmetic of curves and abelian varieties over number fields continue to hold over  $K_\infty$ . The purpose of this chapter is to give counterexamples to potential generalizations of certain theorems of Siegel–Mahler and Shafarevich to  $K_\infty$ . A classical theorem of Siegel [409] and Mahler [295] (e.g. see [1, Theorem 0.2.8]) asserts that  $(\mathbb{P}^1 \setminus \{0, 1, \infty\})(\mathcal{O}_{K,S})$  is finite for any number field  $K$  and any finite set of primes  $S$  (modern proofs can be found in [265], [280], [353]).

We show that the corresponding statement over  $\mathbb{Q}_{\infty,\ell}$  is false, at least for  $\ell = 2, 3, 5, 7$ . We denote by  $v_\ell$  the totally ramified prime of  $\mathbb{Q}_{\infty,\ell}$  above  $\ell$  (the precise meaning of primes in infinite extensions of  $\mathbb{Q}$  is clarified in Section 3.1).

**Theorem 3.1.** *Let  $\ell = 2, 3, 5$  or  $7$ . Let*

$$S = \begin{cases} \{v_\ell\} & \text{if } \ell = 2, 5, 7 \\ \emptyset & \text{if } \ell = 3. \end{cases} \quad (3.1)$$

*Let  $\mathcal{O}_S$  denote the  $S$ -integers of  $\mathbb{Q}_{\infty, \ell}$ . Then  $(\mathbb{P}^1 \setminus \{0, 1, \infty\})(\mathcal{O}_S)$  is infinite.*

**Remarks.**

- There have been several recent papers showing that  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$  and other punctured curves have no or few integral points over various infinite families of number fields e.g. [182], [183], [184], [412], [452]. In particular, it is shown in [182] that  $(\mathbb{P}^1 \setminus \{0, 1, \infty\})(\mathcal{O}_\infty) = \emptyset$  for  $\ell \neq 3$ . The obstruction given in [182] for  $\ell \neq 3$  is local in nature. In essence, Theorem 3.1 complements this result, showing that we can obtain infinitely many integral or  $S$ -integral points in the absence of the local obstruction. The proof of Theorem 3.1 is constructive.
- Theorem 3.1 strongly suggests that the conjecture of Parshin and Zarhin does not admit a straightforward generalization to the broader context of integral points on hyperbolic curves. We also remark that there is a critical difference over  $K_\infty$  between complete curves  $X$  of genus  $\geq 2$  and  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ . For the former, the group of  $K_\infty$ -points of the Jacobian is expected to be finitely generated by Mazur's conjecture. For the latter, the analogue of the Jacobian is the generalized Jacobian which is  $\mathbb{G}_m \times \mathbb{G}_m$ , and its group of  $K_\infty$ -points is  $(\mathbb{G}_m \times \mathbb{G}_m)(K_\infty) = \mathcal{O}_\infty^\times \times \mathcal{O}_\infty^\times$ , which is infinitely generated.

Variants of the proof of Theorem 3.1 give the following.

**Theorem 3.2.** *Let  $\ell = 2, 3$  or  $5$ . Let  $S = \{v_\ell\}$  and write  $\mathcal{O}_S$  for the  $S$ -integers of  $\mathbb{Q}_{\infty, \ell}$ . Let*

$$k \in \begin{cases} \{1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 24\} & \text{if } \ell = 2, 3, \\ \{1, 2, 4\} & \text{if } \ell = 5. \end{cases}$$

*Then  $(\mathbb{P}^1 \setminus \{0, k, \infty\})(\mathcal{O}_S)$  is infinite.*

Let  $\zeta_{\ell^n}$  denote a primitive  $\ell^n$ -th root of 1, and write  $\Omega_{n, \ell} = \mathbb{Q}(\zeta_{\ell^n})$ , and  $\Omega_{n, \ell}^+ = \mathbb{Q}(\zeta_{\ell^n} + \zeta_{\ell^n}^{-1})$ . Let

$$\Omega_{\infty, \ell} = \bigcup_{n=1}^{\infty} \Omega_{n, \ell}, \quad \Omega_{\infty, \ell}^+ = \bigcup_{n=1}^{\infty} \Omega_{n, \ell}^+.$$



We note the inclusions  $\Omega_{\infty,\ell} \supset \Omega_{\infty,\ell}^+ \supset \mathbb{Q}_{\infty,\ell}$ . Nagell [328, page 181] points out that  $1 + \zeta_{\ell^n}$  is a unit for  $\ell$  odd, and that therefore the equation  $\varepsilon + \delta = 1$  has the solution  $\varepsilon = -\zeta_{\ell^n}$ ,  $\delta = 1 + \zeta_{\ell^n}$  in units belonging to  $\Omega_{\infty,\ell}$ . It follows straightforwardly from this (see the beginning of Section 3.2) that  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$  has infinitely many integral points defined over  $\Omega_{\infty,\ell}$ . Many of our constructions of  $S$ -integral points on  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$  apply in greater generality to the fields  $\Omega_{\infty,\ell}$  and  $\Omega_{\infty,\ell}^+$ , where the statements are in fact much cleaner. For example, we prove the following theorem.

**Theorem 3.3.** *Let  $\ell$  be an odd prime. Then  $(\mathbb{P}^1 \setminus \{0, 1, \infty\})(\mathcal{O}(\Omega_{\infty,\ell}^+))$  is infinite.*

Here  $\mathcal{O}(\Omega_{\infty,\ell}^+)$  denotes the integers of  $\Omega_{\infty,\ell}^+$ .

Shafarevich's conjecture asserts that for a number field  $K$ , a dimension  $n$ , a degree  $d$ , and a finite set of places  $S$ , there are only finitely many isomorphism classes of polarized abelian varieties defined over  $K$  of dimension  $n$  with degree  $d$  polarization and with good reduction away from  $S$ . This conjecture was proved by Shafarevich for elliptic curves (i.e.  $n = 1$ ) and by Faltings [164] in complete generality. If we replace  $K$  by  $\mathbb{Q}_{\infty,\ell}$  then the Shafarevich conjecture no longer holds. For example, consider

$$E_\varepsilon : \varepsilon Y^2 = X^3 - X$$

where  $\varepsilon \in \mathcal{O}_\infty^\times$ . This elliptic curve has good reduction away from the primes above 2. Moreover,  $E_\varepsilon, E_\delta$  are isomorphic over  $\mathbb{Q}_\infty$  if and only if  $\varepsilon/\delta$  is a square in  $\mathcal{O}_\infty^\times$ . As  $\mathcal{O}_\infty^\times/(\mathcal{O}_\infty^\times)^2$  is infinite, we deduce that there are infinitely many isomorphism classes of elliptic curves over  $\mathbb{Q}_\infty$  with good reduction away from the primes above 2. It is however natural to wonder if a sufficiently weakened version of the Shafarevich conjecture continues to hold over  $\mathbb{Q}_\infty$ . Indeed, the curves  $E_\varepsilon$  in the above construction form a single  $\overline{\mathbb{Q}}$ -isomorphism class. Thus it is natural to ask if, for suitable  $\ell$  and finite set of primes  $S$ , the set of elliptic curves over  $\mathbb{Q}_\infty$  with good reduction outside  $S$  form infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes?

**Theorem 3.4.** *Let  $\ell = 2, 3, 5$ , or  $7$ . Let  $S$  be given by (3.1) and let  $S' = S \cup \{v_2\}$  where  $v_2$  is the unique prime of  $\mathbb{Q}_{\infty,\ell}$  above 2. Then, there are infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves defined over  $\mathbb{Q}_{\infty,\ell}$  with good reduction away from  $S'$  and with full 2-torsion in  $\mathbb{Q}_{\infty,\ell}$ . Moreover, these elliptic curves form infinitely many distinct  $\mathbb{Q}_{\infty,\ell}$ -isogeny classes.*

## Remarks

- By [182, Lemma 2.1], a rational prime  $p \neq \ell$  is inert in  $\mathbb{Q}_{\infty,\ell}$  if and only if  $p^{\ell-1} \not\equiv 1 \pmod{\ell^2}$ . It follows from this that 2 is inert in  $\mathbb{Q}_{\infty,\ell}$  for  $\ell = 3, 5, 7$

and 11.

- Faltings' proof [164] of the Mordell conjecture can be considered to have three major steps. In the first step, Faltings proves the Tate homomorphism conjecture. In the second step, Faltings derives the Shafarevich conjecture from the Tate homomorphism conjecture, and in the final step Faltings uses the 'Parshin trick' to deduce the Mordell conjecture from the Shafarevich conjecture. Although Zarhin has extended the Tate homomorphism conjecture to  $K_\infty$ , Theorem 3.4 suggests that there is no plausible strategy for proving the conjecture of Parshin and Zarhin by mimicking Faltings' proof of the Mordell conjecture.

It is natural to wonder if the isogeny classes appearing in the proof of Theorem 3.4 are finite or infinite. Rather reassuringly they turn out to be finite.

**Theorem 3.5.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}_{\infty,\ell}$  without potential complex multiplication. Then the  $\mathbb{Q}_{\infty,\ell}$ -isogeny class of  $E$  is finite.*

The original version of Shafarevich's conjecture [473], (also proved by Faltings [164, Korollar 1]) states that for a given number field  $K$ , a genus  $g$  and a finite set of places  $S$ , there are only finitely many isomorphism classes of genus  $g$  curves  $C/K$  with good reduction away from  $S$ . Again this statement becomes false if we replace  $K$  by  $\mathbb{Q}_{\infty,\ell}$ , for any prime  $\ell$ .

**Theorem 3.6.** *Let  $g \geq 2$  and let  $\ell = 3, 5, 7, 11$  or  $13$ . There are infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes of genus  $g$  hyperelliptic curves over  $\mathbb{Q}_{\infty,\ell}$  with good reduction away from  $\{v_2, v_\ell\}$ .*

**Theorem 3.7.** *Let  $\ell \geq 11$  be an odd prime and let  $g = \lfloor \frac{\ell-3}{4} \rfloor$ . There are infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes of genus  $g$  hyperelliptic curves over  $\mathbb{Q}_{\infty,\ell}$  with good reduction away from  $\{v_2, v_\ell\}$ . Moreover, if*

$$\ell \in \{11, 23, 59, 107, 167, 263, 347, 359\},$$

*then the Jacobians of these curves form infinitely many distinct  $\mathbb{Q}_{\infty,\ell}$ -isogeny classes.*

The chapter is structured as follows. In Section 3.1 we recall basic results on units and  $S$ -units of the cyclotomic field  $\mathbb{Q}(\zeta_{\ell^n})$ . In Sections 3.2–3.5 we employ identities between cyclotomic polynomials to give constructive proofs of Theorems 3.1, 3.2

and 3.3. Section 3.6 gives a proof of Theorem 3.5, making use of a deep theorem of Kato to control the  $\mathbb{Q}_{\infty, \ell}$ -points on certain modular curves. Section 3.7 uses the integral and  $S$ -integral points on  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$  furnished by Theorem 3.1 to construct infinite families of elliptic curves over  $\mathbb{Q}_{\infty, \ell}$  for  $\ell = 2, 3, 5, 7$ , with good reduction away from  $\{v_2, v_\ell\}$ , which are used to give a proof of Theorem 3.4. Sections 3.8 and 3.9 give proofs of Theorems 3.6 and 3.7, making use of the relation, due to Kummer, between the class number of  $\mathbb{Q}(\zeta_{\ell^n})^+$ , and the index of cyclotomic units in the full group of units.

We are grateful to Minhyong Kim for drawing our attention to the conjecture of Parshin and Zarhin, and to Alain Kraus and David Loeffler for useful discussions. We thank the referee for many useful comments.

### 3.1 Units and $S$ -units of $\mathbb{Q}(\zeta)$

Let  $K$  be a subfield of  $\overline{\mathbb{Q}}$ . We denote the integers of  $K$  (i.e. the integral closure of  $\mathbb{Z}$  in  $K$ ) by  $\mathcal{O}(K)$ . Let  $p$  be a rational prime. By a **prime of  $K$  above  $p$**  we mean a map  $v : K \rightarrow \mathbb{Q} \cup \{\infty\}$  satisfying the following

- $v(p) = 1, v(0) = \infty$ ;
- $v|_{K^\times} : K^\times \rightarrow \mathbb{Q}$  is a homomorphism;
- $v(1+b) = 0$  whenever  $v(b) > 0$ .

Suppose  $K = \cup K_n$  where  $K_0 \subset K_1 \subset K_2 \subset \dots$  is a tower of number fields (i.e. finite extensions of  $\mathbb{Q}$ ), with  $K_0 = \mathbb{Q}$ . One sees that the primes of  $K$  above  $p$  are in 1–1 correspondence with sequences  $\{\mathfrak{p}_n\}$  where

- $\mathfrak{p}_n$  is a prime ideal of  $\mathcal{O}(K_n)$ ;
- $\mathfrak{p}_{n+1} \mid \mathfrak{p}_n \mathcal{O}(K_{n+1})$ ;
- $\mathfrak{p}_0 = p\mathbb{Z}$ .

Indeed, from  $v$  one obtains the corresponding sequence  $\{\mathfrak{p}_n\}$  via the formula  $\mathfrak{p}_n = \{\alpha \in \mathcal{O}(K_n) : v(\alpha) > 0\}$ . Given a sequence  $\{\mathfrak{p}_n\}$ , we can recover the corresponding  $v$  by letting

$$v(\alpha) = \text{ord}_{\mathfrak{p}_n}(\alpha) / \text{ord}_{\mathfrak{p}_n}(p)$$

whenever  $\alpha \in K_n^\times$ . Given a finite set of primes  $S$  of  $K$ , we define the  $S$ -integers of  $K$  to be the set  $\mathcal{O}(K, S)$  of all  $\alpha \in K$  such that  $v(\alpha) \geq 0$  for every prime  $v \notin S$ .

We let  $\mathcal{O}(K, S)^\times$  be the unit group of  $\mathcal{O}(K, S)$ ; this is precisely the set of  $\alpha \in K^\times$  such that  $v(\alpha) = 0$  for every prime  $v \notin S$ . If  $S = \emptyset$  then  $\mathcal{O}(K, S) = \mathcal{O}(K)$  are the integers of  $K$  and  $\mathcal{O}(K, S)^\times = \mathcal{O}(K)^\times$  are the units of  $K$ .

Fix a rational prime  $\ell$ . For a positive integer  $n$ , let  $\zeta_{\ell^n}$  denote a primitive  $\ell^n$ -th root of 1 which is chosen so that

$$\zeta_{\ell^{n+1}}^\ell = \zeta_{\ell^n}.$$

Let  $\Omega_{n,\ell} = \mathbb{Q}(\zeta_{\ell^n})$ ; this has degree  $\varphi(\ell^n)$  where  $\varphi$  is the Euler totient function. Let

$$\Omega_{\infty,\ell} = \bigcup_{n=1}^{\infty} \Omega_{n,\ell}.$$

The prime  $\ell$  is totally ramified in each  $\Omega_{n,\ell}$ , and we denote by  $\lambda_n$  the unique prime ideal of  $\mathcal{O}(\Omega_{n,\ell})$  above  $\ell$ . Thus

$$\ell \cdot \mathcal{O}(\Omega_{n,\ell}) = \lambda_n^{\varphi(\ell^n)}. \quad (3.2)$$

We write  $v_\ell$  for the unique prime of  $\Omega_{\infty,\ell}$  above  $\ell$ . For now fix  $n \geq 1$  if  $\ell \neq 2$  and  $n \geq 2$  if  $\ell = 2$ . We recall that  $\lambda_n = (1 - \zeta_{\ell^n}) \cdot \mathcal{O}(\Omega_{n,\ell})$ . If  $\ell \nmid s$  then  $(1 - \zeta_{\ell^n}^s) \cdot \mathcal{O}(\Omega_{n,\ell}) = \lambda_n$ ; we can see this by applying the automorphism  $\zeta_{\ell^n} \mapsto \zeta_{\ell^n}^s$  to (3.2).

**Lemma 3.8.** *Let  $s$  be an integer and let  $t = \text{ord}_\ell(s)$ . Suppose  $t < n$ . Then*

$$(1 - \zeta_{\ell^n}^s) \cdot \mathcal{O}(\Omega_{n,\ell}) = \lambda_n^{\ell^t}.$$

Moreover,

$$v_\ell(1 - \zeta_{\ell^n}^s) = \frac{1}{\ell^{n-1-t}(\ell-1)}.$$

*Proof.* Write  $\zeta = \zeta_{\ell^n}$ . Note that  $\zeta^s$  is a primitive  $\ell^{n-t}$ -th root of 1. Thus

$$(1 - \zeta^s) \cdot \mathcal{O}(\Omega_{n-t,\ell}) = \lambda_{n-t}.$$

As  $\ell$  is totally ramified in  $\Omega_{n,\ell}$ , we have

$$(1 - \zeta^s) \cdot \mathcal{O}(\Omega_{n,\ell}) = \lambda_n^{[\Omega_{n,\ell} : \Omega_{n-t,\ell}]} = \lambda_n^{\ell^t}.$$

For the final part of the lemma,

$$v_\ell(1 - \zeta^s) = \frac{\text{ord}_{\lambda_n}(1 - \zeta^s)}{\text{ord}_{\lambda_n}(\ell)} = \frac{\ell^t}{\varphi(\ell^n)} = \frac{1}{\ell^{n-1-t}(\ell-1)}.$$

□

### 3.1.1 Cyclotomic units and $S$ -units

Write  $V_n$  for the subgroup of  $\mathcal{O}(\Omega_n, \{v_\ell\})^\times$  generated by

$$\left\{ \pm \zeta_{\ell^n}, \quad 1 - \zeta_{\ell^n}^k : 1 \leq k < \ell^n \right\}$$

and let

$$C_n = V_n \cap \mathcal{O}(\Omega_n)^\times.$$

The group  $C_n$  is called [475, Chapter 8] the group of **cyclotomic units** in  $\Omega_n$ . We will often find it more convenient to work with the group  $V_n$ .

**Lemma 3.9.** *The abelian group  $V_n / \langle \pm \zeta_{\ell^n} \rangle$  is free with basis*

$$\left\{ 1 - \zeta_{\ell^n}^k : 1 \leq k < \ell^n/2, \quad \ell \nmid k \right\}. \quad (3.3)$$

*Proof.* The torsion subgroup of  $V_n$  is the torsion subgroup of  $\Omega_n^\times$  which is  $\langle \pm \zeta_{\ell^n} \rangle$ . Thus  $V_n / \langle \pm \zeta_{\ell^n} \rangle$  is torsion free. By definition of  $V_n$ , the group  $V_n / \langle \pm \zeta_{\ell^n} \rangle$  is generated by  $1 - \zeta_{\ell^n}^k$  with  $\ell^n \nmid k$ . Write  $k = \ell^r d$  with  $\ell \nmid d$ ; thus  $r < n$ . Suppose  $r \geq 1$ . Then,

$$\begin{aligned} 1 - \zeta_{\ell^n}^k &= 1 - \zeta_{\ell^n}^{\ell^r d} \\ &= \prod_{i=0}^{\ell^r-1} (1 - \zeta_{\ell^n}^d \zeta_{\ell^r}^i) \quad \text{using } 1 - X^{\ell^r} = \prod_{i=0}^{\ell^r-1} (1 - \zeta_{\ell^r}^i X) \\ &= \prod_{i=0}^{\ell^r-1} (1 - \zeta_{\ell^n}^{d+i\ell^{n-r}}). \end{aligned}$$

It follows that  $V_n / \langle \pm \zeta_{\ell^n} \rangle$  is generated by  $1 - \zeta_{\ell^n}^k$  with  $\ell \nmid k$ . If  $\ell^n/2 < k < \ell^n$  and  $\ell \nmid k$  then

$$1 - \zeta_{\ell^n}^k = -\zeta_{\ell^n}^k (1 - \zeta_{\ell^n}^{\ell^n-k}). \quad (3.4)$$

Thus (3.3) certainly generates  $V_n / \langle \pm \zeta_{\ell^n} \rangle$ . Note that (3.3) has cardinality  $\varphi(\ell^n)/2$  where  $\varphi$  is the Euler totient function. It therefore suffices to show that  $V_n$  has rank  $\varphi(\ell^n)/2$ . A well-known theorem [475, Theorem 8.3] states that  $C_n$  has finite index in  $\mathcal{O}(\Omega_n)^\times$  and thus, by Dirichlet's unit theorem,  $C_n$  has rank  $-1 + \varphi(\ell^n)/2$ . We note that  $C_n$  is the kernel of the surjective homomorphism  $V_n \rightarrow \mathbb{Z}$ , sending  $\mu$  to  $\text{ord}_{\lambda_n}(\mu)$ . Thus  $V_n$  has rank  $\varphi(\ell^n)/2$  completing the proof. □

**Lemma 3.10.** *Let  $n \geq 2$  if  $\ell \neq 2$  and  $n \geq 3$  if  $\ell = 2$ . Then  $V_{n-1} \subset V_n$ . Moreover,*

$$\prod_{\substack{1 \leq k < \ell^n/2 \\ \ell \nmid k}} (1 - \zeta_{\ell^n}^k)^{c_k} \in \langle \pm \zeta_{\ell^n}, V_{n-1} \rangle$$

*if and only if  $c_k = c_m$  whenever  $k \equiv m \pmod{\ell^{n-1}}$ .*

*Proof.* The group  $V_{n-1}$  is generated, modulo roots of unity, by  $1 - \zeta_{\ell^{n-1}}^d$  with  $\ell \nmid d$ . By the proof of Lemma 3.9,

$$1 - \zeta_{\ell^{n-1}}^d = 1 - \zeta_{\ell^n}^{\ell d} = \prod_{i=0}^{\ell-1} (1 - \zeta_{\ell^n}^{d+i\ell^{n-1}}).$$

The lemma follows from Lemma 3.9.  $\square$

Given  $a \in \mathbb{Z}_\ell$ , it makes sense to reduce  $a$  modulo  $\ell^n$  and therefore it makes sense to write  $\zeta_{\ell^n}^a$ . We write  $\{a\}_n$  for the unique integer satisfying

$$0 \leq \{a\}_n < \ell^n/2, \quad \{a\}_n \equiv \pm a \pmod{\ell^n}.$$

**Lemma 3.11.** *Let  $a_1, \dots, a_r \in \mathbb{Z}_\ell$  and  $c_1, \dots, c_r \in \mathbb{Z}$ . Suppose*

- (i)  $c_1 \neq 0$ .
- (ii)  $a_1 \not\equiv 0 \pmod{\ell}$ .
- (iii)  $a_1 \not\equiv \pm a_2, \pm a_3, \dots, \pm a_r \pmod{\ell^n}$ .

*Write*

$$\varepsilon_n = \prod_{1 \leq i \leq r} (1 - \zeta_{\ell^n}^{a_i})^{c_i}. \quad (3.5)$$

*Then,  $\varepsilon_n \notin \langle \pm \zeta_{\ell^n}, V_{n-1} \rangle$  for all sufficiently large  $n$ .*

*Proof.* If  $a_j \equiv 0 \pmod{\ell}$  then  $(1 - \zeta_{\ell^n}^{a_j}) \in V_{n-1}$ . We may therefore suppose  $a_j \not\equiv 0 \pmod{\ell}$  for all  $j$ . Write

$$\delta_n = \prod_{1 \leq i \leq r} \left(1 - \zeta_{\ell^n}^{\{a_i\}_n}\right)^{c_i}.$$

In view of the identity (3.4) it will be sufficient to show that  $\delta_n \notin \langle \pm \zeta_{\ell^n}, V_{n-1} \rangle$  for  $n$  sufficiently large. Also, in view of Lemma 3.10, it is sufficient to show for sufficiently large  $n$  that  $\{a_1\}_n \not\equiv \{a_j\}_n \pmod{\ell^n}$  for all  $2 \leq j \leq r$ . This is equivalent to  $a_1 \not\equiv \pm a_j$  for  $2 \leq j \leq r$  which is hypothesis (iii). This completes the proof.  $\square$

The following corollary easily follows from Lemma 3.11.

**Corollary 3.12.** *Let  $a_1, \dots, a_r \in \mathbb{Z}_\ell$  and  $c_1, \dots, c_r \in \mathbb{Z}$ . Suppose*

$$(i) \quad c_1 \equiv 1 \pmod{2}.$$

$$(ii) \quad a_1 \not\equiv 0 \pmod{\ell}.$$

$$(iii) \quad a_1 \not\equiv \pm a_2, \pm a_3, \dots, \pm a_r \pmod{\ell^n}.$$

*Let  $\varepsilon_n$  be as in (3.5). Then,  $\varepsilon_n \notin \langle \pm \zeta_{\ell^n}, V_{n-1}, V_n^2 \rangle$  for all sufficiently large  $n$ .*

### 3.1.2 Units and $S$ -units from cyclotomic polynomials

For  $m \geq 1$ , let  $\Phi_m(X) \in \mathbb{Z}[X]$  be the  $m$ -th cyclotomic polynomial defined by

$$\Phi_m(X) = \prod_{\substack{1 \leq i \leq m \\ (i, m) = 1}} (X - \zeta_m^i).$$

These satisfy the identity [475, Chapter 2]

$$X^m - 1 = \prod_{d|m} \Phi_d(X). \quad (3.6)$$

It follows from the Möbius inversion formula that

$$\Phi_m(X) = \prod_{d|m} (X^d - 1)^{\mu(m/d)} \quad (3.7)$$

where  $\mu$  denotes the Möbius function.

**Lemma 3.13.** *Let  $\ell$  be a prime and  $n \geq 1$ . Let  $m \geq 1$ , and suppose  $\ell^n \nmid m$ .*

$$(a) \quad \Phi_m(\zeta_{\ell^n}) \in V_n \subseteq \mathcal{O}(\Omega_{n,\ell}, S)^\times, \text{ where } S = \{v_\ell\}.$$

$$(b) \quad \text{If } m \neq \ell^u \text{ for all } u \geq 0, \text{ then } \Phi_m(\zeta_{\ell^n}) \in C_n \subseteq \mathcal{O}(\Omega_{n,\ell})^\times.$$

Moreover,

$$v_\ell(\Phi_{\ell^t}(\zeta_{\ell^n})) = \begin{cases} \frac{1}{\ell^{n-1}(\ell-1)} & t = 0 \\ \frac{1}{\ell^{n-t}} & 1 \leq t \leq n-1. \end{cases}$$

*Proof.* Let  $t = \text{ord}_\ell(m) < n$ . Observe that  $\Phi_m(X) \mid (X^m - 1)$ . Hence  $\Phi_m(\zeta_{\ell^n}) \cdot \mathcal{O}(\Omega_{n,\ell})$  divides  $(1 - \zeta_{\ell^n}^m) \cdot \mathcal{O}(\Omega_{n,\ell})$ . By Lemma 3.8 we have  $(1 - \zeta_{\ell^n}^m) \cdot \mathcal{O}(\Omega_{n,\ell}) = \lambda_n^{\ell^t}$ , giving (a).

For (b), write  $m = \ell^t k$  where  $k > 1$ . Then  $\Phi_m(X)$  divides the polynomial  $(X^m - 1)/(X^{\ell^t} - 1)$ . Therefore  $\Phi_m(\zeta_{\ell^n}) \cdot \mathcal{O}(\Omega_{n,\ell})$  divides

$$\frac{(1 - \zeta_{\ell^n}^m)}{(1 - \zeta_{\ell^n}^{\ell^t})} \cdot \mathcal{O}(\Omega_{n,\ell}) = \frac{\lambda_n^{\ell^t}}{\lambda_n^{\ell^t}} = 1 \cdot \mathcal{O}(\Omega_{n,\ell}).$$

Thus  $\Phi_m(\zeta_{\ell^n})$  is a unit, giving (b).

The final part of the Lemma follows from Lemma 3.8, and the formulae

$$\Phi_{\ell^t}(X) = \begin{cases} X - 1 & t = 0 \\ (X^{\ell^t} - 1)/(X^{\ell^{t-1}} - 1) & t \geq 1. \end{cases}$$

□

**Lemma 3.14.** *Let  $n \geq 2$  if  $\ell \neq 2$  and  $n \geq 3$  if  $\ell = 2$ . Then  $V_n/\langle \pm \zeta_{\ell^n} \rangle$  is free with basis*

$$\{\Phi_m(\zeta_{\ell^n}) : 1 \leq m < \ell^n/2, \ell \nmid m\}.$$

*Proof.* This follows from Lemma 3.9 thanks to identities (3.6) and (3.7). □

### 3.2 The $S$ -unit equation over $\mathbb{Q}(\zeta_{\ell^n})^+$

We continue with the notation of the previous section. In particular, let  $K$  be a subfield of  $\overline{\mathbb{Q}}$  and  $S$  be a finite set of primes of  $K$ . Let  $k$  be a non-zero rational integer. We shall make frequent use of the correspondence between elements of  $(\mathbb{P}^1 \setminus \{0, k, \infty\})(\mathcal{O}(K, S))$  and the set of solutions to the  $S$ -unit equation

$$\varepsilon + \delta = k, \quad \varepsilon, \delta \in \mathcal{O}(K, S)^\times,$$

sending  $\varepsilon \in (\mathbb{P}^1 \setminus \{0, k, \infty\})(\mathcal{O}(K, S))$  to  $(\varepsilon, \delta) = (\varepsilon, k - \varepsilon)$ .

Now, as before, let  $\ell$  be a rational prime and  $n$  a positive integer. If  $\ell = 2$  suppose  $n \geq 2$ . Let  $\zeta = \zeta_{\ell^n}$ , and write  $\Omega_{n,\ell}^+ = \mathbb{Q}(\zeta + 1/\zeta)$  for the index 2 totally real subfield of  $\Omega_{n,\ell}$ . Let

$$\Omega_{\infty,\ell}^+ = \bigcup_{n=1}^{\infty} \Omega_{n,\ell}^+.$$

In this section, for suitable  $S$ , we produce solutions to  $S$ -unit equations over  $\Omega_{\infty,\ell}^+$ .

As before,  $\Phi_m$  denotes the  $m$ -th cyclotomic polynomial. It is convenient to record the first few  $\Phi_m$ :

$$\Phi_1 = X - 1, \quad \Phi_2 = X + 1, \quad \Phi_3 = X^2 + X + 1,$$



$$\begin{aligned}
\Phi_4 &= X^2 + 1, & \Phi_5 &= X^4 + X^3 + X^2 + X + 1, \\
\Phi_6 &= X^2 - X + 1, & \Phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, \\
\Phi_8 &= X^4 + 1, & \Phi_9 &= X^6 + X^3 + 1, & \Phi_{10} &= X^4 - X^3 + X^2 - X + 1.
\end{aligned}$$

A monic polynomial  $F \in \mathbb{Z}[X]$  having all their roots in the unit disc is called a **Kronecker polynomial**. These were studied by Kronecker [271] who proved that such polynomials have all their non-zero roots on the unit circle. Damianou [128] further proved that all Kronecker polynomials are of the form  $X^m f_1 f_2 \cdots f_k$  where each  $f_i(X)$  is a cyclotomic polynomial.

We know, thanks to Lemma 3.13, that if  $F$  is Kronecker and  $\ell$  is a prime, then  $F(\zeta_{\ell^n}) \in \mathcal{O}(\Omega_n, \{v_\ell\})^\times$  for  $n$  sufficiently large. We wrote a short computer program that lists all Kronecker polynomials of degree at most 20 and searches for ternary relations of the form  $F - G = kH$  with  $F, G, H$  Kronecker,  $\gcd(F, G, H) = 1$  and  $k$  is a positive integer. Note that any such relation  $F - G = kH$  gives points  $\varepsilon_n = F(\zeta_{\ell^n})/H(\zeta_{\ell^n}) \in (\mathbb{P}^1 \setminus \{0, k, \infty\})(\mathcal{O}(\Omega_n, \{v_\ell\}))$ , for  $n$  sufficiently large. We found the following ternary relations between Kronecker polynomials.

$$\Phi_2(X)^2 - \Phi_3(X) = X; \quad (3.8)$$

$$\Phi_2(X)^2 - \Phi_4(X) = 2X; \quad (3.9)$$

$$\Phi_2(X)^2 - \Phi_6(X) = 3X; \quad (3.10)$$

$$\Phi_2(X)^2 - \Phi_1(X)^2 = 4X; \quad (3.11)$$

$$\Phi_2(X)^4 - \Phi_{10}(X) = 5X\Phi_3(X); \quad (3.12)$$

$$\Phi_2^2(X)\Phi_3(X) - \Phi_1(X)^2\Phi_6(X) = 6X\Phi_4(X); \quad (3.13)$$

$$\Phi_7(X) - \Phi_1(X)^6 = 7X\Phi_6(X)^2; \quad (3.14)$$

$$\Phi_2(X)^4 - \Phi_1(X)^4 = 8X\Phi_4(X); \quad (3.15)$$

$$\Phi_2(X)^4\Phi_5(X) - \Phi_1(X)^4\Phi_{10}(X) = 10X\Phi_4(X)^3. \quad (3.16)$$

From the identities (3.6) and (3.7) one easily sees that  $F(X^k)$  is Kronecker for any Kronecker polynomial  $F$  and any positive integer  $k$ , thus each of the nine identities above in fact yields an infinite family of identities. We pose the following open problems:

- Are there ternary linear relations  $F - G = kH$  between Kronecker polynomials for values of  $k$  not equal to 1, 2, 3, 4, 5, 6, 7, 8, or 10?
- Classify all ternary linear relations between Kronecker polynomials.

**Lemma 3.15.** *Let  $c : \Omega_\ell \rightarrow \Omega_\ell$  denote complex conjugation. Let  $n \geq 1$  and let  $\zeta = \zeta_{\ell^n}$  be an  $\ell^n$ -th root of 1. Let  $m \geq 1$  and suppose  $\ell^n \nmid m$ . Then*

$$\frac{\Phi_m(\zeta)^c}{\Phi_m(\zeta)} = \begin{cases} \zeta^{-\varphi(m)} & m \geq 2 \\ -\zeta^{-1} & m = 1. \end{cases}$$

*Proof.* Note that  $\zeta^c = \zeta^{-1}$ . So

$$\frac{\Phi_1(\zeta)^c}{\Phi_1(\zeta)} = \frac{\zeta^{-1} - 1}{\zeta - 1} = -\zeta^{-1}, \quad \frac{\Phi_2(\zeta)^c}{\Phi_2(\zeta)} = \frac{\zeta^{-1} + 1}{\zeta + 1} = \zeta^{-1}.$$

Let  $m \geq 3$ . The polynomial  $\Phi_m$  is monic of degree  $\varphi(m)$ , and its roots are the primitive  $m$ -th roots of 1 which come in distinct pairs  $\eta, \eta^{-1}$ . Thus the trailing coefficient is 1. It follows that  $X^{\varphi(m)}\Phi_m(X^{-1})$  is monic and has the same roots as  $\Phi_m$ , therefore

$$\Phi_m(X) = X^{\varphi(m)}\Phi_m(X^{-1}).$$

Hence

$$\frac{\Phi_m(\zeta)^c}{\Phi_m(\zeta)} = \frac{\Phi_m(\zeta^{-1})}{\Phi_m(\zeta)} = \zeta^{-\varphi(m)}.$$

□

**Lemma 3.16.** *Let  $\ell$  be a prime. Let  $F \in \mathbb{Z}[X]$  be a product of powers of cyclotomic polynomials. Suppose that the exponents of  $\Phi_1(X)$  and  $\Phi_2(X)$  in the factorization of  $F$  are both even. Then  $F$  has even degree and, for suitably large  $n$ , we have*

$$\zeta^{-\deg(F)/2}F(\zeta) \in \mathcal{O}(\Omega_{n,\ell}^+, S)^\times$$

where  $\zeta = \zeta_{\ell^n}$  and  $S = \{v_\ell\}$ .

*Proof.* We note that  $\Phi_m$  has degree  $\varphi(m)$  which is even for  $m \geq 3$ . It follows from this that  $F$  has even degree. From Lemma 3.13 we have  $\zeta^{-\deg(F)/2}F(\zeta) \in \mathcal{O}(\Omega_{n,\ell}, S)^\times$  for suitably large  $n$ . To prove the lemma we need to show that  $\zeta^{-\deg(F)/2}F(\zeta)$  is fixed by complex conjugation. Let  $G$  be either  $\Phi_1^2$ , or  $\Phi_2^2$ , or  $\Phi_m$  with  $m \geq 3$ . We claim that  $\zeta^{-\deg(G)/2}G(\zeta)$  is fixed by complex conjugation. Since  $F$  is a product of such  $G$ , the lemma follows from our claim. The claim is trivially true for  $G = \Phi_1^2$  and  $G = \Phi_2^2$ , and follows immediately from Lemma 3.15 for  $G = \Phi_m$  with  $m \geq 3$ . □

**Lemma 3.17.** *Let  $S = \{v_\ell\}$ . Let*

$$k \in \{1, 2, 3, 4, 5, 6, 7, 8, 10\}.$$

Then  $(\mathbb{P}^1 \setminus \{0, k, \infty\})(\mathcal{O}(\Omega_{\infty, \ell}^+, S))$  is infinite.

*Proof.* The proof makes use of identities (3.8)–(3.16). Each identity has the form  $P - Q = kXR$  where  $P$ ,  $Q$ , and  $R$  are Kronecker polynomials. Let  $n$  be sufficiently large so that  $\zeta_{\ell^n}$  is not a root of  $PQR$ , and write

$$\varepsilon_n = \frac{P(\zeta_{\ell^n})}{\zeta_{\ell^n} R(\zeta_{\ell^n})}, \quad \delta_n = \frac{-Q(\zeta_{\ell^n})}{\zeta_{\ell^n} R(\zeta_{\ell^n})}.$$

From the identity  $P - Q = kXR$  we see that  $\varepsilon_n + \delta_n = k$ . We note the following features of the triples  $(P, Q, R)$  common to all the identities (3.8)–(3.16):

- In every case,  $P$ ,  $Q$ ,  $R$  are products of powers of cyclotomic polynomials where the exponents of  $\Phi_1$  and  $\Phi_2$  are both even.
- Write  $d = \deg(P)$ . Then  $\deg(Q) = d$  and  $\deg(R) = d - 2$ . Indeed as Kronecker polynomials are monic, the relation  $P - Q = kXR$  forces  $P$  and  $Q$  to have the same degree as soon as  $k \geq 2$ .

We may rewrite  $\varepsilon_n$  as

$$\varepsilon_n = \frac{\zeta_{\ell^n}^{-d/2} P(\zeta_{\ell^n})}{\zeta_{\ell^n}^{-(d-2)/2} R(\zeta_{\ell^n})}, \quad \delta_n = \frac{-\zeta_{\ell^n}^{-d/2} Q(\zeta_{\ell^n})}{\zeta_{\ell^n}^{-(d-2)/2} R(\zeta_{\ell^n})}.$$

By Lemma 3.16, we have  $\varepsilon_n, \delta_n \in \mathcal{O}(\Omega_{n, \ell}^+, S)^\times$  for  $n$  suitably large, and therefore  $\varepsilon_n$  is an  $\mathcal{O}(\Omega_{\infty, \ell}^+, S)$ -point on  $\mathbb{P}^1 \setminus \{0, k, \infty\}$ . To complete the proof we need to show that we obtain infinitely many distinct points as we vary  $n$ . We will do this for  $k = 10$ . The other cases are similar. Note that

$$\varepsilon_n = \frac{\Phi_2(\zeta_{\ell^n})^4 \Phi_5(\zeta_{\ell^n})}{\zeta_{\ell^n} \Phi_4(\zeta_{\ell^n})^3} = \frac{(1 - \zeta_{\ell^n}^2)^7 (1 - \zeta_{\ell^n}^5)}{\zeta_{\ell^n} (1 - \zeta_{\ell^n})^5 (1 - \zeta_{\ell^n}^4)^3} \in V_n.$$

To show that we obtain infinitely many distinct  $\varepsilon_n$  it is enough to show that  $\varepsilon_n \notin V_{n-1}$  for  $n$  sufficiently large. This follows by an easy application of Lemma 3.10; to illustrate this let  $\ell = 5$  and suppose  $\varepsilon_n \in V_{n-1}$ . Note that  $1 - \zeta_{5^n}^5 \in V_{n-1}$ . It follows that

$$(1 - \zeta_{5^n})^{-5} (1 - \zeta_{5^n}^2)^7 (1 - \zeta_{5^n}^4)^{-3} \in \langle \pm \zeta_{\ell^n}, V_{n-1} \rangle.$$

Now in the product on the left the exponent of  $1 - \zeta_{5^n}$  is  $-5$  whereas the exponent of  $1 - \zeta_{5^n}^{1+5^{n-1}}$  is 0, contradicting Lemma 3.10. The proof is similar for  $\ell = 2$ , and for  $\ell \neq 2, 5$ . It follows that we have infinitely many  $\mathcal{O}(\Omega_{\infty, \ell}^+, S)$ -points on  $\mathbb{P}^1 \setminus \{0, 10, \infty\}$ .  $\square$

### 3.2.1 Proof of Theorem 3.2 for $\ell = 2$ and 3

For  $\ell = 2, 3$ , we have  $\Omega_{\infty, \ell}^+ = \mathbb{Q}_{\infty, \ell}$ . Indeed, if  $\ell = 2$  then  $\mathbb{Q}_{n, 2} = \Omega_{n+2, 2}^+$  and if  $\ell = 3$  then  $\mathbb{Q}_{n, 3} = \Omega_{n+1, 3}^+$ . Therefore Theorem 3.2 with  $\ell = 2$  and 3 follows immediately from Lemma 3.17 for  $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 10\}$ .

Also, if  $\ell = 2$ , then the infinitely many solutions  $\varepsilon + \delta = 6$  yields infinitely many solutions for  $2\varepsilon + 2\delta = 12$  and  $4\varepsilon + 4\delta = 24$ . And if  $\ell = 3$ , then the infinitely many solutions  $\varepsilon + \delta = 4$  yields infinitely many solutions  $3\varepsilon + 3\delta = 12$ , and similarly infinitely many solutions  $\varepsilon + \delta = 8$  yields infinitely many solutions  $3\varepsilon + 3\delta = 24$ . This proves Theorem 3.2 for  $\ell = 2, 3$  and  $k \in \{12, 24\}$ .  $\square$

### 3.2.2 Proof of Theorem 3.1 for $\ell = 2$

Theorem 3.1 for  $\ell = 2$  is simply a special case of Theorem 3.2.  $\square$

## 3.3 The unit equation over $\mathbb{Q}(\zeta_{\ell^n})^+$

For roots of unity  $\alpha, \beta$ , we let

$$E(\alpha, \beta) = \frac{\alpha^2 + \alpha^{-2}}{(\alpha\beta^{-1} + \alpha^{-1}\beta)(\alpha\beta + \alpha^{-1}\beta^{-1})} = \frac{\Phi_8(\alpha)}{\Phi_4(\alpha\beta)\Phi_4(\alpha/\beta)},$$

$$F(\alpha, \beta) = \frac{\beta^2 + \beta^{-2}}{(\alpha\beta^{-1} + \alpha^{-1}\beta)(\alpha\beta + \alpha^{-1}\beta^{-1})} = \frac{\Phi_8(\beta)}{\Phi_4(\alpha\beta)\Phi_4(\beta/\alpha)}.$$

We easily check that

$$E(\alpha, \beta) + F(\alpha, \beta) = 1. \quad (3.17)$$

**Lemma 3.18.** *Suppose  $\ell$  is odd and  $n \geq 1$ . Let  $\zeta = \zeta_{\ell^n}$ . Let  $i, j$  be integers satisfying  $i, j, i+j, i-j \not\equiv 0 \pmod{\ell^n}$ . Then  $E(\zeta^i, \zeta^j), F(\zeta^i, \zeta^j) \in \mathcal{O}(\Omega_{n, \ell}^+)^{\times}$ , and satisfy the unit equation*

$$\varepsilon + \delta = 1, \quad \varepsilon, \delta \in \mathcal{O}(\Omega_{n, \ell}^+)^{\times}. \quad (3.18)$$

Moreover,

$$v_{\ell}(E(\zeta^i, \zeta^j) - F(\zeta^i, \zeta^j)) = \frac{\ell^{\text{ord}_{\ell}(i+j)} + \ell^{\text{ord}_{\ell}(i-j)}}{\ell^{n-1}(\ell-1)}. \quad (3.19)$$

*Proof.* It is clear that  $E(\zeta^i, \zeta^j), F(\zeta^i, \zeta^j)$  are fixed by complex conjugation  $\zeta \mapsto \zeta^{-1}$  and so belong to  $\Omega_{n, \ell}^+$ . By Lemma 3.13,  $E(\zeta^i, \zeta^j)$  and  $F(\zeta^i, \zeta^j)$  are units. It remains to check (3.19). We observe

$$E(\zeta^i, \zeta^j) - F(\zeta^i, \zeta^j) = \frac{(\zeta^{i-j} - \zeta^{j-i})(\zeta^{i+j} - \zeta^{-i-j})}{(\zeta^{i-j} + \zeta^{j-i})(\zeta^{i+j} + \zeta^{-i-j})} = \frac{(\zeta^{2(i-j)} - 1)(\zeta^{2(i+j)} - 1)}{\Phi_4(\zeta^{i-j})\Phi_4(\zeta^{i+j})}.$$

The denominator is a unit by Lemma 3.13. Now (3.19) follows from Lemma 3.8.  $\square$

*Proof of Theorem 3.3.* We deduce this from Lemma 3.18. Let us take for example  $i = 2$  and  $j = 1$ . Let  $n \geq 2$  and let

$$\varepsilon_n = E(\zeta_{\ell^n}^2, \zeta_{\ell^n}), \quad \delta_n = F(\zeta_{\ell^n}^2, \zeta_{\ell^n}).$$

By Lemma 3.18,  $\varepsilon_n, \delta_n \in \mathcal{O}(\Omega_{\infty, \ell}^+)^{\times}$  and satisfy  $\varepsilon_n + \delta_n = 1$ . Thus  $\varepsilon_n \in (\mathbb{P}^1 \setminus \{0, 1, \infty\})(\mathcal{O}(\Omega_{\infty, \ell}^+))$ . Moreover,

$$v_{\ell}(2\varepsilon_n - 1) = v_{\ell}(\varepsilon_n - \delta_n) = \begin{cases} \frac{2}{\ell^{n-1}(\ell-1)} & \ell > 3 \\ \frac{2}{3^{n-1}} & \ell = 3, \end{cases}$$

by (3.19). Thus  $\varepsilon_n \neq \varepsilon_m$  whenever  $n \neq m$ . Hence  $(\mathbb{P}^1 \setminus \{0, 1, \infty\})(\mathcal{O}(\Omega_{\infty, \ell}^+))$  is infinite.  $\square$

**Remark.** Theorem 3.3 applies only for  $\ell$  odd; for  $\ell = 2$  it is easy to show that the statement is false. Indeed, let  $\eta_n$  be the prime ideal of  $\mathcal{O}(\Omega_{n, 2}^+)$  above 2. Then  $\mathcal{O}(\Omega_{n, 2}^+)/\eta_n \cong \mathbb{F}_2$ , and a solution to  $\varepsilon + \delta = 1$  with  $\varepsilon, \delta \in \mathcal{O}(\Omega_{n, 2}^+)^{\times}$  reduced modulo  $\eta_n$  gives  $1 + 1 \equiv 1 \pmod{2}$  which is impossible.

### Proof of Theorem 3.1 for $\ell = 3$

We recall that  $\mathbb{Q}_{\infty, 3} = \Omega_{\infty, 3}^+$ . Therefore Theorem 3.1 for  $\ell = 3$  follows immediately from Theorem 3.3.  $\square$

## 3.4 The $S$ -unit equation over $\mathbb{Q}_{\infty, 5}$

The purpose of this section is to prove Theorems 3.1 and 3.2 for  $\ell = 5$ . These in fact follow immediately from the following lemma.

**Lemma 3.19.** *Let  $v_5$  be the unique prime of  $\mathbb{Q}_{\infty, 5}$  above 5, and write  $S = \{v_5\}$ . Then*

(i)  $(\mathbb{P}^1 \setminus \{0, k, \infty\})(\mathcal{O}(\mathbb{Q}_{\infty, 5}, S))$  is infinite for  $k = 1, 4$ ;

(ii)  $(\mathbb{P}^1 \setminus \{0, 2, \infty\})(\mathcal{O}(\mathbb{Q}_{\infty, 5}))$  is infinite.

*Proof.* Let  $a \in \mathbb{Z}_5^{\times}$  be the element satisfying

$$a^2 = -1, \quad a \equiv 2 \pmod{5};$$

such an element exists and is unique by Hensel's Lemma. Let  $\sigma : \Omega_{\infty,5} \rightarrow \Omega_{\infty,5}$  be the field automorphism satisfying

$$\sigma(\zeta_{5^n}) = \zeta_{5^n}^a$$

for  $n \geq 1$ . Note that  $\sigma$  is an automorphism of order 4, and fixes a subfield of  $\Omega_{\infty,5}$  of index 4. This subfield is precisely  $\mathbb{Q}_{\infty,5}$ .

Let

$$\begin{aligned} F &= (x_1x_2^2 + x_3x_4^2)(x_1^2x_4 + x_2x_3^2), \\ G &= (x_1^2x_2 + x_3^2x_4)(x_1x_4^2 + x_2^2x_3), \\ H &= (x_1 - x_3)(x_2 - x_4)(x_1x_2 - x_3x_4)(x_1x_4 - x_2x_3). \end{aligned}$$

Observe  $F, G, H$  are invariant under the 4-cycle  $(x_1, x_2, x_3, x_4)$ . One can check that  $F - G = H$ . Let  $n \geq 2$  and write  $\zeta = \zeta_{5^n}$ . Let

$$\varepsilon_n = \frac{F(\zeta, \zeta^a, \zeta^{a^2}, \zeta^{a^3})}{H(\zeta, \zeta^a, \zeta^{a^2}, \zeta^{a^3})}, \quad \delta_n = -\frac{G(\zeta, \zeta^a, \zeta^{a^2}, \zeta^{a^3})}{H(\zeta, \zeta^a, \zeta^{a^2}, \zeta^{a^3})}.$$

From the identity  $F - G = H$  we have  $\varepsilon_n + \delta_n = 1$ . We shall show that  $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}_{\infty,5}, S)^\times$ .

Since  $\sigma$  cyclically permutes  $\zeta, \zeta^a, \zeta^{-1}, \zeta^{-a}$  we conclude that  $f(\zeta, \zeta^a, \zeta^{-1}, \zeta^{-a}) \in \mathbb{Q}_{\infty,5}$  for  $f = F, G, H$ . Thus  $\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,5}$ . Moreover,

$$\begin{aligned} F &= x_2x_3^3x_4^2 \cdot \Phi_2(x_1x_2^2/x_3x_4^2)\Phi_2(x_1^2x_4/x_2x_3^2), \\ G &= x_2^2x_3^3x_4 \cdot \Phi_2(x_1^2x_2/x_3^2x_4)\Phi_2(x_1x_4^2/x_2^2x_3), \\ H &= x_2x_3^3x_4^2 \cdot \Phi_1(x_1/x_3) \cdot \Phi_1(x_2/x_4) \cdot \Phi_1(x_1x_2/x_3x_4) \cdot \Phi_1(x_1x_4/x_2x_3). \end{aligned}$$

Hence

$$\begin{aligned} \varepsilon_n &= \frac{\Phi_2(\zeta^{2+4a})\Phi_2(\zeta^{4-2a})}{\Phi_1(\zeta^2)\Phi_1(\zeta^{2a})\Phi_1(\zeta^{2+2a})\Phi_1(\zeta^{2-2a})} \\ &= \frac{(1 - \zeta^{4+8a})(1 - \zeta^{8-4a})}{(1 - \zeta^2)(1 - \zeta^{2a})(1 - \zeta^{2+2a})(1 - \zeta^{2-2a})(1 - \zeta^{2+4a})(1 - \zeta^{4-2a})}. \end{aligned}$$

and

$$\begin{aligned} \delta_n &= \frac{-\zeta^{2a}\Phi_2(\zeta^{4+2a})\Phi_2(\zeta^{2-4a})}{\Phi_1(\zeta^2)\Phi_1(\zeta^{2a})\Phi_1(\zeta^{2+2a})\Phi_1(\zeta^{2-2a})} \\ &= \frac{-\zeta^{2a}(1 - \zeta^{8+4a})(1 - \zeta^{4-8a})}{(1 - \zeta^2)(1 - \zeta^{2a})(1 - \zeta^{2+2a})(1 - \zeta^{2-2a})(1 - \zeta^{4+2a})(1 - \zeta^{2-4a})}. \end{aligned}$$

We checked, using the fact that  $a \equiv 7 \pmod{25}$ , that the exponents of  $\zeta$  in the above

expressions for  $\varepsilon_n$  and  $\delta_n$  all have 5-adic valuation 0 or 1. It follows from this that  $\varepsilon_n, \delta_n \in V_n \subseteq \mathcal{O}(\Omega_n, S)^\times$  for  $n \geq 2$ . Hence  $\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,5} \cap \mathcal{O}(\Omega_n, S)^\times = \mathcal{O}(\mathbb{Q}_{\infty,5}, S)^\times$  for  $n \geq 2$ . To complete the proof of the lemma for  $k = 1$  it is enough to show that  $\varepsilon_n \neq \varepsilon_m$  for  $n > m$ , and for this it is enough to show that  $\varepsilon_n \notin \langle \pm \zeta_{5^n}, V_{n-1} \rangle$  for  $n \geq 2$ . Since  $a \equiv 7 \pmod{25}$  we see that

$$4 + 8a \equiv 10, \quad 8 - 4a \equiv 5, \quad 2 + 4a \equiv 5, \quad 4 - 2a \equiv 15 \pmod{25}.$$

Thus the factors

$$1 - \zeta^{4+8a}, \quad 1 - \zeta^{8-4a}, \quad 1 - \zeta^{2+4a}, \quad 1 - \zeta^{4-2a}$$

all belong to  $V_{n-1}$ . Hence it is enough to show that

$$(1 - \zeta^2)(1 - \zeta^{2a})(1 - \zeta^{2+2a})(1 - \zeta^{2-2a}) \quad (3.20)$$

does not belong to  $\langle \pm \zeta_{5^n}, V_{n-1} \rangle$ . However, the exponents 2,  $2a$ ,  $2 + 2a$ ,  $2 - 2a$  are respectively 2, 4, 1, 3 modulo 5, and hence certainly distinct modulo  $5^{n-1}$ . It follows from Lemma 3.10 that the product (3.20) does not belong to  $\langle \pm \zeta_{5^n}, V_{n-1} \rangle$  completing the proof for  $k = 1$ .

The proof for  $k = 2$  is similar, and is based on the identity  $F - G = 2H$  where

$$\begin{aligned} F &= (x_1^2 + x_1x_3 + x_3^2)(x_2^2 + x_2x_4 + x_4^2) = x_3^2x_4^2 \cdot \Phi_3(x_1/x_3) \cdot \Phi_3(x_2/x_4), \\ G &= (x_1^2 - x_1x_3 + x_3^2)(x_2^2 - x_2x_4 + x_4^2) = x_3^2x_4^2 \cdot \Phi_6(x_1/x_3) \cdot \Phi_6(x_2/x_4), \\ H &= (x_1x_4 + x_2x_3)(x_1x_2 + x_3x_4) = x_2x_3^2x_4 \cdot \Phi_2(x_1x_4/x_2x_3) \cdot \Phi_2(x_1x_2/x_3x_4), \end{aligned}$$

and likewise the proof for  $k = 4$  is based on the identity  $F - G = 4H$  where

$$\begin{aligned} F &= (x_1 + x_3)^2(x_2 + x_4)^2 = x_3^2x_4^2 \cdot \Phi_2(x_1/x_3)^2 \Phi_2(x_2/x_4)^2, \\ G &= (x_1 - x_3)^2(x_2 - x_4)^2 = x_3^2x_4^2 \cdot \Phi_1(x_1/x_3)^2 \Phi_1(x_2/x_4)^2, \\ H &= (x_1x_2 + x_3x_4)(x_1x_4 + x_2x_3) = x_2x_3^2x_4 \cdot \Phi_2(x_1x_2/x_3x_4) \Phi_2(x_1x_4/x_2x_3). \end{aligned}$$

□

**Remark.** It is appropriate to remark on how the identities in the above proof were found. Write

$$\Psi_m(X, Y) = Y^{\varphi(m)} \Phi_m(X/Y)$$

for the homogenization of the  $m$ -th cyclotomic polynomial. Now consider

$$f(x_1, x_2, x_3, x_4) = \Psi_m(u, v)$$

where  $u, v$  are monomials in variables  $x_1, x_2, x_3, x_4$ . Let  $\ell$  be a prime. We see that evaluating any such  $f$  at  $(\zeta^\alpha, \zeta^\beta, \zeta^\gamma, \zeta^\delta)$  gives an element of  $V_n$  (provided that it does not vanish). We considered products of such  $f$  of total degree up to 20 and picked out ones that are invariant under the 4-cycle  $(x_1, x_2, x_3, x_4)$ , and searched for ternary relations between them. This yielded the identities used in the above proof.

*Proof of Theorems 3.1 and 3.2 for  $\ell = 5$ .* Theorems 3.1 and 3.2 for  $\ell = 5$  follow immediately from Lemma 3.19.  $\square$

**Remark.** Another (equivalent) way to think about constructing infinitely many  $S$ -units in  $\mathbb{Q}_{\infty,5}$  is, for each  $n \geq 1$ , constructing a suitable  $S$ -unit in  $\Omega_{n,5}^+$  and then taking its relative norm over  $\mathbb{Q}_{n-1,5}$ . In particular, for the case  $k = 1$ , one can take the construction

$$\varepsilon_n := \text{Nm}_{\Omega_{n,5}^+/\mathbb{Q}_{n-1,5}} \left( \frac{\zeta^{2a-1} + \zeta^{1-2a}}{\zeta^{2-a} + \zeta^{a-2}} \right)$$

Noting that  $\text{Gal}(\Omega_{n,5}^+/\mathbb{Q}_{n-1,5})$  is generated by the order 2 map  $\zeta + \zeta^{-1} \mapsto \zeta^a + \zeta^{-a}$ , a direct computation (e.g. using Sage) shows that

$$\varepsilon_n - 1 = \text{Nm}_{\Omega_{n,5}^+/\mathbb{Q}_{n-1,5}} \left( \frac{(\zeta^{1-a} - \zeta^{a-1})(\zeta^a - \zeta^{-a})}{\zeta^{2-a} + \zeta^{a-2}} \right)$$

which proves  $\varepsilon_n, \varepsilon_n - 1 \in \mathcal{O}(\mathbb{Q}_{\infty,5}, S)^\times$ .

### 3.5 The $S$ -unit equation over $\mathbb{Q}_{\infty,7}$

**Lemma 3.20.** *Let  $v_7$  be the unique prime of  $\mathbb{Q}_{\infty,7}$  above 7, and write  $S = \{v_7\}$ . Then  $(\mathbb{P}^1 \setminus \{0, 1, \infty\})(\mathcal{O}(\mathbb{Q}_{\infty,7}, S))$  is infinite.*

*Proof.* In view of the proof of Lemma 3.19, it would be natural to seek polynomials  $F, G, H$  in variables  $x_1, \dots, x_6$  satisfying the following properties

- $F \pm G = H$ ;
- $F, G, H$  are invariant under the 6-cycle  $(x_1, x_2, \dots, x_6)$ ;
- each is a product of polynomials

$$f(x_1, x_2, \dots, x_6) = \Psi_m(u, v)$$



with  $u, v$  monomials in  $x_1, \dots, x_6$ .

Unfortunately, an extensive search has failed to produce any such triple of polynomials. We therefore need to proceed a little differently.

Let  $a \in \mathbb{Z}_7$  be the element satisfying

$$a^2 + a + 1 = 0, \quad a \equiv 2 \pmod{7};$$

such an element exists and is unique by Hensel's Lemma. Let  $\sigma, c : \Omega_{\infty,7} \rightarrow \Omega_{\infty,7}$  be the field automorphisms satisfying

$$\sigma(\zeta_{7^n}) = \zeta_{7^n}^a, \quad c(\zeta_{7^n}) = \zeta_{7^n}^{-1}$$

for  $n \geq 1$ . Then  $\mathbb{Q}_{\infty,7}$  is the field fixed by the subgroup of  $\text{Gal}(\Omega_{\infty,7}/\mathbb{Q})$  generated by  $\sigma$  and  $c$ . We work with polynomials in variables  $x_1, x_2, x_3$ . Let

$$\begin{aligned} F &= (x_1x_2^2 + x_3^3)(x_2x_3^2 + x_1^3)(x_3x_1^2 + x_2^3) \\ G &= (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)(x_1x_2 - x_3^2)(x_2x_3 - x_1^2)(x_3x_1 - x_2^2) \\ H &= (x_1^2x_2 + x_3^3)(x_2^2x_3 + x_1^3)(x_3^2x_1 + x_2^3). \end{aligned}$$

These satisfy the identity  $F - G = H$ . Moreover, they are invariant under the 3-cycle  $(x_1, x_2, x_3)$  and all the factors are of the form  $\Psi_m(u, v)$  where  $m = 1$  or  $2$ , and where  $u, v$  are suitable monomials in  $x_1, x_2, x_3$ . Evaluating any of  $F, G, H$  at  $(\zeta, \zeta^a, \zeta^{a^2})$  yields an  $S$ -unit belonging to  $\Omega_{n,7}^{(\sigma)}$ . Now we let

$$F' = \frac{F(x_1^2, x_2^2, x_3^2)}{x_1^6 x_2^6 x_3^6}, \quad G' = \frac{G(x_1^2, x_2^2, x_3^2)}{x_1^6 x_2^6 x_3^6}, \quad H' = \frac{H(x_1^2, x_2^2, x_3^2)}{x_1^6 x_2^6 x_3^6}.$$

Observe that the rational functions  $F', G', H'$  satisfy  $F' - G' = H'$  and are moreover invariant under the 3-cycle  $(x_1, x_2, x_3)$ . Moreover,  $F', G', H'$  evaluated at  $(\zeta, \zeta^a, \zeta^{a^2})$  yield  $S$ -units belonging to  $\Omega_{n,7}^{(\sigma)}$ . We need to check that these in fact belong to  $\mathbb{Q}_{n-1,7} = \Omega_{n,7}^{(\sigma,c)}$  and so we need to check that these expressions are invariant under  $c$ . This follows immediately on observing that  $F', G', H'$  may be rewritten as

$$\begin{aligned} F' &= \left( \frac{x_1x_2^2}{x_3^3} + \frac{x_3^3}{x_1x_2^2} \right) \left( \frac{x_2x_3^2}{x_1^3} + \frac{x_1^3}{x_2x_3^2} \right) \left( \frac{x_3x_1^2}{x_2^3} + \frac{x_2^3}{x_3x_1^2} \right) \\ G' &= \left( \frac{x_1}{x_2} - \frac{x_2}{x_1} \right) \left( \frac{x_2}{x_3} - \frac{x_3}{x_2} \right) \left( \frac{x_3}{x_1} - \frac{x_1}{x_3} \right) \left( \frac{x_1x_2}{x_3^2} - \frac{x_3^2}{x_1x_2} \right) \left( \frac{x_2x_3}{x_1^2} - \frac{x_1^2}{x_2x_3} \right) \left( \frac{x_3x_1}{x_2^2} - \frac{x_2^2}{x_3x_1} \right) \\ H' &= \left( \frac{x_1^2x_2}{x_3^3} + \frac{x_3^3}{x_1^2x_2} \right) \left( \frac{x_2^2x_3}{x_1^3} + \frac{x_1^3}{x_2^2x_3} \right) \left( \frac{x_3^2x_1}{x_2^3} + \frac{x_2^3}{x_3^2x_1} \right). \end{aligned}$$

Thus  $F', G', H'$  evaluated at  $(\zeta, \zeta^a, \zeta^{a^2})$  yield elements of  $\mathcal{O}(\mathbb{Q}_{\infty,7}, S)^\times$ . We write

$$\varepsilon_n = \frac{F'(\zeta, \zeta^a, \zeta^{a^2})}{H'(\zeta, \zeta^a, \zeta^{a^2})}, \quad \delta_n = -\frac{G'(\zeta, \zeta^a, \zeta^{a^2})}{H'(\zeta, \zeta^a, \zeta^{a^2})}.$$

Then  $\varepsilon_n, \delta_n$  belong to  $\mathcal{O}(\mathbb{Q}_{\infty,7}, S)^\times$  and satisfy  $\varepsilon_n + \delta_n = 1$ . In fact it is straightforward to check that  $\varepsilon_n \notin \langle \pm \zeta_{7^n}, V_{n-1} \rangle$ , from which it follows that  $\varepsilon_n \neq \varepsilon_m$  for  $n > m$ . The details are similar to those of the proof of Lemma 3.19 and we omit them.  $\square$

**Remark.** As with the  $\ell = 5$  case, one can also alternatively think of the above construction in terms of taking relative norms over  $\mathbb{Q}_{n-1,7}$ . In particular, we can take

$$\varepsilon_n := \text{Nm}_{\Omega_{n,7}^+/\mathbb{Q}_{n-1,7}} \left( \frac{\zeta^{a+3} + \zeta^{-a-3}}{\zeta^{3a+1} + \zeta^{-3a-1}} \right). \quad (3.21)$$

Noting that  $\text{Gal}(\Omega_{n,7}^+/\mathbb{Q}_{n-1,7})$  is generated by the order 3 map  $\zeta + \zeta^{-1} \mapsto \zeta^a + \zeta^{-a}$ , a similar direct computation shows that

$$\varepsilon_n - 1 = -\text{Nm}_{\Omega_{n,7}^+/\mathbb{Q}_{n-1,7}} \left( \frac{(\zeta^{-a-2} - \zeta^{a+2})(\zeta - \zeta^{-1})}{\zeta^{3a+1} + \zeta^{-3a-1}} \right)$$

which proves  $\varepsilon_n, \varepsilon_n - 1 \in \mathcal{O}(\mathbb{Q}_{\infty,7}, S)^\times$ .

In a similar spirit to asking whether other ternary relations between Kronecker polynomials exist, it's natural to also ask whether similar constructions to (3.21) exist for larger primes  $\ell$ . In particular, given a prime  $\ell \geq 11$  we can ask if there exist integers  $k, m \in \mathbb{Z}$  such that

$$\varepsilon_n := \text{Nm}_{\Omega_{n,\ell}^+/\mathbb{Q}_{n-1,\ell}} \left( \frac{\zeta^k + \zeta^{-k}}{\zeta^m + \zeta^{-m}} \right)$$

is in  $(\mathbb{P}^1 \setminus \{0, 1, \infty\})(\mathcal{O}(\mathbb{Q}_{\infty,\ell}, \{v_\ell\}))$  for all  $n \geq 1$ ? A brute force check has confirmed that no such integers  $k, m$  exist for  $\ell \in \{11, 13\}$  and  $1 \leq n \leq 5$ . At this point, we must also mention a beautiful recent project of Li and Otgonbayar [282] which gives some heuristic evidence to suggest why solutions are harder to find for primes  $\ell \geq 11$ .

### 3.6 Isogeny classes of elliptic curves over $\mathbb{Q}_{\infty,\ell}$

The purpose of this section is to prove Theorem 3.5. Since isogenous elliptic curves share the same set of bad primes, the corresponding theorem over number fields is an immediate consequence of Shafarevich's theorem. However, as we intend to show in the following section, Shafarevich's theorem does not generalize to elliptic curves

over  $\mathbb{Q}_{\infty, \ell}$ . We shall instead rely on a theorem of Kato to control  $\mathbb{Q}_{\infty, \ell}$ -points on certain modular Jacobians.

Our first lemma shows that there are only finitely many primes that can divide the degree of a cyclic isogeny of  $E$ .

**Lemma 3.21.** *Let  $\ell$  be a prime and let  $E/\mathbb{Q}_{\infty, \ell}$  be an elliptic curve without potential complex multiplication. Then there is a constant  $B$ , depending only on  $E$ , such that for all primes  $p \geq B$ , the elliptic curve  $E$  has no  $p$ -isogenies defined over  $\mathbb{Q}_{\infty, \ell}$ .*

*Proof.* Let  $n$  be the least positive integer such that  $E$  admits a model defined over  $\mathbb{Q}_{n, \ell}$ . By a famous theorem of Serre [393], there is a constant  $B$ , depending on  $E$ , such that for  $p \geq B$  the mod  $p$  representation

$$\bar{\rho}_{E, p} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_{n, \ell}) \rightarrow \text{GL}_2(\mathbb{F}_p)$$

is surjective. We may suppose that  $B \geq 5$ . Thus, for  $p \geq B$ , the Galois group  $\text{Gal}(\mathbb{Q}_{n, \ell}(E[p])/\mathbb{Q}_{n, \ell})$  is isomorphic to  $\text{GL}_2(\mathbb{F}_p)$  which is non-solvable. We will show that  $E$  has no  $p$ -isogeny defined over  $\mathbb{Q}_{\infty, \ell}$ . Suppose otherwise. Then such an isogeny is in fact defined over  $\mathbb{Q}_{m, \ell}$  for some  $m \geq n$ . It follows that the extension  $\mathbb{Q}_{m, \ell}(E[p])/\mathbb{Q}_{m, \ell}$  has Galois group isomorphic to a subgroup of a Borel subgroup of  $\text{GL}_2(\mathbb{F}_p)$ , which is solvable. As the extension  $\mathbb{Q}_{m, \ell}/\mathbb{Q}_{n, \ell}$  is cyclic, we conclude that  $\mathbb{Q}_{m, \ell}(E[p])/\mathbb{Q}_{n, \ell}$  is solvable. However, this contains the non-solvable subextension  $\mathbb{Q}_{n, \ell}(E[p])/\mathbb{Q}_{n, \ell}$ , giving a contradiction.  $\square$

We shall make use of the following theorem of Kato [254, Theorem 14.4] building on work of Rohrlich [367].

**Theorem 3.22** (Kato). *Let  $\ell$  be a prime. Let  $A$  be an abelian variety defined over  $\mathbb{Q}$  and admitting a surjective map  $J_1(N) \rightarrow A$  for some  $N \geq 1$ . Then  $A(\mathbb{Q}_{\infty, \ell})$  is finitely generated.*

**Lemma 3.23.** *Let  $p, \ell$  be primes. Let  $E$  be an elliptic curve defined over  $\mathbb{Q}_{\infty, \ell}$  without potential complex multiplication. Then, for  $m$  sufficiently large,  $E$  has no  $p^m$ -isogenies defined over  $\mathbb{Q}_{\infty, \ell}$ .*

*Proof.* Let  $r$  be the least positive integer such that the modular curve  $X = X_0(p^r)$  has genus at least 2, and write  $J = J_0(p^r)$  for the corresponding modular Jacobian. It follows from Kato's theorem that  $J(\mathbb{Q}_{\infty, \ell})$  is finitely generated, and therefore that  $J(\mathbb{Q}_{\infty, \ell}) = J(\mathbb{Q}_{n, \ell})$  for some  $n \geq 1$ . Consider the Abel-Jacobi map

$$X \hookrightarrow J, \quad P \mapsto [P - \infty]$$

where  $\infty \in X(\mathbb{Q})$  denotes the infinity cusp. It follows from this embedding that  $X(\mathbb{Q}_{\infty,\ell}) = X(\mathbb{Q}_{n,\ell})$ . By Faltings' theorem, this set is finite.

Let  $k = \#X(\mathbb{Q}_{\infty,\ell})$  and let  $s = kr$ . To prove the lemma we in fact show that  $E$  has no cyclic isogenies of degree  $p^s$  defined over  $\mathbb{Q}_{\infty,\ell}$ . Suppose otherwise, and let  $\psi : E \rightarrow E'$  be a cyclic isogeny of degree  $p^s$  defined over  $\mathbb{Q}_{\infty,\ell}$ . Then, we may factor  $\psi$  into a sequence of cyclic isogenies defined over  $\mathbb{Q}_{\infty,\ell}$

$$E = E_0 \xrightarrow{\psi_1} E_1 \xrightarrow{\psi_2} E_2 \cdots \xrightarrow{\psi_k} E_k = E'$$

where  $\psi_i$  is of degree  $p^r$ . Note that  $E_i$  and  $E_j$  are non-isomorphic over  $\overline{\mathbb{Q}}$  for  $i \neq j$ ; indeed since they are related by a cyclic isogeny, then if  $E_i$  and  $E_j$  were isomorphic over  $\overline{\mathbb{Q}}$ , this would imply that  $E_i$  has a nontrivial cyclic self-isogeny over  $\overline{\mathbb{Q}}$ , contradicting the fact that  $E$  does not have potential complex multiplication. Thus the elliptic curves  $E_0, E_1, \dots, E_k$  support distinct  $\mathbb{Q}_{\infty,\ell}$ -points on  $X = X_0(p^r)$ . This contradicts the fact that  $\#X(\mathbb{Q}_{\infty,\ell}) = k$ .  $\square$

**Remark.** A famous theorem of Serre [392, Section 2.1] asserts that the  $p$ -adic Tate module of a non-CM elliptic curve defined over a number field is irreducible. It is in fact possible to deduce Lemma 3.23 from Serre's theorem for  $\ell \neq p$ , but we have been unable to do this for  $\ell = p$ .

*Proof of Theorem 3.5.* Let  $E'$  belong to the  $\mathbb{Q}_{\infty,\ell}$ -isogeny class of  $E$ . Let  $\psi : E \rightarrow E'$  be an isogeny defined over  $\mathbb{Q}_{\infty,\ell}$ . This has kernel of the form  $\mathbb{Z}/a \times \mathbb{Z}/ab$  where  $a, b$  are positive integers, and so it can be factored into a composition

$$E \rightarrow E/E[a] \cong E \rightarrow E'$$

where the final morphism is cyclic of degree  $b$ . Thus to prove the proposition, it is enough to show that  $E$  has finitely many cyclic isogenies defined over  $\mathbb{Q}_{\infty,\ell}$ . The degree of any such isogeny is divisible by primes  $p < B$  where  $B$  is as in Lemma 3.21. Also, for any  $p < B$ , we know the exponent of  $p$  in the degree of a cyclic isogeny  $E \rightarrow E'$  is bounded by Lemma 3.23. Thus there are finitely many cyclic isogenies of  $E$  defined over  $\mathbb{Q}_{\infty,\ell}$ .  $\square$

### 3.7 From $S$ -unit equations to elliptic curves

The aim of this section is to prove Theorem 3.4. We start by recalling a few facts about Legendre elliptic curves (Proposition III.1.7 of [415] and its proof). Let  $K$  be

a field of characteristic  $\neq 2$  and let  $\lambda \in (\mathbb{P}^1 \setminus \{0, 1, \infty\})(K)$ . Associated to  $\lambda$  is the Legendre elliptic curve

$$E_\lambda : Y^2 = X(X-1)(X-\lambda).$$

This model respectively has discriminant and  $j$ -invariant

$$\Delta = 16\lambda^2(1-\lambda)^2, \quad j = \frac{64(\lambda^2 - \lambda + 1)^3}{\lambda^2(1-\lambda)^2}. \quad (3.22)$$

Moreover, for  $\lambda, \mu \in (\mathbb{P}^1 \setminus \{0, 1, \infty\})(K)$ , the Legendre elliptic curves  $E_\lambda$  and  $E_\mu$  are isomorphic over  $K$  (or over  $\bar{K}$ ) if and only if

$$\mu \in \left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda} \right\}.$$

Now let  $K$  be a number field and  $S$  a finite set of non-archimedean places. We let  $S'$  be the set of non-archimedean places which are either in  $S$  or above 2. We let  $\lambda \in (\mathbb{P}^1 \setminus \{0, 1, \infty\})(\mathcal{O}(K, S))$ . Then  $\lambda, 1-\lambda \in \mathcal{O}(K, S)^\times$ . It follows from the expression for the discriminant that  $E_\lambda$  has good reduction away from  $S'$ .

### Proof of Theorem 3.4

Let  $\ell = 2, 3, 5$  or  $7$ . Let  $S$  be given by (3.1) and let  $S' = S \cup \{v_2\}$  as in the statement of Theorem 3.4. In proving Theorem 3.1 we constructed, for each positive integer  $n$ , elements  $\varepsilon_n, \delta_n = 1 - \varepsilon_n$ , belonging to  $\mathbb{Q}_{\infty, \ell} \cap V_n \subseteq \mathcal{O}(\mathbb{Q}_{\infty, \ell}, S)^\times$ , and moreover verified, for  $n \geq 2$ , that  $\varepsilon_n \notin \langle \zeta_{\ell^n}, V_{n-1} \rangle$ . We let

$$E_n : Y^2 = X(X-1)(X-\varepsilon_n). \quad (3.23)$$

Then  $E_n$  is defined over  $\mathbb{Q}_{\infty, \ell}$  and has good reduction away from  $S'$ . We claim, for  $n > m$ , that  $E_n$  and  $E_m$  are not isomorphic, even over  $\bar{\mathbb{Q}}$ . To see this, suppose  $E_n$  and  $E_m$  are isomorphic. Then  $\varepsilon_n$  equals one of  $\varepsilon_m^{\pm 1}, \delta_m^{\pm 1}, (-\varepsilon_m \delta_m)^{\pm 1}$ . This gives a contradiction as all of these belong to  $\langle \pm \zeta_{\ell^n}, V_{n-1} \rangle$ . This proves the claim.

It remains to show that the  $E_n$  form infinitely many isogeny classes over  $\mathbb{Q}_{\infty, \ell}$ . However, this immediately follows from Theorem 3.5 and the following lemma.  $\square$

**Lemma 3.24.** *For  $n$  sufficiently large,  $E_n$  does not have potential complex multiplication.*

*Proof.* Suppose  $E_n$  has potential complex multiplication by an order  $R$  in an imaginary quadratic field  $K$ . Write  $j = j(E_n)$ . We claim that  $\mathbb{Q}(j)/\mathbb{Q}$  is a cyclic Galois

extension of order  $\ell^n$  for some  $n$ . Note that  $\mathbb{Q}(j)$  is a subextension of  $\mathbb{Q}_{\infty,\ell}$  of finite degree, and is thus contained in  $\mathbb{Q}_{m,\ell}$  for some  $m$ . Hence  $\mathbb{Q}(j)$  is the fixed field of some subgroup  $H$  (say) of  $G = \text{Gal}(\mathbb{Q}_{m,\ell}/\mathbb{Q})$ . As  $G$  is cyclic, the group  $H$  is a normal subgroup, and therefore  $\mathbb{Q}(j)/\mathbb{Q}$  is a Galois extension. Moreover,  $\text{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \cong G/H$  which is cyclic of order  $\ell^n$  for some  $n$ , proving our claim.

By standard CM theory [406, Theorem 5.7], we know that  $\text{Gal}(K(j)/K) \cong \text{Pic}(R)$  and  $[\mathbb{Q}(j) : \mathbb{Q}] = [K(j) : K]$ . Since in our case  $\mathbb{Q}(j)/\mathbb{Q}$  is Galois,  $\text{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \cong \text{Gal}(K(j)/K) \cong \text{Pic}(R)$ . However,  $\mathbb{Q}(j) \subset \mathbb{Q}_{\infty,\ell}$  is totally real. It follows [406, page 124] that  $\text{Pic}(R)$  is an elementary abelian 2-group. However  $\mathbb{Q}(j)/\mathbb{Q}$  is cyclic of order  $\ell^n$ . Thus,  $j \in \mathbb{Q}$  if  $\ell \neq 2$ , and  $j \in \mathbb{Q}_{1,2} = \mathbb{Q}(\sqrt{2})$  if  $\ell = 2$ . However, from the expression for  $j$  in (3.22) we know that  $[\mathbb{Q}(\varepsilon_n) : \mathbb{Q}(j)] \leq 6$ . Thus  $\varepsilon_n$  belongs to a subfield of  $\mathbb{Q}_{\infty,\ell}$  of degree at most 12. The lemma follows since, by Siegel–Mahler’s theorem, the  $S$ -unit equation has only finitely many solutions in any number field.  $\square$

**Remark.** It’s worth mentioning that an earlier draft of this chapter gave a different method to proving  $\{E_n\}_{n \geq 1}$  form infinitely many isogeny classes over  $\mathbb{Q}_{\infty,\ell}$  (without showing  $E_n$  does not have potential CM for sufficiently large  $n$ , albeit with more technical computations). To sketch the original proof, fix some prime  $\ell = 2, 3, 5$  or  $7$ , and an elliptic curve  $E_i$  as given in (3.23), and as before assume there exists an isogeny  $\psi : E_i \rightarrow E_j$  over  $\mathbb{Q}_{\infty,\ell}$ . We aim to show there exists only finitely such  $E_j$ . Here, we factor  $\psi$  into two isogenies  $\psi_{\text{even}}$  and  $\psi_{\text{odd}}$ , where  $\psi_{\text{even}}$  is an isogeny of degree  $2^k$  (and thus splits into  $k$  2-isogenies) and  $\psi_{\text{odd}}$  is an isogeny of odd degree (and thus splits into isogenies of odd prime degree).

$$\psi : E_i \xrightarrow{\psi_{\text{even}}} E' \xrightarrow{\psi_{\text{odd}}} E_j.$$

We can then proceed in two steps: (i) computing the possible set of elliptic curves  $E'$  (and their discriminants  $\Delta_{E'}$ ) which are  $2^k$ -isogenous to  $E_i$ , and (ii) computing the possible set of elliptic curves  $E_j$  which are isogenous of odd degree to  $E'$ .

For step (i), as  $\mathbb{Q}_{\infty,\ell}(E_i[2]) = \mathbb{Q}_{\infty,\ell}$ , there exist three elliptic curves  $E_{i,1}$ ,  $E_{i,2}$  and  $E_{i,3}$  which are 2-isogenous to  $E_i$  with discriminants  $256\varepsilon_i(\varepsilon_i - 1)^4$ ,  $-256(\varepsilon_i - 1)\varepsilon_i^4$ , and  $256\varepsilon_i(\varepsilon_i - 1)$  respectively. One can then prove that none of these are squares in  $\mathbb{Q}_{\infty,\ell}$  by writing these in terms of a multiplicative basis for  $V_n$ . This proves  $E' \in \{E_i, E_{i,1}, E_{i,2}, E_{i,3}\}$ .

For step (ii), we can use the main theorem of Dokchitser–Dokchitser [146, Theorem 1.1] which states that if  $\phi : E \rightarrow E'$  is a  $p$ -isogeny (over  $K$ ) for  $p \geq 3$ , then  $\Delta_E^p / \Delta_{E'}$  is a 4th-power in  $K$ . This implies that if  $E'$  is isogenous of odd degree to  $E_j$ , then either  $\Delta_{E'} / \Delta_{E_j}$  or  $\Delta_{E'} \Delta_{E_j}$  is a 4th power in  $\mathbb{Q}_{\infty,\ell}$ . By computing discriminants,

one can show that either  $\pm \varepsilon_i \varepsilon_j (\varepsilon_i - 1)(\varepsilon_j - 1)$  or  $\pm \varepsilon_i \varepsilon_j^{-1} (\varepsilon_i - 1)(\varepsilon_j - 1)^{-1}$  is a square in  $\mathbb{Q}_{\infty, \ell}$ . By again writing these expressions in terms of a multiplicative basis for  $V_n$ , one obtains that only finitely many  $j$  fit the criterion, thereby proving that the family of elliptic curves  $\{E_n\}_{n \geq 1}$  form infinitely many  $\mathbb{Q}_{\infty, \ell}$ -isogeny classes.

### 3.8 Hyperelliptic curves over $\mathbb{Q}_{\infty, \ell}$ with few bad primes

Let  $\ell$  be an odd prime. Let  $g \geq 2$  be an integer satisfying

$$\begin{cases} g \equiv (\ell - 3)/4 \text{ or } -1 \pmod{(\ell - 1)/2} & \text{if } \ell \equiv 3 \pmod{4} \\ g \equiv -1 \pmod{(\ell - 1)/4} & \text{if } \ell \equiv 1 \pmod{4}. \end{cases} \quad (3.24)$$

Then there is a positive integer  $k$  such that

$$k \cdot \left( \frac{\ell - 1}{2} \right) = \begin{cases} 2g + 1 \text{ or } 2g + 2 & \text{if } \ell \equiv 3 \pmod{4} \\ 2g + 2 & \text{if } \ell \equiv 1 \pmod{4}. \end{cases} \quad (3.25)$$

Let  $n \geq 2$  be a positive integer satisfying

$$\ell^{n-1} \geq k. \quad (3.26)$$

In this section we construct a hyperelliptic curve  $D_n$  of genus  $g$  defined over  $\mathbb{Q}_{n-1, \ell}$  with good reduction away from the primes above 2,  $\ell$ .

Write

$$\mathcal{Z}_n = \{ \zeta \in \Omega_{n, \ell} : \zeta^{\ell^n} = 1, \zeta^{\ell^i} \neq 1 \text{ if } i < n \}$$

for the set of primitive  $\ell^n$ -th roots of 1. Write

$$\mathcal{Z}_n^+ = \{ \zeta + \zeta^{-1} : \zeta \in \mathcal{Z}_n \} \subset \Omega_{n, \ell}^+.$$

We note that any element of  $\mathcal{Z}_n^+$  generates  $\Omega_{n, \ell}^+$ .

**Lemma 3.25.**  $\# \mathcal{Z}_n^+ = \ell^{n-1}(\ell - 1)/2$ .

*Proof.* We note that  $\# \mathcal{Z}_n = \varphi(\ell^n) = \ell^{n-1}(\ell - 1)$ . Suppose  $\alpha, \beta \in \mathcal{Z}_n$ . Then

$$(\alpha + \alpha^{-1}) - (\beta + \beta^{-1}) = \alpha^{-1} \cdot (1 - \alpha\beta) \cdot (1 - \alpha\beta^{-1}). \quad (3.27)$$

Thus  $\alpha + \alpha^{-1} = \beta + \beta^{-1}$  if and only if  $\alpha = \beta$  or  $\alpha = \beta^{-1}$ . The lemma follows.  $\square$

Write

$$G_n = \text{Gal}(\Omega_{n,\ell}^+/\mathbb{Q}_{n-1,\ell}), \quad H_n = \text{Gal}(\Omega_{n,\ell}^+/\Omega_{n-1,\ell}^+).$$

We note that these are both cyclic subgroups of  $\text{Gal}(\Omega_{n,\ell}^+/\mathbb{Q})$  having orders

$$\#G_n = (\ell - 1)/2, \quad \#H_n = \ell.$$

**Lemma 3.26.** *Fix  $\zeta \in \mathcal{Z}_n$ . Let*

$$\eta_i = \zeta^{1+\ell^{n-1}(i-1)} + \zeta^{-1-\ell^{n-1}(i-1)}, \quad 1 \leq i \leq \ell. \quad (3.28)$$

*Then  $\eta_1, \dots, \eta_\ell \in \mathcal{Z}_n^+$  form a single orbit under the action of  $H_n$ , but have pairwise disjoint orbits under the action of  $G_n$ .*

*Proof.* Let  $\kappa \in \text{Gal}(\Omega_{n,\ell}/\mathbb{Q})$  be given by  $\kappa(\zeta) = \zeta^{1+\ell^{n-1}}$ . We note that  $\kappa$  has order  $\ell$  and fixes  $\Omega_{n-1,\ell}$ . We denote the restriction of  $\kappa$  to  $\Omega_{n,\ell}^+$  by  $\tau$ ; this is a cyclic generator of  $H_n$ . Note that

$$\eta_i = \tau^{i-1}(\zeta + \zeta^{-1}), \quad 1 \leq i \leq \ell.$$

Let  $\sigma_1, \sigma_2 \in G_n$ . Let  $1 \leq i < j \leq \ell$  and suppose  $\sigma_1(\eta_i) = \sigma_2(\eta_j)$ . Thus  $\sigma_1\tau^{i-1}(\eta_1) = \sigma_2\tau^{j-1}(\eta_1)$ , so  $\tau^{1-j}\sigma_2^{-1}\sigma_1\tau^{i-1}$  fixes  $\eta_1$ . As  $\eta_1$  generates  $\Omega_{n,\ell}^+$ , we have  $\tau^{1-j}\sigma_2^{-1}\sigma_1\tau^{i-1} = 1$  is the identity element in  $\text{Gal}(\Omega_{n,\ell}^+/\mathbb{Q})$ . However,  $\text{Gal}(\Omega_{n,\ell}^+/\mathbb{Q})$  is abelian, so

$$\tau^{i-j} = \sigma_1^{-1}\sigma_2 \in G_n \cap H_n = \{1\}.$$

Since  $1 \leq i \leq j \leq \ell$  and  $\tau$  has order  $\ell$  we have  $i = j$ . □

The Galois group  $G_n$  acts faithfully on  $\mathcal{Z}_n^+$ . This action has  $\ell^{n-1}$  orbits. Assumption (3.26) ensures that the number of orbits is at least  $k$ . If  $k > \ell$ , then we **extend** the list  $\eta_1, \dots, \eta_\ell \in \mathcal{Z}_n^+$  to  $\eta_1, \dots, \eta_k \in \mathcal{Z}_n^+$ , so that the  $\eta_i$  continue to have disjoint orbits under the action of  $G_n$ ; if  $\ell = 3$  the choice of  $\eta_4$  will be important later, and we choose  $\eta_4 = \zeta^2 + \zeta^{-2}$ . Consider the curve

$$D_n : Y^2 = \prod_{j=1}^k \prod_{\sigma \in G_n} (X - \eta_j^\sigma). \quad (3.29)$$

**Lemma 3.27.** *The curve  $D_n$  is hyperelliptic of genus  $g$ , is defined over  $\mathbb{Q}_{n-1,\ell}$ , and has good reduction away from the primes above 2 and  $\ell$ .*

*Proof.* Our assumption on the orbits ensures that the polynomial on the right hand-side of (3.29) is separable. By (3.25), the degree of the polynomial is either  $2g + 1$



or  $2g + 2$ . Thus  $D_n$  is a hyperelliptic curve of genus  $g$ . A priori,  $D_n$  is defined over  $\Omega_{n,\ell}^+$ . However, the roots of the hyperelliptic polynomial are permuted by the action of  $G_n = \text{Gal}(\Omega_{n,\ell}^+/\mathbb{Q}_{n-1,\ell})$  and so the polynomial belongs to  $\mathbb{Q}_{n-1,\ell}[X]$ . Hence  $D_n$  is defined over  $\mathbb{Q}_{n-1,\ell}$ .

Let  $u_1, \dots, u_d$  be the roots of the hyperelliptic polynomial. Then the discriminant of the hyperelliptic polynomial is

$$\prod_{1 \leq i < j \leq d} (u_i - u_j)^2.$$

However,  $u_i, u_j$  are distinct elements of  $\mathcal{Z}_n^+$ . Thus there are  $\alpha, \beta \in \mathcal{Z}_n$  with  $\alpha \neq \beta$ ,  $\beta^{-1}$  such that  $u_i = \alpha + \alpha^{-1}$ ,  $u_j = \beta + \beta^{-1}$ . From the identity (3.27),

$$u_i - u_j = \alpha^{-1}(1 - \alpha\beta^{-1})(1 - \alpha\beta).$$

Since  $\alpha\beta$  and  $\alpha\beta^{-1}$  are non-trivial  $\ell$ -power roots of 1, we see that  $u_i - u_j$  is a  $\{v_\ell\}$ -unit, and hence the discriminant of the hyperelliptic polynomial of  $D_n$  is a  $\{v_\ell\}$ -unit.  $\square$

Furthermore, by explicitly computing the valuations  $v_\ell(u_i - u_j)$  over all pairs of roots  $u_i, u_j$ , we can prove that  $D_n$  has potential good reduction at  $v_\ell$  in the case where  $g = \lfloor (\ell - 3)/4 \rfloor$  (equivalently  $k = 1$ , in the notation of Section 3.8).

**Lemma 3.28.** *Let  $g = \lfloor (\ell - 3)/4 \rfloor$ , and let  $D_n/\mathbb{Q}_{n-1,\ell}$  be the genus  $g$  hyperelliptic curve*

$$D_n : Y^2 = \prod_{\sigma \in G_n} (X - \eta_1^\sigma), \quad \eta_1 = \zeta_{\ell^n} + \zeta_{\ell^n}^{-1}$$

*as defined in Section 3.8. Then  $D_n$  has potential good reduction away from the primes above 2.*

*Proof.* The claim follows by Lemma 3.27 and using Theorem 1.11 to show that the cluster picture  $\Sigma_{v_\ell}$  is trivial. Let  $\mu$  be a generator of  $G_n$  of order  $(\ell - 1)/2$ , where the action of  $\mu$  is given by  $\zeta + \zeta^{-1} \mapsto \zeta^a + \zeta^{-a}$  for some  $a \in \mathbb{Z}$ . We denote  $u_0, \dots, u_{(\ell-3)/2}$  as the roots of the hyperelliptic polynomial of  $D_n$ , where  $u_i = \sigma^i(\eta_1) = \zeta^{a^i} + \zeta^{-a^i}$ .

If  $i < j$ , then note that  $a^i + a^j = a^i(1 + a^{j-i})$ . As  $j - i < (\ell - 1)/2$  and  $\mu$  has order  $(\ell - 1)/2$ , this implies that  $\ell$  cannot divide  $(1 + a^{m-k})$ , and thus  $\text{ord}_\ell(a^i + a^j) = 0$ .

By a similar argument, we also have that  $a^i - a^j = a^i(1 - a^{j-i})$  cannot be divisible by  $\ell$ , and thus  $\text{ord}_\ell(a^i - a^j) = 0$ . Therefore, using Lemma 3.8 we have

$$v_\ell(u_i - u_j) = v_\ell(\zeta^{-a^i}(1 - \zeta^{a^i - a^j}(1 - \zeta^{a^i + a^j})))$$

$$\begin{aligned}
&= \frac{1}{\ell - 1} (\ell^{1 + \text{ord}_\ell(a^i - a^j) - n} + \ell^{1 + \text{ord}_\ell(a^i + a^j) - n}) \\
&= \frac{2\ell^{1-n}}{\ell - 1}.
\end{aligned}$$

Therefore, we have that  $v_\ell(u_i - u_j)$  is constant across all pairs  $i, j$  ( $0 \leq i < j \leq (\ell - 3)/2$ ). Thus, as the cluster picture  $\Sigma_{v_\ell}$  is trivial, this implies  $D_n$  has potential good reduction at the primes above  $\ell$ .  $\square$

Given four pairwise distinct elements  $z_1, z_2, z_3, z_4$  of a field  $K$ , we shall employ the notation  $(z_1, z_2; z_3, z_4)$  to denote the **cross ratio**

$$(z_1, z_2; z_3, z_4) = \frac{(z_1 - z_3)(z_2 - z_4)}{(z_1 - z_4)(z_2 - z_3)}.$$

We extend the cross ratio to four distinct elements  $z_1, z_2, z_3, z_4$  of  $\mathbb{P}^1(K)$  in the usual way. We let  $\text{GL}_2(K)$  act on  $\mathbb{P}^1(K)$  via fractional linear transformations

$$\gamma(z) = \frac{az + b}{cz + d}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

It is well-known and easy to check that these fractional linear transformations leave the cross ratio unchanged:

$$(\gamma(z_1), \gamma(z_2); \gamma(z_3), \gamma(z_4)) = (z_1, z_2; z_3, z_4).$$

**Lemma 3.29.** *Let  $\overline{K}$  be an algebraically closed field of characteristic 0. Let*

$$D : Y^2 = \prod_{i=1}^d (X - a_i), \quad D' : Y^2 = \prod_{i=1}^d (X - b_i),$$

*be genus  $g$  curves defined over  $\overline{K}$  where the polynomials on the right are separable. If  $D, D'$  are isomorphic then there is some permutation  $\mu \in S_d$  such that for all quadruples of pairwise distinct indices  $1 \leq r, s, t, u \leq d$*

$$(a_r, a_s; a_t, a_u) = (b_{\mu(r)}, b_{\mu(s)}; b_{\mu(t)}, b_{\mu(u)}).$$

*Proof.* We shall make use of the following standard description (e.g. [23, Proposition 6.11]) of isomorphisms of hyperelliptic curves: every isomorphism  $\pi : D \rightarrow D'$  is of the form

$$\pi(X, Y) = \left( \frac{aX + b}{cX + d}, \frac{eY}{(cX + d)^{g+1}} \right)$$

for some

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\overline{K}), \quad e \in \overline{K}^\times.$$

Observe that  $\pi(a_i, 0)$  has  $Y$ -coordinate 0; thus

$$\{\gamma(a_1), \dots, \gamma(a_d)\} = \{b_1, \dots, b_d\}.$$

Hence there is a permutation  $\mu \in S_d$  such that  $\gamma(a_i) = b_{\mu(i)}$ . The lemma follows from the invariance of the cross ratio under the action of  $\mathrm{GL}_2(\overline{K})$ .  $\square$

**Lemma 3.30.** *Let  $\ell \geq 11$  be prime. Then there is some  $a \in \mathbb{Z}_\ell^\times$  of order  $\ell - 1$  such that*

$$\begin{aligned} 1 + a^2 \not\equiv 0, \pm(1 - a^2), \pm(a + a^3), \pm(a - a^3), \\ \pm(1 + a^3), \pm(1 - a^3), \pm(a + a^2), \pm(a - a^2) \pmod{\ell}. \end{aligned} \quad (3.30)$$

*Proof.* Making use of the fact that a polynomial of degree  $n$  has at most  $n$  roots, we see that the number of  $a \in \mathbb{F}_\ell$  that **do not satisfy** (3.30) is (very crudely) bounded by 37. An element  $a \in \mathbb{Z}_\ell^\times$  of order  $\ell - 1$  is the unique Hensel lift of an element  $a \in \mathbb{F}_\ell^\times$  of order  $\ell - 1$ . There are precisely  $\varphi(\ell - 1)$  elements of order  $\ell - 1$  in  $\mathbb{F}_\ell^\times$ . A theorem of Shapiro [401, page 23], asserts that  $\varphi(n) > n^{\log 2 / \log 3}$  for  $n \geq 30$ . We note that if  $\ell \geq 317$  then  $\varphi(\ell - 1) \geq 316^{\log 2 / \log 3} \approx 37.8$ , and so the lemma holds for  $\ell \geq 317$ . For the range  $11 \leq \ell \leq 317$  we checked the lemma by brute force computer enumeration.  $\square$

**Lemma 3.31.** *Let  $n > m$  be sufficiently large. Then  $D_n$  and  $D_m$  are non-isomorphic, even over  $\overline{\mathbb{Q}}$ .*

*Proof.* Note that all roots of the hyperelliptic polynomial for  $D_n$  in (3.29) belong to  $\mathcal{Z}_n^+$ . It follows from (3.27) that the cross ratio of any four of them belongs to  $V_n$ . Suppose  $D_n$  and  $D_m$  are isomorphic. Let  $u_1, u_2, u_3, u_4$  be any distinct roots of the hyperelliptic polynomial for  $D_n$  given in (3.29). Then, by Lemma 3.29,

$$(u_1, u_2; u_3, u_4) \in V_m \subseteq V_{n-1}.$$

We shall obtain a contradiction through a careful choice of the four roots  $u_1, \dots, u_4$ .

We first suppose that  $k \geq 2$  and  $\ell \geq 5$ . Let  $\zeta = \zeta_{\ell^n}$  and  $b = 1 + \ell^{n-1}$ . Then, by Lemma 3.26,  $\eta_1 = \zeta + \zeta^{-1}$  and  $\eta_2 = \zeta^b + \zeta^{-b}$ . Let  $a \in \mathbb{Z}_\ell^\times$  have order  $\ell - 1$ . Let  $\kappa \in \mathrm{Gal}(\Omega_{n,\ell}/\mathbb{Q}_{n-1,\ell})$  be given by  $\kappa(\zeta) = \zeta^a$ . Then  $\kappa$  is a cyclic generator for

$\text{Gal}(\Omega_{n,\ell}/\mathbb{Q}_{n-1,\ell})$ . We shall denote the restriction of  $\kappa$  to  $\Omega_{n,\ell}^+$  by  $\mu$ . Then  $\mu$  is a cyclic generator for  $G_n = \text{Gal}(\Omega_{n,\ell}^+/\mathbb{Q}_{n-1,\ell})$  having order  $(\ell - 1)/2$ . We shall take

$$\begin{aligned} u_1 &= \eta_1 = \zeta + \zeta^{-1}, & u_2 &= \mu(\eta_1) = \zeta^a + \zeta^{-a}, \\ u_3 &= \eta_2 = \zeta^b + \zeta^{-b}, & u_4 &= \mu(\eta_2) = \zeta^{ab} + \zeta^{-ab}. \end{aligned}$$

We compute the cross ratio with the help of identity (3.27), finding

$$(u_1, u_2; u_3, u_4) = \frac{(1 - \zeta^{1+b})(1 - \zeta^{1-b})(1 - \zeta^{a+ab})(1 - \zeta^{a-ab})}{(1 - \zeta^{1+ab})(1 - \zeta^{1-ab})(1 - \zeta^{a+b})(1 - \zeta^{a-b})}.$$

As  $b \equiv 1 \pmod{\ell}$ , and clearly  $a \not\equiv \pm 1 \pmod{\ell}$ , it is easy to check that  $1 + b$  is the only one out of the eight exponents of  $\zeta$  above that is  $\pm 2 \pmod{\ell}$ . Therefore by Lemma 3.11, the cross ratio is not an element of  $\langle \pm \zeta_{\ell^n}, V_{n-1} \rangle$  for  $n$  sufficiently large, giving a contradiction for the case  $k \geq 2$  and  $\ell \geq 5$ .

Next we suppose that  $k = 1$ . It follows from (3.25) that  $\ell \geq 11$ . We choose  $a \in \mathbb{Z}_{\ell}^{\times}$  as in Lemma 3.30, and, as above, take  $\mu$  to be the corresponding generator of  $G_n$  of order  $(\ell - 1)/2 \geq 5$ . We take

$$u_i = \mu^{i-1}(\eta_1) = \zeta^{a^{i-1}} + \zeta^{-a^{i-1}}, \quad 1 \leq i \leq 4;$$

observe that these are four roots of the hyperelliptic polynomial of  $D_n$  given in (3.29). The assumption that  $\ell \geq 11$  ensures that  $a$  has order  $\geq 10$  and so  $u_1, u_2, u_3, u_4$  are indeed pairwise distinct. We compute the cross ratio with the help of identity (3.27), finding

$$(u_1, u_2; u_3, u_4) = \frac{(1 - \zeta^{1+a^2})(1 - \zeta^{1-a^2})(1 - \zeta^{a+a^3})(1 - \zeta^{a-a^3})}{(1 - \zeta^{1+a^3})(1 - \zeta^{1-a^3})(1 - \zeta^{a+a^2})(1 - \zeta^{a-a^2})}.$$

Using Lemma 3.10 and our choice of  $a$  given by Lemma 3.30 we conclude that this cross ratio does not belong to  $\langle \pm \zeta_{\ell^n}, V_{n-1} \rangle$  for  $n$  sufficiently large. This gives a contradiction for the case  $k = 1$ .

Finally, we consider  $\ell = 3$ . It follows from (3.25) that  $k \geq 5$ . Recall our choices of  $\eta_1, \eta_2, \eta_3$  in Lemma 3.26, and our choice of  $\eta_4 = \zeta^2 + \zeta^{-2}$  in the particular case  $\ell = 3$ . We choose the four roots  $u_i = \eta_i$  for  $i = 1, \dots, 4$ , and obtain,

$$(u_1, u_2; u_3, u_4) = \frac{(1 - \zeta^{2+2 \times 3^{n-1}})(1 - \zeta^{-2 \times 3^{n-1}})(1 - \zeta^{3+3^{n-1}})(1 - \zeta^{-1+3^{n-1}})}{(1 - \zeta^3)(1 - \zeta^{-1})(1 - \zeta^2)(1 - \zeta^{-3^{n-1}})}.$$

As before, with the help of Lemma 3.11, we easily verify that the cross ratio is not an element of  $\langle \pm \zeta_{\ell^n}, V_{n-1} \rangle$  for  $n$  sufficiently large. This completes the proof.  $\square$

### Proof of Theorem 3.6

If  $\ell = 3$  or  $5$  then (3.24) does not impose any restriction on the genus. Therefore we obtain, as above, for every genus  $g \geq 2$ , infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes of genus  $g$  hyperelliptic curves, defined over  $\mathbb{Q}_{\infty, \ell}$ , with good reduction away from  $\{v_2, v_\ell\}$ .

It remains to deal with  $\ell = 7, 11$  and  $13$ . Here, (3.24) imposes the restriction

$$g \equiv \begin{cases} 1 \text{ or } 2 \pmod{3} & \text{if } \ell = 7 \\ 2 \text{ or } 4 \pmod{5} & \text{if } \ell = 11 \\ 2 \pmod{3} & \text{if } \ell = 13. \end{cases}$$

We very briefly sketch how to remove the restriction. Instead of  $D_n$  defined as in (3.29), we consider the more general

$$D_n : Y^2 = h(X) \cdot \prod_{j=1}^k \prod_{\sigma \in G_n} (X - \eta_j^\sigma)$$

where

- $h$  is a monic divisor of  $X(X-1)(X+1)$ ;
- $k$  and  $h$  are chosen to obtain the desired genus;
- $\eta_j \in \mathcal{Z}_n^+$  are chosen as before.

These  $D_n$  are clearly defined over  $\mathbb{Q}_{n-1, \ell}$ . To check that they have good reduction away from  $S' = \{v_2, v_\ell\}$ , we need to verify that the difference of any two distinct roots  $u, v$  of the hyperelliptic polynomial belongs to  $\mathcal{O}(\Omega_n, S')^\times$ . The proof of Lemma 3.27 shows this if  $u, v \in \mathcal{Z}_n^+$ . For the remaining possible differences it is enough to note that

$$\alpha + \alpha^{-1} = \alpha^{-1}\Phi_4(\alpha), \quad \alpha + \alpha^{-1} + 1 = \alpha^{-1}\Phi_3(\alpha), \quad \alpha + \alpha^{-1} - 1 = \alpha^{-1}\Phi_6(\alpha)$$

which are all units by Lemma 3.13. We omit the remaining details.  $\square$

### 3.9 Isogeny classes of hyperelliptic curves over $\mathbb{Q}_{\infty, \ell}$

A beautiful theorem of Kummer asserts that the index of the cyclotomic units  $C_n$  in the full unit group  $\mathcal{O}(\Omega_{n, \ell})^\times$  equals the class number  $h_n^+$  of  $\Omega_{n, \ell}^+$ . In this section, with the help of Kummer's theorem, we prove for certain primes  $\ell$  the existence

of infinitely many isogeny classes of hyperelliptic Jacobians over  $\mathbb{Q}_{\infty, \ell}$  with good reduction away from  $\ell$ . We first prove a few elementary lemmas.

**Lemma 3.32.** *Let  $K$  be a field of characteristic not 2, and let  $L = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_r})$  where  $\alpha_i \in K^\times$ . Then for any  $x \in K$  such that  $\sqrt{x} \in L$ , we have*

$$x = \alpha_1^{e_1} \cdots \alpha_r^{e_r} q^2$$

for some integers  $e_i \in \mathbb{Z}$  and  $q \in K$ .

*Proof.* Let  $M$  be a field of characteristic not 2, and let  $d \in M$  be a non-square. Let  $x \in M$  and suppose  $\sqrt{x} \in M(\sqrt{d})$ . Then  $\sqrt{x} = y + z\sqrt{d}$  for some  $y, z \in M$ . Squaring, we deduce that  $yz = 0$ . Thus  $x = y^2$  or  $x = dz^2$ .

We now prove the lemma by induction on  $r$ . The above establishes the case  $r = 1$ . Let  $r \geq 2$ , and let  $x \in K$  satisfy  $\sqrt{x} \in L$ . Letting  $M = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_{r-1}})$  we see that  $x \in M$  and  $\sqrt{x} \in M(\sqrt{\alpha_r})$ . Thus, by the above,  $\sqrt{x} \in M$  or  $\sqrt{x\alpha_r} \in M$ . In other words,

$$\sqrt{x \cdot \alpha_r^e} \in M = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_{r-1}})$$

for some  $e \in \{0, 1\}$ . By the inductive hypothesis, there are  $e_1, \dots, e_{r-1} \in \mathbb{Z}$  and  $q \in K$  such that

$$x \cdot \alpha_r^e = \alpha_1^{e_1} \cdots \alpha_{r-1}^{e_{r-1}} q^2.$$

The proof is complete on taking  $e_r = -e$ . □

**Lemma 3.33.** *Let  $\ell$  be an odd prime. Let  $q \in \Omega_{\infty, \ell}$  satisfy  $q^2 \in V_n$ . If the class number  $h_n^+$  of  $\Omega_{n, \ell}^+$  is odd, then  $q \in V_n$ .*

*Proof.* Let  $q \in \Omega_{\infty, \ell}$  satisfy  $q^2 \in V_n \subset \Omega_{n, \ell}$ . As the extension  $\Omega_{\infty, \ell}/\Omega_{n, \ell}$  is pro- $\ell$ , we conclude that  $q \in \Omega_{n, \ell}$ . However,  $V_n \subseteq \mathcal{O}(\Omega_{n, \ell}, \{v_\ell\})^\times$ , where, as usual,  $v_\ell$  denotes the prime above  $\ell$ . Thus  $q \in \mathcal{O}(\Omega_{n, \ell}, \{v_\ell\})^\times$ . We claim that

$$[\mathcal{O}(\Omega_{n, \ell}, \{v_\ell\})^\times : V_n] = h_n^+.$$

The lemma follows immediately from the claim. To prove the claim, consider the commutative diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & C_n & \longrightarrow & V_n & \xrightarrow{\kappa} & \mathbb{Z} \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \mathcal{O}(\Omega_{n, \ell})^\times & \longrightarrow & \mathcal{O}(\Omega_{n, \ell}, \{v_\ell\})^\times & \xrightarrow{\kappa} & \mathbb{Z} \longrightarrow 1 \end{array}$$

where  $\kappa(\alpha) = \text{ord}_{(1-\zeta)}(\alpha)$ . By the snake lemma,

$$\mathcal{O}(\Omega_{n,\ell}, \{v_\ell\})^\times / V_n \cong \mathcal{O}(\Omega_{n,\ell})^\times / C_n.$$

Write  $C_n^+ = C_n \cap \Omega_{n,\ell}^+$ . The aforementioned theorem of Kummer asserts that

$$[\mathcal{O}(\Omega_{n,\ell})^\times : C_n] = [\mathcal{O}(\Omega_{n,\ell}^+)^\times : C_n^+] = h_n^+;$$

see, for example, [475, Exercise 8.5] for the first equality, and [475, Theorem 8.2] for the second. This proves the claim.  $\square$

**Lemma 3.34.** *Let  $K$  be a field of characteristic  $\neq 2$ . Let  $f \in K[X]$  be a monic separable polynomial of odd degree  $d \geq 5$ . Write  $f = \prod_{i=1}^d (X - \alpha_i)$  with  $\alpha_i \in \overline{K}$ . Let  $C/K$  be a hyperelliptic curve given by  $Y^2 = f(X)$  with Jacobian  $J$ . Then*

$$K(J[2]) = K(\alpha_1, \dots, \alpha_d), \quad K(J[4]) = K(J[2]) \left( \left\{ \sqrt{\alpha_i - \alpha_j} \right\}_{1 \leq i, j \leq d} \right).$$

*Proof.* Write  $\infty$  for the point at infinity on the given model for  $C$ . The expression given for  $K(J[2])$  is proven in Theorem 1.8; recall that it follows by noting that the classes of degree 0 divisors  $[(\alpha_i, 0) - \infty]$  with  $i = 1, \dots, d$  generate  $J[2]$  (e.g. see also [377]).

Yelton [485, Theorem 1.2.2] gives a high-powered proof of the given expression for  $K(J[4])$ . For the convenience of the reader we give a more elementary argument. Let  $L = K(J[2])$ . The theory of 2-descent on hyperelliptic Jacobians furnishes, for any field  $M \supseteq L$ , an injective homomorphism [377], [429]

$$J(M)/2J(M) \hookrightarrow \prod_{i=1}^d M^*/(M^*)^2$$

known as the  $X - \Theta$ -map. This in particular sends the 2-torsion point  $[(\alpha_i, 0) - \infty]$  to

$$\left( (\alpha_i - \alpha_1), \dots, (\alpha_i - \alpha_{i-1}), \prod_{j \neq i} (\alpha_i - \alpha_j), (\alpha_i - \alpha_{i+1}), \dots, (\alpha_i - \alpha_d) \right).$$

The field  $K(J[4])$  is the smallest extension of  $M$  of  $L$  such that all the images of the 2-torsion generators  $[(\alpha_i, 0) - \infty]$  are trivial in  $\prod_{i=1}^d M^*/(M^*)^2$ . This is plainly the extension

$$M = L \left( \left\{ \sqrt{\alpha_i - \alpha_j} \right\}_{1 \leq i, j \leq d} \right).$$

□

**Lemma 3.35.** *Let  $p$  be a prime for which 2 is a primitive root (i.e. 2 is a generator for  $\mathbb{F}_p^\times$ ). Let  $G$  be a cyclic group of order  $p$ , and let  $V$  be an  $\mathbb{F}_2[G]$ -module with  $\dim_{\mathbb{F}_2}(V) = p - 1$ . Suppose that the action of  $G$  on  $V \setminus \{0\}$  is free. Then  $V$  is irreducible.*

*Proof.* Let  $W$  be a  $\mathbb{F}_2[G]$ -submodule of  $V$ , and write  $d = \dim_{\mathbb{F}_2}(W)$ . Since the action of  $G$  on  $V \setminus \{0\}$  is free, the set  $W \setminus \{0\}$  consists of  $G$ -orbits, all having size  $p$ . However,  $\#(W \setminus \{0\}) = 2^d - 1$ , and so  $p \mid (2^d - 1)$ . By assumption, 2 is a primitive root modulo  $p$ , therefore  $(p - 1) \mid d$ . Since  $W$  is an  $\mathbb{F}_2$ -subspace of  $V$  which has dimension  $p - 1$ , we see that  $W = 0$  or  $W = V$ . □

**Lemma 3.36.** *Let  $\ell = 2p + 1$ , where  $\ell$  and  $p$  are odd primes. Suppose 2 is a primitive root modulo  $p$ . Let  $g = (\ell - 3)/4$ . Let  $n \geq 2$  and let  $D_n/\mathbb{Q}_{n-1,\ell}$  be the hyperelliptic curve defined in Section 3.8. Let  $A/\mathbb{Q}_{\infty,\ell}$  be an abelian variety and let  $\phi : J(D_n) \rightarrow A$  be an isogeny defined over  $\mathbb{Q}_{\infty,\ell}$ . Then  $\phi = 2^r \phi_{\text{odd}}$  where  $\phi_{\text{odd}} : J(D_n) \rightarrow A$  is an isogeny of odd degree.*

We remark if  $\ell$  and  $p$  are primes with  $\ell = 2p + 1$  then  $p$  is called a Sophie-Germain prime, and  $\ell$  is called a safe prime.

*Proof of Lemma 3.36.* Note that, in the notation of Section 3.8,  $k = 1$ , and the hyperelliptic polynomial for  $D_n$  has odd degree  $2g + 1 = (\ell - 1)/2 = p$ , and consists of a single orbit under action of  $G_n = \text{Gal}(\Omega_n^+/\mathbb{Q}_{n-1,\ell})$ :

$$D_n : Y^2 = \prod_{\sigma \in G_n} (X - \eta_1^\sigma), \quad \eta_1 = \zeta_{\ell^n} + \zeta_{\ell^n}^{-1}.$$

In particular, the hyperelliptic polynomial is irreducible over  $\mathbb{Q}_{\infty,\ell}$ . It follows from this (e.g. [429, Lemma 4.3]) that  $J(\mathbb{Q}_{\infty,\ell})[2] = 0$ , where  $J$  denotes  $J(D_n)$  for convenience. We note, by Lemma 3.34, that  $\mathbb{Q}_{\infty,\ell}(J[2]) = \mathbb{Q}_{\infty,\ell}(\eta_1) = \Omega_{\infty,\ell}^+$ . We consider the action of  $G_\infty := \text{Gal}(\Omega_{\infty,\ell}^+/\mathbb{Q}_{\infty,\ell})$  on  $J[2]$ . The group  $G_\infty$  is cyclic of order  $(\ell - 1)/2 = p$ . Any element fixed by this action belongs to  $J(\mathbb{Q}_{\infty,\ell})[2] = 0$ . Thus  $G_\infty$  acts freely on  $V \setminus \{0\}$ , where  $V := J[2]$ .

Now let  $\phi : J \rightarrow A$  be an isogeny defined over  $\mathbb{Q}_{\infty,\ell}$ . Then  $W := \ker(\phi) \cap J[2]$  is a subgroup of  $V$  stable under the action of  $G_\infty$ , and therefore an  $\mathbb{F}_2[G_\infty]$ -submodule of the  $\mathbb{F}_2[G_\infty]$ -module  $V$ . Observe that  $\dim_{\mathbb{F}_2}(V) = 2g = p - 1$ . By hypothesis, 2 is a primitive root modulo  $p$ . We apply Lemma 3.35 to deduce that  $W = 0$  or  $W = V$ . Therefore, either  $\phi$  already has odd degree, or  $J[2] \subseteq \ker(\phi)$ . In the latter case, observe that  $\phi = 2\phi'$  where  $\phi' : J \rightarrow A$  is an isogeny defined over



$\mathbb{Q}_{\infty,\ell}$  of degree  $\deg(\phi)/2^{2g}$ . As  $\phi$  has finite degree, by repeating the argument we eventually arrive at  $\phi = 2^r \phi_{\text{odd}}$ .  $\square$

**Lemma 3.37.** *Let  $\ell = 2p + 1$ , where  $\ell$  and  $p$  are odd primes. Suppose 2 is a primitive root modulo  $p$ . Suppose that the class number  $h_n^+$  of  $\Omega_{n,\ell}^+$  is odd for all  $n$ . Let  $g = (\ell - 3)/4$ . For  $n \geq 2$  let  $D_n/\mathbb{Q}_{n-1,\ell}$  be the genus  $g$  hyperelliptic curve defined in Section 3.8. Let  $n > m$  be sufficiently large. Then there are no isogenies  $J(D_n) \rightarrow J(D_m)$  defined over  $\mathbb{Q}_{\infty,\ell}$ .*

The assumption that  $h_n^+$  is odd for all  $n$  may seem at first sight very restrictive. However, it is conjectured [85] that  $h_{n+1}^+ = h_n^+$  for all but finitely many pairs  $(\ell, n)$ . Moreover, Washington [474] has shown that  $\text{ord}_p(h_n)$  remains bounded as  $n \rightarrow \infty$ , for any fixed prime  $p$ .

*Proof of Lemma 3.37.* Write  $J_n$  for  $J(D_n)$ . Suppose there is an isogeny  $\phi : J_n \rightarrow J_m$  defined over  $\mathbb{Q}_{\infty,\ell}$ . By Lemma 3.36 we may suppose that  $\phi$  has odd degree, and so  $\ker(\phi) \cap J_n[4] = 0$ . Thus  $\phi$  restricted to  $J_n[4]$  induces an isomorphism of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{\infty,\ell})$ -modules  $J_n[4] \cong J_m[4]$ . In particular,  $\mathbb{Q}_{\infty,\ell}(J_n[4]) = \mathbb{Q}_{\infty,\ell}(J_m[4])$ . As in the proof of Lemma 3.36 we have  $\mathbb{Q}_{\infty,\ell}(J_n[2]) = \mathbb{Q}_{\infty,\ell}(J_m[2]) = \Omega_{\infty,\ell}^+$ . Thus, by Lemma 3.34, the equality  $\mathbb{Q}_{\infty,\ell}(J_n[4]) = \mathbb{Q}_{\infty,\ell}(J_m[4])$  may be rewritten as

$$\Omega_{\infty,\ell}^+ \left( \left\{ \sqrt{\vartheta_{n,i} - \vartheta_{n,j}} \right\}_{1 \leq i,j \leq (\ell-1)/2} \right) = \Omega_{\infty,\ell}^+ \left( \left\{ \sqrt{\vartheta_{m,i} - \vartheta_{m,j}} \right\}_{1 \leq i,j \leq (\ell-1)/2} \right)$$

where  $\vartheta_{r,i} := \mu_r^{i-1}(\zeta_{\ell^r} + \zeta_{\ell^r}^{-1})$  where  $\mu_r$  is a cyclic generator of  $G_r$ . This, in particular, implies that

$$\sqrt{\vartheta_{n,2} - \vartheta_{n,1}} \in \Omega_{\infty,\ell}^+ \left( \left\{ \sqrt{\vartheta_{m,i} - \vartheta_{m,j}} \right\}_{1 \leq i,j \leq (\ell-1)/2} \right)$$

We apply Lemma 3.32 to obtain

$$\vartheta_{n,2} - \vartheta_{n,1} = \pm \prod_{1 \leq i < j \leq \frac{\ell-1}{2}} (\vartheta_{m,i} - \vartheta_{m,j})^{e_{i,j}} \cdot q^2$$

for some integers  $e_{i,j} \in \mathbb{Z}$  and  $q \in \Omega_{\infty,\ell}^+$ . By Lemma 3.33, we have  $q \in V_n$ . The generator  $\mu_n$  of  $G_n$  is given by  $\mu_n(\zeta_{\ell^n} + \zeta_{\ell^n}^{-1}) = \zeta_{\ell^n}^a + \zeta_{\ell^n}^{-a}$  where  $a \in \mathbb{Z}_{\ell}^{\times}$  has order  $(\ell - 1)$ . Note

$$\vartheta_{n,2} - \vartheta_{n,1} = \zeta_{\ell^n}^a + \zeta_{\ell^n}^{-a} - \zeta_{\ell^n} - \zeta_{\ell^n}^{-1} = \zeta_{\ell^n}^{-a}(1 - \zeta_{\ell^n}^{a+1})(1 - \zeta_{\ell^n}^{a-1}).$$

Thus,

$$(1 - \zeta_{\ell^n}^{a+1})(1 - \zeta_{\ell^n}^{a-1}) \in \langle \pm \zeta_{\ell^n}, V_m, V_n^2 \rangle.$$

However,  $(a+1) \not\equiv \pm(a-1) \pmod{\ell}$ . Now Corollary 3.12 gives a contradiction.  $\square$

### Proof of Theorem 3.7

Let  $\ell \geq 11$ . Let

$$g = \lfloor (\ell - 3)/4 \rfloor = \begin{cases} (\ell - 3)/4 & \ell \equiv 3 \pmod{4} \\ (\ell - 5)/4 & \ell \equiv 1 \pmod{4}. \end{cases}$$

Thus  $g$  satisfies (3.24). Let  $D_n$  be as in Section 3.8. By Lemma 3.27, the hyperelliptic curve  $D_n/\mathbb{Q}_{n-1,\ell}$  has genus  $g$ , and good reduction away from  $\{v_2, v_\ell\}$ . Moreover, by Lemma 3.31, we have  $D_n$  and  $D_m$  are non-isomorphic, even over  $\overline{\mathbb{Q}}$ , for  $n > m$  sufficiently large.

Now suppose

- (i)  $\ell = 2p + 1$  where  $p$  is also an odd prime;
- (ii) 2 is a primitive root modulo  $p$ .

It then follows from Lemma 3.37 that  $J(D_n)$  and  $J(D_m)$  are non-isogenous over  $\mathbb{Q}_{\infty,\ell}$  provided  $h_n^+$  is odd for all  $n$ , where  $h_n^+$  denotes the class number of  $\Omega_{n,\ell}^+$ . Write  $h_n$  for the class number of  $\Omega_{n,\ell}$ . It is known thanks to the work of Estes [158] that  $h_1$  is odd for all primes  $\ell$  satisfying (i) and (ii) (a simplified proof of this result is given Stevenhagen [425, Corollary 2.3]). Moreover, Ichimura and Nakajima [229] show, for primes  $\ell \leq 509$ , that the ratio  $h_n/h_1$  is odd for all  $n$ . The primes  $11 \leq \ell \leq 509$  satisfying both (i) and (ii) are 11, 23, 59, 107, 167, 263, 347, 359. Thus for these primes  $h_n$  is odd for all  $n$ . As  $h_n^+ \mid h_n$  (see for example [475, Theorem 4.10]), we know for these primes that  $h_n^+$  is odd for all  $n$ . This completes the proof.  $\square$

### Remarks.

- A key step in our proof of Theorem 3.7 is showing that  $J(D_n)[2]$  is irreducible as an  $\mathbb{F}_2[G_\infty]$ -module whenever  $\ell = 2p + 1$  where  $p$  is a prime having 2 as a primitive root. It can be shown for all other  $\ell$  that the  $\mathbb{F}_2[G_\infty]$ -module  $J(D_n)[2]$  is in fact reducible.
- Another key step is the argument in the proof of Lemma 3.37 showing that for  $n > m$  sufficiently large, the Jacobians  $J(D_n)$  and  $J(D_m)$  are not related

via odd degree isogenies defined over  $\mathbb{Q}_{\infty, \ell}$ . This step can be made to work, with very minor modifications to the argument, for all  $\ell \geq 11$ , and all choices of genus  $g$  given in (3.24).

### 3.10 Endomorphism rings

To conclude this chapter, we study the possible endomorphism rings of the Jacobians of our elliptic curve and hyperelliptic curve constructions. We begin by stating a trivial corollary of Lemma 3.24.

**Corollary 3.38.** *Let  $\ell = 2, 3, 5$ , or  $7$ , and let  $S = \{v_2, v_\ell\}$ . There are infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves defined over  $\mathbb{Q}_{\infty, \ell}$  with good reduction away from  $S$  whose geometric endomorphism ring  $\text{End}(E_{\overline{\mathbb{Q}}})$  is  $\mathbb{Z}$ .*

*Proof.* This follows immediately from Lemma 3.24 as an elliptic curve  $E/K$  has potential CM if and only if  $\text{End}(E_{\overline{\mathbb{Q}}}) \neq \mathbb{Z}$ .  $\square$

This naturally motivates the question of whether similar statements for higher genus hyperelliptic curves exist. We thus conjecture the following strengthening of Theorem 3.6.

**Conjecture.** *Let  $g \geq 2$  and let  $\ell = 3, 5, 7, 11$  or  $13$ . There are infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes of genus  $g$  hyperelliptic curves  $C$  over  $\mathbb{Q}_{\infty, \ell}$  with good reduction away from  $\{v_2, v_\ell\}$ , such that their Jacobian  $J = \text{Jac}(C)$  satisfies  $\text{End}(J_{\overline{\mathbb{Q}}}) = \mathbb{Z}$ .*

Whilst this seems out of reach with current methods, we can show the following weaker results.

**Theorem 3.39.** *Let  $\ell = 2p + 1$ , where  $\ell$  and  $p$  are odd primes. Suppose  $2$  is a primitive root modulo  $p$ . Let  $g = (\ell - 3)/4$ . Let  $n \geq 2$  and let  $D_n/\mathbb{Q}_{n-1, \ell}$  be the genus  $g$  hyperelliptic curve*

$$D_n : Y^2 = \prod_{\sigma \in G_n} (X - \eta_1^\sigma), \quad \eta_1 = \zeta_{\ell^n} + \zeta_{\ell^n}^{-1} \quad (3.31)$$

*as defined in Section 3.8. Then the Jacobian  $J$  of  $D_n$  is  $\mathbb{Q}_{\infty, \ell}$ -simple.*

*Proof.* Noting that  $G_\infty$  is cyclic of order  $p$  and that  $\dim_{\mathbb{F}_2} J(D_n)[2] = p - 1$ , we can apply Lemma 3.35 to get that  $J(D_n)[2]$  is irreducible as an  $\mathbb{F}_2[G_\infty]$ -module. This proves the claim.  $\square$

To obtain results on the possible geometric endomorphism rings  $\text{End}(J_{\overline{\mathbb{Q}}})$  that can occur for the Jacobians  $J = \text{Jac}(D_n)$ , we can state the following two theorems, applying some recent work of Pip Goodman [195, 196].

**Theorem 3.40.** *Let  $\ell = 2p + 1$ , where  $\ell$  and  $p$  are odd primes. Suppose 2 is a primitive root modulo  $p$ . Let  $g = (\ell - 3)/4$ . Let  $n \geq 2$ , let  $D_n/\mathbb{Q}_{n-1,\ell}$  be the genus  $g$  hyperelliptic curve as given in (3.31), and let  $J = \text{Jac}(D_n)$  denote the Jacobian of  $D_n$ . Then one of the following two things is true:*

1. *The geometric endomorphism algebra  $E := \text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$  is a number field (and where 2 is totally inert in  $E/\mathbb{Q}$  and the order  $\text{End}(J_{\overline{\mathbb{Q}}})$  is 2-maximal in  $E$ ; i.e. the index of  $\text{End}(J_{\overline{\mathbb{Q}}})$  in  $\mathcal{O}_E$  is odd)*
2.  *$J$  is isogenous over  $\overline{\mathbb{Q}}$  to the power of an absolutely simple abelian variety with CM by a proper subfield of  $\mathbb{Q}(\zeta_p)$ .*

*Proof.* This follows from the main theorem of Goodman [196, Theorem 1.1].  $\square$

In the particular case where  $\ell = 11$  and  $D_n$  is a genus 2 curve, we can show that the second case above never occurs.

**Theorem 3.41.** *Let  $\ell = 11$  and  $g = 2$  and let  $D_n/\mathbb{Q}_{n-1,11}$  be the genus 2 hyperelliptic curve*

$$Y^2 = \prod_{\sigma \in G_n} (X - \eta_1^\sigma), \quad \eta_1 = \zeta_{11^n} + \zeta_{11^n}^{-1}.$$

*Then  $\text{Jac}(D_n)$  is absolutely simple and does not have CM.*

*Proof.* Recall that  $D_n$  has genus 2 and is defined over  $\mathbb{Q}_{n-1,11}$ . Since  $\mathbb{Q}(\eta_1) = \Omega_{n,11}^+$ , we have that  $\text{Gal}(\mathbb{Q}_{n-1,11}(J[2])/\mathbb{Q}_{n-1,11}) = \text{Gal}(\Omega_{n,11}^+/\mathbb{Q}_{n-1,11}) \cong C_5$ . We can therefore apply a theorem of Goodman [196, Theorem 2.10] to deduce that  $J(D_n)$  is absolutely simple.

Furthermore, using [195, Corollary 2.3.15], if  $J(D_n)$  has CM, then  $\mathbb{Q}_{n-1,11}$  must contain a real quadratic field, which is impossible as the degree of  $\mathbb{Q}_{n-1,11}$  is  $11^{n-1}$  which is odd. Thus  $J(D_n)$  does not have CM.  $\square$

**Remark.** Goodman's results [196, Theorem 2.10] furthermore show that, for  $\ell = 11$  and  $g = 2$ , the geometric endomorphism ring  $\text{End}(J_{\overline{\mathbb{Q}}})$  is either  $\mathbb{Z}$ , or  $\mathbb{Z}[\frac{1+r\sqrt{D}}{2}]$  for some positive integer  $D \equiv 5 \pmod{8}$  and odd integer  $r$ , or is a 2-maximal order in a degree 4 CM field which is totally inert at 2. It seems reasonable to conjecture that  $\text{End}(J_{\overline{\mathbb{Q}}})$  is always  $\mathbb{Z}$  for the Jacobians  $J$  of all our curves  $\{D_n\}_{n \geq 1}$  defined in (3.31), although we have been unable to prove this.

## Chapter 4

# Abelian surfaces $A/\mathbb{Q}$ with full rational 2-torsion

Recall Faltings' [164] celebrated proof that, given any number field  $K$ , dimension  $d$ , and finite set of places  $S$  in  $K$ , there are only finitely many isomorphism classes of dimension  $d$  abelian varieties  $A/K$  with good reduction away from  $S$ . However, other than some cases where either  $d = 1$  or  $S = \emptyset$ , effectively determining all such abelian varieties  $A/K$  with good reduction away from  $S$  remains a hard problem!

In this chapter, we shall take the first step towards solving the effective Shafarevich conjecture (Conjecture 1.5) in the case where  $d = 2$ ,  $K = \mathbb{Q}$  and  $S = \{2\}$ . In particular, we shall classify all isogeny classes of principally polarised abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 and satisfying  $\mathbb{Q}(A[2]) = \mathbb{Q}$ . To our knowledge, this is one of the first cases of the effective Shafarevich conjecture being partially solved for some  $(d, K, S)$  where  $d \geq 2$  and  $S \neq \emptyset$  with no condition on the conductor  $N$ , albeit with a condition on the field of 2-torsion  $\mathbb{Q}(A[2])$ .

As a warm-up, let's begin by considering the dimension 1 (elliptic curve) case:

**Theorem 4.1** (Ogg). *Let  $E/\mathbb{Q}$  be an elliptic curve with good reduction away from 2, and with full rational 2-torsion. Then  $E$  is isomorphic to either  $E_1 : y^2 = x^3 - x$  or  $E_2 : y^2 = x^3 - 4x$ .*

While Ogg [337] gave a full classification of all 24 elliptic curves  $E/\mathbb{Q}$  with good reduction away from 2, we can give a very short elementary proof in the case where  $E$  has full rational 2-torsion:

*Proof.* Since  $\mathbb{Q}(E[2]) = \mathbb{Q}$ , we note that  $E/\mathbb{Q}$  can be given by some globally minimal model  $y^2 = x(x - a)(x - b)$  for some distinct  $a, b \in \mathbb{Z}$ . As  $E/\mathbb{Q}$  has good reduction

away from 2, this implies  $\Delta = 16a^2b^2(a-b)^2$  is a power of two, and thus  $a$ ,  $b$  and  $a-b$  are all powers of 2 (up to a sign). If  $a = \pm 2^\alpha$  for some integer  $\alpha \geq 0$ , an easy check yields just three possibilities for  $b$ , namely  $b \in \{\pm 2^{\alpha-1}, \mp 2^\alpha, \pm 2^{\alpha+1}\}$ , with all cases being  $\mathbb{Q}$ -isomorphic to either  $E_1$  or  $E_2$ .  $\square$

Generalising the above proof to abelian surfaces  $A/\mathbb{Q}$  is far more non-trivial. Whilst elliptic curves have very simple models that allow for elementary arguments such as those given above, equations describing abelian surfaces are highly non-elementary, e.g. in general, models for abelian surfaces  $A/\mathbb{Q}$  require 72 equations in  $\mathbb{P}^{15}$ , as shown by Cassels–Flynn [98]. This is not a particularly pleasant thing to do. We therefore require techniques to classify abelian surfaces which avoid using any specific models.

We make the following conjecture.

**Conjecture 4.2.** *Let  $A/\mathbb{Q}$  be an abelian surface with good reduction away from 2, and with full rational 2-torsion. Then  $A$  is isomorphic to either  $E_1 \times E_1$ ,  $E_1 \times E_2$ , or  $E_2 \times E_2$ , where  $E_1$  and  $E_2$  are the elliptic curves  $E_1 : y^2 = x^3 - x$  and  $E_2 : y^2 = x^3 - 4x$ .*

Whilst the conjecture is still open, our main result in this chapter is successfully proving that any principally polarised abelian surfaces  $A/\mathbb{Q}$  such that  $\mathbb{Q}(A[2]) = \mathbb{Q}$  and with good reduction away from 2 must be isogenous to one of the three abelian surfaces above.

**Theorem 4.3.** *(Theorem 4.20) There are exactly three isogeny classes of principally polarised abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 which contain surfaces with full rational 2-torsion. These are given by  $E_1 \times E_1$ ,  $E_1 \times E_2$  and  $E_2 \times E_2$ , where  $E_1$  and  $E_2$  are the elliptic curves  $E_1 : y^2 = x^3 - x$  and  $E_2 : y^2 = x^3 - 4x$ .*

It's worth remarking that one advantage to dealing with the specific case of principally polarised abelian surfaces, compared to arbitrary abelian surfaces, is the following classification theorem:

**Theorem.** [193, Theorem 3.1] *Let  $K$  be a number field, and let  $A/K$  be a principally polarised abelian surface. Then  $A/K$  (as a polarised abelian variety) is isomorphic to one of the following three cases:*

1.  $A \cong \text{Jac}(C)$  where  $C/K$  is smooth genus 2 curve.
2.  $A \cong E_1 \times E_2$  where  $E_1, E_2$  are elliptic curves over  $K$ .

3.  $A \cong \text{Res}_{L/K} E$ , is the Weil restriction of an elliptic curve  $E/L$  where  $L$  is a quadratic extension of  $K$  (note  $A \cong_L E \times E^\sigma$  where  $\text{Gal}(L/K) = \langle \sigma \rangle$ ).

We note that classifying principally polarised abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 which fall in the second or third case above, can be reduced to essentially classifying elliptic curves over  $K$  with good reduction away from 2, where  $K$  is either  $\mathbb{Q}$ ,  $\mathbb{Q}(i)$ ,  $\mathbb{Q}(\sqrt{2})$  or  $\mathbb{Q}(\sqrt{-2})$ . Since all these cases have been dealt with by previous authors [337, 347, 245], a full classification of principally polarised abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 would thus follow from resolving the following problem, first proposed by Poonen [352, p. 301]:

**Problem 4.1** (Poonen 1996). List all genus 2 curves  $C/\mathbb{Q}$  whose Jacobians  $\text{Jac}(C)$  have good reduction away from 2.

So far, we have found 512 such genus 2 curves  $C/\mathbb{Q}$  via various methods (including 366 found by Smart [418]) divided into 175 isogeny classes, although so far we have only been able to prove completeness in certain particular cases where either the bad primes for  $C$  are bounded, or the field of 2-torsion for  $C$  is bounded. We will describe further computational methods to explicitly compute such genus 2 curves in Chapter 5 and give a list of all such known curves in Chapter 6.

The remainder of this chapter will now focus on setting up the necessary theoretical and computational prerequisites to prove Theorem 4.3.

## 4.1 Fields of 2-power torsion

**Lemma 4.4.** *Let  $A/\mathbb{Q}$  be an abelian surface with good reduction away from 2. Then  $\mathbb{Q}(A[2])$  is a 2-extension of  $\mathbb{Q}$  of degree at most  $2^6$ , unramified away from 2.*

*Proof.* Let  $\bar{\rho}_{A,2} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_4(\mathbb{F}_2)$  be the mod-2 Galois representation of  $A/\mathbb{Q}$ . As  $A/\mathbb{Q}$  has good reduction away from 2, this implies  $\bar{\rho}_{A,2}$  is unramified away from 2 (see e.g. [319, p. 141]) and thus it factors through  $\text{Gal}(\Omega_2/\mathbb{Q})$  where  $\Omega_2$  denotes the maximal extension of  $\mathbb{Q}$  unramified away from 2.

Let  $\rho : \text{Gal}(\Omega_2/\mathbb{Q}) \rightarrow \text{GL}_4(\mathbb{F}_2)$  be the induced Galois representation on  $A[2]$ . We have that  $\text{Gal}(\mathbb{Q}(A[2])/\mathbb{Q})$  is isomorphic to the image of  $\rho$ . By a result of Rasmussen–Tamagawa [360, Proposition 4.1], the image of  $\rho$  in  $\text{GL}_4(\mathbb{F}_2)$  is a 2-group, and so  $\mathbb{Q}(A[2])$  is a 2-extension of  $\mathbb{Q}$  unramified away from 2.

To bound the degree, we note that  $|\text{GL}_4(\mathbb{F}_2)| = \prod_{i=0}^3 (2^4 - 2^i) = 2^6 \cdot 315$ , and thus  $\text{im}(\rho)$  must have order at most  $2^6$ .  $\square$

**Remark.** It's worth mentioning that one cannot extend the above result to abelian varieties  $A/\mathbb{Q}$  of arbitrarily large dimension, as Rasmussen–Tamagawa [360] give an example of a dimension 272 abelian variety  $A/\mathbb{Q}$  with good reduction away from 2 where  $\mathbb{Q}(A[2])$  contains a degree 272 field unramified away from 2.

By using classical Hermite-Minkowski bounds, Lemma 4.4 implies we have only finitely many possibilities for  $\mathbb{Q}(A[2])$ . Indeed, if  $A$  is a principally polarised abelian surface, then it is known that  $\mathbb{Q}(A[2])$  is some compositum of the following ten fields

$$\begin{aligned} \mathbb{Q}, \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{1+\sqrt{-1}}), \mathbb{Q}(\sqrt{1+\sqrt{2}}), \\ \mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt[4]{-2}), \mathbb{Q}(\sqrt{-2-\sqrt{2}}), \mathbb{Q}(\sqrt{2+\sqrt{2}}). \end{aligned}$$

as shown in Table 5.4.

Whilst it may be possible to classify all such 2-torsion fields, for now we shall simply restrict our attention to the case where we have full rational 2-torsion (i.e.  $\mathbb{Q}(A[2]) = \mathbb{Q}$ ). In this case, we can uniquely determine the 4-torsion field  $\mathbb{Q}(A[4])$  and the 8-torsion field  $\mathbb{Q}(A[8])$  for any such abelian surface  $A/\mathbb{Q}$  with good reduction away from 2.

**Lemma 4.5.** *Let  $A/\mathbb{Q}$  be an abelian variety with full rational 2-torsion (i.e.  $\mathbb{Q}(A[2]) = \mathbb{Q}$ ). Then for all  $n \geq 1$ , the Galois group  $\text{Gal}(\mathbb{Q}(A[2^{n+1}])/\mathbb{Q}(A[2^n]))$  is an elementary abelian 2-group; in particular all non-identity elements of  $\text{Gal}(\mathbb{Q}(A[2^{n+1}])/\mathbb{Q}(A[2^n]))$  have order 2 and  $\text{Gal}(\mathbb{Q}(A[2^{n+1}])/\mathbb{Q}(A[2^n])) \cong C_2^k$  for some integer  $k \geq 0$ .*

*Proof.* We consider the mod  $2^{n+1}$  representation  $\bar{\rho}_{A,2^{n+1}} : \text{Gal}(\mathbb{Q}(A[2^{n+1}])/\mathbb{Q}) \rightarrow \text{GL}_{2d}(\mathbb{Z}/2^{n+1}\mathbb{Z})$ . Let  $\sigma \in \text{Gal}(\mathbb{Q}(A[2^{n+1}])/\mathbb{Q}(A[2^n]))$  and let  $M_\sigma := \bar{\rho}_{A,2^{n+1}}(\sigma)$ . As  $\sigma$  fixes the  $2^n$ -torsion field  $\mathbb{Q}(A[2^n])$ , we have that  $M_\sigma$  is an element of the matrix group  $R$ , defined as

$$R := \{M \in \text{GL}_{2d}(\mathbb{Z}/2^{n+1}\mathbb{Z}) : M \equiv I \pmod{2^n}\}.$$

Therefore, we can write  $M_\sigma = I + 2^n N_\sigma$  for some matrix  $N_\sigma \in \text{M}_{2d}(\mathbb{F}_2)$ . Thus, we note that

$$M_\sigma^2 = (I + 2^n N_\sigma)^2 = I + 2^{n+1} N_\sigma + 2^{2n} N_\sigma^2 \equiv I \pmod{2^{n+1}}$$

noting that  $n \geq 1$ . Therefore,  $M_\sigma^2$  is the identity in  $R$ , and thus  $\bar{\rho}_{A,2^{n+1}}(\sigma^2)$  is the identity matrix in  $\text{GL}_{2d}(\mathbb{Z}/2^{n+1}\mathbb{Z})$ . As  $\bar{\rho}_{A,2^{n+1}}$  is an injective map, this implies  $\sigma$  has order (at most) 2, and so  $\text{Gal}(\mathbb{Q}(A[2^{n+1}])/\mathbb{Q}(A[2^n]))$  is an elementary abelian



2-group. □

**Theorem 4.6.** *Let  $A/\mathbb{Q}$  be a principally polarised abelian variety with good reduction away from 2 and with full rational 2-torsion (i.e.  $\mathbb{Q}(A[2]) = \mathbb{Q}$ ). Then  $A$  has field of 4-torsion  $\mathbb{Q}(\zeta_8)$  and moreover, if  $\dim A \leq 2$ , then  $A$  has field of 8-torsion  $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$ .*

*Proof.* Let  $d$  be the dimension of  $A/\mathbb{Q}$ . As  $A/\mathbb{Q}$  has good reduction away from 2, this implies  $\mathbb{Q}(A[2^n])$  is unramified away from 2 for all  $n \geq 1$ . Furthermore, Lemma 4.5 implies that each element of  $\text{Gal}(\mathbb{Q}(A[2^{n+1}])/\mathbb{Q}(A[2^n]))$  has order at most 2, thus we obtain that the field  $\mathbb{Q}(A[2^{n+1}])$  is some compositum of degree 2 extensions of  $\mathbb{Q}(A[2^n])$  unramified away from 2. This allows us to inductively compute the possible fields for  $\mathbb{Q}(A[2^{n+1}])$  from  $\mathbb{Q}(A[2^n])$ .

By classical Hermite-Minkowski bounds, for each number field  $K$ , there are only finitely such bounded degree extensions of  $K$  unramified away from 2. Thus, for small  $n$ , we can classify all possibilities:

- **Case  $n = 1$ .** Note that the only quadratic extensions of  $\mathbb{Q}$  unramified away from 2 are  $\mathbb{Q}(i)$ ,  $\mathbb{Q}(\sqrt{2})$ , and  $\mathbb{Q}(\sqrt{-2})$ . The compositum of these three fields is  $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$ , and thus  $\mathbb{Q}(A[4]) \subset \mathbb{Q}(\zeta_8)$ .

Let  $K = \mathbb{Q}(A[4])$  be the 4-torsion field of  $A$ . As  $K$  is unramified away from 2, we can apply a theorem of Katz [255, p. 502] to obtain that the torsion subgroup  $A(K)_{\text{tors}}$  injects into  $A(\mathbb{F}_{\mathfrak{p}})$  for all odd primes  $\mathfrak{p}$  in  $K$ .

Thus, by Weil's inequality (e.g. see [18, p. 201]), we must have

$$|A(K)_{\text{tors}}| \leq |A(\mathbb{F}_{\mathfrak{p}})| \leq (N(\mathfrak{p}) + 1 + 2\sqrt{N(\mathfrak{p})})^d \quad (4.2)$$

for every odd prime  $\mathfrak{p}$  in  $K$ , noting that  $A$  has good reduction at  $\mathfrak{p}$  and  $K$  is unramified at  $\mathfrak{p}$ . As  $K$  must contain all  $4^{2d}$  4-torsion points, we must have  $|A(K)_{\text{tors}}| \geq 4^{2d}$ , and so (4.2) implies that  $N(\mathfrak{p}) \geq 9$  for all odd primes  $\mathfrak{p}$  in  $K$ .

This eliminates the possibility that  $\mathbb{Q}(A[4])$  is one of the three quadratic number fields, and thus the only remaining possibility is  $\mathbb{Q}(A[4]) = \mathbb{Q}(\zeta_8)$ .

- **Case  $n = 2$ .** Computing the quadratic extensions of  $\mathbb{Q}(\zeta_8)$  unramified away from 2, we get four (non-isomorphic) possible fields:  $\mathbb{Q}(\zeta_{16})$ ,  $\mathbb{Q}(\zeta_8, \sqrt[4]{2})$ ,  $\mathbb{Q}(\zeta_8, \sqrt{i+1})$ , and  $\mathbb{Q}(\sqrt{\zeta_8+1})$ .

As with the previous case, we have that  $\mathbb{Q}(A[8])$  must lie within the compositum of all four fields (i.e. the degree 32 field  $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}, \sqrt{\zeta_8+1})$ ), and additionally an analogous argument using the Weil inequalities imply that  $N(\mathfrak{p}) \geq 49$  for all odd primes  $\mathfrak{p}$  in  $\mathbb{Q}(A[8])$ .

Checking each case, this leaves us with only two possibilities for the field of 8-torsion: either the degree 16 field  $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$ , or the degree 32 field  $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}, \sqrt{\zeta_8 + 1})$ .

Assuming  $d \leq 2$ , we can now eliminate the latter case by considering the image of the mod 8 Galois representations  $\bar{\rho}_{A,8} : \text{Gal}(\mathbb{Q}(A[8])/\mathbb{Q}) \rightarrow \text{GSp}_4(\mathbb{Z}/8\mathbb{Z})$ . As  $\mathbb{Q}(A[2]) = \mathbb{Q}$ , this implies that  $\text{Gal}(\mathbb{Q}(A[8])/\mathbb{Q})$  must be isomorphic to a subgroup of  $R$  where

$$R := \{M \in \text{GSp}_4(\mathbb{Z}/8\mathbb{Z}) : M \equiv I \pmod{2}\}.$$

Calculating  $\text{Gal}(K/\mathbb{Q})$  for each of the two fields above gives the Galois groups **16T10** ( $C_2^2 \rtimes C_4$ ) and **32T19** ( $C_2^3 \rtimes C_4$ ) respectively, given as LMFDB labels. A brute force computer search tells us the latter is not a subgroup of  $R$ , and thus we must have  $\mathbb{Q}(A[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$ .

□

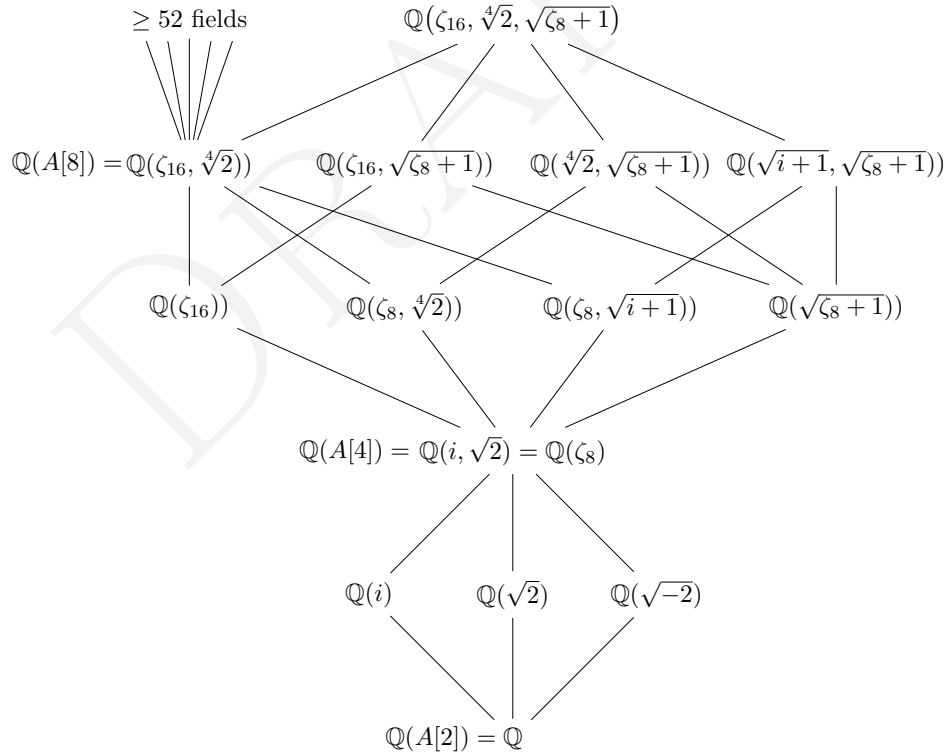


Figure 4.1: Field diagram of various 2-extensions of  $\mathbb{Q}$  unramified away from 2. In the case of Theorem 4.6, we have that  $\mathbb{Q}(A[4]) = \mathbb{Q}(\zeta_8)$  and  $\mathbb{Q}(A[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$ .

**Remarks.**

- For elliptic curves  $E/\mathbb{Q}$  with good reduction away from 2 and with full 2-torsion, a further computational calculation shows that  $\mathbb{Q}(E[16])$  is a particular degree 64 number field, whose Galois group has GAP ID  $\langle 64, 6 \rangle$ . Furthermore, a similar (albeit longer) computation to the above, shows that any principally polarised abelian surface  $A/\mathbb{Q}$  with good reduction away from 2 and with full 2-torsion has at most three possibilities for the Galois group  $\text{Gal}(\mathbb{Q}(A[16])/\mathbb{Q})$ , as shown in Theorem 4.19.
- In principle, one can effectively repeat the above procedure to obtain a finite list of possible fields for  $\mathbb{Q}(A[32])$ ,  $\mathbb{Q}(A[64])$ ,  $\mathbb{Q}(A[128])$ , etc. However, as shown in Figure 4.1, the rank of  $\{2\}$ -units grows very quickly as we increase the field of  $2^n$ -torsion, and so we obtain many more quadratic extensions to compute. E.g. doing a computation in Sage shows there are (at least) 53 non-isomorphic quadratic extensions of  $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$  unramified away from 2. Computing all the possible compositums and checking if their Galois group can be embedded in  $\text{GL}_{2d}(\mathbb{Z}/16\mathbb{Z})$  would not be feasible computationally.
- If  $\dim A \leq 2$ , then one can show that  $A[2^\infty]$  lies in the maximal pro-2 extension of  $\mathbb{Q}(\zeta_{2^\infty}) := \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{2^n})$ , without any condition on the field of 2-torsion (shown by Rasmussen–Tamagawa [360] in the dimension 2 case).

**4.2 The Faltings–Serre method**

Whilst Faltings’ proof of the Shafarevich conjecture is not fully effective, one can at least obtain an explicit upper bound on the number of isogeny classes of dimension  $d$  abelian varieties  $A/K$  with good reduction outside  $S$ . At the heart of this process lies the Faltings–Serre method. This was outlined by Serre [396] in a letter to Tate, with many recent surveys and applications of the method given by Livné [289, Section 4], Boston [60], Schütt [389, Section 5], Grenié [201], Chênevert [100, Chapter 5], Dieulefait–Guerberoff–Pacetti [139, Section 4], Duan [152], and Sánchez Rodríguez [375]. We must also thank Ignasi Sánchez Rodríguez for many useful discussions on the Faltings–Serre method. We shall give a brief overview of the method below.

Let  $A/K$  be an abelian variety of dimension  $d$ . Recall that  $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2d}$ . In order to study the  $\ell^n$  torsion  $A[\ell^n]$  for some prime  $\ell$  and various  $n$ , we define the  $\ell$ -adic Tate module

$$T_\ell(A) := \varprojlim_m A[\ell^m].$$

We have that  $T_\ell(A)$  is a free  $\mathbb{Z}_\ell$ -module of rank  $2d$ . We are interested in how the absolute Galois group  $G := \text{Gal}(\overline{K}/K)$  acts on  $T_\ell(A)$ , and so we define the map  $\rho_{A,\ell}$ :

$$\rho_{A,\ell} : \text{Gal}(\overline{K}/K) \rightarrow \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(A))$$

where  $\sigma \in \text{Gal}(\overline{K}/K)$  is sent to its natural action on  $T_\ell(A)$ . We note that, for any particular  $n \geq 1$ , we can factor this map as:

$$\rho_{A,\ell} : \text{Gal}(\overline{K}/K) \rightarrow \text{Gal}(K(A[\ell^n])/K) \rightarrow \text{Aut} A[\ell^n] \cong \text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$$

Our methods will rely on the key observation that knowing information about the possible fields  $K(A[\ell^n]/A)$  could narrow down possibilities for  $\rho_{A,\ell}(\text{Frob}_{\mathfrak{p}})$  and thus narrow down the possible characteristic polynomials  $L_{\mathfrak{p}}(T)$ .

#### 4.2.1 Deviation groups

To set up the basic construction in the Faltings-Serre method, we first introduce the notion of the deviation group attached to a pair of representations  $(\rho_1, \rho_2)$ . Here, we'll closely follow the constructions and exposition as given in Ch enevert [100] (who himself followed the methods outlined in Serre [396]).

**Definition 4.3** (Deviation group). [100, p. 106] Let  $G$  be a group, and let  $\rho_1, \rho_2 : G \rightarrow \text{GL}_n(\mathbb{Z}_2)$  be two representations of  $G$ . Let  $\rho$  denote the product homomorphism  $\rho_1 \times \rho_2$  extended to a  $\mathbb{Z}_2$ -algebra, i.e.

$$\begin{aligned} \rho : \mathbb{Z}_2[G] &\rightarrow \text{M}_n(\mathbb{Z}_2) \oplus \text{M}_n(\mathbb{Z}_2) \\ \sum_{g \in G} a_g g &\mapsto \left( \sum_{g \in G} a_g \rho_1(g), \sum_{g \in G} a_g \rho_2(g) \right). \end{aligned}$$

where  $a_g \in \mathbb{Z}_2$  and  $a_g = 0$  for all but finitely many elements  $g \in G$ . Let  $M$  be the image of  $\rho$  in  $\text{M}_n(\mathbb{Z}_2) \oplus \text{M}_n(\mathbb{Z}_2)$ , and consider the composition

$$\delta : G \rightarrow M^\times \rightarrow (M/2M)^\times$$

We define the image of  $\delta$  in  $(M/2M)^\times$  as the **deviation group** of the pair of representations  $(\rho_1, \rho_2)$ . We denote this group as  $\delta(G)$ .

**Remark.** We note that one can more generally define deviation groups for any two representations  $\rho_1, \rho_2 : G \rightarrow \text{GL}_n(\mathcal{O})$  where  $\mathcal{O}$  is the ring of integers in any local field  $E$ , however it suffices for our purposes to only consider representations in  $\text{GL}_n(\mathbb{Z}_2)$ .

It's also worth repeating the caution mentioned in Chênevert [100, p. 107] that  $\delta(G)$  is in general *not* a subgroup of  $\mathrm{GL}_n(\mathbb{F}_2) \times \mathrm{GL}_n(\mathbb{F}_2)$ .

Classifying the possibilities for the deviation group  $\delta(G)$  lies at the heart of the Faltings-Serre method. It can be shown that  $\delta(G)$  is always a finite group (in particular  $|\delta(G)| < 2^{2n^2}$ , e.g. see [100, p. 107]). Moreover, one can prove the following important proposition which allows us to read off a finite set of primes  $\mathfrak{p} \in \mathcal{T}$  such that the set  $\{\mathrm{tr}(\mathrm{Frob}_{\mathfrak{p}})\}_{\mathfrak{p} \in \mathcal{T}}$  uniquely determines  $\rho$  up to semi-simplification.

**Proposition 4.7.** [100, Proposition 5.2.3] *Let  $\rho_1, \rho_2 : G \rightarrow \mathrm{GL}_n(\mathbb{Z}_2)$  be two representations. Let  $\Sigma$  be a finite subset of  $G$  surjecting onto  $\delta(G)$  (i.e.  $\delta(\Sigma) = \delta(G)$ ), such that  $\mathrm{tr}(\rho_1(g)) = \mathrm{tr}(\rho_2(g))$  for all  $g \in \Sigma$ . Then  $\rho_1$  and  $\rho_2$  are isomorphic up to semi-simplification.*

*Proof.* [100, p. 108] Assume for contradiction that  $\rho_1$  is not isomorphic (up to semisimplification) to  $\rho_2$ . By the Brauer–Nesbitt theorem (e.g. see [276, p. 650]) we have that  $\mathrm{tr} \rho_1 \neq \mathrm{tr} \rho_2$ . Let  $\alpha$  be the largest integer such that  $\mathrm{tr} \rho_1 \equiv \mathrm{tr} \rho_2 \pmod{2^\alpha}$ . Note that we can define a  $\mathbb{Z}_2$ -linear map  $f : \mathbb{Z}_2[G] \rightarrow \mathbb{Z}_2$  given by

$$f : \mathbb{Z}_2[G] \rightarrow \mathbb{Z}_2, \quad \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g 2^{-\alpha} (\mathrm{tr} \rho_1(g) - \mathrm{tr} \rho_2(g))$$

where, by definition of  $\alpha$ , the image of  $f$  is not contained in  $2\mathbb{Z}_2$ . This descends to a  $\mathbb{Z}_2$ -linear map on  $M$ :

$$\theta : M \rightarrow \mathbb{Z}_2, \quad (A, B) \mapsto 2^{-\alpha} (\mathrm{tr} A - \mathrm{tr} B)$$

where again we note  $\theta(M) \not\subseteq 2\mathbb{Z}_2$ . This further descends to a nonzero  $\mathbb{F}_2$ -linear map  $M/2M \rightarrow \mathbb{F}_2$  and thus to a function

$$\Theta : \delta(G) \rightarrow \mathbb{F}_2$$

By the definition of  $M$ , we note that  $\delta(G)$  spans  $M/2M$  and thus  $\Theta$  is nonzero.. Therefore there exists some  $g \in \Sigma$  such that  $\Theta(\delta(g)) \neq 0$ . In particular, this implies

$$2^{-\alpha} (\mathrm{tr} \rho_1(g) - \mathrm{tr} \rho_2(g)) \notin 2\mathbb{Z}_2$$

and so  $\mathrm{tr} \rho_1(g) \neq \mathrm{tr} \rho_2(g)$ , which gives us a contradiction.  $\square$

This proposition therefore allows us to determine whether two semisimple representations  $\rho_1$  and  $\rho_2$  are isomorphic by comparing their traces for finitely many elements in  $G$ . By classifying all the possible deviation groups  $\delta(G)$ , this gives an

effective algorithm to determine whether two representations  $\rho_1$  and  $\rho_2$  are isomorphic.

Applying this to the case of Galois representations  $G = \text{Gal}(\bar{K}/K)$ , this allows us to prove the following key theorem, which Faltings used to prove finiteness of the number of isogeny classes of dimension  $d$  abelian varieties  $A/K$  with good reduction outside  $S$ .

**Theorem 4.8.** [484, Proposition 2.7] *Let  $K$  be a number field and  $S$  a finite set of places of  $K$ . Suppose  $\rho_1, \rho_2 : \text{Gal}(\bar{K}/K) \rightarrow \text{GL}_n(\mathbb{Q}_2)$  are continuous representations unramified outside  $S$ . Then there exists an effectively computable finite set of primes  $\mathcal{T}$ , disjoint from  $S$ , such that if*

$$\text{tr}(\rho_1(\text{Frob}_{\mathfrak{p}})) = \text{tr}(\rho_2(\text{Frob}_{\mathfrak{p}}))$$

*for all  $\mathfrak{p} \in \mathcal{T}$ , then  $\rho_1$  and  $\rho_2$  are isomorphic up to semi-simplification.*

*Proof.* We can explicitly construct such a set  $\mathcal{T}$ . Using classical Hermite–Minkowski bounds, we recall there are only a finite number of Galois extensions  $L/K$  unramified outside  $S$  with degree at most  $2^{2n^2}$ . As remarked in Chapter 2, such fields can explicitly be computed by doing a Hunter search [109, p. 445]. Let  $\tilde{K}$  be a finite Galois extension of  $K$  containing all such extensions  $L$ .

Thus, by the Chebotarov density theorem, there exists a finite set of primes  $\mathcal{T}$  such that the Frobenius elements  $\{\text{Frob}_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{T}}$  cover all conjugacy classes of  $\text{Gal}(\tilde{K}/K)$ .

As the representations  $\rho_1$  and  $\rho_2$  are unramified outside  $S$ , they factor over  $\text{Gal}(\tilde{K}/K)$ . Since  $|\delta(G)| < 2^{2n^2}$ , this implies that the set  $\{\text{Frob}_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{T}}$  surjects onto the deviation group  $\delta(G)$ . We can therefore apply Proposition 4.7 to obtain that this set  $\mathcal{T}$  works, concluding the proof.  $\square$

Whilst the set  $\mathcal{T}$  can in principle always be effectively computed given any  $(K, S, n)$ , e.g. see Achter [6] for explicit bounds on  $\text{Nm}(\mathfrak{p})$  for  $\mathfrak{p} \in \mathcal{T}$ , doing the above procedure usually gives a set  $\mathcal{T}$  which is far too large to be of practical use, unless some further conditions on either the characteristic polynomials  $L_p(T)$  or the residual representations  $\bar{\rho}_1$  and  $\bar{\rho}_2$  are assumed.

To therefore get the best effective result, we need to study the deviation group more closely for particular cases. In the next section, we'll prove some specific results in the cases where our representations satisfy  $\bar{\rho}_1 = \bar{\rho}_2 = I \pmod{2}$

### 4.2.2 The case where $\bar{\rho}_i$ is trivial

The following theorem is essentially a simplification of the proposition of Ch enevert [100, Proposition 5.3.1] in the case where the residual representations  $\bar{\rho}_2$  and  $\bar{\rho}_2$  are trivial.

**Proposition 4.9.** *Let  $\rho_1, \rho_2 : G \rightarrow \mathrm{GL}_n(\mathbb{Z}_2)$  be two non-isomorphic representations. Assume that  $\rho_1 \equiv \rho_2 \equiv I \pmod{2}$  and let  $\beta$  be the largest integer such that  $\rho_1 \equiv \rho_2 \pmod{2^\beta}$ . Define the function*

$$\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow M_n(\mathbb{F}_2)$$

*given by  $g \mapsto 2^{-\beta}(\rho_1(g) - \rho_2(g)) \pmod{2}$ . Then  $\varphi$  is a group homomorphism which factors through the deviation group  $\delta(G)$  (i.e.  $\ker \delta \subset \ker \varphi$ ).*

*Proof.* We can easily show that  $\varphi$  is an (additive) group homomorphism by a direct computation. Indeed, let  $g, h \in G$ . Then using that

$$\begin{aligned} \rho_1(g) &= \rho_2(g) + 2^\beta \varphi(g) \pmod{2^{\beta+1}} \\ \text{and } \rho_1(h) &= \rho_2(h) + 2^\beta \varphi(h) \pmod{2^{\beta+1}}, \end{aligned}$$

we get

$$\rho_1(gh) = (\rho_2(g) + 2^\beta \varphi(g))(\rho_2(h) + 2^\beta \varphi(h)) \pmod{2^{\beta+1}}.$$

Equating this with  $\rho_1(gh) = \rho_2(gh) + 2^\beta \varphi(gh) \pmod{2^{\beta+1}}$  and dividing out by  $2^\beta$ , we get

$$\varphi(gh) = \varphi(g)\rho_2(h) + \rho_2(g)\varphi(h) + 2^\beta \varphi(g)\varphi(h) \pmod{2}.$$

Since  $\rho_1 \equiv \rho_2 \equiv I \pmod{2}$  by assumption (and thus also  $\beta \geq 1$ ), this implies

$$\varphi(gh) = \varphi(g) + \varphi(h),$$

which proves  $\varphi$  is a group homomorphism.

We now show that  $\ker \delta \subset \ker \varphi$ . Let  $g \in \ker \delta$ . By definition of  $\delta$  this implies that  $\rho_1(g), \rho_2(g) \in I + 2M$ , where we recall  $M$  as the image of  $\rho : \mathbb{Z}_2[G] \rightarrow M_n(\mathbb{Z}_2) \oplus M_n(\mathbb{Z}_2)$  where  $\rho$  is the extension of  $\rho_1 \times \rho_2$  to  $\mathbb{Z}_2[G]$ . Thus, we can write

$$\rho(g) = 1 + 2 \sum_{h \in G} a_h \rho(h)$$

for some  $a_h \in \mathbb{Z}_2$ , where  $a_h = 0$  for all but finitely many  $h \in G$ . This implies

$$\rho_1(g) = 1 + 2 \sum_{h \in G} a_h \rho_1(h) \quad \text{and} \quad \rho_2(g) = 1 + 2 \sum_{h \in G} a_h \rho_2(h)$$

Thus,

$$\begin{aligned} 1 + 2 \sum_{h \in G} a_h \rho_1(h) &= \rho_1(g) = \rho_2(g) + 2^\beta \varphi(g) \\ &= 1 + 2 \sum_{h \in G} a_h \rho_2(h) + 2^\beta \varphi(g) \pmod{2^{\beta+1}} \end{aligned}$$

which implies

$$\varphi(g) = 2 \sum_{h \in G} a_h \varphi(h) \equiv 0 \pmod{2}$$

and thus  $g \in \ker \varphi$ . □

**Remarks.**

- One can more generally show that, even if we assume that the mod 2 representations  $\overline{\rho_1}$  and  $\overline{\rho_2}$  are non-trivial (but still assuming  $\beta \geq 1$ ), then the more general map  $\varphi : G \rightarrow M_n(\mathbb{F}_2) \rtimes \text{GL}_n(\mathbb{F}_2)$  given by

$$g \mapsto (2^{-\beta}(\rho_2(g)\rho_1^{-1}(g) - I) \bmod 2, \rho_1 \bmod 2)$$

is also a group homomorphism which factors through  $\delta$ .

- If one also assumes that  $\det \rho_1 = \det \rho_2$ , then one can show that the image of  $\varphi$  is contained in  $M_n^0(\mathbb{F}_2)$  (the set of  $n \times n$  matrices of trace 0 over  $\mathbb{F}_2$ ).
- From the proof of Theorem 4.9, the fact that  $\ker \delta \subset \ker \varphi$  implies we have a surjective map  $\delta(G) \twoheadrightarrow \varphi(G)$ , however this is *not* in general an isomorphism; indeed  $\delta(G)$  can be a lot bigger than  $\varphi(G)$ .

Other than some trivial cases, computing the deviation group  $\delta(G)$ , even for a single non-trivial pair of representations  $(\rho_1, \rho_2)$ , seems to be a very difficult problem, whereas computing the possibilities for  $\varphi(G)$  is more doable. To give some examples, one can show that the only possibilities for  $\varphi(G)$  in the case of representations  $\rho_1, \rho_2 : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}_2)$  satisfying  $\det(\rho_1) = \det(\rho_2)$  and  $\overline{\rho_1} = \overline{\rho_2}$  surjective in  $\text{GL}_2(\mathbb{F}_2)$ , are the following three groups [100, p. 115]:

$$\{\pm 1\} \times S_3, \quad V_4 \rtimes S_3 \cong S_4, \quad \text{and} \quad (\mathbb{F}_2 \oplus V_4) \rtimes S_3 \cong \{\pm 1\} \times S_4.$$



Purely out of interest, we note the following proposition of Chênevert which gives a simple description of the deviation group  $\delta(G)$  and  $\varphi(G)$  in the case of representations from  $G = \mathbb{Z}_2$ :

**Proposition 4.10.** [100, Proposition 5.3.2] *Let  $\rho_1, \rho_2 : \mathbb{Z}_2 \rightarrow \mathrm{GL}_n(\mathbb{Z}_2)$  be two continuous representations such that  $\bar{\rho}_1 = \bar{\rho}_2 = 1$ . Then we have that  $\varphi(\mathbb{Z}_2) \cong \mathbb{F}_2$ . If furthermore  $\rho_1 = 1$ , then  $\delta(\mathbb{Z}_2) \cong \mathbb{F}_2$ .*

*Proof.* For any  $n \in \mathbb{Z}$ , as  $\varphi$  is a group homomorphism, we have  $\varphi(n) = n\varphi(1) \pmod{2}$ . As  $\rho_1$  and  $\rho_2$  are continuous, this implies that  $\varphi$  is continuous and thus we have that  $\varphi(n) = n\varphi(1) \pmod{2}$  for all  $n \in \mathbb{Z}_2$ . As  $\varphi$  is non-trivial by definition, in particular this implies that  $\varphi(1)$  is nonzero, and thus we have  $\ker \varphi = 2\mathbb{Z}_2$ . Therefore  $\varphi(\mathbb{Z}_2) \cong \mathbb{Z}_2/2\mathbb{Z}_2 \cong \mathbb{F}_2$ .

By furthermore assuming that  $\rho_1$  is trivial (i.e. identically constant), then [100, Proposition 5.3.2] proves that  $\delta(\mathbb{Z}_2) \cong \mathbb{F}_2$ .  $\square$

**Remarks.** It's worth mentioning some remarks about how the integers  $\alpha$  (as given in the proof of Proposition 4.7) and  $\beta$  (given in Proposition 4.9) compare. Since  $\rho_1 \equiv \rho_2 \pmod{2^\beta}$  clearly implies  $\mathrm{tr} \rho_1 \equiv \mathrm{tr} \rho_2 \pmod{2^\beta}$ , it's obvious that  $\alpha \geq \beta$ , however equality need not necessarily hold in general.

However, we note that it's a theorem of Carayol [93, Theoreme 1] that  $\alpha = \beta$  if  $\bar{\rho}_1 \equiv \bar{\rho}_2$  is an *absolutely irreducible* subgroup of  $\mathrm{GL}_n(\mathbb{F}_2)$ . In this case, an explicit algorithm to compute a suitable set of primes  $\mathcal{T}$  is given by Brumer–Pacetti–Poor–Tornaria–Voight–Yuen [83, Algorithm 2.4.1]. Whilst there are some generalisations of this result by Urban [455] and Brown [72] where  $\bar{\rho}_1, \bar{\rho}_2$  are certain reducible subgroups of  $\mathrm{GL}_n(\mathbb{F}_2)$ , it can in general happen that  $\alpha > \beta$ .

Although in the case where  $\alpha = \beta$ , one can instead use  $\varphi(G)$  instead of the deviation group  $\delta(G)$  in the proof of Proposition 4.7, which can allow for a much easier classification of the set  $\mathcal{T}$  of primes that one can take in Theorem 4.8 (e.g. see [100, p. 115]).

Motivated by this, we pose the following problem:

**Problem 4.4.** Given two representations  $\rho_1, \rho_2 : G \rightarrow \mathrm{GL}_n(\mathbb{Z}_2)$ , give necessary and sufficient conditions for when  $\alpha = \beta$ .

### 4.2.3 Livné's criterion

We now consider the special case of 2-dimensional Galois representations  $\rho_1, \rho_2 : \mathrm{Gal}(\bar{K}/K) \rightarrow \mathrm{GL}_2(\mathbb{Q}_2)$ ; these are the representations attached to elliptic curves

$E/K$ . In the  $\mathrm{GL}_2$  case, we have the following criterion by Livné [289] which gives a strong bound on the set of primes  $\mathcal{T}$  we can take in Theorem 4.8.

**Theorem 4.11** (Livné’s criterion). [289, Theorem 4.3] *Let  $K$  be a number field, and  $S$  a finite set of primes of  $K$ . Let  $K_S$  be the compositum of all quadratic extensions of  $K$  unramified outside  $S$ . Suppose  $\rho_1, \rho_2 : \mathrm{Gal}(\overline{K}/K) \rightarrow \mathrm{GL}_2(\mathbb{Q}_2)$  are continuous representations unramified outside  $S$  such that*

$$\mathrm{tr} \rho_1 \equiv \mathrm{tr} \rho_2 \equiv 0 \pmod{2} \quad \text{and} \quad \det \rho_1 \equiv \det \rho_2 \equiv 1 \pmod{2}.$$

*Let  $\mathcal{T}$  be a finite set of primes of  $K$  disjoint from  $S$  for which*

(i) *The image of  $\{\mathrm{Frob}_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{T}}$  in  $\mathrm{Gal}(K_S/K)$  is non-cubic (i.e. if  $U$  denotes the image  $\{\mathrm{Frob}_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{T}}$  in  $\mathrm{Gal}(K_S/K)$ , then every degree 3 homogenous polynomial which vanishes on  $U$  vanishes on  $\mathrm{Gal}(K_S/S)$ , considered as an  $\mathbb{F}_2$ -vector space).*

(ii)  *$\mathrm{tr} \rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{tr} \rho_2(\mathrm{Frob}_{\mathfrak{p}})$  and  $\det \rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \det \rho_2(\mathrm{Frob}_{\mathfrak{p}})$  for all  $\mathfrak{p} \in \mathcal{T}$ .*

*Then  $\rho_1$  and  $\rho_2$  have isomorphic semi-simplifications.*

**Remark.** We note that Livné’s criterion was generalised by Chênevert [100, Theorem 5.5.15] to only require the weaker condition that  $\mathrm{tr} \rho_1 \equiv \mathrm{tr} \rho_2 \pmod{2}$ .

To illustrate the effectiveness of this criterion, we can apply Livné’s criterion to deduce the following classification for elliptic curves:

**Corollary 4.12.** *Let  $E_1/\mathbb{Q}$  and  $E_2/\mathbb{Q}$  be elliptic curves with full rational 2-torsion and good reduction outside 2. Let  $\rho_1$  and  $\rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}_2(\mathbb{Q}_2)$  be the Galois representations associated to  $E_1$  and  $E_2$  respectively. Then if*

$$\mathrm{tr}(\rho_1(\mathrm{Frob}_p)) = \mathrm{tr}(\rho_2(\mathrm{Frob}_p))$$

*for all  $p \in \{3, 5, 7\}$ , then  $E_1$  is isogenous to  $E_2$ .*

*Proof.* If  $E/\mathbb{Q}$  has full rational 2-torsion, then this implies  $\rho_1 \equiv \rho_2 \equiv I \pmod{2}$ , and so clearly  $\mathrm{tr} \rho_1 \equiv \mathrm{tr} \rho_2 \equiv 0 \pmod{2}$  and  $\det \rho_1 \equiv \det \rho_2 \equiv 1 \pmod{2}$ , allowing us to apply Livné’s criterion. As shown in Theorem 4.6, we have that  $\mathbb{Q}_{\{2\}}$  is the compositum of  $\mathbb{Q}(\sqrt{-1})$ ,  $\mathbb{Q}(\sqrt{-2})$  and  $\mathbb{Q}(\sqrt{2})$  and so  $\mathbb{Q}_{\{2\}} = \mathbb{Q}(\zeta_8)$ , thus  $\mathrm{Gal}(\mathbb{Q}_{\{2\}}/\mathbb{Q}) \cong C_2^2$ . By Livné’s criterion, it suffices to find a set of odd primes  $\mathcal{T}$  such that the image of  $\{\mathrm{Frob}_p\}_{p \in \mathcal{T}}$  in  $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$  gives all three non-identity elements in  $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$  (noting that this is a non-cubic subset of  $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ ). We can easily check that

the Frobenius automorphisms  $\text{Frob}_3$ ,  $\text{Frob}_5$ , and  $\text{Frob}_7$  suffice; indeed we can compute the action on  $\zeta_8$  as follows (also giving the action on  $i$  and  $\sqrt{2}$  for reference):

$$\begin{aligned}\text{Frob}_3 : \zeta_8 &\mapsto \zeta_8^3 & (i &\mapsto -i, \sqrt{2} \mapsto -\sqrt{2}), \\ \text{Frob}_5 : \zeta_8 &\mapsto -\zeta_8 & (i &\mapsto i, \sqrt{2} \mapsto -\sqrt{2}), \\ \text{Frob}_7 : \zeta_8 &\mapsto -\zeta_8^3 & (i &\mapsto -i, \sqrt{2} \mapsto \sqrt{2}).\end{aligned}$$

Therefore, we can take  $\mathcal{T} = \{3, 5, 7\}$ .<sup>1</sup> □

We note that the above result is not particularly useful in the dimension 1 case, given that numerous other methods (e.g. solving  $S$ -unit or Mordell equations) have been developed to effectively classify elliptic curves with good reduction outside a finite set of primes  $S$ . However, our key observation here is that the above method has the crucial advantage of not requiring the use of any particular model of elliptic curves, and thus is far more adaptable to classify isogeny classes of higher dimension abelian varieties, compared to the methods given in Section 1.1.1.

#### 4.2.4 Grenié's criterion

We would like to deduce a similar criterion to Livné for higher dimensions  $n$ . Unfortunately, it's no longer sufficient to simply take a set of primes  $\mathcal{T}$  such that  $\{\text{Frob}_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{T}}$  covers the compositum  $K_S$  of all quadratic extensions of  $K$  unramified away from  $S$ . Instead, as we'll see, we'll need to iterate this construction several times to ensure we have a sufficient number of primes to cover the deviation group  $\delta(G)$ . We therefore give a theorem of Grenié (in the case of  $\text{GL}_n(\mathbb{Q}_2)$ ) which uses the theory of pro- $p$  groups to generalise Livné's criterion. Much of this section is taken from Grenié [201] and specialised to the case of representations  $\rho_1, \rho_2 : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_n(\mathbb{Q}_2)$ .

We begin by first defining a necessary condition required to apply Grenié's main theorem.

**Definition 4.5.** [201, Definition 1] Let  $M_1$  and  $M_2$  be two matrices in  $M_n(\mathbb{Q}_2)$ , and let  $F$  be a finite extension of  $\mathbb{Q}_2$  containing the eigenvalues of  $M_1$  and  $M_2$ . Let  $\mathfrak{p}_F$  be the maximal ideal of  $F$  and  $\omega_F$  a uniformiser. We say that  $M_1$  and  $M_2$  have **congruent eigenvalues** if there exists some  $\lambda \in \mathcal{O}_F^\times$  and  $v \in \mathbb{Z}$  such that the characteristic polynomials of  $\omega_F^v M_1$  and  $\omega_F^v M_2$  are in  $\mathcal{O}_F[x]$  and congruent to  $(X - \lambda)^n$  modulo  $\mathfrak{p}_F$ .

---

<sup>1</sup>If we want the stronger condition that  $\{\text{Frob}_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{T}}$  surjects onto  $\mathbb{Q}(\zeta_8)$ , then an easy check shows that  $\text{Frob}_{17}$  induces the identity in  $\mathbb{Q}(\zeta_8)$ , and hence one can take the set of primes  $\mathcal{T} = \{3, 5, 7, 17\}$ .

**Remark.** Note that in particular, if  $\rho_1, \rho_2 : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_n(\mathbb{Z}_2)$  are representations such that  $\overline{\rho}_1 \equiv \overline{\rho}_2 \equiv I \pmod{2}$ , then the characteristic polynomials of  $\rho_1$  and  $\rho_2$  are simply  $(X - 1)^n \pmod{2}$ , and hence have congruent eigenvalues. In fact, one can more generally show that, if  $\rho_{A,2}$  is the 2-adic representation attached to an abelian variety  $A/\mathbb{Q}$  where  $\mathbb{Q}(A[2])$  has degree a power of 2, then the characteristic polynomials of  $\rho_{A,2}$  are  $(X - 1)^n \pmod{2}$ .

We can now state Grenié's main theorem (in the case  $p = 2$ ).

**Theorem 4.13** (Grenié's criterion [201, Theorem 3]). *Let  $K$  be a number field, and  $S$  a finite set of primes of  $K$ , and  $n \geq 2$  an integer. We define a chain of number fields  $K = K_0 \subset K_1 \subset K_2 \subset \dots$  inductively as follows: For each  $i \geq 0$ , let  $K_{i+1}$  be the maximal abelian extension of  $K_i$  unramified outside  $S$  such that  $\text{Gal}(K_{i+1}/K_i)$  is an elementary 2-group. Define  $K_S$  as the number field*

$$K_S := K_{\lceil \log_2(n^5(n-1)) \rceil + \lceil \log_2 n \rceil}.$$

*Suppose  $\rho_1, \rho_2 : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_n(\mathbb{Q}_2)$  are continuous representations unramified outside  $S$  such that  $\rho_1(\sigma)$  and  $\rho_2(\sigma)$  have congruent eigenvalues, for all  $\sigma \in \text{Gal}(\overline{K}/K)$ .*

*Let  $\mathcal{T}$  be a finite set of primes of  $K$ , disjoint from  $S$  for which*

- 1. Each maximal cyclic subgroup of  $\text{Gal}(K_S/K)$  has a generator of the form  $\text{Frob}_t$  for some  $t \in \mathcal{T}$  and some prime  $\mathfrak{t}$  above  $t$  in  $K_S$ .*
- 2.  $\rho_1(\text{Frob}_t)$  and  $\rho_2(\text{Frob}_t)$  have equal characteristic polynomials (where  $\text{Frob}_t$  is any Frobenius element above  $t$ ) for all  $t \in \mathcal{T}$ .*

*Then  $\rho_1$  and  $\rho_2$  have isomorphic semi-simplifications.*

To classify abelian surfaces  $A/\mathbb{Q}$ , we would like to apply this criterion in the case where  $n = 4$ . If we do so, this gives us  $\lceil \log_2(n^5(n-1)) \rceil + \lceil \log_2 n \rceil = 14$ , and thus  $K_S = K_{14}$ . Even in the case where  $K_1 = \mathbb{Q}$  and  $S = \{2\}$ , this is far beyond what we can practically compute; indeed we were unable to compute even just the field  $K_4$ .

To therefore obtain a construction for  $K_S$  which is more computationally feasible, one needs to impose some further conditions on what the possible extensions  $K_{i+1}/K_i$  can be. This was done implicitly in Grenié's work [201, Section 4], but stated more explicitly in the work of Duan [152, Section 6.2].

**Theorem 4.14** (Optimised Grenié–Duan's criterion [152, Section 6.2]). *Let  $K$ ,  $S$ ,  $n$ ,  $\rho_1$ ,  $\rho_2$  be as stated above in Theorem 4.13. Let  $K_S$  now be defined as follows:*

Take  $K_0 = K$ . For each  $i \geq 0$ , list all quadratic extensions  $L/K_i$  which satisfy the following two conditions:

- (i)  $L/K_i$  is unramified outside  $S$ .
- (ii) For every odd prime  $\mathfrak{p}$  in  $K$  and for every prime  $\mathfrak{P}$  in  $L$  above  $\mathfrak{p}$ , the corresponding local field extension  $L_{\mathfrak{P}}/K_{\mathfrak{p}}$  has Galois group of exponent at most 4.

Let  $K_{i+1}$  be the compositum of all such quadratic extensions  $L/K_i$  satisfying conditions (i) and (ii). Repeat this process for  $K_{i+2}$  etc. until either

1. There are no such quadratic extensions  $L/K_i$  satisfying conditions (i) and (ii), or;
2.  $i = \lceil \log_2(n^5(n-1)) \rceil + \lceil \log_2 n \rceil$ , as given in Theorem 4.13.

Let  $K_S := K_i$  be the number field at which this algorithm terminates. Then the statement of Theorem 4.13 holds for this choice of  $K_S$ .

**Proposition 4.15.** [201, Proposition 14] Let  $K$ ,  $S$ ,  $n$ ,  $\rho_1$ ,  $\rho_2$  be as stated in Theorem 4.13. Let  $K'$  be the compositum of all odd degree  $d$  extensions of  $K$  unramified outside  $S$ , over all odd  $d \leq 2^n - 1$  such that  $d$  divides  $\prod_{i=2}^n (2^i - 1)$ .

Let  $\rho'_1$  and  $\rho'_2$  denote the restriction of  $\rho_1$  and  $\rho_2$  to  $\text{Gal}(\overline{K}/K')$ . Then  $\rho'_1(\sigma)$  and  $\rho'_2(\sigma)$  have congruent eigenvalues for all  $\sigma \in \text{Gal}(\overline{K}/K')$ .

*Proof.* This is simply the statement of [201, Proposition 14] in the case of  $p = 2$ ,  $E = \mathbb{Q}_2$ , and  $k = \mathbb{F}_2$  (and thus  $q = 2$ ).  $\square$

**Theorem 4.16.** [201, p. 617] Let  $n = 2, 3$  or  $4$ , and let  $\rho_1$  and  $\rho_2 : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_n(\mathbb{Q}_2)$  be two representations unramified away from  $\{2, \infty\}$ . Then if either

- $\text{tr}(\rho_1(\text{Frob}_p)) = \text{tr}(\rho_2(\text{Frob}_p))$  for all  $p \in \{5, 7, 11, 13, 17, 19, 23, 31, 73, 137, 257, 337\}$ , or
- $\chi(\rho_1(\text{Frob}_p)) = \chi(\rho_2(\text{Frob}_p))$  for all  $p \in \{5, 7, 11, 17, 23, 31\}$ , (where  $\chi(M)$  denotes the characteristic polynomial of  $M$ ),

then  $\rho_1$  and  $\rho_2$  have isomorphic semi-simplifications.

Whilst this theorem is already stated and implicitly proven by Grenié [201, Section 4], due to its importance in this chapter, we'll provide a brief sketch proof here. We thank Ignasi Sánchez Rodríguez [376] for very generously providing Magma code to compute the field  $K_S$  as defined in Theorem 4.14.

*Proof sketch.* [201, Section 4.2] Let  $n = 2, 3$  or  $4$ , and let  $\rho_1$  and  $\rho_2 : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_n(\mathbb{Q}_2)$  be two representations unramified away from  $\{2, \infty\}$ . We first use Proposition 4.15 to show that  $\rho_1$  and  $\rho_2$  satisfy the conditions required to apply Theorem 4.13. Indeed, by the work of Tate [441] and Jones [239, Theorem 2.1], there does not exist any odd degree  $d \leq 15$  number field  $L$  unramified away from  $\{2, \infty\}$ , therefore proving that  $\rho_1(\sigma)$  and  $\rho_2(\sigma)$  have congruent eigenvalues for all  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ .

We now construct the field  $K_S$  by running the algorithm described in Theorem 4.14. We have  $K_0 = \mathbb{Q}$ . Using similar arguments to those given in Theorem 4.6, we compute  $K_1$  as the degree 8 field  $\mathbb{Q}(\zeta_8)$  (the compositum of all quadratic extensions of  $\mathbb{Q}$  unramified away from 2), and  $K_2$  as the degree 32 field  $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}, \sqrt{\zeta_8 + 1})$  (the compositum of all quadratic extensions of  $\mathbb{Q}(\zeta_8)$  unramified away from 2).

We then found that  $K_3$  is a degree 64 field, in particular the splitting field of  $x^8 + 4x^6 + 4x^4 - 2$  (an explicit defining polynomial for  $K_3$  is given in [201, p. 617]), and verified that no quadratic extensions of  $K_3$  unramified outside  $\{2, \infty\}$  satisfy condition (ii) of Theorem 4.14. This proves that  $K_S = K_3$ . A standard computation shows that the order 64 group  $\text{Gal}(K_S/K)$ , which has GAP ID  $\langle 64, 34 \rangle$ , has 6 maximal cyclic subgroups, up to conjugacy,. Using Magma's `FrobeniusElement` function, we can verify that each such subgroup is generated by  $\text{Frob}_5$ ,  $\text{Frob}_7$ ,  $\text{Frob}_{11}$ ,  $\text{Frob}_{17}$ ,  $\text{Frob}_{23}$ , and  $\text{Frob}_{31}$  respectively. By therefore taking the set of primes  $\mathcal{T} = \{5, 7, 11, 17, 23, 31\}$  in the statement of Theorem 4.13, this proves the second assertion.

Finally, as  $\rho_1$  and  $\rho_2$  have dimension at most 4, we can alternatively compute the characteristic polynomial of a matrix  $M \in \text{GL}_n(\mathbb{Q}_2)$  by instead computing the traces  $\text{tr}(M)$ ,  $\text{tr}(M^2)$ ,  $\text{tr}(M^3)$ , and  $\text{tr}(M^4)$ . This proves the first assertion.  $\square$

### Remarks.

- It's worth noting that Theorem 4.16 does not hold for  $n \geq 8$ , as there does exist a degree 17 field unramified away from 2 [215], and 17 divides  $2^8 - 1$ .
- It's clear that the sets of primes  $\{5, 7, 11, 13, 17, 19, 23, 31, 73, 137, 257, 337\}$  and  $\{5, 7, 11, 17, 23, 31\}$  given in Theorem 4.16 are not unique, as any particular prime  $p$  can instead be replaced by  $q$  if  $\text{Frob}_p$  lies in the same conjugacy class as  $\text{Frob}_q$  in  $\text{Gal}(K_S/K)$ . In particular, by instead taking the smallest primes possible, we may instead use the sets of primes  $\{3, 5, 7, 11, 13, 17, 23, 31, 41, 73, 113, 337\}$  for testing  $\text{tr}(\rho_i(\text{Frob}_p))$  and  $\{3, 5, 7, 17, 23, 31\}$  for testing  $\chi(\rho_i(\text{Frob}_p))$ .

Therefore, in the case of  $n = 4$ , we can apply the above Theorem to the 2-adic Galois representations  $\rho_1, \rho_2 : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_4(\mathbb{Q}_2)$  attached to abelian surfaces

$A/\mathbb{Q}$  and  $B/\mathbb{Q}$  respectively, both with good reduction away from 2. By Faltings' isogeny theorem, this gives our desired result.

**Corollary 4.17.** *[201, p. 617] Let  $A/\mathbb{Q}$  and  $B/\mathbb{Q}$  be two abelian surfaces with good reduction outside 2. For each odd prime  $p$ , let  $a_p(A)$  and  $a_p(B)$  denote the trace of Frobenius at the prime  $p$  for  $A$  and  $B$  respectively. Similarly, let  $L_p(A, T)$  and  $L_p(B, T)$  denote the local Euler factor at the prime  $p$  for  $A$  and  $B$  respectively. Then if either*

- $a_p(A) = a_p(B)$  for all  $p \in \{5, 7, 11, 13, 17, 19, 23, 31, 73, 137, 257, 337\}$ , or
- $L_p(A, T) = L_p(B, T)$  for all  $p \in \{5, 7, 11, 17, 23, 31\}$ ,

then  $A$  is  $\mathbb{Q}$ -isogenous to  $B$ .

### 4.3 Computational results

Taking inspiration from the recent algorithm of Alpöge–Lawrence [11], the above criterion suggests one attempt to give a general approach to classify dimension  $d$  abelian varieties  $A/K$  with good reduction outside  $S$ :

1. Given some finite set of primes  $S$  of bad reduction, use Theorem 4.8 (the Faltings-Serre method) to compute a finite set of primes  $\mathcal{T}$  for which the set of local Euler factors  $\{L_{\mathfrak{p}}(T) : \mathfrak{p} \in \mathcal{T}\}$  uniquely determines the  $L$ -function  $L(A/K, s)$  of  $A/K$ .
2. For each  $\mathfrak{p} \in \mathcal{T}$ , use the Weil inequalities to compute a finite set of possible characteristic polynomials  $L_{\mathfrak{p}}(T)$  (This already gives an effective, albeit weak, upper bound on the number of isogeny classes).
3. For a suitable prime  $\ell$  and positive integer  $n \geq 1$ , classify the possible  $\ell^n$ -torsion fields  $A[\ell^n]$  and use that  $\text{Gal}(K(A[\ell^n])/K) \hookrightarrow \text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  is an injective homomorphism to narrow down possibilities for  $L_{\mathfrak{p}}(T)$ . Here, a larger value for  $n$  narrows down the possibilities for  $L_{\mathfrak{p}}(T)$  further, but at the cost of being more computationally intensive.
4. For each remaining set of characteristic polynomials  $\{L_{\mathfrak{p}}(T) : \mathfrak{p} \in \mathcal{T}\}$  which correspond to a valid embedding of  $\text{Gal}(K(A[\ell^n])/K)$  in  $\text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ , search for an abelian variety corresponding to this set.

5. After computing all the information we can about the possible Galois groups  $\text{Gal}(K(A[\ell^n])/K)$  and its image in  $\text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ , we hope that the only remaining possible Euler factors  $L_p(T)$  correspond to explicit examples of abelian varieties already found.

This approach does seem rather ambitious, and is almost certainly not computationally feasible for all but the simplest of cases. Unlike the Alpöge–Lawrence algorithm, we make no claim that this will (even conjecturally) terminate for most choices of  $(K, S, d)$ . We summarise our results in the case that  $K = \mathbb{Q}$  and  $S = \{2\}$  with the condition  $\mathbb{Q}(A[2]) = \mathbb{Q}$  in the next two sections, first for  $d = 1$  and then  $d = 2$ .

### 4.3.1 Elliptic curves

To illustrate the above method, we shall first compute all elliptic curves  $E$  over  $\mathbb{Q}$  with good reduction away from 2 and with full rational 2-torsion. Of course, this clearly has a very elementary solution, as shown in the proof of Theorem 4.1, but let's for a moment assume we know absolutely nothing regarding explicit models of elliptic curves other than that they are dimension 1 abelian varieties. By Corollary 4.12, it suffices to compute the possibilities for the local Euler factors at the first three odd primes:  $L_3(T)$ ,  $L_5(T)$  and  $L_7(T)$ . As each Euler factor is a degree 2 polynomial of the form  $L_p(T) = pT^2 - a_pT + 1$ , they are each uniquely determined by the trace  $a_p$  at  $p = 3, 5, 7$  respectively.

Our first attempt is to do a brute force search for matrices  $M$  in  $\text{GL}_2(\mathbb{Z}_2)$  such that  $M \equiv I \pmod{2}$  and compute the possible values for the trace of  $M$ . Of course, as  $\text{GL}_2(\mathbb{Z}_2)$  is infinite, we instead search modulo some sufficiently large power of 2, where in Table 4.1 we've taken mod  $2^{10}$ . We also use the Hasse-Weil bounds to restrict to matrices  $M$  where  $|\text{tr}(M)| \leq 2\sqrt{p}$ .

Table 4.1: A list of the possible values for  $\text{tr}(M)$ , where  $M \in \text{GL}_2(\mathbb{Z}/2^{10}\mathbb{Z})$  such that  $M \equiv I \pmod{2}$ ,  $\det(M) = p$ , and  $|\text{tr}(M)| \leq 2\sqrt{p}$ .

Prime $p$	Possible values for $\text{tr}(\text{Frob}_p)$
<b>3</b>	0
<b>5</b>	2, -2
<b>7</b>	-4, 0, 4
<b>11</b>	-4, 0, 4
<b>13</b>	-6, -2, 2, 6
<b>17</b>	-6, -2, 2, 6
<b>19</b>	-8, -4, 0, 4, 8



Table 4.1 shows that, for any elliptic curve  $E/\mathbb{Q}$  with full rational 2-torsion and with good reduction outside 2, we must have  $\text{tr}(\text{Frob}_3) = 0$ ,  $\text{tr}(\text{Frob}_5) \in \{2, -2\}$  and  $\text{tr}(\text{Frob}_7) \in \{-4, 0, 4\}$ . This already gives an upper bound of 6 possible distinct isogeny classes for  $E$ .

**Remark.** For  $p = 17$ , since  $\text{Frob}_{17}$  fixes  $\zeta_8$ , this implies by Theorem 4.6 that  $\text{Frob}_{17}$  fixes all 4-torsion, and thus  $\rho_{E,2}(\text{Frob}_{17}) \equiv I \pmod{4}$ . Using this stronger condition for  $\rho_{E,2}(\text{Frob}_{17})$ , we can actually show that the only possibility for the trace at 17 is  $\text{tr}(\text{Frob}_{17}) = 2$ .

In order to further narrow down the possible values for  $\text{tr}(\text{Frob}_7)$ , we must make use of Theorem 4.6. This implies that the Galois group of  $\mathbb{Q}(E[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$  is a subgroup of  $\{M \in \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) : M \equiv I \pmod{2}\}$

We therefore run a brute force search computing all possible embeddings of  $\text{Gal}(\mathbb{Q}(E[8])/\mathbb{Q}) = C_2^2 \rtimes C_4$  in  $\{M \in \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) : M \equiv I \pmod{2}\}$  and computing the possible traces of the matrices  $M$  such that  $\det(M) = 7 \pmod{8}$ .

By doing this, we obtain that  $\text{tr}(\text{Frob}_7) \equiv 0 \pmod{8}$ . By combining this with the results from Table 4.1, this proves that  $\text{tr}(\text{Frob}_7) = 0$ , and therefore there are exactly two isogeny classes of elliptic curves  $E$  over  $\mathbb{Q}$  good away from 2 with full rational 2-torsion.

Whilst it is certainly not necessary to use the Faltings–Serre method to classify elliptic curves, given Theorem 4.1 and the numerous other methods available, the major advantage of the above method is that one can apply the same methods to classify abelian surfaces, whereby we simply replace  $\text{GL}_2$  with  $\text{GL}_4$ , or  $\text{GSp}_4$  if we assume principal polarisation.

### 4.3.2 Abelian surfaces

We now look at the  $d = 2$  case. We first compute the possible local Euler factors  $L_p(T)$  for the first few odd primes  $p$ . This can be obtained by using known bounds on the roots of  $L_p(T)$  to obtain a bound on the coefficients, and thus one can proceed by a standard finite brute computational search to compute all possibilities, as shown in Algorithm 7.

From Table 4.2, if we naively apply Corollary 4.17 to compute an upper bound for the number of isogeny classes of abelian surfaces over  $\mathbb{Q}$  with good reduction outside 2, we get  $129 \cdot 207 \cdot 401 \cdot 765 \cdot 1193 \cdot 1861$  which yields a very weak (albeit effective) upper bound of  $\approx 1.8 \cdot 10^{16}$  distinct isogeny classes.

By a similar argument to the elliptic case, if we instead use that these matrices

Table 4.2: For each odd prime  $p = 3, 5, \dots, 31$ , we tabulate the number of good Euler factors  $L_p(T)$  for dimension 2 abelian varieties  $A/\mathbb{Q}$ .

Prime $p$	3	5	7	11	13	17	19	23	29	31
<b>Num good <math>L_p(T)</math></b>	63	129	207	401	513	765	897	1193	1683	1861

must be elements in  $\mathrm{GSp}_4(\mathbb{Z}/16\mathbb{Z})$  with certain properties, then this gives us a tighter bound of at most  $4 \cdot 6 \cdot 9 \cdot 15 \cdot 22 \cdot 32 \approx 2.3 \cdot 10^6$  distinct isogeny classes, as summarised in Table 4.3. This is an improvement, but still far from the true number of such isogeny classes.

Table 4.3: For each odd prime  $p$ , we tabulate the number of possible Euler factors  $L_p(T)$  of good reduction which correspond to some matrix  $M \in \mathrm{GSp}_4(\mathbb{Z}/2^n\mathbb{Z})$  such that  $M \equiv I \pmod{2}$  and  $\det(M) \equiv p^2 \pmod{2^n}$ .

Prime $p$	$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$
<b>3</b>	17	6	2	1	1	1
<b>5</b>	35	12	5	4	4	4
<b>7</b>	53	16	8	6	6	6
<b>11</b>	103	30	14	9	9	9
<b>13</b>	129	36	19	12	12	12
<b>17</b>	195	54	25	15	15	15
<b>19</b>	227	62	32	19	19	19
<b>23</b>	301	80	40	22	22	22
<b>29</b>	425	112	57	32	32	32
<b>31</b>	467	122	60	32	32	32

Unlike the elliptic case, it is not sufficient to check matrices mod 8, but rather must instead work mod 64 here. The last column of Table 4.3 also illustrates that it is not sufficient to simply consider each Euler factor individually, but rather we must also take into account precisely how  $\mathrm{Gal}(\mathbb{Q}(A[64])/\mathbb{Q})$  embeds inside  $\mathrm{GSp}_4(\mathbb{Z}/64\mathbb{Z})$ .

To achieve this goal, we first need the following theorem which allows us to inductively compute the  $2^n$ -torsion Galois groups  $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$  based off the possibilities for  $\mathrm{Gal}(\mathbb{Q}(A[2^{n-1}])/\mathbb{Q})$ .

**Theorem 4.18.** *Let  $A/\mathbb{Q}$  be an abelian variety with good reduction away from 2 and with full rational 2-torsion. Then for any  $n \geq 2$ ,  $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$  is a central  $C_2^k$ -extension of  $\mathrm{Gal}(\mathbb{Q}(A[2^{n-1}])/\mathbb{Q})$  for some  $k \geq 0$ , and is a quotient of the group  $\langle a, b \mid a^2 = 1 \rangle$ .*

*Proof.* For any  $n \geq 2$ , we note that we have the following short exact sequence

$$1 \rightarrow \text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q}(A[2^{n-1}])) \rightarrow \text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(A[2^{n-1}])/\mathbb{Q}) \rightarrow 1.$$

Since every element in  $\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})/\text{Gal}(\mathbb{Q}(A[2^{n-1}])/\mathbb{Q})$  has order 2, this implies  $\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})/\text{Gal}(\mathbb{Q}(A[2^{n-1}])/\mathbb{Q}) \cong C_2^k$  for some  $k \geq 0$ . Furthermore, as  $A$  has good reduction away from 2, this implies  $\mathbb{Q}(A[2^n])$  is a subfield of  $\Omega_2$ ; the maximal pro-2 extension of  $\mathbb{Q}$  unramified away from 2. By a well-known result of Markšaitis [301], this has Galois group  $\langle a, b \mid a^2 = 1 \rangle$ ; i.e. the free product of  $\mathbb{Z}$  and  $C_2$ .  $\square$

Theorem 4.18 therefore reduces the problem of classifying the possible Galois groups  $\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$  to the problem of computing central  $C_2^k$ -extensions of  $\text{Gal}(\mathbb{Q}(A[2^{n-1}])/\mathbb{Q})$  which are quotients of  $\langle a, b \mid a^2 = 1 \rangle$ .

We therefore require the following theorem which extends Theorem 4.6 to give an explicit finite list of possible Galois groups  $\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$  for abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 and with full rational 2-torsion, for all  $n \leq 6$ .

**Theorem 4.19.** *Let  $A/\mathbb{Q}$  be a principally polarised abelian surface with good reduction away from 2 and with full rational 2-torsion. Then  $\mathbb{Q}(A[16])$  has degree either 32, 64, or 128, with the first two cases corresponding to two particular degree 32 and degree 64 fields. In particular, the Galois group  $\text{Gal}(\mathbb{Q}(A[16])/\mathbb{Q})$  is (as an abstract group) one of the following three groups (given with GAP IDs):*

$$C_2^2 \rtimes C_8 \langle 32, 5 \rangle, \quad D_4 \rtimes C_8 \langle 64, 6 \rangle, \quad C_2^2.C_4 \wr C_2 \langle 128, 2 \rangle.$$

Furthermore,  $\text{Gal}(\mathbb{Q}(A[32])/\mathbb{Q})$  is one of 15 possible groups of order at most  $2^{10}$ , and  $\text{Gal}(\mathbb{Q}(A[64])/\mathbb{Q})$  is one of 521 possible groups of order at most  $2^{15}$ .

*Proof.* We proceed in a similar fashion to that of Theorem 4.6. Since explicitly computing field extensions (unramified away from 2) of degree 32 or more, quickly becomes computationally unfeasible, we instead use properties of  $\text{Gal}(\mathbb{Q}(A[2^{n+1}])/\mathbb{Q}(A[2^n]))$  to directly construct group extensions to obtain the possibilities for  $\text{Gal}(\mathbb{Q}(A[2^{n+1}])/\mathbb{Q})$  (as abstract groups).

From Theorem 4.6, we know that  $\mathbb{Q}(A[8])$  is the degree 16 field  $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$ , and therefore  $\text{Gal}(\mathbb{Q}(A[8])/\mathbb{Q}) = C_2^2 \rtimes C_4$ . We now compute (using Algorithm 3) all central  $C_2^k$ -extensions of  $C_2^2 \rtimes C_4$  which are quotients of the group  $\langle a, b \mid a^2 = 1 \rangle$ . By a standard Magma implementation, this gives 13 possibilities, for which the GAP

IDs are

$$\text{Gal}(\mathbb{Q}(A[16])/\mathbb{Q}) = \begin{cases} \langle 32, 5 \rangle, \langle 32, 6 \rangle, \langle 32, 7 \rangle, \langle 32, 9 \rangle, \text{ or } \langle 32, 11 \rangle & \text{if } \deg \mathbb{Q}(A[16]) = 2^5, \\ \langle 64, 4 \rangle, \langle 64, 6 \rangle, \langle 64, 8 \rangle, \langle 64, 10 \rangle, \\ \langle 64, 12 \rangle, \langle 64, 29 \rangle, \text{ or } \langle 64, 38 \rangle & \text{if } \deg \mathbb{Q}(A[16]) = 2^6, \\ \langle 128, 2 \rangle & \text{if } \deg \mathbb{Q}(A[16]) = 2^7. \end{cases}$$

By checking which of these can occur both as Galois groups of 2-extensions of  $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$  unramified away from 2, and as subgroups of  $\{M \in \text{GSp}_4(\mathbb{Z}/16\mathbb{Z}) : M \equiv I \pmod{2}\}$ , we obtain the only three remaining possible groups are  $\langle 32, 5 \rangle$ ,  $\langle 64, 6 \rangle$  and  $\langle 128, 2 \rangle$ .

We can proceed in a similar way to compute the possible groups  $\text{Gal}(\mathbb{Q}(A[32])/\mathbb{Q})$  and  $\text{Gal}(\mathbb{Q}(A[64])/\mathbb{Q})$ . We again run Algorithm 3 for each of the three groups given for  $\text{Gal}(\mathbb{Q}(A[16])/\mathbb{Q})$  where we obtain many possible candidate groups  $\text{Gal}(\mathbb{Q}(A[32])/\mathbb{Q})$ , all of order at most 2048. We've listed the first few GAP IDs of the groups below, although to save space, we left out descriptions of the groups of order  $\geq 2^9$ :

$$\begin{aligned} & \langle 64, 4 \rangle, \langle 64, 6 \rangle, \langle 64, 29 \rangle, \langle 64, 30 \rangle, \langle 64, 31 \rangle \text{ if } \deg \mathbb{Q}(A[32]) = 2^6, \\ & \langle 128, 2 \rangle, \langle 128, 46 \rangle, \langle 128, 47 \rangle, \langle 128, 48 \rangle, \langle 128, 50 \rangle, \langle 128, 61 \rangle, \\ & \langle 128, 62 \rangle, \langle 128, 63 \rangle, \langle 128, 65 \rangle, \langle 128, 67 \rangle, \langle 128, 68 \rangle \text{ if } \deg \mathbb{Q}(A[32]) = 2^7, \\ & \langle 256, 56 \rangle, \langle 256, 58 \rangle, \langle 256, 62 \rangle, \langle 256, 90 \rangle, \langle 256, 91 \rangle, \langle 256, 93 \rangle, \\ & \langle 256, 94 \rangle, \langle 256, 95 \rangle, \langle 256, 98 \rangle, \langle 256, 100 \rangle, \langle 256, 102 \rangle, \langle 256, 103 \rangle, \\ & \langle 256, 104 \rangle, \langle 256, 367 \rangle, \langle 256, 368 \rangle, \langle 256, 371 \rangle, \langle 256, 373 \rangle \text{ if } \deg \mathbb{Q}(A[32]) = 2^8, \\ & (51 \text{ possible groups}) \text{ if } \deg \mathbb{Q}(A[32]) = 2^9, \\ & (31 \text{ possible groups}) \text{ if } \deg \mathbb{Q}(A[32]) = 2^{10}, \\ & (3 \text{ possible groups}) \text{ if } \deg \mathbb{Q}(A[32]) = 2^{11}. \end{aligned}$$

We now again check which of the above groups can occur as subgroups of  $\{M \in \text{GSp}_4(\mathbb{Z}/32\mathbb{Z}) : M \equiv I \pmod{2}\}$ . Doing this now gives us the possible groups  $\langle 64, 6 \rangle$ ,  $\langle 64, 29 \rangle$ ,  $\langle 128, 2 \rangle$ ,  $\langle 128, 61 \rangle$ ,  $\langle 128, 63 \rangle$ ,  $\langle 128, 65 \rangle$ ,  $\langle 256, 56 \rangle$ ,  $\langle 256, 58 \rangle$ ,  $\langle 256, 90 \rangle$ ,  $\langle 256, 100 \rangle$ ,  $\langle 512, 17 \rangle$ ,  $\langle 512, 62 \rangle$ , and three further groups of order  $2^{10}$ , which can be

given as one of the following matrix group presentations:

$$\left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 2 \\ 4 & 1 & 2 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 7 & 0 & 2 & 2 \\ 4 & 3 & 2 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 3 & 4 & 2 & 2 \\ 0 & 3 & 2 & 0 \\ 0 & 2 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

in  $\mathrm{GL}_4(\mathbb{Z}/32\mathbb{Z})$ .

We finally run Algorithm 3 one more time on each of the 15 possibilities for  $\mathrm{Gal}(\mathbb{Q}(A[32])/\mathbb{Q})$  listed above in order to compute the possible groups  $\mathrm{Gal}(\mathbb{Q}(A[64])/\mathbb{Q})$ . Doing so, we obtain a total of 521 possible groups for  $\mathrm{Gal}(\mathbb{Q}(A[64])/\mathbb{Q})$ , the largest one having order  $2^{15}$ .<sup>2</sup>  $\square$

This result finally allows to prove our main theorem:

**Theorem 4.20.** *There are exactly 3 isogeny classes of principally polarised abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 which contain surfaces with full rational 2-torsion. These are given by  $E_1 \times E_1$ ,  $E_1 \times E_2$  and  $E_2 \times E_2$ , where  $E_1, E_2$  are the elliptic curves  $E_1 : y^2 = x^3 - x$  and  $E_2 : y^2 = x^3 - 4x$ .*

*Proof.* We first apply Corollary 4.17 to obtain that any abelian surface  $A/\mathbb{Q}$  with good reduction away from 2 is uniquely determined up to  $\mathbb{Q}$ -isogeny by the six Euler factors  $L_5(T)$ ,  $L_7(T)$ ,  $L_{11}(T)$ ,  $L_{17}(T)$ ,  $L_{23}(T)$ , and  $L_{31}(T)$ .

In a similar method done in Section 4.3.1, we therefore compute the possible such Euler factors by brute forcing all possible ways that the group  $\mathrm{Gal}(\mathbb{Q}(A[64])/\mathbb{Q})$  can embed inside  $R = \{M \in \mathrm{GSp}_4(\mathbb{Z}/64\mathbb{Z}) : M \equiv I \pmod{2}\}$  and computing the characteristic polynomials of the relevant matrices in  $\mathrm{GSp}_4(\mathbb{Z}/64\mathbb{Z})$ . We provide pseudocode for such an implementation in Algorithm 6.

In summary, we ran Algorithm 6 for  $d = 2$ ,  $n \leq 6$ , and for each  $p \in \{5, 7, 11, 17, 23, 31\}$ . For  $p = 5$ , we obtained three possible Euler factors for  $L_5(T)$  which were  $(5T^2 + 2T + 1)^2$ ,  $(5T^2 - 2T + 1)^2$  and  $(5T^2 + 2T + 1)(5T^2 - 2T + 1)$ . We obtained only one Euler factor for each of  $L_7(T)$ ,  $L_{11}(T)$ ,  $L_{17}(T)$ ,  $L_{23}(T)$ , and  $L_{31}(T)$ .

A summary of our results modulo successively larger powers of 2 up to 64 is given in Table 4.4.

This therefore proves there are at most three isogeny classes of abelian surfaces good away from 2 with full rational 2-torsion. However, we can easily find three such non-isogenous surfaces, namely the product surfaces  $E_1 \times E_1$ ,  $E_1 \times E_2$  and

<sup>2</sup>There are no GAP IDs for 2-groups of order greater than  $2^9$ , so to save space, we shall omit giving a presentation for each of the possible groups for  $\mathrm{Gal}(\mathbb{Q}(A[64])/\mathbb{Q})$  here.

Table 4.4: For each  $n \leq 6$ , we tabulate the possibilities for the  $2^n$ -torsion field  $\mathbb{Q}(A[2^n])$  (if known), its Galois group  $\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ , and the corresponding number of valid Euler factors obtained for  $L_p(T)$  obtained from  $\text{GSp}_4(\mathbb{Z}/2^n\mathbb{Z})$  using Algorithm 6.

$n$	$\mathbb{Q}(A[2^n])$	$\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_5(T)$	$\#L_7(T)$	$\#L_{11}(T)$	$\#L_{17}(T)$	$\#L_{23}(T)$	$\#L_{31}(T)$
0	$\mathbb{Q}$	$C_1$	129	207	401	765	1193	1861
1	$\mathbb{Q}$	$C_1$	35	53	103	195	301	467
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	12	16	30	53	77	119
3	$\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$	$C_2^2 \rtimes C_4$	5	6	8	8	22	34
4	?	$C_2^2 \rtimes C_8,$ $D_4 \rtimes C_8,$ $C_2^2.C_4 \wr C_2$	4	2	2	3	7	9
5	?	(many)	3	1	1	2	2	3
6	?	(many)	3	1	1	1	1	1

$E_2 \times E_2$ , where  $E_1, E_2$  are the elliptic curves  $E_1 : y^2 = x^3 - x$  and  $E_2 : y^2 = x^3 - 4x$ , as shown in Table 4.5. This proves the theorem!  $\square$

Table 4.5: A summary of the Euler factors  $L_p(T)$  for the three isogeny classes of principally polarised abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 and with  $\mathbb{Q}(A[2]) = \mathbb{Q}$

$L_p(A/\mathbb{Q}, T)$	$A = E_1 \times E_1$	$A = E_1 \times E_2$	$A = E_2 \times E_2$
$L_5(A/\mathbb{Q}, T)$	$(5T^2 + 2T + 1)^2$	$(5T^2 + 2T + 1)(5T^2 - 2T + 1)$	$(5T^2 - 2T + 1)^2$
$L_7(A/\mathbb{Q}, T)$	$(7T^2 + 1)^2$	$(7T^2 + 1)^2$	$(7T^2 + 1)^2$
$L_{11}(A/\mathbb{Q}, T)$	$(11T^2 + 1)^2$	$(11T^2 + 1)^2$	$(11T^2 + 1)^2$
$L_{17}(A/\mathbb{Q}, T)$	$(17T^2 - 2T + 1)^2$	$(17T^2 - 2T + 1)^2$	$(17T^2 - 2T + 1)^2$
$L_{23}(A/\mathbb{Q}, T)$	$(23T^2 + 1)^2$	$(23T^2 + 1)^2$	$(23T^2 + 1)^2$
$L_{31}(A/\mathbb{Q}, T)$	$(31T^2 + 1)^2$	$(31T^2 + 1)^2$	$(31T^2 + 1)^2$

#### Remarks.

- It should in principle be possible to remove the principal polarisation assumption in the proof of Theorem 4.20 by running the exact same computations within  $\text{GL}_4$  instead of  $\text{GSp}_4$ . Although running Algorithm 6 for all of  $\text{GL}_4$  would've taken too long, as least with our implementation.

- It should also be possible to extend this result to classifying all *isomorphism classes* of such principally polarised abelian surfaces (instead of only isogeny classes). This would follow by computing all genus 2 curves  $C/\mathbb{Q}$  such that  $\text{Jac}(C)$  is isogenous to  $E_1 \times E_1$ ,  $E_1 \times E_2$ , or  $E_2 \times E_2$ . A further discussion of this is given in Section 5.3.
- Furthermore, it is not even clear if one can give a clear description of all (not necessarily principally polarised) isomorphism classes of abelian surfaces  $A/\mathbb{Q}$ . Although if we restrict to principally polarised abelian surfaces, then it seems reasonable to conjecture that  $E_1 \times E_1$ ,  $E_1 \times E_2$ , and  $E_2 \times E_2$  are the only such abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 and with full rational 2-torsion (Conjecture 4.2).

We now give an overview of some of the algorithms used for our computations.

#### 4.3.3 Solving the conjugacy problem for $\text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$

One of our main computational obstacles doing this approach is having to consider all possible subgroups of  $\text{GSp}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ . Doing this via a naive brute force search would be far too impractical, even for  $d = \ell = 2$ . For instance, the order of  $\text{GSp}_4(\mathbb{Z}/64\mathbb{Z})$  is  $2^{59} \cdot 3^2 \cdot 5 \approx 2.6 \cdot 10^{19}$  and the number of subgroups of  $\text{GSp}_4(\mathbb{Z}/64\mathbb{Z})$  would still be far larger than this! One immediate observation is that, since we only care about the characteristic polynomials of matrices in  $\text{GSp}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ , we only need to consider our subgroups up to conjugacy in  $\text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ .

In general, given an arbitrary commutative ring  $R$  and a positive integer  $N \geq 2$ , the problem of determining whether two matrices  $A, B \in M_N(R)$  are conjugate as well as the related problem of computing a complete set of conjugacy class representatives of  $M_N(R)$  (and more generally conjugacy classes of subgroups of  $M_N(R)$ ) is highly non-trivial. If  $A$  and  $B$  are conjugate, then it's clear they must have the same minimal and characteristic polynomials, but the converse is not true in general. In the case where  $R$  is a field, it's a well-known result that conjugacy classes can essentially be uniquely characterised by the *Frobenius normal form* (e.g. see Dickson [138, Chapter V] or Hoffman–Kunze [223, p. 238]). More generally, if  $R$  is a local principal ideal ring which is not a field (e.g.  $R = \mathbb{Z}/\ell^n\mathbb{Z}$  for  $n \geq 2$ ), and  $N \geq 3$ , then the conjugacy classes of  $M_N(R)$  have only been fully classified in a few special cases. Nechaev [329] classified the conjugacy classes for  $M_3(\mathbb{Z}/\ell^2\mathbb{Z})$  with Avni–Onn–Prasad–Vaserstein [19] classifying conjugacy classes for  $M_3(R)$  where  $R$  is a finite quotient of a complete discrete valuation ring. Recently, Prasad–Singla–Spallone [359] have classified conjugacy classes for  $M_4(\mathbb{Z}/\ell^2\mathbb{Z})$ . For results related

more to our conjugacy problem, we mention that the sizes and representatives for conjugacy classes of  $\mathrm{GSp}_4(\mathbb{Z}/\ell^n\mathbb{Z})$  have been computed by Williams [483]. We also mention some further work of Achter–Williams [5] giving a computation of the conjugacy classes of  $\mathrm{GSp}_4(\mathbb{F}_\ell)$  corresponding to abelian surfaces.

We note that Magma does already have a rather sophisticated implementation of computing conjugacy class representatives for a wide range of matrix rings (e.g. see [132, 131]), however we found that it was still best to implement our own probabilistic conjugacy algorithm based on a randomised approach. Since we didn't need an exact set of conjugacy class representatives, we contented ourselves with an algorithm which takes as input two matrices  $A, B \in \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  and always returns **false** if  $A, B$  are not conjugate, and returns **true** in *almost all* cases where  $A, B$  are conjugate. Here, we first solve the linear system  $AP = PB$  modulo  $\ell^n$ , and then do a random search over such solutions  $P$  which are invertible mod  $\ell$ .  $r$  is a parameter denoting the number of attempts to search for such a matrix. A value of  $r = 100$  seemed to do well in practice for the case  $\mathrm{GL}_4(\mathbb{Z}/32\mathbb{Z})$ . This algorithm is implemented as given in Algorithm 1.

---

**Algorithm 1** Probabilistic algorithm to compute whether  $A, B \in \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  are conjugate

---

```

1: procedure ISSTRONGCONJUGATE( $A, B, r$ )
2:   Let  $\mathcal{R}$  be the set of all matrices  $P \in \mathrm{M}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  such that  $AP = PB$  (using
   a linear algebra solver).
3:   for  $i = 1$  to  $r$  do
4:     Let  $P$  be a random element in  $\mathcal{R}$ .
5:     if  $\det(P)$  is not divisible by  $\ell$  then
6:       return true ( $A, B$  definitely conjugate)
7:     end if
8:   end for
9:   return false ( $A, B$  probably not conjugate)
10: end procedure

```

---

We can therefore use Algorithm 1 to obtain a list of matrices  $M$  in  $\mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  for which we can guarantee that every conjugacy class is represented at least once. To do this efficiently, we perform a lifting algorithm modulo successively higher powers of  $\ell$ .

To summarise the method, we let  $\mathcal{R}_1$  be a set of conjugacy class representatives for  $\mathrm{GL}_{2d}(\mathbb{Z}/\ell\mathbb{Z})$  (e.g. using the default Magma implementation). Then, for each  $R \in \mathcal{R}_1$ , we consider each of its  $\ell^{4d^2}$  possible lifts in  $\mathrm{GL}_{2d}(\mathbb{Z}/\ell^2\mathbb{Z})$  and run Algorithm 1 to determine a set of conjugacy class representatives  $\mathcal{R}_2$  for  $\mathrm{GL}_{2d}(\mathbb{Z}/\ell^2\mathbb{Z})$ . We then repeat the process until we get to  $\mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ . This is implemented as



shown in Algorithm 2.

---

**Algorithm 2** Probabilistic algorithm to compute a set of conjugacy class representatives in  $\text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$

---

```

1: procedure CONJUGACYCLASSREPS( $d, n, \ell$ )
2:   Let  $\mathcal{R}_{\text{old}}$  be a set of conjugacy class representatives for  $\text{GL}_{2d}(\mathbb{Z}/\ell\mathbb{Z})$ .
3:   for  $i = 1$  to  $n - 1$  do
4:     Let  $\mathcal{R}_{\text{new}} = \emptyset$ .
5:     for  $R$  in  $\mathcal{R}_{\text{old}}$  do
6:       Let  $\mathcal{C} := \emptyset$ .
7:       for  $N$  in  $\text{M}_{2d}(\mathbb{Z}/\ell\mathbb{Z})$  do
8:         Let  $M := R + \ell^i N \pmod{\ell^{i+1}}$ 
9:         for  $C$  in  $\mathcal{C}$  do
10:          if  $M$  definitely conjugate to  $C$  with (using Algorithm 1) then
11:            break
12:          end if
13:        end for
14:        Else, add  $M$  to  $\mathcal{C}$ .
15:      end for
16:      Add all elements of  $\mathcal{C}$  to  $\mathcal{R}_{\text{new}}$ 
17:    end for
18:    Let  $\mathcal{R}_{\text{old}} = \mathcal{R}_{\text{new}}$ 
19:  end for
20:  return  $\mathcal{R}_{\text{new}}$ 
21: end procedure

```

---

#### 4.3.4 Computing the possible Galois groups $\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$

Recall that a key ingredient in our proof of Theorem 4.20 is obtaining a finite list of possible Galois groups  $\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$  for  $n \leq 6$ . Recall that Theorem 4.18 states that  $\text{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$  is a quotient of  $\langle a, b \mid a^2 = 1 \rangle$  and is a central  $C_2^k$ -extension of  $\text{Gal}(\mathbb{Q}(A[2^{n-1}])/\mathbb{Q})$ .

To determine such groups up to order 512, we can directly look these up in the GAP SMALLGROUPS database [34], distributed with Magma. However, for the 2-groups of order beyond 512, we must compute these ourselves. Recall that central extensions of a group  $G$  by  $C_2^k$  are in one-to-one correspondence with elements of the 2nd cohomology group  $H^2(G, C_2^k)$  (e.g. see [388, Remark 3.27]).<sup>3</sup> Here, we can make use of the Magma functions `CohomologyModule`, `CohomologyGroup` and `Extension` developed by Derek Holt [224] to explicitly compute such central extensions. This

---

<sup>3</sup>We note it's possible that two distinct elements in  $H^2(G, C_2^k)$  could yield groups  $A_1$  and  $A_2$  which are inequivalent as  $C_2^k$ -extensions of  $G$ , but isomorphic as abstract groups.

is implemented as shown in Algorithm 3, where we compute a  $C_2^k$ -extension by successively computing  $C_2$ -extensions until we no longer find such extensions which are quotients of  $\langle a, b \mid a^2 = 1 \rangle$ .

---

**Algorithm 3** Computing all central  $C_2^k$ -extensions  $H$  of a finite group  $G$  such that  $H$  is a quotient of  $\langle a, b \mid a^2 = 1 \rangle$ .

---

```

1: procedure COMPUTE2EXTENSIONS(Group  $G$ )
2:   Let  $\mathcal{G} = \{G\}$ 
3:   Let  $\mathcal{H} = \emptyset$ .
4:   Let  $k := 1$ .
5:   while  $\mathcal{G}$  not empty do
6:     Let  $\mathcal{G}_{\text{new}} = \emptyset$ 
7:     for  $H$  in  $\mathcal{G}$  do
8:       for all central 2-extensions  $H'$  of  $H$  do
9:         if  $H'$  is quotient of  $\langle a, b \mid a^2 = 1 \rangle$  then
10:          if  $H'$  has a central subgroup isomorphic to  $C_2^k$  then
11:            Add  $H'$  to  $\mathcal{G}_{\text{new}}$ .
12:            Add  $H'$  to  $\mathcal{H}$ 
13:          end if
14:        end if
15:      end for
16:    end for
17:    Let  $\mathcal{G} = \mathcal{G}_{\text{new}}$ 
18:     $k := k + 1$ ;
19:  end while
20:  return  $\mathcal{H}$ .
21: end procedure

```

---

#### 4.3.5 Searching for rank 2 subgroups of $\text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$

Finally, once we've obtained a finite list of candidate  $\ell^n$ -torsion groups  $\text{Gal}(\mathbb{Q}(A[\ell^n])/\mathbb{Q})$ , we run Algorithm 6 to compute the possible embeddings of these groups in  $\text{GSp}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  and hence the possible candidate Euler factors  $L_p(T)$ .

Note that by Theorem 4.18, every candidate subgroup will be generated by some order 2 element  $C$  and one other element  $D$ . As we only need to consider all such subgroups up to conjugacy, we may assume without loss of generality that  $C$  is one of our conjugacy class representatives of order 2, found using Algorithm 2. Furthermore, by conjugating by a matrix  $P \in \text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  which keeps  $C$  constant (i.e. such that  $C = P^{-1}CP$ ), we can also assume that  $D$  is a representative of one of these “restricted” conjugacy classes.

To make this explicit, we define the following stronger notion of conjugacy.

**Definition 4.6.** Let  $n, d \geq 1$ , and fix a prime  $\ell$  and a matrix  $C \in \text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ . We say that two matrices  $A, B \in \text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  are  **$C$ -stable conjugate** if there exists some  $P \in \text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  such that  $A = P^{-1}BP$  and  $C = P^{-1}CP$ . We denote this as  $A \sim_C B$ .

It's clear that  $\sim_C$  is an equivalence relation on  $\text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ . Let  $\mathcal{D} \subset \text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  be a set of representative elements containing at least one element from each  $C$ -stable conjugacy class in  $\text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  induced by  $\sim_C$ . Then we may assume that  $D \in \mathcal{D}$ . We give pseudocode to compute such a set  $\mathcal{D}$  in Algorithm 5; this is essentially the same as Algorithm 2 with the extra condition that  $C = P^{-1}CP$ .

---

**Algorithm 4** Probabilistic algorithm to compute whether two matrices  $A, B \in \text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  are  $C$ -stable conjugate.

---

```

1: procedure ISCSTABLESTRONGCONJUGATE( $A, B, r, C$ )
2:   Let  $\mathcal{R}$  be the set of all matrices  $P \in \text{M}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$  such that  $AP = PB$  and
      $PC = CP$  (using a linear algebra solver).
3:   for  $i = 1$  to  $r$  do
4:     Let  $P$  be a random element in  $\mathcal{R}$ .
5:     if  $\det(P)$  is not divisible by  $\ell$  then
6:       return true ( $A, B$  definitely  $C$ -stable conjugate)
7:     end if
8:   end for
9:   return false ( $A, B$  probably not  $C$ -stable conjugate)
10: end procedure

```

---

Most of the above algorithms were implemented using Magma [58] and Sage [373] with the exception of the mod 64 case for Algorithm 6 which was implemented in C++ for maximum efficiency. By distributing the workload across several of the outer for-loops into separate threads, most of the above algorithms were easily parallelisable, and so extensive use was made of GNU Parallel [440].

---

**Algorithm 5** Probabilistic algorithm to compute  $C$ -stable conjugacy class representatives in  $\text{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$ .

---

```

1: procedure CSTABLECONJUGACYCLASSREPS( $d, n, \ell, C$ )
2:   Let  $\mathcal{R}_{\text{old}}$  be a set of conjugacy class representatives (stable with respect to
    $C$ ) for  $\text{GL}_{2d}(\mathbb{Z}/\ell\mathbb{Z})$  (e.g. using a brute force algorithm).
3:   for  $i = 1$  to  $n - 1$  do
4:     Let  $\mathcal{R}_{\text{new}} = \emptyset$ .
5:     for  $R$  in  $\mathcal{R}_{\text{old}}$  do
6:       Let  $\mathcal{C} := \emptyset$ .
7:       for  $N$  in  $\text{M}_{2d}(\mathbb{Z}/\ell\mathbb{Z})$  do
8:         Let  $M := R + \ell^i N \pmod{\ell^{i+1}}$ 
9:         for  $D$  in  $\mathcal{C}$  do
10:          if  $M$  definitely  $C$ -stable conjugate to  $D$  (using Algorithm 4)
11:            then
12:              break
13:            end if
14:          else, add  $M$  to  $\mathcal{C}$ .
15:        end for
16:      Add all elements of  $\mathcal{C}$  to  $\mathcal{R}_{\text{new}}$ 
17:    end for
18:    Let  $\mathcal{R}_{\text{old}} = \mathcal{R}_{\text{new}}$ 
19:  end for
20:  return  $\mathcal{R}_{\text{new}}$ 
21: end procedure

```

---

---

**Algorithm 6** Compute the possible Euler factors  $L_p(T)$  at an odd prime  $p$  for a dimension  $d$  abelian variety  $A/\mathbb{Q}$  with good reduction away from 2 (using  $\mathrm{GSp}_{2d}(\mathbb{Z}/2^n\mathbb{Z})$ )

---

```

1: procedure COMPUTEPOSSIBLEFACTORS( $d, n, p$ )
2:   Let  $\mathcal{G}$  be a list of the possible Galois groups  $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$  (using Algo-
   rithm 3).
3:   Let  $\mathcal{C}$  be a set of conjugacy class representatives of order 2 elements in
    $\mathrm{GSp}_{2d}(\mathbb{Z}/2^n\mathbb{Z})$  (using Algorithm 2).
4:   Let  $\mathcal{L}_{\mathrm{all}}$  be the set of all possible good Euler factors at  $p$  (using Algorithm 7).
5:   Let  $\mathcal{L} := \emptyset$ .
6:   for  $C$  in  $\mathcal{C}$  do
7:     Let  $\mathcal{D}$  be a list of  $C$ -stable conjugacy class representatives in
      $\mathrm{GSp}_{2d}(\mathbb{Z}/2^n\mathbb{Z})$  (using Algorithm 5).
8:     for  $D$  in  $\mathcal{D}$  do
9:       Let  $H$  be the rank 2 subgroup of  $\mathrm{GL}_{2d}(\mathbb{Z}/2^n\mathbb{Z})$  generated by the ma-
       trices  $C$  and  $D$ .
10:      for  $G$  in  $\mathcal{G}$  do
11:        if  $H$  is isomorphic to  $G$  then
12:          if  $\forall \text{primes } p, \exists M \in H$  such that  $\det(M) \equiv p^d \pmod{2^n}$  then
13:            for  $M$  in  $H$  do
14:              if  $\det(M) \equiv p^d \pmod{2^n}$  then
15:                for all  $L_p(T)$  in  $\mathcal{L}_{\mathrm{all}}$  do
16:                  if  $\chi(M) \equiv L_p(T) \pmod{2^n}$  then
17:                    Add  $L_p(T)$  to  $\mathcal{L}$ .
18:                  end if
19:                end for
20:              end if
21:            end for
22:          end if
23:        end if
24:      end for
25:    end for
26:  end for
27:  return A list  $\mathcal{L}$  of possible Euler factors at  $p$  for  $A/\mathbb{Q}$ .
28: end procedure

```

---

## Chapter 5

# Computing abelian surfaces $A/\mathbb{Q}$ with good reduction outside 2

Recall that Faltings' proof of the Shafarevich conjecture implies that there are only finitely many abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2. In this chapter, we shall describe our various attempts to compute such abelian surfaces. That is, our ideal (but not yet achieved) goal would be to solve Conjecture 1.5 (Effective Shafarevich II) in the case where  $K = \mathbb{Q}$ ,  $d = 2$  and  $S = \{2\}$ . This was originally posed as a problem by Bjorn Poonen [352, p. 301] and still remains unsolved to this day!

Whilst a provably complete classification of all abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2 still unfortunately appears out of reach, we have employed various methods and algorithms to compute as many such abelian surfaces as we can. In this spirit, we present the following theorem which gives some partial progress towards answering Poonen's question.

**Theorem 5.1.** *There are at least 234  $\mathbb{Q}$ -isogeny classes of abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2, presented in Table 6.20. In particular, there are at least 512  $\mathbb{Q}$ -isomorphism classes of genus 2 curves  $C/\mathbb{Q}$  whose Jacobian has good reduction away from 2 (divided amongst 175  $\mathbb{Q}$ -isogeny classes), presented in Table 6.21. Our Table 6.21 contains all such genus 2 curves  $C/\mathbb{Q}$  such that  $C$  and its Jacobian  $J$  satisfy at least one of the eleven following conditions:*

- (i)  $C/\mathbb{Q}$  has good reduction away from  $\{2, 3\}$ ,  $\{2, 5\}$ , or  $\{2, 7\}$ .
- (ii)  $C/\mathbb{Q}$  has good reduction away from  $\{2, 3, 5\}$  and  $\mathbb{Q}(J[2]) \subseteq \mathbb{Q}(\zeta_{16})$ .
- (iii)  $C/\mathbb{Q}$  has good reduction away from  $\{2, 3, 7\}$  and  $\mathbb{Q}(J[2]) \subseteq \mathbb{Q}(\zeta_{16})$  or  $\mathbb{Q}(J[2]) \subseteq \mathbb{Q}(\sqrt[4]{2\sqrt{2}-3})$ .

- (iv)  $C/\mathbb{Q}$  has good reduction away from  $\{2, 5, 7\}$  and  $\mathbb{Q}(J[2]) \subseteq \mathbb{Q}(\zeta_{16})$  or  $\mathbb{Q}(J[2]) \subseteq \mathbb{Q}(\zeta_8, \sqrt[4]{2})$ .
- (v)  $C/\mathbb{Q}$  has good reduction away from  $\{2, 3, 5, 7\}$  and either  $\mathbb{Q}(J[2]) \subseteq \mathbb{Q}(i)$ ,  $\mathbb{Q}(J[2]) \subseteq \mathbb{Q}(\sqrt{-2})$  or  $\mathbb{Q}(J[2]) \subseteq \mathbb{Q}(\sqrt{2})$ .
- (vi)  $C/\mathbb{Q}$  has good reduction away from  $\{2, 3, 5, 7, 11, 13\}$  and  $\mathbb{Q}(J[2]) = \mathbb{Q}$ .
- (vii)  $C/\mathbb{Q}$  has trivial geometric endomorphism ring and is  $\mathbb{Q}$ -isogenous to one of the 512 curves in Table 6.21.
- (viii)  $C/\mathbb{Q}$  is  $\mathbb{Q}$ -isogenous of 2-power degree to one of the 512 curves in Table 6.21.
- (ix)  $C/\mathbb{Q}$  satisfies the Hasse-Weil conjecture and has conductor at most  $2^7$  or conductor  $2^9$ .
- (x)  $C/\mathbb{Q}$  has absolute minimal discriminant  $|\Delta_{\min}|$  at most  $10^{14}$ .
- (xi) There exist elliptic curves  $E_1/\mathbb{Q}$  and  $E_2/\mathbb{Q}$  with good reduction away from 2, and elliptic subcovers  $C \rightarrow E_1$  and  $C \rightarrow E_2$  each of degree  $n$ , for some  $n \leq 7$ .

Furthermore, assuming the paramodular conjecture, Table 6.21 contains at least one representative genus 2 curve  $C/\mathbb{Q}$  from all isogeny classes which have conductor at most  $2^9$ , and all isogeny classes of conductor  $2^{10}$  which contain at least one abelian surface  $A/\mathbb{Q}$  satisfying  $\#A(\mathbb{Q})[2] \geq 8$ .

**Remark.** We emphasize that our computations have not computed *all* genus 2 curves  $C/\mathbb{Q}$  which satisfy any one of the above eleven conditions (i)–(xi), but only the subset of those for which  $\text{Jac}(C)$  has good reduction away from 2.

Recall that Faltings' theorem implies there are only finitely many principally polarised abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2. Given that a genus 2 curve  $C/\mathbb{Q}$  is uniquely determined by its Jacobian  $\text{Jac}(C)$  (as a *principally polarised* abelian surface), this implies there are only finitely many genus 2 curves  $C/\mathbb{Q}$  (up to  $\mathbb{Q}$ -isomorphism) whose Jacobians have good reduction away from 2.<sup>1</sup>

At this stage, we unfortunately don't yet have an unconditional effective algorithm to yield all such genus 2 curves  $C/\mathbb{Q}$ . We therefore focus our efforts on rather giving as complete a list of possible, by considering three possible approaches: (i) directly computing rational degree 4  $L$ -functions of conductor  $2^n$ , (ii) computing

<sup>1</sup>Given that there are  $2^9$  known genus 2 curves  $C/\mathbb{Q}$  whose Jacobians have good reduction outside 2, Barinder Banwait has recently (and somewhat amusingly) posed the question of whether, for any prime  $p$ , the number of genus  $p$  curves  $X/\mathbb{Q}$  whose Jacobians have good reduction away from  $p$  is a power of  $p$  [491, Problem 9].

genus 2 curves  $C/\mathbb{Q}$  with good reduction outside a small finite set  $S$  of primes, and (iii) gluing elliptic curves  $E/\mathbb{Q}$  with good reduction away from 2. These are each described in the following three sections respectively.

## 5.1 Computing $L$ -functions of 2-power conductor

Here we prove the following theorem, extending a result of Farmer–Koutsoliotas–Lemurell [166].

**Theorem 5.2.** *Assume the paramodular conjecture. Then there are no abelian surfaces  $A/\mathbb{Q}$  of conductor  $2^n$  for all  $n \leq 7$  and  $n = 9$ . Moreover, there is only one isogeny class of abelian surfaces  $A/\mathbb{Q}$  of conductor  $2^8$  and only one isogeny class of abelian surfaces  $A/\mathbb{Q}$  of conductor  $2^{10}$  consisting of a surface  $A/\mathbb{Q}$  such that  $(\mathbb{Z}/2\mathbb{Z})^3 \subseteq A(\mathbb{Q})$ .*

It's worth mentioning that Mestre [316] showed that any dimension  $d$  abelian variety  $A/\mathbb{Q}$  whose  $L$ -function satisfies the Hasse-Weil conjecture has conductor greater than  $10^d$ , thus proving already that no modular abelian surface has conductor  $\leq 2^6$ . We should mention that this theorem will be mostly superseded by a more general classification of abelian surfaces  $A/\mathbb{Q}$  of small conductor  $N \leq 1000$ , which is currently work in progress by Booker and Sutherland [55].

There are many axiomatic definitions of  $L$ -functions, e.g. see Selberg [390], Piatetski-Shapiro [346], or Carletti-Monti Bragadin-Perelli [96], but here we'll follow the definitions given in Farmer–Pitale–Ryan–Schmidt [168] for tempered balanced analytic  $L$ -functions.

**Definition 5.1** ( $L$ -function). [168, p. 263] A (tempered balanced) analytic  $L$ -function is a Dirichlet series

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad a_n \in \mathbb{C}$$

satisfying the following five axioms:

1. (*Analyticity*)  $L(s)$  converges absolutely for  $\operatorname{Re}(s) > 1$  and has a meromorphic continuation to  $\mathbb{C}$  such that all poles with positive real part lie on the line  $\operatorname{Re}(s) = 1$ .
2. (*Functional equation*) There exists a positive integer  $N$  (the **conductor**), a positive integer  $d$  (the **degree**), a pair of non-negative integers  $(d_1, d_2)$  (the **signature**) satisfying  $d_1 + 2d_2 = d$  and complex numbers  $\{\mu_j\}$  and  $\{\nu_j\}$  (**spectral**



**parameters**) such that the completed  $L$ -function

$$\Lambda(s) = N^{s/2} \prod_{j=1}^{d_1} \Gamma_{\mathbb{R}}(s + \mu_j) \prod_{k=1}^{d_2} \Gamma_{\mathbb{C}}(s + \nu_k) \cdot L(s)$$

satisfies the following two properties: (i) Away from the poles of the  $L$ -function,  $\Lambda(s)$  is bounded in vertical strips  $\sigma_1 < \operatorname{Re}(s) < \sigma_2$ , and (ii), there exists  $\varepsilon \in \mathbb{C}$  such that  $\Lambda(s) = \varepsilon \bar{\Lambda}(1-s)$ .<sup>2</sup>

We denote the quadruple  $(d, N, (\mu_1, \dots, \mu_{d_1} : \nu_1, \dots, \nu_{d_2}), \varepsilon)$  as the **Selberg data** of  $L(s)$ .

3. (*Euler product*) There is a product formula

$$L(s) = \prod_{p \text{ prime}} F_p(p^{-s})^{-1}$$

which absolutely converges for  $\operatorname{Re}(s) > 1$ , and such that  $F_p$  is a degree  $d_p$  polynomial such that  $F_p(0) = 1$  and  $d_p \leq d$  with equality if and only if  $p \nmid N$ .

4. (*Temperedness*) (4a) The spectral parameters satisfy  $\operatorname{Re}(\mu_j) \in \{0, 1\}$  and  $\operatorname{Re}(\nu_j) \in \{\frac{1}{2}, 1, \frac{3}{2}, 2, \dots\}$  for all  $j$ . (4b) Let  $F_p(z) = (1 - \alpha_{1,p}z) \cdots (1 - \alpha_{d_p,p}z)$  with  $\alpha_{j,p} \neq 0$ . Then if  $p \nmid N$ , then  $|\alpha_{j,p}| = 1$  for all  $j$ , and if  $p|N$  then  $|\alpha_{j,p}| = p^{-m_j/2}$  for some  $m_j \in \{0, 1, 2, \dots\}$ , and  $\sum m_j \leq d - d_p$ .
5. (*Central character*) There exists a Dirichlet character  $\chi \bmod N$  (the **central character**) such that: (i) For every prime  $p$ ,  $F_p(z) = 1 - a_p z + \cdots + (-1)^d \chi(p) z^d$ , (ii)  $\operatorname{Im}(\sum \mu_j + \sum (2\nu_k + 1)) = 0$ , and (iii)  $\chi(-1) = (-1)^{\sum \mu_j + \sum (2\nu_k + 1)}$ .

We say that an analytic  $L$ -function  $L(s)$  is **primitive** if  $L(s)$  cannot be written non-trivially as  $L(s) = L_1(s)L_2(s)$  for some analytic  $L$ -functions  $L_1(s)$  and  $L_2(s)$ , neither of which are the constant function 1.

An important subset of analytic  $L$ -functions are  $L$ -functions of arithmetic type. We thus also state the following definition of Farmer–Pitale–Ryan–Schmidt [168].

**Definition 5.2** (Arithmetic  $L$ -functions). [168, Definition 4.2] Let  $L(s) = \sum a_n n^{-s}$  be a (tempered balanced) analytic  $L$ -function. We say that  $L$  is of **arithmetic type** if there exists some integer  $w \in \mathbb{Z}$  and a number field  $F$  such that  $a_n n^{w/2} \in \mathcal{O}_F$  for all  $n$ . The smallest such  $F$  is called the **field of coefficients** of  $L$ , and the smallest such  $w$  is called the **arithmetic weight** (or **motivic weight**) of  $L$ .

<sup>2</sup>Here,  $\bar{\Lambda}$  denotes the Schwartz reflection of  $\Lambda$ , i.e.  $\bar{\Lambda}(z) = \overline{\Lambda(\bar{z})}$  is the dual of  $\Lambda$ .

In particular, a **rational** analytic  $L$ -function is an  $L$ -function whose field of coefficients is  $\mathbb{Q}$ .

Given an analytic  $L$ -function  $L(s) = \sum a_n n^{-s}$  of arithmetic type and weight  $w$ , we denote the **arithmetic normalisation** of  $L$  as the function  $L_{\text{ar}}(s) := L(s - \frac{w}{2})$ . (equivalently, the  $L$ -function with Dirichlet coefficients  $a_n n^{w/2}$ ). This moves the line of symmetry of  $L_{\text{ar}}$  to  $\text{Re}(s) = \frac{w+1}{2}$ , where the functional equation of  $L_{\text{ar}}$  relates  $s$  to  $1 + w - s$ . Conversely, given an arithmetic  $L$ -function  $L(s)$  whose functional equation relates  $s$  with  $w + 1 - s$  we can define its **analytic normalisation** as  $L_{\text{an}}(s) := L(s + \frac{w}{2})$ . This moves the critical line (the line of symmetry) of  $L_{\text{an}}(s)$  to  $\text{Re}(s) = \frac{1}{2}$  where the functional equation of  $L_{\text{an}}(s)$  now relates  $s$  to  $1 - s$ .

We note that the Hasse-Weil conjecture implies that our definition of  $L$ -functions of abelian varieties, as given in Definition 1.20, is the arithmetic normalisation of a (tempered balanced) analytic  $L$ -function of motive weight 1. Therefore, given an abelian variety  $A/K$ , we refer to its *analytically normalised  $L$ -function* as the analytic  $L$ -function  $L_{\text{an}}(A/K, s) := L(A/K, s + \frac{1}{2})$ .

We remark that the above definition is a priori stronger than the axioms given by Selberg; e.g. the Selberg axioms allow for non-integral degrees, and has no condition on the (half)-integrality of  $\text{Re}(\mu_j)$  and  $\text{Re}(\nu_j)$ . However, it's conjectured that any  $L$ -function satisfying the Selberg axioms also satisfies the Farmer–Pitale–Ryan–Schmidt axioms.

Proving that every such  $L$ -function satisfying the above axioms arises from a suitable automorphic form or motive is still very far from being achieved. However some progress has been done in small degree cases. One of the first such converse results was a theorem by Hamburger [212] showing that the only  $L$ -function of degree  $d = 1$ , conductor  $N = 1$ , and spectral parameter  $\mu_1 = 0$  is the Riemann zeta function  $\zeta(s)$ .

Conrey-Ghosh [117] showed the constant 1  $L$ -functions are the only degree 0  $L$ -functions. A full classification of degree 1  $L$ -functions was done by Kaczorowski–Perelli [240] who proved that the only degree  $d = 1$   $L$ -functions are the Riemann zeta function  $\zeta(s)$  and Dirichlet  $L$ -functions associated to primitive characters  $\chi$ .

For larger degrees, a full classification has not been provided, although many partial results have been shown for degree  $d = 2$ , originating with Hecke [220] and Weil [479], with further converse theorems shown by Booker [52], Farmer [169], Conrey–Farmer [116], Kaczorowski–Perelli [241, 242, 243], and Dimitrov [141]. These results usually assume some further conditions either on the conductor  $N$ , the poles of  $L(s)$ , the spectral parameters  $\{\mu_j\}, \{\nu_j\}$ , integrality of the coefficients  $a_n$ , or that

the twisted  $L$ -functions  $\sum a_n \chi(n) n^{-s}$  over primitive Dirichlet characters  $\chi$  have meromorphic continuation and satisfy analogous functional equations.

Much less is known regarding converse theorems for degree  $\geq 3$ . Nonetheless, we mention some recent computations in the case of degree  $d = 3$  and conductor  $N = 1$ , done by Farmer–Koutsoliotas–Lemurell–Roberts [167].

With the above axiomatic definition of Farmer–Pitale–Ryan–Schmidt [168] in mind, we mention the following conjecture.

**Conjecture 5.3.** *Let  $d, N \geq 1$  be positive integers and  $\varepsilon \in \{-1, +1\}$ . Then every rational (tempered balanced) analytic  $L$ -function of motive weight 1, degree  $2d$ , conductor  $N$ , signature  $(0, d)$ , sign  $\varepsilon$ , and spectral parameters  $\nu_1 = \nu_2 = \cdots = \nu_d = \frac{1}{2}$  is the analytically normalised  $L$ -function of some dimension  $d$  conductor  $N$  abelian variety  $A/\mathbb{Q}$ .*

This is still very far from being proven; indeed this is essentially a vastly simplified example of far more general conjectures arising from the Langlands programme, e.g. see some conjectures described by Clozel [104, 105] and Buzzard–Gee [87].<sup>3</sup>

By computing Jacobians of genus 2 curves, products of elliptic curves over  $\mathbb{Q}$ , and Weil restrictions of elliptic curves over quadratic fields  $K$  unramified away from 2, we have found a total of 234 known degree 4 rational motivic weight 1  $L$ -functions of 2-power conductor, listed in Table 5.1. Using the LMFDB, we also verified our list contained all  $L$ -functions of dimension 2 isogeny factors of  $J_1(N)$  for  $N$  a power of 2.

*Remark:* By a result of Brumer and Kramer [77], one can check that the highest exponent of 2 in the conductor of a genus 2 curve over  $\mathbb{Q}$  is 20.

We can thus state the following strengthening of Conjecture 5.3 for degree  $d = 4$  and conductor  $2^n$ :

**Conjecture 5.4.** *There are exactly 234 degree 4 rational motivic weight 1  $L$ -functions of 2-power conductor. In particular, every such primitive  $L$ -function arises from either one of Smart’s list of 366 genus 2 curves  $C/\mathbb{Q}$  with good reduction away from 2, or from a Weil restriction of an elliptic curve over a quadratic field  $K$  unramified away from 2.*

We are still very far from proving anything close to Conjecture 5.4, however we can at least make some partial progress towards a conditional classification of  $L$ -functions with small conductor  $N$ .

<sup>3</sup>A beautiful diagram showing connections between  $L$ -functions, automorphic forms, motives, and Galois representations is given on the  *$L$ -functions and modular forms database* (LMFDB) [290, LMFDB Universe].

Table 5.1: List of all 234 known degree 4 rational motivic weight 1  $L$ -functions of conductor  $2^n$ , each corresponding to an isogeny class of abelian surfaces  $A/\mathbb{Q}$  of conductor  $2^n$ . The set of  $L$ -functions for  $N \leq 2^9$  is conditionally complete, assuming the paramodular conjecture.

Conductor $N$	Rank			Split	Simple	Totals
	0	1	2	(over $\overline{\mathbb{Q}}$ )		
$\leq 2^7$	0	0	0	0	0	<b>0</b>
$2^8$	1	0	0	1	0	<b>1</b>
$2^9$	0	0	0	0	0	<b>0</b>
$2^{10}$	1	0	0	1	0	<b>1</b>
$2^{11}$	1	0	0	1	0	<b>1</b>
$2^{12}$	6	1	0	7	0	<b>7</b>
$2^{13}$	7	3	0	10	0	<b>10</b>
$2^{14}$	13	5	1	19	0	<b>19</b>
$2^{15}$	10	10	2	22	0	<b>22</b>
$2^{16}$	11	7	3	21	0	<b>21</b>
$2^{17}$	11	12	1	16	8	<b>24</b>
$2^{18}$	16	8	6	24	6	<b>30</b>
$2^{19}$	17	22	5	24	20	<b>44</b>
$2^{20}$	23	22	9	40	14	<b>54</b>
<b>Total:</b>	<b>117</b>	<b>90</b>	<b>27</b>	<b>186</b>	<b>48</b>	<b>234</b>

### 5.1.1 Computing $L$ -functions of 2-power conductor

One of the first approaches to classifying isogeny classes of abelian surfaces of conductor  $N$  is to note that the Hasse-Weil  $L$ -function of an abelian surface  $A/\mathbb{Q}$  is an arithmetically normalised degree 4 motive weight 1  $L$ -function of conductor  $N$ , as defined in 5.1. Using the above axioms, one can attempt to classify all possible  $L$ -functions with good Euler factors outside 2.

In order to do this, we follow the procedure done by Farmer-Koutsoliotas-Lemurell [166], where they generate  $L$ -functions purely from the assumption of its functional equation, without any prior knowledge of the coefficients. We note that similar methods for determining unknown Dirichlet coefficients  $a_n$  were also done by Booker [51] and Bian [39].

In summary, the procedure is as follows: We fix some small conductor  $N$  and

sign  $\varepsilon$  which is either  $+1$  or  $-1$ . We then consider an  $L$ -function

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

for some coefficients  $a_n \in \mathbb{Z}$  satisfying a Ramanujan bound  $a_n = \mathcal{O}(n^{1/2+\varepsilon})$ . By the results of Boxer–Gee–Calegari–Pilloni [66], we may also assume that the completed  $L$ -function

$$\Lambda(s) := N^{s/2} \Gamma_{\mathbb{C}}(s)^2 L(s)$$

satisfies the functional equation

$$\Lambda(s) = \varepsilon \Lambda(2-s).$$

Note that here we take the *arithmetic normalisation* convention for  $L(s)$ ; that is, the functional equation relates  $\Lambda(s)$  with  $\Lambda(2-s)$ . We remark that Farmer–Koutsoliotas–Lemurell [166] adopts the *analytic normalisation* convention for  $L(s)$ , as given in the axiomatic definition. This allows one to relate  $\Lambda(s)$  with  $\Lambda(1-s)$  at the cost of having non-rational coefficients  $a_n$ , although the method is essentially still the same.

At this stage, we form a system of linear inequalities, from which we hope to at least solve for the first few Dirichlet coefficients  $a_n$ . To do this, we shall use the following approximate functional equation:

**Theorem 5.5.** [371, p. 444] *Let  $L(s) = \sum a_n n^{-s}$  be a degree 4  $L$ -function as described above, with completed  $L$ -function  $\Lambda(s)$ , and assume that  $\Lambda(s)$  has analytic continuation to  $\mathbb{C}$ . Let  $g : \mathbb{C} \rightarrow \mathbb{C}$  be an entire function such that, for a fixed  $s$ , we have*

$$|\Lambda(z+s)g(z+s)z^{-1}| \rightarrow 0 \quad (5.3)$$

as  $|Im(z)| \rightarrow \infty$  in vertical strips where  $-x_0 \leq Re(z) \leq x_0$  for some  $x_0 \in \mathbb{R}_+$ . Also define  $Q := \sqrt{N}/\pi^2$ . Then for any  $s$  for which  $\Lambda(s)$  is well-defined, we have

$$\Lambda(s)g(s) = \sum_{n=1}^{\infty} a_n \left( \left( \frac{Q}{n} \right)^s f_1(s, n) + \varepsilon \left( \frac{Q}{n} \right)^{2-s} f_2(s, n) \right) \quad (5.4)$$

where  $f_1(s, n)$  and  $f_2(s, n)$  are defined to be

$$f_1(s, n) := \frac{1}{2\pi i} \int_{\nu-i\infty}^{\nu+i\infty} \Gamma_{\mathbb{C}}(s)^2 z^{-1} g(s+z) (Q/n)^z dz, \quad \text{and}$$

$$f_2(s, n) := \frac{1}{2\pi i} \int_{\nu-i\infty}^{\nu+i\infty} \Gamma_{\mathbb{C}}(2-s)^2 z^{-1} g(s-z) (Q/n)^z dz$$

such that  $\nu > \max(0, -\operatorname{Re}(s))$ .

*Proof sketch.* [371, p. 445] The result follows by the standard argument of computing a suitable contour integral and a straightforward application of Cauchy's Theorem. Choose some sufficiently large  $\alpha$  and  $T$ , and let  $C$  be the rectangle with vertices  $(-\alpha, -iT)$ ,  $(\alpha, -iT)$ ,  $(\alpha, iT)$ ,  $(-\alpha, iT)$ . Given any  $s \in \mathbb{C}$ , we evaluate the integral

$$\frac{1}{2\pi i} \int_C \Lambda(z+s)g(z+s)z^{-1}dz. \quad (5.5)$$

By Cauchy's theorem, (5.5) evaluates to  $\Lambda(s)g(s)$ . Also, we can directly compute the integral in (5.5) by individually computing the integral over each edge of the rectangle  $C$ :

$$\int_C = \int_{\alpha-iT}^{\alpha+iT} + \int_{\alpha+iT}^{-\alpha+iT} + \int_{-\alpha+iT}^{-\alpha-iT} + \int_{-\alpha-iT}^{\alpha-iT}.$$

The second and fourth integrals above go to 0 as  $T \rightarrow \infty$ , given condition (5.3). The first and third integrals together give the right hand side in (5.4) as  $T \rightarrow \infty$ , by applying the functional equation  $\Lambda(s) = \varepsilon \Lambda(2-s)$  and a standard computation. Further details of the calculations (for an analytic normalisation of  $\Lambda(s)$ ) are given in Rubinstein [371, p. 445–446].  $\square$

By thus using the approximate functional equation for various points  $s \in \mathbb{Z}$  and functions  $g$ , we can divide through by  $g(s)$  to yield several equations of the form

$$\Lambda(s) = c_{g,s,1}a_1 + c_{g,s,2}a_2 + \cdots + c_{g,s,i}a_i + \cdots$$

where  $c_{g,s,i}$  are explicitly calculated coefficients depending on the weight function  $g$  and the point  $s$ , given by

$$c_{g,s,n} := \frac{N^{s/2}f_1(s,n)}{n^s\pi^{2s}g(s)} + \varepsilon \frac{N^{1-s/2}f_2(s,n)}{n^{2-s}\pi^{4-2s}g(s)} \quad (5.6)$$

We can therefore generate an arbitrary number of these equations by simply choosing different points  $s \in \mathbb{Z}$  and functions  $g$ . By comparing two different weight functions  $g$  and  $h$  at the same point  $s$ , we obtain the following linear constraints on the Dirichlet coefficients  $a_1, a_2, \dots$ :

$$0 = (c_{g,s,1} - c_{h,s,1})a_1 + (c_{g,s,2} - c_{h,s,2})a_2 + \cdots$$

Whilst this is a single equation with infinitely many variables, by making a careful choice of  $g$  and  $h$  to be exponentially decaying, we can make this into an

effective constraint on the first few coefficients  $a_1, a_2, \dots, a_M$ .

By choosing the weight function  $g(s) = e^{cs}$  for various real values of  $c$  between  $-2$  and  $2$ , we obtain that the coefficients  $c_{g,s,i}$  decay exponentially. By then truncating the equation at  $M$  we obtain the following linear inequality giving an effective constraint:

$$|(c_{g,s,1} - c_{h,s,1})a_1 + \dots + (c_{g,s,M} - c_{h,s,M})a_M| < C_\epsilon \frac{M^{1/2+\epsilon}}{e^M} \quad (5.7)$$

where  $C$  is some effectively computable constant. By setting up a system of such linear inequalities, this allows us to rule out certain choices of the first few coefficients  $a_1, a_2, \dots, a_M$ , and thus allows us to effectively solve for the first few Dirichlet coefficients  $a_n$ .

This procedure is done by performing a breadth first search; for each prime  $p$  from 2 to 149, we try each of the possible Euler factors  $L_p(T)$ , whilst pruning the branches which yield no solutions. The idea is that this eventually whittles down the number of possible candidate  $L$ -functions to just a handful of candidate solutions for  $L(s)$ , at which stage we can do a brute force search for genus 2 curves  $C/\mathbb{Q}$  having the  $L$ -function  $L(s)$ .

For our purposes, we do this for all possible Euler factors  $L_p(T)$  for all primes  $p < 150$ . We can thus summarise the general algorithm as follows:

1. First generate a list of all bad Euler factors  $L_{2,i}$  for  $p = 2$ , and a list of all good Euler factors  $L_{p,i}$  for odd primes  $p < 150$ .
2. Choose a list of various points  $s$ , and weight functions  $g$ , and calculate the values  $c_{g,s,n}$  for sufficiently many  $n$ . This generates a system of equations for the Dirichlet coefficients  $a_n$  to satisfy.
3. Initialise a list of possible  $L$ -functions  $\mathcal{L}$  (where each element in  $\mathcal{L}$  consists of a tuple of Euler factors  $(L_{2,j_1}, L_{3,j_2}, \dots)$ ).
4. For each prime  $p$  from 2 to 149, do the following:
  - (a) For each candidate  $L$ -function  $L$  in  $\mathcal{L}$ , and for each Euler factor  $L_{p,i}$ , append  $L_{p,i}$  to  $L$ .
  - (b) Check if the tuple of Euler factors  $L$  is consistent with our system of equations.
  - (c) If so, update  $L$  to include  $L_{p,i}$ . Otherwise, if the system is not consistent for any Euler factor  $L_{p,i}$ , remove  $L$  from  $\mathcal{L}$ .

After doing the above breadth-first search, our hope is that either at some stage, no possible candidate  $L$ -functions are left, in which case we have proven that no  $L$ -function of conductor  $N$  exists. Or alternatively we are left with just a few candidate  $L$ -functions, from which for each one we can hopefully find an explicit abelian surface that gives the desired  $L$ -function.

First, we present an algorithm to compute all possible Euler factors at a prime  $p$ , with Algorithm 7 computing the good Euler factors and Algorithm 8 computing the bad Euler factors. We note that Sage can already list all possible good factors using the `WeilPolynomial` method, so it is only necessary for us to code-up in the case of bad reduction at  $p$ .

---

**Algorithm 7** Compute all possible rational degree  $2g$  good Euler factors at  $p$

---

```

1: procedure COMPUTEGOODEULERFACTORS( $g, p$ )
2:   Initialise a list  $\mathcal{L}_p := \{\}$  of possible Euler factors for  $p$ .
3:   for all  $a_1, \dots, a_g \in \mathbb{Z}$  such that  $|a_i| \leq \binom{2g}{i} p^{i/2}$  do
4:     Let  $F(T) := 1 + a_1 T + \dots + a_g T^g + p a_{g-1} T^{g+1} + \dots + p^g T^{2g}$ .
5:     IsValid := True
6:     for all roots  $\alpha_1, \dots, \alpha_{2g-1}$  of  $F(T)$  do
7:       if  $|\alpha_i| \neq \sqrt{p}$  then
8:         IsValid := False
9:       end if
10:    end for
11:    if IsValid then
12:      Add  $F(T)$  to  $\mathcal{L}_p$ .
13:    end if
14:  end for
15:  return A list of possible good degree  $2g$  Euler factors  $\mathcal{L}_p$  for the prime  $p$ .
16: end procedure

```

---

We can now give the breadth-first search algorithm as done by Farmer–Koutsoliotas–Lemurell [166] in Algorithm 9.

### 5.1.2 Results

We ran Algorithm 9 for conductors  $N = 2^a$  for powers  $a = 1, \dots, 10$ , and  $\varepsilon \in \{-1, +1\}$ , implemented with Sage [373] using complex ball arithmetic. This allowed us to rigorously compute the constant  $c_{g,s,n}$  to an arbitrary amount of precision and thus check unconditionally whether the inequalities hold for a choice of weights  $g, h$  and point  $s$ .

We verified Farmer–Koutsoliotas–Lemurell’s [166] results that no rational degree 4 motive weight 1  $L$ -functions of conductor  $N \leq 2^7$  exist, and that there exists



---

**Algorithm 8** Compute all possible rational degree  $2g$  bad Euler factors at  $p$ 


---

```

1: procedure COMPUTEBADEULERFACTORS( $g, p$ )
2:   Initialise a list  $\mathcal{L}_p := \{\}$  of possible Euler factors for  $p$ .
3:   for all  $a_1, \dots, a_{2g-1} \in \mathbb{Z}$  such that  $|a_i| \leq \binom{2g}{i} p^{i/2}$  do
4:     Let  $F(T) := 1 + a_1 T + \dots + a_{2g-1} T^{2g-1}$ .
5:     IsValid := True
6:     for all roots  $\alpha_1, \dots, \alpha_{2g-1}$  of  $F(T)$  do
7:       if  $2 \log |\alpha_i| / \log p$  not in  $\mathbb{N}$  then
8:         IsValid := False
9:       end if
10:    end for
11:    if IsValid then
12:      Add  $F(T)$  to  $\mathcal{L}_p$ .
13:    end if
14:  end for
15:  return A list of possible bad degree  $2g$  Euler factors  $\mathcal{L}_p$  for the prime  $p$ .
16: end procedure

```

---

exactly one such  $L$ -function of conductor  $N = 2^8$ , corresponding to the square of the elliptic curve isogeny class [4.4.2048.1-1.1-a](#).

We furthermore obtained that no such  $L$ -function exists with conductor  $2^9$ , yielding a small extension to their results. However, without imposing any further constraints or optimisations, the above algorithm as is tends to break down beyond conductor  $N \approx 600$ . As an example, for conductor  $N = 2^{10}$  and sign  $\varepsilon = +1$ , even if we assume the first Euler factor  $L_2(T)$  is 1, after searching through the first four odd primes, no pruning occurs and all  $63 \cdot 129 \cdot 207 \cdot 401 = 674\,597\,889$  branches are still possible, which makes the breadth first search quickly become unbearably slow.

Whilst Algorithm 9 is in principle effective for any conductor  $N$ , to extend these results further in a practical way, one needs to either optimise the above algorithm, e.g. by choosing better weight functions  $g(s)$ , or otherwise impose additional constraints on these possible Dirichlet coefficients  $a_n$ .

### 5.1.3 Further constraining the Jacobian 2-torsion

Whilst we were unable to unconditionally prove that there is only one conductor  $2^{10}$  rational  $L$ -function of degree 4, we can get a partial result by assuming some conditions on the Euler factors  $L_p(T)$ .

We first show that, for every prime  $p$  of good reduction, we have that  $\# \text{Jac}(C)(\mathbb{Q})[2]$  divides both  $L_p(1)$  and  $L_p(-1)$ .

---

**Algorithm 9** A breadth-first search algorithm to compute all possible tuples of the first few Dirichlet coefficients  $(a_1, a_2, \dots, a_{p_k})$  of a rational degree 4 motivic weight 1  $L$ -function of conductor  $N$  and sign  $\varepsilon$ .

---

```

1: procedure COMPUTELFUNCTION( $N, \varepsilon$ )
2:   for  $k$  from 1 to 60 do
3:     Initialise a list  $\mathcal{L}_{p_k}$  of all possible degree 4 Euler factors for  $p_k$ .
4:   end for
5:   Initialise a list  $\mathcal{S}_0 := [1]$  of (partial)  $L$ -functions
6:   Initialise a list of candidate weight functions  $\mathcal{G} := \{e^{-2s}, e^{-3s/2}, e^{-s}, e^{-s/2},$ 
    $e^{s/2}, e^s, e^{3s/2}, e^{2s}\}$ .
7:   for  $k$  from 1 to 60 do
8:     Initialise a list  $\mathcal{S}_k := \{\}$  of valid tuples of the first  $k$  Euler factors.
9:     for  $L'$  in  $\mathcal{S}_{k-1}$  do
10:      for  $F_{p_k}$  in  $\mathcal{L}_{p_k}$  do
11:        Define  $L := L' \cdot F_{p_k}$ 
12:        Compute the Dirichlet coefficients  $a_1, a_2, \dots, a_{p_k}$  of  $L$ .
13:        IsValid := True
14:        for  $s$  in  $[1+i, 1+2i, 1+3i]$  do
15:          for  $(g, h)$  in  $\mathcal{G} \times \mathcal{G}$  do
16:            Compute  $c_{g,s,i} - c_{h,s,i}$  for all  $i = 1, 2, \dots, p_k$  given in (5.6)
17:            if Dirichlet coefficients  $a_1, a_2, \dots, a_{p_k}$  don't satisfy inequality (5.7) then
18:              IsValid := False
19:            end if
20:          end for
21:        end for
22:        if IsValid then
23:          Add  $L$  to  $\mathcal{S}_k$ .
24:        end if
25:      end for
26:    end for
27:  end for
28:  return A list  $\mathcal{S}_{60}$  of (possibly empty) partial candidate  $L$ -functions.
29: end procedure

```

---

**Proposition 5.6.** *Let  $A/\mathbb{Q}$  be an abelian surface with good reduction away from 2. Then for every odd prime  $p$ ,  $\#A(\mathbb{Q})[2]$  divides both  $L_p(1)$  and  $L_p(-1)$ .*

*Proof.* We first recall that, for an abelian variety  $A/\mathbb{Q}$  with good reduction at  $p$ , we have  $\#A(\mathbb{F}_p) = L_p(1)$  (e.g. see [18, p. 203] or [294, Corollary 8.6.3]). We also note that the torsion subgroup  $A(\mathbb{Q})_{\text{tors}}$  injects into  $A(\mathbb{F}_p)$  for a prime  $p$  of good reduction (e.g. see [255, p. 502]). Thus, we have that the number of rational 2-torsion points  $\#A(\mathbb{Q})[2]$  divides  $\#A(\mathbb{F}_p) = L_p(1)$ .

Now, we consider a non-trivial quadratic twist of  $A^\chi/\mathbb{F}_p$  of  $A/\mathbb{F}_p$ .<sup>4</sup> We note that one has a Galois equivariant isomorphism  $A[2] \xrightarrow{\sim} A^\chi[2]$  (e.g. see [322, p. 854]), and also note that the local Euler factor of  $A^\chi/\mathbb{F}_p$  is  $L_p(-T)$ . Together this implies that  $\#A(\mathbb{Q})[2]$  divides  $\#A^\chi(\mathbb{F}_p) = L_p(-1)$  and thus proves the proposition.  $\square$

Therefore, if we introduce a lower bound on the number of rational 2-torsion points that such an abelian surface  $A/\mathbb{Q}$  has, then Proposition 5.6 allows us to reduce the number of possible Euler factors  $L_p(T)$  we have to consider for primes  $p$  of good reduction.

Table 5.2: Number of Euler factors  $L_p(T)$  such that both  $L_p(1)$  and  $L_p(-1)$  are divisible by  $\#\text{Jac}(C)(\mathbb{Q})[2]$

$\#\text{Jac}(C)(\mathbb{Q})[2]$	3	5	7	11	13	17	19	23	29	31
16	1	4	14	17	12	15	33	82	32	122
8	6	11	28	54	37	53	118	156	113	240
4	18	36	58	108	134	198	232	308	430	474
2	33	67	107	205	259	387	453	603	847	937
1	63	129	207	401	513	765	897	1193	1683	1861

Using this condition, if one assumes that 8 divides  $\#\text{Jac}(C)(\mathbb{Q})[2]$ , then the number of possible Euler factors for  $L_p(T)$  for odd primes  $p$  goes down to 6, 11, 28, 54,  $\dots$ . This significantly speeds up the breadth first search.

We can go one step further. We can furthermore use the fact that  $L_p(T)$  is the characteristic polynomial of a matrix  $M_p$  in  $\text{GL}_4(\mathbb{Z}_2)$  such that  $M_p$  fixes at least 8 points over  $\mathbb{F}_2$ . As shown in Table 5.3 we can apply the condition that  $M_p$  fixes 8 points over  $\mathbb{F}_2$  to further constrain the possibilities for  $L_p(T)$ .

We can now run Algorithm 9 again, but with a single change in line 3; this time initialising  $\mathcal{L}_p$  to only be the Euler factors  $L_p(T)$  allowed by the above constraints. By therefore repeating the breath first search using these fewer number of possible Euler factors as constrained by the above table, this allows us to prove the following theorem for conductor  $2^{10}$ :

**Theorem 5.7.** *Assuming the paramodular conjecture, there is exactly one  $\mathbb{Q}$ -isogeny class of abelian surfaces of conductor  $2^{10}$  which contain at least one abelian surface  $A/\mathbb{Q}$  satisfying  $\#A(\mathbb{Q})[2] \geq 8$ ; in particular this is the isogeny class of the  $\mathbb{Q}$ -split abelian surface  $E \times E$ , where  $E$  is the conductor  $2^5$  elliptic curve  $y^2 = x^3 - x$ .*

<sup>4</sup>To illustrate an example, if  $A$  is the Jacobian of the hyperelliptic curve  $y^2 = f(x)$ , then one can take  $A^\chi$  as the Jacobian of  $y^2 = df(x)$  where  $d$  is some quadratic non-residue mod  $p$ .

Table 5.3: For each odd prime  $p \leq 31$ , we tabulate the number of possible degree 4 Euler factors  $L_p(T)$  of good reduction which are the characteristic polynomial of some matrix  $M \in \mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$  such that  $M$  fixes at least 8 points (mod 2).

Prime $p$	$\mathrm{GL}_4(\mathbb{Z}/2\mathbb{Z})$	$\mathrm{GL}_4(\mathbb{Z}/4\mathbb{Z})$	$\mathrm{GL}_4(\mathbb{Z}/8\mathbb{Z})$	$\mathrm{GL}_4(\mathbb{Z}/16\mathbb{Z})$	$\mathrm{GL}_4(\mathbb{Z}/32\mathbb{Z})$
<b>3</b>	17	10	4	4	4
<b>5</b>	35	20	11	11	11
<b>7</b>	53	30	16	16	16
<b>11</b>	103	56	28	28	28
<b>13</b>	129	68	37	37	37
<b>17</b>	195	102	53	53	53
<b>19</b>	227	118	62	62	62
<b>23</b>	301	156	80	80	80
<b>29</b>	425	218	113	113	113
<b>31</b>	467	240	122	122	122

## 5.2 Computing genus 2 curves with good reduction outside $S$ .

In this section, we now aim to explicitly compute all genus 2 curves  $C/\mathbb{Q}$  whose Jacobians have good reduction away from 2 and such that  $C$  has good reduction away from some fixed small finite set of primes  $S$ . Throughout this section, we'll assume that  $2 \in S$ . We note that such a list must contain all 366  $\mathbb{Q}$ -isomorphism classes of genus 2 curves with good reduction outside 2, given by Smart [418].

We'll first recall the effective approach taken by Evertse–Győry, as sketched in Chapter 2. Let  $C/\mathbb{Q} : y^2 = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_6)$  be a genus 2 curve whose Jacobian has good reduction away from 2 and such that  $C$  has good reduction away from  $S$ . We can effectively compute the possible roots  $\alpha_1, \dots, \alpha_6$  as follows:

1. Classify all possible 2-torsion fields  $\mathbb{Q}(J[2])$  by computing number fields of degree  $\leq 6$  unramified away from 2 (e.g. using a Hunter search [109, p. 445]).
2. For each possible 2-torsion field  $L = \mathbb{Q}(J[2])$ , compute the set of  $S$ -units  $x, y \in \mathcal{O}_{L,S}^\times$  such that  $x + y = 1$  (e.g. using the methods of von Känel and Matschke [471]).
3. For every combination of a triple of  $S$ -units  $(\lambda_1, \lambda_2, \lambda_3)$  and the possible discriminant  $\Delta$ , use either the Evertse–Győry identity (2.1) or Smart's identity (2.2) to compute the possible values of  $\alpha_i - \alpha_j$ .
4. For each  $\beta \in \mathbb{Z}/6\mathbb{Z}$ , add the constraint  $\alpha_1 + \cdots + \alpha_6 = \beta$  and then solve for

the roots  $\alpha_1, \dots, \alpha_6$  using (2.3).

Whilst this does give a fully effective algorithm to compute all possible genus 2 curves  $C/\mathbb{Q}$  whose Jacobian is good outside 2 and such that  $C$  is good outside  $S$ , the above algorithm is not very practical once  $S$  gets sufficiently large. Indeed, even in the simplest case of  $S = \{2\}$ , Smart [418] needed to employ further optimisations to compute his list of 366 genus 2 curves  $C/\mathbb{Q}$  good away from 2. In particular, the vast majority of the possible triples of  $S$ -units  $(\lambda_1, \lambda_2, \lambda_3)$  in step 3 above get thrown out as they either do not yield a genus 2 curve  $C$  defined over  $\mathbb{Q}$  or give a model for which the Jacobian has bad reduction at some odd prime  $p$ .

In order to therefore present an algorithm which is practical for our purposes, we employ a combination of some further optimisations both from Smart [418] and our own to solve this problem for larger sets  $S$ .

A summary of our approach for this section is as follows: As before, let  $C/\mathbb{Q} : y^2 = c(x - \alpha_1) \cdots (x - \alpha_6)$  be a genus 2 curve whose Jacobian has good reduction away from 2 and  $C$  has good reduction away from  $S$ .

1. As before, classify all possible 2-torsion fields  $\mathbb{Q}(J[2])$  by computing number fields of degree  $\leq 6$  unramified away from 2.
2. For each possible field  $L = \mathbb{Q}(J[2])$ , let  $\psi_1, \psi_2, \dots, \psi_t \in \mathcal{O}_{L,S}^\times$  be a generating set for the group of  $S$ -units in  $L$ .
3. For each pair  $1 \leq i < j \leq 6$  and  $1 \leq k \leq t$ , let  $a_{i,j,k} \in \mathbb{Z}$  be given by  $\alpha_i - \alpha_j = \psi_1^{a_{1,i,j}} \psi_2^{a_{2,i,j}} \cdots \psi_t^{a_{t,i,j}}$ .
4. Impose as many linear constraints on the variables  $a_{k,i,j}$  as we can, e.g. using Galois symmetries, cluster pictures for odd primes  $p$ , solutions to  $S$ -unit equations etc.
5. Solve the resulting linear system (e.g. via brute force, closest vector problem, integer programming, etc.) to obtain a possible solution for  $a_{k,i,j}$  and thus for  $\alpha_i - \alpha_j$ .

For the remainder of this section, we shall go through each of the steps above, concluding with an implementation to solve for  $a_{i,j,k}$  using both the closest vector method and an integer programming method.

The first step is to compute all number fields of small degree unramified away from 2.

### 5.2.1 Number fields unramified away from 2

Let  $C/\mathbb{Q}$  be a genus 2 curve whose Jacobian  $\text{Jac}(C)$  has good reduction outside 2. Then if  $\mathcal{R}$  denotes the Weierstrass points of  $C$ , then by Theorem 1.11, we have that  $\mathbb{Q}(\mathcal{R})/\mathbb{Q}$  is unramified outside 2. Thus, our first task is to classify all such number fields  $\mathbb{Q}(\mathcal{R})$ .

Fortunately, this has already been well-studied for small degrees. By using an algorithm of Pohst [350] to classify number fields of small discriminant, Merriman-Smart [314] gave the following classification:

**Theorem 5.8.** [314, Proposition 1] *Let  $K$  be a number field with  $[K : \mathbb{Q}] \leq 6$  and  $K/\mathbb{Q}$  unramified outside 2. Then  $[K : \mathbb{Q}] \in \{1, 2, 4\}$ , and the 11 possibilities for  $K$  (up to Galois conjugation) are:<sup>5</sup>*

$$\begin{aligned} & \mathbb{Q} \quad \text{if } [K : \mathbb{Q}] = 1 \\ & \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \quad \text{if } [K : \mathbb{Q}] = 2 \\ & \mathbb{Q}(\sqrt[4]{-1}), \mathbb{Q}(\sqrt{1 + \sqrt{-1}}), \mathbb{Q}(\sqrt{1 + \sqrt{2}}), \\ & \mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt[4]{-2}), \mathbb{Q}(\sqrt{-2 - \sqrt{2}}), \mathbb{Q}(\sqrt{2 + \sqrt{2}}), \quad \text{if } [K : \mathbb{Q}] = 4 \end{aligned}$$

Therefore, if  $\alpha$  is a Weierstrass point of  $C$ , then  $\mathbb{Q}(\alpha)$  must be one of the above extensions, and thus  $\mathbb{Q}(\mathcal{R})$  is some compositum of the above fields of degree no more than 8.<sup>6</sup>

For brevity, we shall adopt the same notation as Smart [418, p. 290] for number fields unramified away from 2. That is, we let  $K_1, K_2, K_3$  denote the three quadratic fields  $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2})$  respectively, and  $L_1, L_2, \dots, L_7$  denote the seven quartic fields  $\mathbb{Q}(\sqrt[4]{-1}), \mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt[4]{-2}), \mathbb{Q}(\sqrt{2 + \sqrt{2}}), \mathbb{Q}(\sqrt{-2 - \sqrt{2}}), \mathbb{Q}(\sqrt{1 + \sqrt{2}}), \mathbb{Q}(\sqrt{1 + \sqrt{-1}})$  respectively. We summarise these fields below in Table 5.4.

From a technical standpoint, it's perhaps also worth noting that all possible extensions  $\mathbb{Q}(\mathcal{R})$  will have class number 1 in the case of genus 2 curves  $C/\mathbb{Q}$  whose Jacobian has good reduction away from 2, however this need not be true in the general case.

We now introduce the notion of field system for a hyperelliptic curve  $C$ .

<sup>5</sup>We remark that the quartic number field  $\mathbb{Q}(i, \sqrt{2})$  (i.e. the compositum of the quadratic number fields unramified away from 2) is the same as  $L_1 = \mathbb{Q}(\sqrt[4]{-1})$ .

<sup>6</sup>At this stage, it would be reasonable to conjecture that any number field  $K$  unramified outside 2 has degree a power of 2. Whilst this is true if  $[K : \mathbb{Q}] \leq 16$ , remarkably there is a degree 17 field unramified outside 2 which gives a counterexample to this conjecture, found by Harbater [215, p. 57] (e.g. see the OEIS sequence A368056).

Table 5.4: Summary of the number fields of degree at most 6 unramified away from 2

Label	Field	LMFDB	Defining polynomial	Galois group
$K_1$	$\mathbb{Q}(\sqrt{-1})$	<a href="#">2.0.4.1</a>	$x^2 + 1$	$C_2$
$K_2$	$\mathbb{Q}(\sqrt{-2})$	<a href="#">2.0.8.1</a>	$x^2 + 2$	$C_2$
$K_3$	$\mathbb{Q}(\sqrt{2})$	<a href="#">2.2.8.1</a>	$x^2 - 2$	$C_2$
$L_1$	$\mathbb{Q}(\sqrt[4]{-1})$	<a href="#">4.0.256.1</a>	$x^4 + 1$	$C_2 \times C_2$
$L_2$	$\mathbb{Q}(\sqrt[4]{2})$	<a href="#">4.2.2048.1</a>	$x^4 - 2$	$D_4$
$L_3$	$\mathbb{Q}(\sqrt[4]{-2})$	<a href="#">4.0.2048.1</a>	$x^4 + 2$	$D_4$
$L_4$	$\mathbb{Q}(\sqrt{2 + \sqrt{2}})$	<a href="#">4.4.2048.1</a>	$x^4 - 4x^2 + 2$	$C_4$
$L_5$	$\mathbb{Q}(\sqrt{-2 - \sqrt{2}})$	<a href="#">4.0.2048.2</a>	$x^4 + 4x^2 + 2$	$C_4$
$L_6$	$\mathbb{Q}(\sqrt{1 + \sqrt{2}})$	<a href="#">4.2.1024.1</a>	$x^4 - 2x^2 - 1$	$D_4$
$L_7$	$\mathbb{Q}(\sqrt{1 + \sqrt{-1}})$	<a href="#">4.0.512.1</a>	$x^4 - 2x^2 + 2$	$D_4$

**Definition 5.8.** [[418](#), p. 273] Let  $C/K$  be a genus  $g$  hyperelliptic curve, and let  $y^2 = f(x)$  be a simplified model for  $C$  where  $\deg(f) = 2g + 2$ . Let  $f(x)$  factor over  $K$  as

$$f(x) = cf_1(x)f_2(x) \cdots f_m(x)$$

where  $f_i(x)$  are irreducible polynomials over  $K$ . Let  $M_i$  be the root field of  $f_i$ ; i.e. the field  $K(\alpha_i)$  where  $f_i(\alpha_i) = 0$ . The tuple of fields  $(M_1, M_2, \dots, M_m)$  is the **field system** for  $C/K$ .

As any  $K$ -isomorphism between two hyperelliptic curves is given by a fractional linear transformation, it's easy to see that field systems are invariant (up to ordering) under  $K$ -isomorphism [[418](#), p. 273].

From Theorem [5.8](#), it's not hard to observe that there are only a finite number of possible field systems for genus 2 curves  $C$  where  $\text{Jac}(C)$  has good reduction outside 2. A summary of the types of fields systems are given in Table [5.5](#) with a full list of all 48 possible field systems given in Table [A.1](#) in the appendix. We can also use Theorem [1.8](#) to deduce the number of rational 2-torsion points on  $\text{Jac}(C)$  from the field system of  $C$ .

### 5.2.2 Solving the $S$ -unit equations

We now focus on solving the  $S$ -unit equation  $x + y = 1$  for  $S$ -units  $x, y \in \mathcal{O}_{L,S}^\times$  over the possible 2-torsion fields  $L = \mathbb{Q}(J[2])$ , following the procedure laid out by Smart

Table 5.5: List of possible types of field systems for genus 2 curves  $C : y^2 = f(x)$  with  $\mathbb{Q}(\mathcal{R})$  unramified outside 2. Here  $K_*$  (resp.  $L_*$ ) denotes an arbitrary number field of degree 2 (resp. 4) unramified away from 2. The number of rational 2-torsion points on  $\text{Jac}(C)$  corresponding to each field system is also tabulated.

Field system	$\# \text{Jac}(C)[2](\mathbb{Q})$
$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}]$	16
$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_i]$	8
$[\mathbb{Q}, \mathbb{Q}, K_i, K_j]$	4
$[\mathbb{Q}, \mathbb{Q}, L_i]$	2
$[K_i, K_j, K_k]$	4
$[K_i, L_j]$	2

[418, Section 8].

From the list of possible field systems for  $C$ , we note that  $\mathbb{Q}(\mathcal{R})$  is a subfield of one of the three following Galois octic fields, as shown in Table 5.6.

Table 5.6: Summary of the three possible octic fields which contain  $\mathbb{Q}(\mathcal{R})$ .

Label	Field	LMFDB	Defining polynomial	Galois group
$M_1$	$\mathbb{Q}(\sqrt[8]{-1})$	<a href="#">8.0.16777216.1</a>	$x^8 + 1$	$C_4 \times C_2$
$M_2$	$\mathbb{Q}(\zeta_8, \sqrt[4]{2})$	<a href="#">8.0.16777216.2</a>	$x^8 - 4x^6 + 8x^4 - 4x^2 + 1$	$D_4$
$M_3$	$\mathbb{Q}(\sqrt[4]{2\sqrt{2}-3})$	<a href="#">8.0.4194304.1</a>	$x^8 + 6x^4 + 1$	$D_4$

For future reference, we remark that all four fields  $K_1, K_2, K_3, L_1$  lie in the three fields  $M_1, M_2, M_3$ . Furthermore, the field  $M_1$  also contains  $L_4$  and  $L_5$ ; the field  $M_2$  contains  $L_2$  and  $L_3$ , and the field  $M_3$  contains  $L_6$  and  $L_7$ .

Our primary goal is to solve the  $S$ -unit equation  $\tau_1 + \tau_2 = 1$  in the three above fields for  $S$  being the primes above  $\{2, 3\}$ ,  $\{2, 5\}$  and  $\{2, 7\}$ . Matschke [307] very kindly ran these computations and provided all  $S$ -unit solutions, described below:

1. We first consider the octic field  $M_1$ . Solving the  $S$ -unit equation

$$\tau_1 + \tau_2 = 1$$

for  $\tau_1, \tau_2$   $S$ -units where  $S$  denotes all primes in  $\mathcal{O}_{M_1}$  above  $\{2, 3\}$ ,  $\{2, 5\}$  and  $\{2, 7\}$ , yields a total of 2019, 1155, and 7881 solutions respectively.

2. For the octic field  $M_2$ , the number of solutions to the  $S$ -unit equation  $\tau_1 + \tau_2 = 1$



where  $S$  denotes all primes in  $\mathcal{O}_{M_2}$  above  $\{2, 3\}$ ,  $\{2, 5\}$  and  $\{2, 7\}$ , yields a total of 59 595, 807, 7197 respectively.

3. Finally, for the octic field  $M_3$ , the number of solutions obtained was 3723, 33 387, and 18 501 respectively.

The  $S$ -unit equation  $\tau_1 + \tau_2 = 1$  was also solved for  $S$  being just the primes above 2, for each of the above octic fields. We note that the number of solutions obtained agreed with the totals given by Smart [418, Sec. 8].

We note that the times taken to run these solutions varied from just a few minutes to several weeks. To see how far we could extend these result, Matschke furthermore computed the above  $S$ -unit equations for various other subsets of  $\{2, 3, 5, 7\}$  of size 3. A summary of these  $S$ -unit solutions is given in Table 5.7.

Table 5.7: Number of  $S$ -unit solutions to  $\tau_1 + \tau_2 = 1$  where  $\tau_i \in \mathcal{O}_S^\times$  over the field  $K$ . All computations were run by Matschke [307]. For each  $S$ -unit equation, the total CPU time in seconds (rounded to the nearest second) is also given.

Field	Set $S =$ all primes above:						
	$\{2\}$	$\{2, 3\}$	$\{2, 5\}$	$\{2, 7\}$	$\{2, 3, 5\}$	$\{2, 3, 7\}$	$\{2, 5, 7\}$
$M_1$	795	2019	1155	7881	4653	21 927	13 401
	(81s)	(453s)	(355s)	(8822s)	(4925s)	(769 586s)	(388 501s)
$M_2$	459	59 595	807	7197	?	?	11 877
	(62s)	(54 061s)	(304s)	(8528s)			(380 463s)
$M_3$	1335	3723	33 387	18 501	?	52 563	?
	(88s)	(766s)	(37 920s)	(18 853s)		(1 986 021s)	

We note that, even in the case where  $|S| = 3$ , some of the above  $S$ -unit solutions were not able to be computed in a reasonable time-frame. Furthermore, one also obtains a large amount of variability between different fields with the same rational primes below  $S$ , due to the fact that different rational primes will have different splitting behaviour over differing fields, thus changing the rank of  $S$ , and therefore affecting the CPU time.

Therefore, to obtain results in these cases and furthermore when  $|S| > 3$ , we need to employ some further optimisations. We shall give an overview of several strategies: (i) using Galois symmetries, (ii) using cluster pictures, (iii) rephrasing in terms of the closest vector problem, and (iv) using integer linear programming. The first optimisation was used by Smart to practically obtain all 366 genus 2 curves with good reduction away from 2, however we are not aware of the latter three strategies being used yet to classify genus 2 curves.

### 5.2.3 $S$ -unit Galois constraints

To speed up the computation of our  $S$ -unit solutions  $\tau_1 + \tau_2 = 1$ , we now consider making essential use of the fact that  $\tau_1, \tau_2$  arise from roots from polynomials, which are in one of the fields listed in Theorem 5.8.

To illustrate this idea, consider the example where we have a curve  $C : y^2 = f(x)$ , where the roots of  $f(x)$  are given by  $f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_6)$ . As shown on page 18, we can write  $f(x)$  in Rosenhain normal form as  $x(x - 1)(x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$  where

$$\lambda_1 = \frac{(\alpha_3 - \alpha_2)(\alpha_4 - \alpha_1)}{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_4)}, \quad \lambda_2 = \frac{(\alpha_3 - \alpha_2)(\alpha_5 - \alpha_1)}{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_5)}, \quad \lambda_3 = \frac{(\alpha_3 - \alpha_2)(\alpha_6 - \alpha_1)}{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_6)}$$

Now, assume that four of the roots  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  of  $f(x)$  arise from one of the fields  $L_i$  given in Theorem 5.8. Let  $\sigma \in \text{Gal}(L_i/\mathbb{Q})$  be an automorphism of order 4 which permutes the roots in the order  $\alpha_1 \mapsto \alpha_3 \mapsto \alpha_2 \mapsto \alpha_4 \mapsto \alpha_1$ . Then we have

$$\sigma(\lambda_1) = \frac{(\sigma(\alpha_3) - \sigma(\alpha_2))(\sigma(\alpha_4) - \sigma(\alpha_1))}{(\sigma(\alpha_2) - \sigma(\alpha_1))(\sigma(\alpha_3) - \sigma(\alpha_4))} = \frac{(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_1)}{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_4)} = 1 - \lambda_1$$

This therefore yields the constraint that  $\sigma(\lambda_1) = 1 - \lambda_1$ , which heavily constrains the number of  $S$ -unit solutions. In general, by a standard computation, one can show that, for any permutation  $\sigma \in S_4$  of the roots  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ , then  $\sigma(\lambda_1)$  will be one of the six values

$$\lambda_1, \quad 1 - \lambda_1, \quad \frac{1}{\lambda_1}, \quad \frac{1}{1 - \lambda_1}, \quad \frac{\lambda_1 - 1}{\lambda_1}, \quad \frac{\lambda_1}{\lambda_1 - 1}$$

depending on the choice of  $\sigma \in \text{Gal}(L_i/\mathbb{Q})$ . This is summarised in Table 5.8.

We note that there are faster algorithms (e.g. see Smart [417]) to solve  $S$ -unit equations of the form

$$\tau + \sigma(\tau) = 1$$

These are called *simple  $S$ -unit equations* [418, p. 278], and we can therefore solve the equation  $\tau + \sigma(\tau) = 1$  for  $S$ -units  $\tau \in \mathcal{O}_{L,S}^\times$  for larger sets  $S$  than shown in Table 5.7.

Recall from Table 5.4 that the Galois group  $\text{Gal}(M/\mathbb{Q})$  for  $M$  being any of the three quadratic fields  $K_1, K_2, K_3$  is simply  $C_2$ . Furthermore, the Galois group for the Galois quartic fields are  $\text{Gal}(L_1/\mathbb{Q}) = C_2^2$ , and  $\text{Gal}(L_i/\mathbb{Q}) = C_4$  for  $i = 4, 5$ . Note that the quartic fields  $L_2, L_3, L_5, L_6$  are not Galois but do have automorphism group  $\text{Aut}(L_i/\mathbb{Q}) = C_2$  (where  $C_n$  denotes the cyclic group of order  $n$ ).

Therefore, with the exception of the quartic field  $L_1$ , for all others  $M$  listed in Table 5.4, we have the existence of a unique order 2 automorphism  $\sigma \in \text{Aut}(M/\mathbb{Q})$ ,

Table 5.8: Summary of all possible values of  $\sigma(\lambda)$  for the cross ratio  $\lambda = (\alpha_i - \alpha_j)(\alpha_k - \alpha_\ell)/((\alpha_i - \alpha_k)(\alpha_j - \alpha_\ell))$  for all 24 possible permutations  $\sigma \in S_4$

Permutation $\sigma$	Cross-ratio $\frac{(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})(\alpha_{\sigma(k)} - \alpha_{\sigma(\ell)})}{(\alpha_{\sigma(i)} - \alpha_{\sigma(k)})(\alpha_{\sigma(j)} - \alpha_{\sigma(\ell)})}$
id, $(i j)(k \ell)$ , $(i k)(j \ell)$ , $(i \ell)(j k)$	$\lambda$
$(k \ell)$ , $(i k)$ , $(i j k \ell)$ , $(i \ell k j)$	$1 - \lambda$
$(j k)$ , $(i, \ell)$ , $(i j \ell k)$ , $(i k \ell j)$	$\frac{1}{\lambda}$
$(j k \ell)$ , $(i j \ell)$ , $(i k j)$ , $(i \ell k)$	$\frac{1}{1 - \lambda}$
$(j \ell k)$ , $(i j k)$ , $(i k \ell)$ , $(i \ell j)$	$\frac{\lambda - 1}{\lambda}$
$(k \ell)$ , $(i j)$ , $(i k j \ell)$ , $(i \ell j k)$	$\frac{\lambda}{\lambda - 1}$

noting that  $\text{Gal}(L_1/\mathbb{Q})$  contains three such order 2 automorphisms. With the above Galois constraints in mind, we therefore aim to solve  $\tau_1 + \tau_2 = 1$  such that  $\sigma(\tau_1) = 1 - \tau_1$  for some order 2 automorphism  $\sigma$ . A summary of the computations, all run by Matschke [307], are given in Table 5.9.

#### 5.2.4 Equivalence classes of polynomials

Once we've solved the  $S$ -unit solutions, recall that our aim is to solve for the roots  $\alpha_1, \dots, \alpha_6$  of  $f(x)$ . Unlike  $S$ -unit solutions to  $x + y = 1$ , if we impose no further constraints, we note that we will obtain infinitely many possibilities for the roots  $\alpha_i$ , as by applying any fractional linear transformation  $x \mapsto \frac{ax+b}{cx+d}$  to  $f(x)$ , one will obtain infinitely many models  $y^2 = f(x)$  for a given  $\mathbb{Q}$ -isomorphism class of genus 2 curves  $C/\mathbb{Q}$ . We must therefore introduce the notion of equivalence classes of polynomials.

**Definition 5.9.** Let  $f(x), g(x) \in \mathcal{O}_S[x]$ . We'll say that  $f$  and  $g$  are **weakly equivalent** if there exist  $a, b, c, d \in \mathcal{O}_S$  and  $\lambda \in \mathbb{Q}^\times$  such that  $ad - bc = 1$  and  $g(x) = \lambda(cx + d)^{\deg(f)} f((ax + b)/(cx + d))$ . We'll say that  $f(x), g(x)$  are **equivalent** if such a choice exists where  $ad - bc \neq 0$  and  $\lambda \in \mathcal{O}_S^\times$ .

It was shown by Birch and Merriman [45] that there are only finitely many equivalence classes of polynomials of given degree  $n$  and discriminant  $\Delta$ , with effective results given by Evertse and Györy [160].

Table 5.9: The number of  $S$ -unit solutions to  $\tau_1 + \tau_2 = 1$  where  $\tau_i \in \mathcal{O}_S^\times$  such that  $\sigma(\tau_1) = 1 - \tau_1$  for an order 2 automorphism  $\sigma \in \text{Gal}(M/\mathbb{Q})$ , and where  $S$  denotes all primes in  $M$  above the first  $N$  rational primes. All computations were run by Matschke [307]. Note that  $\sigma$  is uniquely determined in almost all cases, except for  $M = L_1$  for which the number of solutions are given for the automorphisms  $\sigma_1 : \zeta_8 \mapsto -\zeta_8$ ,  $\sigma_2 : \zeta_8 \mapsto -\zeta_8^3$ , and  $\sigma_3 : \zeta_8 \mapsto \zeta_8^3$  respectively.

Field $M$	$N$							
	1	2	3	4	5	6	7	8
$K_1$	9	9	75	93	105	441	1455	1731
$K_2$	3	45	57	69	321	375	1293	3831
$K_3$	21	33	39	213	279	333	1119	1311
$L_1$	75	225	351	825	1479	.	.	.
	21	99	249	471	999	.	.	.
	51	99	255	615	981	.	.	.
$L_2$	33	111	123	843	1539	.	.	.
$L_3$	9	147	159	351	1797	.	.	.
$L_4$	99	123	135	243	243	.	.	.
$L_5$	3	3	3	279	279	.	.	.
$L_6$	39	45	129	879	927	.	.	.
$L_7$	27	27	243	447	483	.	.	.

The following lemma is essentially a small modification of a result of Smart [418, Lemma 2].

**Lemma 5.9.** *Fix a number field  $K$ , a positive integer  $n \geq 3$  and a finite set of primes  $S$  of  $K$ . Let  $f(x) = c(x - \beta_1) \cdots (x - \beta_n) \in \mathcal{O}_S[x]$  be a degree  $n$  polynomial over  $K$  and assume that  $\Delta_f \in \mathcal{O}_S^\times$ . Then  $f(x)$  is equivalent to a form  $g(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ , such that the values  $\Omega_i := \prod_{i \neq k} (\alpha_i - \alpha_k)$  come from an effectively computable finite set (depending only on  $K, n, S$ ).*

*Proof.* Let  $M$  be a splitting field for  $f$ , and let  $\Lambda_i := \prod_{i \neq k} (\beta_i - \beta_k)$ . By scaling  $x$ , we may assume  $\beta_i$  are integral in  $M$ , and thus  $\Lambda_i \in \mathcal{O}_{M,S}^\times$ . Let  $\psi_1, \psi_2, \dots, \psi_t$  be a set of generators for the group of  $S$ -units in  $M$ . We therefore have that

$$\Lambda_i = \psi_1^{a_{1,i}} \psi_2^{a_{2,i}} \cdots \psi_t^{a_{t,i}}$$

for some integers  $a_{j,i} \in \mathbb{Z}$ . By the remainder theorem, we can write  $a_{j,i} = (n -$

$2)(2n-2)b_{j,i} + c_{j,i}$  for some  $b_{j,i}, c_{j,i} \in \mathbb{Z}$  such that  $|c_{j,i}| \leq (n-2)(n-1)$ . Now for each  $i = 1, \dots, n$ , define

$$\varepsilon_i := \psi_1^{-b_{1,i}} \psi_2^{-b_{2,i}} \dots \psi_t^{-b_{t,i}},$$

where we have that  $\varepsilon_i \in \mathcal{O}_S^\times$ . Now if we define  $\alpha_i$  as

$$\alpha_i := \frac{\varepsilon_i^{2n-2}}{\varepsilon_1 \dots \varepsilon_n} \beta_i$$

then  $f(x)$  is equivalent to the polynomial  $g(x) := c(x - \alpha_1) \dots (x - \alpha_n)$ . By a standard computation, we obtain that

$$\Omega_i = \prod_{i \neq k} (\alpha_i - \alpha_k) = \Lambda_i \left( \frac{\varepsilon_i^{2n-2}}{\varepsilon_1 \dots \varepsilon_n} \right)^{n-2} \prod_{k=1}^n \frac{\varepsilon_k^{2n-2}}{\varepsilon_1 \dots \varepsilon_n} = \varepsilon_i^{(n-2)(2n-2)} \Lambda_i = \prod_{j=1}^t \psi_j^{c_{j,i}}$$

As  $|c_{j,i}| \leq (n-1)(n-2)$ , this implies there are at most  $((n-2)(2n-2))^t$  possible values for each  $\Omega_i$ , and thus  $\Omega_i$  arises from an effectively computable finite set.  $\square$

### 5.2.5 Initialising the linear system

Let  $C : y^2 = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_6)$  be a genus 2 curve with good reduction outside  $S$  and whose Jacobian has good reduction outside 2. Recall that our goal is to compute the possible integers  $a_{k,i,j} \in \mathbb{Z}$  where  $\alpha_i - \alpha_j = \psi_1^{a_{1,i,j}} \psi_2^{a_{2,i,j}} \dots \psi_t^{a_{t,i,j}}$ . We assume that  $C$  has field system  $[M_1, M_2, \dots, M_u]$  with 2-torsion field  $M$ . We now list all the constraints that we impose on the integers  $a_{k,i,j}$ . We remark that many of these constraints will not be independent from each other, although this doesn't particularly matter, and in fact serves as a useful sanity check to make sure our code is correct.

1. **Galois constraints:** For each automorphism  $\sigma \in \text{Gal}(M/\mathbb{Q})$ , this acts naturally on the set of roots  $\alpha_1, \dots, \alpha_6$ . By a slight abuse of notation, we will also denote by  $\sigma \in S_6$  the corresponding permutation on the roots induced by  $\sigma$ ; that is  $\alpha_{\sigma(i)} := \sigma(\alpha_i)$ . Note that  $\sigma$  also acts on the set of  $S$ -unit generators  $\psi_1, \psi_2, \dots, \psi_t$  in the natural way; similarly, we denote  $\psi_{\sigma(i)} := \sigma(\psi_i)$ . Thus, for each pair  $i, j$  we have that

$$\begin{aligned} \psi_{\sigma(1)}^{a_{1,i,j}} \psi_{\sigma(2)}^{a_{2,i,j}} \dots \psi_{\sigma(t)}^{a_{t,i,j}} &= \sigma(\psi_1^{a_{1,i,j}} \psi_2^{a_{2,i,j}} \dots \psi_t^{a_{t,i,j}}) \\ &= \sigma(\alpha_i - \alpha_j) = \alpha_{\sigma(i)} - \alpha_{\sigma(j)} \\ &= \psi_1^{a_{1,\sigma(i),\sigma(j)}} \psi_2^{a_{2,\sigma(i),\sigma(j)}} \dots \psi_t^{a_{t,\sigma(i),\sigma(j)}}. \end{aligned}$$

Therefore, for each  $\sigma \in \text{Gal}(M/\mathbb{Q})$ ,  $1 \leq i < j \leq 6$  and  $1 \leq k \leq t$ , we have the linear constraint:

$$a_{k,i,j} = a_{\sigma(k),\sigma(i),\sigma(j)}$$

2. **Field system constraints:** For each pair  $\alpha_i, \alpha_j$ , we can determine a field  $M_{i,j}$  which both roots lie in, which in general may be smaller than the whole 2-torsion field  $M$ . Thus, for all  $\sigma \in \text{Gal}(M/M_{i,j})$  we have  $\sigma(\alpha_i - \alpha_j) = \alpha_i - \alpha_j$ , which gives the constraint

$$a_{\sigma(k),i,j} = a_{k,i,j}$$

3.  **$S$ -unit solutions:** Now let  $\lambda_1, \lambda_2, \lambda_3$  be three solutions to the  $S$ -unit equation  $x+y=1$  found using methods described in the previous section. Let  $\lambda_{k,i} \in \mathbb{Z}$  be the corresponding exponents of  $\lambda_i$  with respect to the generators  $\psi_1, \dots, \psi_t$ ; i.e.

$$\lambda_1 = \psi_1^{\lambda_{1,1}} \dots \psi_t^{\lambda_{t,1}}, \quad \lambda_2 = \psi_1^{\lambda_{1,2}} \dots \psi_t^{\lambda_{t,2}}, \quad \lambda_3 = \psi_1^{\lambda_{1,3}} \dots \psi_t^{\lambda_{t,3}}.$$

We now impose the constraint:

$$\lambda_1 = \frac{(\alpha_3 - \alpha_2)(\alpha_4 - \alpha_1)}{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_4)}, \quad \lambda_2 = \frac{(\alpha_3 - \alpha_2)(\alpha_5 - \alpha_1)}{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_5)}, \quad \lambda_3 = \frac{(\alpha_3 - \alpha_2)(\alpha_6 - \alpha_1)}{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_6)}$$

By therefore equating the exponents of  $\psi_k$  for each  $k = 1, \dots, t$ , we thus have these linear constraints:

$$a_{k,3,2} + a_{k,4,1} - a_{k,2,1} - a_{k,3,4} = \lambda_{k,1}$$

$$a_{k,3,2} + a_{k,5,1} - a_{k,2,1} - a_{k,3,5} = \lambda_{k,2}$$

$$a_{k,3,2} + a_{k,6,1} - a_{k,2,1} - a_{k,3,6} = \lambda_{k,3}$$

We also note that all the cross-ratios  $(\alpha_i - \alpha_j)(\alpha_k - \alpha_\ell) / ((\alpha_i - \alpha_k)(\alpha_j - \alpha_\ell))$  are determined from just three. Thus, by computing the integers  $\lambda_{h,i,j,k,\ell}$  defined by

$$\frac{(\lambda_i - \lambda_j)(\lambda_k - \lambda_\ell)}{(\lambda_i - \lambda_k)(\lambda_j - \lambda_\ell)} = \psi_1^{\lambda_{1,i,j,k,\ell}} \psi_2^{\lambda_{2,i,j,k,\ell}} \dots \psi_t^{\lambda_{t,i,j,k,\ell}}$$

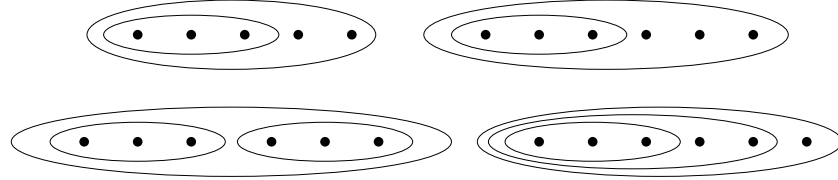
for every subset  $i, j, k, \ell$  of  $\{1, \dots, 6\}$  where  $i \neq k, j \neq \ell$  and  $h = 1, \dots, t$ , we can more generally also add the following linear constraints:

$$a_{h,i,j} + a_{h,k,\ell} - a_{h,i,k} - a_{h,j,\ell} = \lambda_{h,i,j,k,\ell}.$$

We remark that for certain cross-ratios of roots  $\alpha_i, \alpha_j, \alpha_k, \alpha_\ell$  corresponding to

certain field systems, we can make use of the set of *simple*  $S$ -unit solutions computed in Table 5.9.

4. **Jacobian cluster picture constraints:** Recall that, for a genus 2 curve  $C/\mathbb{Q}$ , the cluster picture  $\Sigma_p$  at all odd primes  $p$  of good reduction for  $\text{Jac}(C)$  and bad reduction for  $C$  must be one of the following four pictures:



Each cluster  $\mathfrak{s} \in \Sigma_p$  gives a constraint on the valuations  $v_p(\alpha_i - \alpha_j)$  across all pairs of roots  $\alpha_i, \alpha_j \in \mathfrak{s}$  which are not contained in any children of  $\mathfrak{s}$ . In particular, let  $\psi_{i_p}$  be an  $S$ -unit generator lying above  $p$ . Then for each  $\mathfrak{s} \in \Sigma_p$ , we have

$$a_{i_p, i, j} = a_{i_p, k, \ell}$$

for all  $i, j, k, \ell$  such that  $\alpha_i, \alpha_j, \alpha_k, \alpha_\ell$  lie in  $\mathfrak{s}$  and such that there is no child  $\mathfrak{s}' \subsetneq \mathfrak{s}$  such that  $\alpha_i, \alpha_j \in \mathfrak{s}'$  or  $\alpha_k, \alpha_\ell \in \mathfrak{s}'$ .

By therefore considering all the relevant cases, we can thus implement these cases as a further linear constraint on  $a_{k, i, j}$ . Such constraints are summarised below in Table 5.10.

In the case where  $S$  contains at least two odd primes, we must take care to note that the possible cluster pictures may differ (both in shape and ordering of the roots  $a_i$ ) between different odd primes  $p$ . Thus, as  $|S|$  increases, the number of possible combinations of cluster pictures increase exponentially. It's thus only feasible (at least in our implementation) to add these constraints for one or two odd primes at most, for large  $S$ .

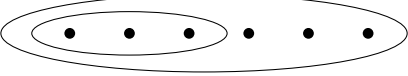
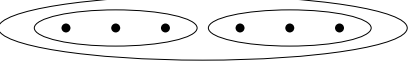
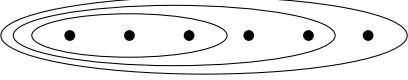
5. **Restrictions from Lemma 5.9:** Recall that we can assume that the values  $\Omega_i = \prod_{i \neq k} (\alpha_i - \alpha_k)$  come from an effectively computable finite set; in particular we have  $\Omega_i = \psi_1^{c_{1,i}} \psi_2^{c_{2,i}} \cdots \psi_t^{c_{t,i}}$  where  $|c_{k,i}| \leq (6-2)(6-1) = 20$ . Thus, by again equating exponents of  $\psi_k$ , we have the following constraints:

$$a_{k,1,2} + a_{k,1,3} + \cdots + a_{k,1,6} = c_{k,1}$$

$$a_{k,2,1} + a_{k,2,3} + \cdots + a_{k,2,6} = c_{k,2}$$

$$\vdots$$

Table 5.10: The system of linear constraints corresponding to each possible cluster picture  $\Sigma_p$  of an odd prime  $p$  of almost good reduction for a genus 2 curve  $C : y^2 = f(x)$  where  $\deg(f) = 6$ . Here  $\psi_p$  denotes an  $S$ -unit generator lying above the prime  $p$ .

Cluster picture $\Sigma_p$	Linear constraints
	$a_{i_p,1,2} = a_{i_p,1,3} = a_{i_p,2,3}$ , and $a_{i_p,1,4} = a_{i_p,1,5} = a_{i_p,1,6} = a_{i_p,2,4}$ $= a_{i_p,2,5} = a_{i_p,2,6} = a_{i_p,3,4} = a_{i_p,3,5}$ $= a_{i_p,3,6} = a_{i_p,4,5} = a_{i_p,4,6} = a_{i_p,5,6}$
	$a_{i_p,1,2} = a_{i_p,1,3} = a_{i_p,2,3}$ , and $a_{i_p,4,5} = a_{i_p,4,6} = a_{i_p,5,6}$ , and $a_{i_p,1,4} = a_{i_p,1,5} = a_{i_p,1,6} = a_{i_p,2,4}$ $= a_{i_p,2,5} = a_{i_p,2,6} = a_{i_p,3,4} = a_{i_p,3,5}$ $= a_{i_p,3,6}$
	$a_{i_p,1,2} = a_{i_p,1,3} = a_{i_p,2,3}$ , and $a_{i_p,1,4} = a_{i_p,1,5} = a_{i_p,2,4} = a_{i_p,2,5}$ $= a_{i_p,3,4} = a_{i_p,3,5} = a_{i_p,4,5}$ , and $a_{i_p,1,6}$ $= a_{i_p,2,6} = a_{i_p,3,6} = a_{i_p,4,6} = a_{i_p,5,6}$

$$a_{k,6,1} + a_{k,6,2} + \cdots + a_{k,6,5} = c_{k,6}$$

where the  $c_{k,i}$  are integers with absolute value at most 20.

Now one possible method to solve the above system would be to take all  $40^{6t}$  different combinations for the  $6t$ -tuple of integers  $(c_{1,1}, \dots, c_{k,i}, \dots, c_{t,6})$  and solve the corresponding linear system using the above constraints. This does give a fully effective algorithm to determine all genus 2 curves with good reduction outside  $S$ , however, this would not be very practical once  $t$  becomes moderately big.

One alternative would be to use a closest vector solver:

### 5.2.6 Closest Vector Problem

Note that, to find representatives for equivalence classes of degree  $n$  polynomials, Lemma 5.9 proves that it's sufficient to take  $\Omega_i$  such that  $|c_{j,i}| \leq (n-1)(n-2)$ , i.e.  $\Omega_i$  can be thought of as an  $nt$ -dimensional vector in a box bounded in absolute value by  $(n-1)(n-2)$ .

If we put this bounding box inside a ball, this gives us the bound  $c_{1,i}^2 + \cdots + c_{t,i}^2 \leq t(n-1)^2(n-2)^2$ . We can therefore interpret this condition in terms of finding all vectors  $\mathbf{v}$  in a given lattice  $\mathcal{L} \subset \mathbb{R}^{6t}$  such that  $\mathbf{v}$  is within a prescribed



distance from a given vector  $\mathbf{w} \in \mathbb{R}^{6t}$ . This is classically known as the *closest vector problem* (CVP), for which some of the earliest algorithms were developed by Fincke–Pohst [170, 171] and Kannan [252, 253]. Whilst lattice problems (in particular CVP) are generally NP-hard, in practice there are many efficient modern algorithms (e.g. `fp111` [181]) which perform well, e.g. see Hanrot–Pujol–Stehlé [213] for an excellent survey on algorithms to solve the shortest vector problem (SVP) and closest vector problem (CVP). For our purposes, the default implementation provided in Magma (developed by Damien Stehlé) seems to work well in practice as long as  $t$  is not too large.

Let  $\mathbf{a}$  be the vector  $(a_{1,1,2}, \dots, a_{k,i,j}, \dots, a_{t,5,6})$  for which we want to solve. We encode the first four linear constraints given above in Section 5.2.5 as a big matrix equation

$$\mathbf{A}\mathbf{a} = \mathbf{b}.$$

Here, the matrix  $\mathbf{A}$  consists only of zeros and ones, with each row containing only a small number of non-zero coefficients.

We can solve this systems using Magma’s `Solution(A, b)` function to get a particular solution  $\mathbf{p}$  and a set of independent vectors  $\mathbf{a}_1, \dots, \mathbf{a}_m$  such that

$$\mathbf{a} \in \mathbb{Z}\mathbf{a}_1 + \dots + \mathbb{Z}\mathbf{a}_m + \mathbf{p}$$

Now encode the final constraint in Section 5.2.5 as  $\mathbf{C}\mathbf{a} = \mathbf{c}$  where  $\mathbf{C}$  is another 0-1 matrix and where  $\mathbf{c} = (c_{1,1}, c_{1,2}, \dots, c_{t,6})$  is a vector where each integer  $c_{k,i}$  satisfies  $|c_{k,i}| \leq 20$ . This gives the bound  $|\mathbf{C}\mathbf{a}| = |\mathbf{c}| = (c_{1,1}^2 + \dots + c_{t,6}^2)^{1/2} \leq 20\sqrt{6t}$ . Therefore, we wish to find integers  $m_1, m_2, \dots, m_m \in \mathbb{Z}$  such that

$$|m_1\mathbf{C}\mathbf{a}_1 + m_2\mathbf{C}\mathbf{a}_2 + \dots + m_m\mathbf{C}\mathbf{a}_m - (-\mathbf{C}\mathbf{p})| \leq 20\sqrt{6t}.$$

By therefore defining the lattice  $\mathcal{L}$  spanned by  $\{\mathbf{C}\mathbf{a}_1, \mathbf{C}\mathbf{a}_2, \dots, \mathbf{C}\mathbf{a}_m\}$ , we now use Magma’s `CloseVectors` function to easily find all lattice points in  $\mathcal{L}$  which are within a distance of  $20\sqrt{6t}$  to the fixed point  $-\mathbf{C}\mathbf{p}$ , and thus all possible solutions  $\mathbf{a} = (a_{1,1,2}, \dots, a_{t,5,6})$ .

We note that, for the vast majority of choices of tuples  $(\lambda_1, \lambda_2, \lambda_3)$  of  $S$ -unit solutions, the linear system  $\mathbf{A}\mathbf{a} = \mathbf{b}$  won’t have any solution, which can easily be checked with Magma. In the cases where  $\mathbf{A}\mathbf{a} = \mathbf{b}$  does have a solution, we can first use Magma’s `ClosestVector` function to determine the closest vector in  $\mathcal{L}$  to  $-\mathbf{C}\mathbf{p}$ . If this already has distance greater than  $20\sqrt{6t}$ , this avoids needing to compute all possible vectors. This therefore allows us to run `CloseVectors` only in a small

reasonable number of cases. Pseudocode for this algorithm is given in Algorithm 10.

---

**Algorithm 10** Algorithm to compute all genus 2 curves  $C/\mathbb{Q}$  with good reduction outside  $S$  and such that  $\text{Jac}(C)$  has good reduction outside 2 (using the Closest Vector approach)

---

```

1: procedure COMPUTEGENUS2( $S$ )
2:   for all 2-torsion fields  $M$  do
3:     Compute the set  $\mathcal{S}_M$  of  $S$ -unit solutions to  $x + y = 1$  for  $x, y \in \mathcal{O}_S^\times$  over  $M$ .
4:   end for
5:   for all field systems  $[M_1, M_2, \dots, M_m]$  do
6:     for all  $\lambda_1, \lambda_2, \lambda_3$  in  $\mathcal{S}_M$  do
7:       Initialise the linear system  $\mathbf{A}\mathbf{a} = \mathbf{b}$  described in Section 5.2.5.
8:       Let  $\mathbf{p}$  be a particular solution, and compute  $\ker(\mathbf{A}) = \mathbb{Z}\mathbf{a}_1 + \mathbb{Z}\mathbf{a}_2 + \dots + \mathbb{Z}\mathbf{a}_m$ .
9:       Let  $L$  be the integer lattice with basis  $\mathbf{Ca}_1, \mathbf{Ca}_2, \dots, \mathbf{Ca}_m$ .
10:      Use Magma's CloseVectors function to compute all vectors  $(m_1, \dots, m_m)$  in  $L$  of distance at most  $20\sqrt{6t}$  from  $-\mathbf{Cp}$ .
11:      for vectors  $(m_1, \dots, m_m)$  found do
12:        Construct the vector  $\mathbf{a} = m_1\mathbf{a}_1 + \dots + m_m\mathbf{a}_m + \mathbf{p}$ .
13:        Construct the curve  $C/\mathbb{Q} : y^2 = f(x)$  corresponding to the values  $a_{k,i,j}$  from  $\mathbf{a}$ .
14:        if  $C$  has 2-power conductor then
15:          Add  $C$  (and all twists) to  $\mathcal{C}$ 
16:        end if
17:      end for
18:    end for
19:  end for
20:  return A list of genus 2 curves  $\mathcal{C}$ .
21: end procedure

```

---

Using Matschke's  $S$ -unit solutions, we were able to successfully run Algorithm 10 for the following pairs of the primes  $(S, L)$  where  $S$  is the set of primes of bad reduction for  $C/\mathbb{Q}$  and  $L$  is the largest 2-torsion field  $\mathbb{Q}(J[2])$ :

$$\begin{aligned}
&(\{2, 3\}, M_1), (\{2, 3\}, M_2), (\{2, 3\}, M_3), (\{2, 5\}, M_1), (\{2, 5\}, M_2), (\{2, 5\}, M_3), \\
&(\{2, 7\}, M_1), (\{2, 7\}, M_2), (\{2, 7\}, M_3), (\{2, 3, 5\}, M_1), (\{2, 3, 7\}, M_1), (\{2, 3, 7\}, M_3), \\
&(\{2, 5, 7\}, M_1), (\{2, 5, 7\}, M_2), (\{2, 3, 5, 7\}, K_1), (\{2, 3, 5, 7\}, K_2), (\{2, 3, 5, 7\}, K_3) \\
&(\{2, 3, 5, 7, 11, 13\}, \mathbb{Q}).
\end{aligned}$$

Finally, we should mention that we also ran Algorithm 10 for many other larger sets  $S$  and 2-torsion fields  $\mathbb{Q}(J[2])$ , even if we were unable to completely solve

for all  $S$ -unit solutions to  $x+y=1$  over  $\mathbb{Q}(J[2])$ . In these cases, we can still set up the linear system as a matrix equation  $\mathbf{A}\mathbf{a}=\mathbf{b}$  described in Section 5.2.5, whilst leaving out the  $S$ -unit constraints. Whilst this gives us infinitely many potential solutions, we did a brute force run iterating through the possible values of  $(a_1, \dots, a_m)$  which allowed us to find a few new curves; e.g. this is how we found the genus 2 curve  $y^2 = (3x^2 + 2x + 1)(x^4 - 4x^3 - 254x^2 - 252x - 2047)$  which has bad reduction at  $S = \{2, 3, 11\}$  and has 2-torsion field  $\mathbb{Q}(J[2]) = M_2$ .

### 5.2.7 Integer Linear Programming

We also give an alternative method to finding all solutions to the corresponding linear system, noting that all values for  $a_{k,i,j}$  must be integers. Given that we wish to thus find all integer solutions within a bounded region, this also suggests trying an *integer linear programming* (ILP) approach. Like the CVP method, ILPs are also NP-hard in general, although similarly many cases can be practically solved if  $t$  is not too big; e.g. see Padberg [341] or Beasley [30] for an overview of various algorithms in linear programming.

One hopeful advantage of this method is that this uses the stronger “bounding box” condition  $|c_{1,1}|, |c_{1,2}|, \dots, |c_{t,6}| \leq 20$  instead of the weaker “bounding ball” condition  $|\mathbf{c}| \leq 20\sqrt{6t}$  used in the CVP method. Here, we used Sage’s `MixedIntegerLinearProgram` functionality [373]. There are a number of various integer solvers one can use in Sage; for our implementation we stuck with the default GLPK (GNU Linear Programming Kit) solver [192].

As with the closest vector problem, we begin by initialising a linear system of equations  $\mathbf{A}\mathbf{a}=\mathbf{b}$ , and solving for the solution space  $\mathbf{a} \in \mathbb{Z}\mathbf{a}_1 + \dots + \mathbb{Z}\mathbf{a}_m + \mathbf{p}$ . We also impose the constraint that each element of the vector  $\mathbf{C}\mathbf{a}$  has absolute value at most 20. Now recall that we wish to find all possible integers  $m_1, \dots, m_m \in \mathbb{Z}$  such that the vector  $\mathbf{a} = m_1\mathbf{a}_1 + \dots + m_m\mathbf{a}_m + \mathbf{p}$  satisfies the above linear constraints and inequalities.

Using the GLPK solver in Sage, we can compute the minimum possible integer value for  $m_1$  and the maximum possible integer value for  $m_1$ . We can then loop through each integer  $k_1$  from  $\min(m_1)$  to  $\max(m_1)$ , and add the constraint that  $m_1 = k_1$ . We then repeat the process by using GLPK to compute  $\min(m_2)$  and  $\max(m_2)$ , looping through each possible integer  $k_2$  from  $\min(m_2)$  to  $\max(m_2)$ , and adding the constraint  $m_2 = k_2$ . By iterating this procedure  $m$  times, this would in principle hit all possible solutions for  $\mathbf{a}$ . We give pseudocode for this procedure in Algorithm 11.

It’s difficult to predict in advance how long Algorithm 11 would take to run,

---

**Algorithm 11** Algorithm to compute all genus 2 curves  $C/\mathbb{Q}$  with good reduction outside  $S$  and such that  $\text{Jac}(C)$  has good reduction outside 2 (using the integer linear programming (ILP) method)

---

```

1: procedure COMPUTE GENUS2( $S$ )
2:   for all 2-torsion fields  $M$  do
3:     Compute the set  $\mathcal{S}_M$  of  $S$ -unit solutions to  $x + y = 1$  for  $x, y \in \mathcal{O}_S^\times$  over  $M$ .
4:   end for
5:   for all field systems  $[M_1, M_2, \dots, M_m]$  do
6:     for all  $\lambda_1, \lambda_2, \lambda_3$  in  $\mathcal{S}_M$  do
7:       Initialise the linear system  $\mathbf{A}\mathbf{a} = \mathbf{b}$  described in Section 5.2.5.
8:       Compute a basis  $\mathbf{a}_1, \dots, \mathbf{a}_m$  for  $\ker(\mathbf{A})$  and a particular solution  $\mathbf{p}$ .
9:       Run the GLPK solver with the constraint on  $\mathbf{C}\mathbf{a}$  to compute  $\min(m_1)$ 
and  $\max(m_1)$ 
10:      for  $k_1$  from  $\min(m_1)$  to  $\max(m_1)$  do
11:        Add the linear constraint  $m_1 = k_1$ .
12:        Run the GLPK solver to compute  $\min(m_2)$  and  $\max(m_2)$ 
13:        for  $k_2$  from  $\min(m_2)$  to  $\max(m_2)$  do
14:          Add the linear constraint  $m_2 = k_2$ .
15:          Run the GLPK solver to compute  $\min(m_3)$  and  $\max(m_3)$ 
16:          for  $k_3$  from  $\min(m_3)$  to  $\max(m_3)$  do
17:             $\vdots$ 
18:          for  $k_m$  from  $\min(m_m)$  to  $\max(m_m)$  do
19:            Construct the vector  $\mathbf{a} = k_1\mathbf{a}_1 + \dots + k_m\mathbf{a}_m + \mathbf{p}$ .
20:            Construct the curve  $C/\mathbb{Q} : y^2 = f(x)$  corresponding to
the values  $a_{k,i,j}$  from  $\mathbf{a}$ .
21:            if  $C$  has 2-power conductor then
22:              Add  $C$  (and all twists) to  $\mathcal{C}$ 
23:            end if
24:          end for
25:         $\vdots$ 
26:      end for
27:    end for
28:  end for
29:  end for
30:  end for
31:  return A list of genus 2 curves  $\mathcal{C}$ .
32: end procedure

```

---

as this depends heavily on the values for  $\min(a_i)$  and  $\max(a_i)$  computed by the GLPK solver.

Note that in our implementation, we used GLPK to compute the minimum

and maximum of the possible integers  $a_1, a_2, \dots, a_m$ . It's however very likely that the most optimal approach is to instead find the minimum and maximum of suitably chosen linear combinations of  $a_1, \dots, a_m$ ; i.e. we iteratively compute the minimum and maximum of the  $m$  linear combinations:

$$\begin{aligned} w_{1,1}a_1 + w_{1,2}a_2 + \dots + w_{1,m}a_m, \\ w_{2,1}a_1 + w_{2,2}a_2 + \dots + w_{2,m}a_m, \\ \vdots \\ w_{m,1}a_1 + w_{m,2}a_2 + \dots + w_{m,m}a_m, \end{aligned}$$

where  $w_{i,j} \in \mathbb{Z}$  are some suitably chosen integers (in Algorithm 11, this is chosen as  $w_{i,j} = \delta_{i,j}$ ). It seems reasonable to conjecture that a suitable choice of  $w_{i,j}$  could be much faster in practice than the default choice of  $w_{i,j} = \delta_{i,j}$  as shown in Algorithm 11.

We should remark that, in least in our cases, the above implementation of Algorithm 11 didn't seem to yield much faster results than the closest vector approach and didn't find any new curves which couldn't be found with the CVP method; although we should remark that we didn't make much effort to further optimise the above implementation.

It seems likely that a carefully optimised implementation which combines the closest vector method together with the integer linear programming method (with optimally chosen integers  $w_{i,j}$ ) would by far yield the best results, however we did not consider this for this thesis and will be left for future projects.

### 5.3 Gluing elliptic curves

One particular case of interest for us is to construct genus 2 curves  $C/\mathbb{Q}$  whose Jacobians  $\text{Jac}(C)$  are isogenous to a product of elliptic curves  $E_1 \times E_2$ . We'll therefore conclude this chapter by summarising some methods on how one can construct such genus 2 curves  $C$  whose Jacobian has good reduction away from 2 by gluing together elliptic curves  $E_1$  and  $E_2$  with good reduction away from 2. We first briefly review what it means to glue elliptic curves.

Let  $K$  be a field and  $C/K$  be a genus 2 curve such that there exists a non-constant morphism  $\phi_1 : C \rightarrow E_1$  to an elliptic curve  $E_1$  such that  $\phi_1$  does not factor over a non-trivial isogeny of  $E$ ; i.e.  $\phi_1$  is an *elliptic subcover* of  $C$ . Assuming  $\phi_1$  has minimal degree  $n$ , one obtains a complementary elliptic subcover  $\phi_2 : C \rightarrow E_2$  also

of degree  $n$  and thus an isogeny

$$\Phi : E_1 \times E_2 \rightarrow \text{Jac}(C).$$

of degree  $n^2$ . This construction is referred to as *gluing*  $E_1$  and  $E_2$  along their  $n$ -torsion and we say that  $\text{Jac}(C)$  is  $(n, n)$ -decomposable. A natural question is thus to ask whether, given any two elliptic curves  $E_1, E_2$  over  $K$  and an integer  $n \geq 2$ , does there exist a genus 2 curve  $C/K$  which admits two degree  $n$  elliptic subcovers  $\phi_1 : C \rightarrow E_1$  and  $\phi_2 : C \rightarrow E_2$ ?<sup>7</sup>

This question was considered by Frey and Kani [186], who gave a positive answer in the case where  $K$  is algebraically closed,  $\text{char}(K) \nmid n$ , and  $E_1$  is not  $K$ -isogenous to  $E_2$ . In particular, Kani [249, 248] (based on the work of Frey–Kani [186]) showed that the existence of such a genus 2 curve  $C/K$  follows from the existence of an irreducible anti-symplectic isomorphism  $E_1[n] \xrightarrow{\sim} E_2[n]$ :

**Theorem 5.10.** [249] *Let  $K$  be an algebraically closed field. Let  $E_1/K$  and  $E_2/K$  be two elliptic curves over  $K$  and let  $n \geq 2$ . Let  $\psi : E_1[n] \xrightarrow{\sim} E_2[n]$  be an irreducible anti-symplectic isomorphism. Then there exists a genus 2 curve  $C/K$  which admits two elliptic subcovers  $C \rightarrow E_1$  and  $C \rightarrow E_2$  of degree  $n$ , and in particular  $\text{Jac}(C)$  is  $K$ -isogenous to  $E_1 \times E_2$  of degree  $n^2$ .*

Here, *anti-symplectic* means an isomorphism  $\psi : E_1[n] \xrightarrow{\sim} E_2[n]$  which inverts the Weil pairing; i.e.  $e_{2,n}(\psi(x), \psi(y)) = e_{1,n}(x, y)^{-1}$  for all  $x, y \in E_1[n]$ , where  $e_{1,n} : E_1[n] \times E_1[n] \rightarrow \mu_n$  and  $e_{2,n} : E_2[n] \times E_2[n] \rightarrow \mu_n$  are the Weil pairings on  $E_1[n]$  and  $E_2[n]$  respectively. In the case where  $n$  is prime, the *irreducible* condition is equivalent to the statement that, for all  $1 \leq k < n$ , there does not exist any isogeny  $h : E_1 \rightarrow E_2$  of degree  $k(n - k)$  such that  $\psi \circ [k] = h|_{E_1[n]}$  [249, Theorem 3]. A complete definition of an *irreducible anti-symplectic isomorphism*  $\psi : E_1[n] \xrightarrow{\sim} E_2[n]$  for all  $n$  is given by Kani [249].<sup>8</sup> In the special case of  $n = 2$ , one can show that such a genus 2 curve  $C/K$  exists if and only if there exists an isomorphism  $\psi : E_1[2] \xrightarrow{\sim} E_2[2]$  which is not the restriction of an isomorphism  $E_1/K \xrightarrow{\sim} E_2/K$  [226, Prop. 3].

<sup>7</sup>It's worth mentioning that the related question of the existence of genus 2 curves  $C/K$  such that  $\text{Jac}(C)$  is *isomorphic* to  $E_1 \times E_2$  has also been well-studied, e.g. see Hayashida–Nishi [219], Ibukiyama–Katsura–Oort [228], and Kani [250, 251].

<sup>8</sup>It's worth mentioning that Frey–Kani [186, p. 155] remarked that their construction “*seems to be known in principle*” (e.g. see Serre [394], Ibukiyama–Katsura–Oort [228]) although to their knowledge doesn't appear explicitly in the literature prior to their work.

### 5.3.1 Gluing elliptic curves $E/\mathbb{Q}$ with good reduction away from 2

For our purposes, we considered all 55 isogeny classes of abelian surfaces over  $\mathbb{Q}$  which are isogenous to a product of two elliptic curves  $E/\mathbb{Q}$  with good reduction away from 2.

There are exactly 10 such isogeny classes of elliptic curves  $E/\mathbb{Q}$  with good reduction outside 2, classified by Ogg [337]. We tabulate a list of these classes, shown in Table 5.11 (note that the Cremona labels agree with the LMFDB labels (up to a period) in these cases).

Table 5.11: List of the 10  $\mathbb{Q}$ -isogeny classes of elliptic curves  $E/\mathbb{Q}$  with good reduction outside 2, as classified by Ogg [337]. Here  $N$  denotes the conductor,  $\text{End}(E_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$  the geometric endomorphism algebra,  $\text{ST}(E)$  the Sato-Tate group, and  $\#E/\mathbb{Q}$  the number of elliptic curves  $E/\mathbb{Q}$  in this isogeny class.

Cremona label	$N$	Rank	$\text{End}(E_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$\text{ST}(E)$	$\#E/\mathbb{Q}$
32a	$2^5$	0	$\mathbb{Q}(\sqrt{-1})$	$N(\text{U}(1))$	4
64a	$2^6$	0	$\mathbb{Q}(\sqrt{-1})$	$N(\text{U}(1))$	4
128a	$2^7$	1	$\mathbb{Q}$	$\text{SU}(2)$	2
128b	$2^7$	0	$\mathbb{Q}$	$\text{SU}(2)$	2
128c	$2^7$	0	$\mathbb{Q}$	$\text{SU}(2)$	2
128d	$2^7$	0	$\mathbb{Q}$	$\text{SU}(2)$	2
256a	$2^8$	1	$\mathbb{Q}(\sqrt{-2})$	$N(\text{U}(1))$	2
256b	$2^8$	1	$\mathbb{Q}(\sqrt{-1})$	$N(\text{U}(1))$	2
256c	$2^8$	0	$\mathbb{Q}(\sqrt{-1})$	$N(\text{U}(1))$	2
256d	$2^8$	0	$\mathbb{Q}(\sqrt{-2})$	$N(\text{U}(1))$	2

First let  $E_1/\mathbb{Q}$  and  $E_2/\mathbb{Q}$  be non-isogenous elliptic curves with good reduction away from 2. Whilst Theorem 5.10 can produce many examples of genus 2 curves  $C/\overline{\mathbb{Q}}$  which are  $\overline{\mathbb{Q}}$ -isogenous to  $E_1 \times E_2$ , most of these curves  $C$  will not admit a model over  $\mathbb{Q}$ .

We thus wish to find all integers  $n \geq 2$  such that there exists an irreducible *Galois-equivariant* anti-symplectic isomorphism  $\psi : E_1[n] \rightarrow E_2[n]$ . In particular, the existence of such an Galois-equivariant isomorphism  $\psi$  implies that the mod  $n$  Galois representations  $\bar{\rho}_{E_1, n}$  and  $\bar{\rho}_{E_2, n}$  attached to  $E_1$  and  $E_2$  respectively, are isomorphic up to semisimplification (e.g. see [225, p. 128] or [126, p. 20]). We can therefore eliminate many possibilities for  $n$  by thus comparing  $a_p(E_1)$  and  $a_p(E_2)$  mod  $p$  for sufficiently many odd primes  $p$ .<sup>9</sup>

<sup>9</sup>Alternatively, since all elliptic curves  $E/\mathbb{Q}$  with good reduction away from 2 have conductor

We thus computed  $\gcd\{a_p(E_1) - a_p(E_2) : p \text{ odd}, p < 1000\}$  over all pairs of non-isogenous elliptic curves  $E_1/\mathbb{Q}$  and  $E_2/\mathbb{Q}$  with good reduction away from 2, and obtained a value of 2, 4 or 8 in every such case. Thus, by simply computing Richelot and double Richelot isogenies (e.g. using Magma's `TwoPowerIsogenies` function), we were able to find all smooth genus 2 curves  $C/\mathbb{Q}$  which can be obtained by gluing together two non-isogenous elliptic curves  $E_1/\mathbb{Q}$  and  $E_2/\mathbb{Q}$  with good reduction away from 2.

In the case where  $E_1/\mathbb{Q}$  and  $E_2/\mathbb{Q}$  are two *isogenous* elliptic curves, it seems to be not as trivial to determine all possible gluings between these curves. In these cases, we explicitly computed all possible gluings along their 2-torsion (by an algorithm of Howe-Leprévost-Poonen [226, Proposition 4]) and all possible gluings along their 3-torsion (by an algorithm of Bröker–Howe–Lauter–Stevenhagen [69, Algorithm 5.4]). We also ran some Magma code of Sijsling [410], based on a Magma package developed by Hanselman–Schiaivone–Sijsling [214]. This uses an analytic method to glue elliptic curves along their  $n$ -torsion, and we ran this for all  $n \leq 7$ .<sup>10</sup>

A summary of the number of genus 2 curves  $C/\mathbb{Q}$  we obtained in each of the 55 isogeny classes by gluing is given in Table 5.12.

We remark that Table 5.12 is not guaranteed to be complete. In other words, given two elliptic curves  $E_1/\mathbb{Q}$  and  $E_2/\mathbb{Q}$  with good reduction away from 2, we haven't guaranteed that we have found all genus 2 curves  $C/\mathbb{Q}$  such that  $\text{Jac}(C)$  is isogenous to  $E_1 \times E_2$ . We therefore pose the following problem:

**Problem 5.10.** Given two elliptic curves  $E_1/\mathbb{Q}$  and  $E_2/\mathbb{Q}$ , implement a practical algorithm to compute all smooth genus 2 curves  $C/\mathbb{Q}$  such that  $\text{Jac}(C)$  is isogenous to  $E_1 \times E_2$ .

In particular, this requires finding all  $n$  such that there exists an irreducible Galois equivariant anti-symplectic isomorphism  $\psi : E_1[n] \xrightarrow{\sim} E_2[n]$ . It's known that there are only finitely many such  $n$  by Faltings' theorem [164], and furthermore one can in principle prove effective bounds on the possible values of  $n$  by the isogeny estimates of Masser–Wüstholz [302] and Bost [59] (e.g. see Gaudron–Rémond [189, Theorem 1.4] for an explicit such bound), however these bounds are unfortunately far too large to be useful in practice.

---

at most 256, we can apply a recent theorem of Cremona–Freitas [126, Theorem 1.3] stating that if  $E_1/\mathbb{Q}$  and  $E_2/\mathbb{Q}$  are elliptic curves with conductors  $\leq 500\,000$  and  $E_1[p] \cong E_2[p]$  for some prime  $p > 17$ , then  $E_1$  and  $E_2$  are  $\mathbb{Q}$ -isogenous.

<sup>10</sup>There has been some recent work of Djukanović [142] on determining when a cyclic isogeny between two elliptic curves  $E_1/K$  and  $E_2/K$  without CM induces an  $(n, n)$ -isogeny between  $E_1 \times E_2$  and the Jacobian  $\text{Jac}(C)$  of a smooth genus 2 curve  $C/K$ . We checked that no such curves  $C/\mathbb{Q}$  exist via this construction for the four isogeny classes  $128a \times 128a$ ,  $128b \times 128b$ ,  $128c \times 128c$ , and  $128d \times 128d$ .



Table 5.12: Table of all 55 isogeny classes of abelian surfaces  $A$  which split over  $\mathbb{Q}$ , i.e. where  $A$  is  $\mathbb{Q}$ -isogenous to  $E_1 \times E_2$  for some two elliptic curves  $E_1, E_2$  over  $\mathbb{Q}$  with good reduction outside 2. Each cell in the table gives the number of known genus 2 curves  $C/\mathbb{Q}$  whose Jacobian is isogenous to  $E_1 \times E_2$  (with the rows (resp. columns) denoting the Cremona label of the isogeny class of  $E_1$  (resp.  $E_2$ )).

	32a	64a	128a	128b	128c	128d	256a	256b	256c	256d
32a	4	10	6	6	6	6	8	4	4	8
64a		4	6	6	6	6	8	4	4	8
128a			1	4	3	3	4	2	2	4
128b				1	3	3	4	2	2	4
128c					1	4	4	2	2	4
128d						1	4	2	2	4
256a							2	4	4	6
256b								0	4	4
256c									0	4
256d										2

In general, given a number field  $K$  and an abelian surface  $A/K$ , whilst the results of [304, 59] prove there exists an effective algorithm to determine all abelian surfaces  $B/K$  which are  $K$ -isogenous to  $A/K$ , practically doing so is still a highly non-trivial problem. However, we do remark that practical algorithms have now been implemented by van Bommel–Chidambaram–Costa–Kieffer [459] to compute the isogeny classes of principally polarised abelian surfaces  $A/\mathbb{Q}$  whose geometric endomorphism ring  $\text{End}(A_{\overline{\mathbb{Q}}})$  is  $\mathbb{Z}$ , with some work in progress on extending this to larger endomorphism rings.

## Chapter 6

# List of abelian surfaces $A/\mathbb{Q}$ with good reduction outside 2

In this chapter, we finally present all the results of the algorithms implemented in the previous chapter using a combination of Magma [58] and Sage [373] code. Details of similar computations on genus 2 curves are also given by Booker–Sijlsing–Sutherland–Voight–Yasaki [54]. This chapter is dedicated to all contributors of the *L-functions and modular forms database* (LMFDB) [290]; indeed most of the computations done in this chapter were inspired by the many arithmetic invariants computed on the LMFDB. Performing all these computations gave us a small glimpse into the immense amount of work and expertise that goes into maintaining such a large database!

In total we found 512 distinct  $\mathbb{Q}$ -isomorphism classes of genus 2 curves  $C/\mathbb{Q}$  whose Jacobian has good reduction away from 2. In addition to Smart’s list of 366 genus 2 curves with good reduction away 2, this also includes 146 additional curves  $C/\mathbb{Q}$  which have bad reduction at at least one odd prime.<sup>1</sup> These were separated into 27  $\overline{\mathbb{Q}}$ -isogeny classes, 67  $\overline{\mathbb{Q}}$ -isomorphism classes, and 175  $\mathbb{Q}$ -isogeny classes.

A webpage with downloadable links to all curves and further data (both in computer-readable and human-readable formats) can be found at:

<https://warwick.ac.uk/fac/sci/math/people/staff/visser/genus2/>

---

<sup>1</sup>We should remark that, in addition to the tables of Merriman–Smart [314] and Smart [418], most of the 146 genus 2 curves  $C/\mathbb{Q}$  found containing an odd prime  $p$  of almost good reduction, have already been computed using various other methods by Booker–Sijlsing–Sutherland–Voight–Yasaki [54], Booker–Sutherland [55] and Sutherland [435]

## 6.1 Computational results and Statistics

### 6.1.1 Minimal Weierstrass model

For each curve  $C/\mathbb{Q}$ , we calculated a minimal Weierstrass model for  $C$  using the Magma function `ReducedMinimalWeierstrassModel`. This returns a globally minimal integral model of  $C/\mathbb{Q}$  which is reduced with respect to the action of  $\mathrm{SL}_2(\mathbb{Z})$  using an algorithm of Michael Stoll. Most of the genus 2 curves (486 out of 512) had a globally minimal model which was also in the simplified form  $y^2 = f(x)$ ; only 26 curves did not have such a model. The 26 curves which did not have an integral model which is both simplified and minimal are indicated by a footnote next to the shown simplified model in the main Table 6.21.

By factorising the discriminant  $\Delta_{\min}$  of a minimal Weierstrass model, we computed the set of primes  $p$  of bad reduction for the curve  $C$ . We found that the first five odd primes 3, 5, 7, 11, and 13 all occurred as possible primes of almost good reduction for  $C$ , as shown in Table 6.1. For all genus 2 curves  $C/\mathbb{Q}$  found, if  $C/\mathbb{Q}$  has bad reduction at  $p$ , then it also has geometric bad reduction at  $p$ .

Table 6.1: Primes of (geometric) bad reduction for  $C/\mathbb{Q}$

Bad primes for $C$	$\{2\}$	$\{2, 3\}$	$\{2, 5\}$	$\{2, 7\}$	$\{2, 13\}$	$\{2, 3, 7\}$	$\{2, 3, 11\}$
<b>Num curves</b>	366	78	28	24	8	4	4
<b>Num <math>\overline{\mathbb{Q}}</math> classes</b>	51	8	3	2	1	1	1


Furthermore, by factorising the polynomial  $f$  in a simplified model  $y^2 = f(x)$ , we computed the field system for  $C/\mathbb{Q}$ . We give a summary of the types of field systems obtained in Table 6.2. Recall that  $K_1, K_2, K_3$  denote the three quadratic fields unramified away from 2, and  $L_1, \dots, L_7$  denote the seven quartic fields unramified away from 2 (defined in Table 5.4). Our computations did not find any genus 2 curve  $C/\mathbb{Q}$  with full rational 2-torsion whose Jacobian has good reduction away from 2. As noted in Theorem 5.1, if such a curve exists, it must have bad reduction at some prime  $p \geq 17$ .

Table 6.2: Possible types of field systems for our genus 2 curves  $C/\mathbb{Q}$

Field system	$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_i]$	$[\mathbb{Q}, \mathbb{Q}, K_i, K_j]$	$[\mathbb{Q}, \mathbb{Q}, L_i]$	$[K_i, K_j, K_k]$	$[K_i, L_j]$
<b>Num curves</b>	6	28	178	35	265

A full breakdown of all 48 possible unique field systems and the number of genus 2 curves  $C/\mathbb{Q}$  obtained for each field system is given in the appendix in

Table A.1.

The 29 genus 2 curves satisfying  $|\Delta_{\min}| \leq 10^6$  are also listed on the LMFDB [290]. These are indicated in the table by the icon , with links to each of the respective webpages of these curves on the LMFDB.

### 6.1.2 Automorphism group

It's well-known that the automorphism group  $\text{Aut}(C)$  of any smooth projective curve  $C$  of genus  $g > 1$  is finite, with uniform bounds known in terms of the genus  $g$  (e.g. see Hurwitz [227]). In particular, the possible automorphism groups for genus 2 curves  $C/\mathbb{Q}$  have been fully classified by Shaska and Völklein [403, Theorem 2].

The automorphism group over both  $\mathbb{Q}$  and  $\overline{\mathbb{Q}}$  were computed for all our curves using the default Magma functions `AutomorphismGroup` and `GeometricAutomorphismGroup` respectively. For our curves, the possible automorphism groups  $\text{Aut}(C)$  over  $\mathbb{Q}$  were  $C_2$ ,  $C_2 \times C_2$ ,  $C_4$ , and  $D_4$ , and the possible geometric automorphism groups  $\text{Aut}(C_{\overline{\mathbb{Q}}})$  (over  $\overline{\mathbb{Q}}$ ) were  $C_2$ ,  $C_2 \times C_2$ ,  $D_4$ , and  $\text{GL}_2(\mathbb{F}_3)$ .<sup>2</sup> The number of curves with given automorphism group over  $\mathbb{Q}$  and  $\overline{\mathbb{Q}}$  are given in Table 6.3 and Table 6.4 respectively.

Table 6.3: Automorphism groups for  $C$  over  $\mathbb{Q}$

$\text{Aut}(C)$	$C_2$	$C_2 \times C_2$	$C_4$	$D_4$
<b>Num curves</b>	289	190	23	10

Table 6.4: Automorphism groups for  $C$  over  $\overline{\mathbb{Q}}$

$\text{Aut}(C_{\overline{\mathbb{Q}}})$	$C_2$	$C_2 \times C_2$	$D_4$	$\text{GL}_2(\mathbb{F}_3)$
<b>Num curves</b>	140	248	102	22
<b>Num <math>\overline{\mathbb{Q}}</math> classes</b>	35	24	7	1

Here  $C_n$  denotes the cyclic group of order  $n$  and  $D_n$  denotes the dihedral group of order  $2n$ .

### 6.1.3 Torsion subgroup

The torsion subgroup of  $\text{Jac}(C)(\mathbb{Q})$  was computed for all curves using the default `TorsionSubgroup` Magma function, using  $p$ -adic methods by Stoll [428, Section 11]. Noting the possible field systems that a genus 2 curve  $C/\mathbb{Q}$  whose Jacobian is good

<sup>2</sup>We note that in general genus 2 curves  $C/\mathbb{Q}$  can have other automorphism groups than the ones listed in our tables, e.g. the genus 2 curve  $C/\mathbb{Q} : y^2 = x^5 - 5x^3 - 5x^2 - x$  [290, Genus 2 curve 2704.a.43264.1] has  $\text{Aut}(C) = C_6$  and  $\text{Aut}(C_{\overline{\mathbb{Q}}}) = D_6$ .

outside 2 can have (see Table 5.5), we see there always exists at least one nontrivial rational torsion point of order 2. In all tables ahead, we use the common shorthand  $\mathbb{Z}/N$  to mean the order  $N$  cyclic group  $\mathbb{Z}/N\mathbb{Z}$ .

Rather interestingly, all 512 genus 2 curves except for one, had torsion order being a power of two. Statistics for the number of genus 2 curves with given torsion subgroup are shown in Table 6.5.

Table 6.5: Torsion subgroup  $J(\mathbb{Q})_{\text{tors}}$  of the Jacobian  $J$  of  $C/\mathbb{Q}$

Torsion subgroup	$\mathbb{Z}/2 \times \mathbb{Z}/10$	$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	$\mathbb{Z}/2 \times \mathbb{Z}/2$	$\mathbb{Z}/2$
Num curves	1	6	57	371

Torsion subgroup	$\mathbb{Z}/2 \times \mathbb{Z}/4$	$\mathbb{Z}/4$	$\mathbb{Z}/4 \times \mathbb{Z}/4$	$\mathbb{Z}/8$
Num curves	4	59	1	13

We note that the subgroup of rational 2-torsion  $J(\mathbb{Q})[2]$  has order consistent with the field systems given in Table 6.2.

The only genus 2 curve we found which had a rational point on the Jacobian of odd order is the curve  $y^2 + y = 2x^5 - 3x^4 + x^3 + x^2 - x$  [290, Genus 2 curve 256.a.512.1], which is in fact a model for the modular curve  $X_1(16)$ .

In contrast to Mazur’s theorem [310] in the elliptic curve case, in general very little is known about the possible torsion subgroups  $A(\mathbb{Q})_{\text{tors}}$  that can occur for abelian surfaces  $A/\mathbb{Q}$ ; in particular no uniform bound on the order  $|A(\mathbb{Q})_{\text{tors}}|$  is known. Although we should mention one recent result of Laga-Schembri-Schmidman-Voight [274] proving a classification of the possible groups  $A(\mathbb{Q})_{\text{tors}}$  in the case where  $\text{End}(A_{\overline{\mathbb{Q}}})$  is a maximal order in a division quaternion algebra over  $\mathbb{Q}$ .

#### 6.1.4 Conductor

The conductor  $N$  for the Jacobian  $\text{Jac}(C)$  of each curve  $C$  was rigorously computed using the Dokchitser–Doris [149] Magma package. This successfully computed the conductor of almost all curves in the table, with the exception of the two curves  $y^2 = -x^5 + 3x^4 - 2x^3 + 2x^2 - x - 1$  and  $y^2 = -x^5 - 3x^4 - 2x^3 - 2x^2 - x + 1$ ; here Magma struggled to compute a regular model at 2 for these curves. However, we did find curves whose Jacobians are isogenous to the above Jacobians, which allowed for the conductor to be successfully computed, so all results have been verified unconditionally. The conductor was also double checked using the MCLF Sage toolbox [372] by R  th–Wewers, which computes the conductor exponent at 2 by constructing a semistable model of  $C/\mathbb{Q}$  at  $p = 2$ .

In particular, we furthermore computed the tame part  $n_t$  and the wild part  $n_w$  of the conductor exponent at 2, where  $N = 2^{n_t+n_w}$ . We found that, for all but one isogeny classes we had  $n_t = 4$ , the only exception being the unique conductor  $2^8$  isogeny class containing the curve  $y^2 = (x-1)(x+1)(x^2-2x-1)(x^2+1)$ , which had  $n_t = 2$  with corresponding Euler factor  $L_2(T) = 1 + 2T + 2T^2$ .

As a third additional check, we furthermore verified for all curves found, that the Hasse-Weil functional equation for  $L(C/\mathbb{Q}, s)$  as given in (1.15), is numerically satisfied to 100 bits of precision for the value of  $N$  obtained with the Dokchitser–Doris algorithm. This was verified using the Sage implementation of Dokchitser’s  $L$ -function calculator [145].

A summary of the number of genus 2 curves  $C/\mathbb{Q}$  found (and the  $\mathbb{Q}$ -isogeny classes) with conductor  $N$  is given below in Table 6.6.

Table 6.6: Conductor  $N$  of the Jacobian  $\text{Jac}(C)$  for each curve  $C$ 

Conductor	$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$2^{13}$	$2^{14}$	$2^{15}$	$2^{16}$	$2^{17}$	$2^{18}$	$2^{19}$	$2^{20}$
<b>Num curves</b>	2	0	4	10	33	62	65	72	68	64	38	40	54
<b>Num isog classes</b>	1	0	1	1	7	10	19	22	19	24	19	20	32

### 6.1.5 Mordell-Weil group and Rank

For the Jacobian  $J$  of each genus 2 curve  $C/\mathbb{Q}$ , a set of generators for the Mordell-Weil group  $J(\mathbb{Q})$ , and in particular the rank  $r$  of  $\text{Jac}(C)$  over  $\mathbb{Q}$ , was computed using Magma’s `MordellWeilGroupGenus2` function. One of the main approaches is to compute the 2-Selmer group  $\text{Sel}^{(2)}(J)$  of the Jacobian  $J$ , using an algorithm of Stoll [429].

Table 6.7: Two-Selmer groups  $\text{Sel}^{(2)}(J)$  of  $J = \text{Jac}(C)$ 

$\text{Sel}^{(2)}(J)$	$(\mathbb{Z}/2\mathbb{Z})$	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^4$
<b>Num curves</b>	158	250	101	3

By computing  $\text{Sel}^{(2)}(J)$  and  $J(\mathbb{Q})[2]$ , this gives an explicit upper bound on the rank  $r$  of  $J(\mathbb{Q})$  given by  $r \leq \dim_{\mathbb{F}_2} \text{Sel}^{(2)}(J) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]$ . In all cases, the rank of  $J(\mathbb{Q})$  was shown to have an unconditional upper bound of 2, and could be computed exactly for all but two of the curves.

We also computed the analytic rank using Dokchitser’s  $L$ -function calculator [145] in Sage, and confirmed this agreed with the bounds obtained in Magma. Where the algebraic rank could not be unconditionally verified, we instead tabulated the

analytic rank, indicated with an asterisk in Table 6.21. We found only two such curves,  $y^2 = -(x^2 + 1)(x^4 + 8x^3 + 18x^2 - 8x + 1)$  of conductor  $2^{18}$  and  $y^2 = -(x^2 + 1)(x^4 + 4x^3 + 10x^2 - 4x + 1)$  of conductor  $2^{20}$ . Both curves have analytic rank 0, where its algebraic rank is at most 2.

In summary, assuming the two curves above have rank 0, we found in total 269 curves (divided into 87 isogeny classes) of rank 0, 202 curves (divided into 67 isogeny classes) of rank 1, and 41 curves (divided into 21 isogeny classes) of rank 2.

### 6.1.6 Endomorphisms of the Jacobian

Recall that the  $F$ -endomorphism ring for an abelian variety  $A/K$ , denoted  $\text{End}(A_F)$ , is the set of homomorphisms  $\varphi : A \rightarrow A$  defined over the field  $F$ , where  $F$  is some extension of  $K$ . We also define the  $F$ -endomorphism algebra as the  $\mathbb{Q}$ -algebra  $\text{End}(A_F) \otimes_{\mathbb{Z}} \mathbb{Q}$ ; i.e. the  $\mathbb{Q}$ -algebra spanned by  $\text{End}(A_F)$ . Many open questions remain regarding the possibilities for  $\text{End}(A_F)$ . A famous conjecture of Coleman [73, Conjecture  $C(e, g)$ ] states that, for a fixed dimension  $d$  and degree  $e$ , there are only finitely many possible rings  $\mathcal{O}$  which are isomorphic to  $\text{End}(A_K)$  for some dimension  $d$  abelian variety  $A/K$  and a field extension  $L/K$  of a number field  $K$  of degree at most  $e$ . Whilst it's still unknown whether there are finitely many possibilities for  $\text{End}(A)$ , even for abelian surfaces  $A/\mathbb{Q}$ , some progress has been made in certain cases, e.g. see Murabayashi–Umegaki [326] for CM principally polarised abelian surfaces or Fité–Guitart [174] for geometrically split abelian surfaces.

For each Jacobian  $J$  of each of our genus 2 curves  $C/\mathbb{Q}$ , we were able to compute the  $\mathbb{Q}$ -endomorphism rings  $\text{End}(J)$ , the  $\mathbb{Q}$ -endomorphism algebras  $\text{End}(J) \otimes \mathbb{Q}$ , and the real endomorphism algebras  $\text{End}(J) \otimes \mathbb{R}$  using Magma code developed by Costa–Mascot–Sijssling–Voight [120]. Furthermore, the geometric endomorphism data  $\text{End}(J_{\overline{\mathbb{Q}}})$ ,  $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ , and  $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$  was also computed using the same code.<sup>3</sup> A summary of the endomorphism algebras  $\text{End}(J) \otimes \mathbb{Q}$  and  $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$  for the Jacobian  $J = \text{Jac}(C)$  of our genus 2 curves are given in Table 6.8 and Table 6.9 respectively.

Table 6.8: Endomorphism algebra  $\text{End}(J) \otimes \mathbb{Q}$  of  $J = \text{Jac}(C)$

$\text{End}(J) \otimes \mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$M_2(\mathbb{Q})$	$K_1$	$K_2$	$K_3$
<b>Num curves</b>	248	200	16	29	3	16
<b>Num isog classes</b>	91	45	8	19	1	11

<sup>3</sup>For the remainder of this chapter, all tensors are over  $\mathbb{Z}$ .

Table 6.9: Geometric endomorphism algebra  $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$  of  $J = \text{Jac}(C)$ 

$\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$\mathbb{Q} \times K_2$	$K_1 \times K_2$	$L_5$
<b>Num curves</b>	104	64	64	32	48	4
<b>Num isog classes</b>	44	24	16	8	8	2

$\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$M_2(\mathbb{Q})$	$M_2(K_1)$	$M_2(K_2)$	$B_6(\mathbb{Q})$
<b>Num curves</b>	116	42	30	8
<b>Num isog classes</b>	49	10	12	2

Here  $B_6(\mathbb{Q})$  denotes the unique (non-split) quaternion algebra over  $\mathbb{Q}$  of discriminant 6. For example, one can take  $B_6(\mathbb{Q}) = (2, 3)_{\mathbb{Q}}$ ; this is the unique associative dimension 4  $\mathbb{Q}$ -algebra with  $\mathbb{Q}$ -basis  $\{1, i, j, k\}$  such that  $i^2 = 2$ ,  $j^2 = 3$ , and  $ij = -ji = k$ .

The same code also allowed us to compute the endomorphism field  $J_{\text{endo}}$  for each Jacobian  $J$ . This is the unique minimal number field over which all geometric endomorphisms of  $J$  are defined, i.e. the smallest field  $E$  such that  $\text{End}(J_E) = \text{End}(J_{\overline{\mathbb{Q}}})$ . A total of 10 possible such minimal fields  $J_{\text{endo}}$  were computed, as shown in Table 6.10.

Table 6.10: The endomorphism field  $J_{\text{endo}}$  of  $J = \text{Jac}(C)$ ; i.e. the smallest number field over which all  $\overline{\mathbb{Q}}$ -endomorphisms of  $J$  are defined

$J_{\text{endo}}$	$\mathbb{Q}$	$K_1$	$K_2$	$K_3$	$L_1$	$L_4$	$L_5$	$M_1$	$M_2$	$M_3$
<b>Num curves</b>	108	88	52	64	102	16	4	2	48	28
<b>Num isog classes</b>	48	26	16	26	21	12	2	2	12	10

### 6.1.7 Sato-Tate group

For an abelian surface  $A/\mathbb{Q}$ , the Sato-Tate group  $\text{ST}(A)$  is a compact Lie subgroup contained in the unitary symplectic group  $\text{USp}(4)$ . Such groups are related to the distributed of the normalised Euler factors  $N(\mathfrak{p})^{-2} L_{\mathfrak{p}}(A/K, \sqrt{N(\mathfrak{p})}T)$  as  $N(\mathfrak{p}) \rightarrow \infty$ . A full definition of  $\text{ST}(A)$  is given in [175, Section 2].

The possible Sato-Tate groups for abelian surfaces was classified by Fité–Kedlaya–Rotger–Sutherland [175] and recently also for abelian threefolds by Fité–Kedlaya–Sutherland [176, 177].

As remarked in [175, p. 1408], the identity component  $\text{ST}^0(J)$  of the Sato-Tate group  $\text{ST}(J)$  is in one-to-one correspondence with the real geometric endomorphism



algebra  $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$ . By applying a classification by Albert (e.g. see [324, Sec 21. Theorem 2]) of finite rank division algebras over  $\mathbb{Q}$ , together with results of Shimura [405], it follows that there are six possibilities for  $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$ , namely  $\mathbb{R}$ ,  $\mathbb{R} \times \mathbb{R}$ ,  $\mathbb{C} \times \mathbb{R}$ ,  $\mathbb{C} \times \mathbb{C}$ ,  $M_2(\mathbb{R})$ , and  $M_2(\mathbb{C})$ . These correspond to the Sato-Tate identity components  $\text{USp}(4)$ ,  $\text{SU}(2) \times \text{SU}(2)$ ,  $\text{U}(1) \times \text{SU}(2)$ ,  $\text{U}(1) \times \text{U}(1)$ ,  $\text{SU}(2)$ , and  $\text{U}(1)$  respectively.

Using the same code of Costa-Mascot-Sijsling-Voight [120], by computing the real geometric endomorphism algebra  $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$ , we can easily read off the identity component  $\text{ST}^0(J)$  of the Sato-Tate group  $\text{ST}(J)$ , given below in Table 6.11.

Table 6.11: Identity component  $\text{ST}^0(J)$  of the Sato-Tate group  $\text{ST}(J)$ , and the corresponding real geometric endomorphism algebra  $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$

$\text{ST}^0(J)$ $\text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$\text{USp}(4)$ $\mathbb{R}$	$\text{SU}(2) \times \text{SU}(2)$ $\mathbb{R} \times \mathbb{R}$	$\text{U}(1) \times \text{SU}(2)$ $\mathbb{C} \times \mathbb{R}$	$\text{U}(1) \times \text{U}(1)$ $\mathbb{C} \times \mathbb{C}$	$\text{SU}(2)$ $M_2(\mathbb{R})$	$\text{U}(1)$ $M_2(\mathbb{C})$
<b>Num curves</b>	104	64	96	52	124	72
<b>Num isog classes</b>	44	24	24	10	51	22

We can easily read off from the endomorphism algebra which curves have  $\text{GL}_2$ -type. In total, there are 248 curves (divided amongst 76  $\mathbb{Q}$ -isogeny classes) which are of  $\text{GL}_2$ -type over  $\mathbb{Q}$  and 64 such curves (divided amongst 24  $\mathbb{Q}$ -isogeny classes) which are of  $\text{GL}_2$ -type over  $\overline{\mathbb{Q}}$ . We also note that none of our curves have  $\text{GL}_2$ -type over both  $\mathbb{Q}$  and  $\overline{\mathbb{Q}}$ .

Finally, using the table of the full Sato-Tate group given in Fité–Kedlaya–Rotger–Sutherland [175, Table 8], we can compute the Sato-Tate group  $\text{ST}(J)$  by computing the endomorphism algebras  $\text{End}(J_K) \otimes \mathbb{Q}$  over all subfields  $K$  of  $J_{\text{endo}}$ .

In particular, we can almost always uniquely determine  $\text{ST}(J)$  from the data of  $(J_{\text{endo}}, \text{End}(J_{\mathbb{Q}}) \otimes \mathbb{Q}, \text{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q})$ . This uniquely determines  $\text{ST}(J)$  for all but 10 curves, for which this could only determine  $\text{ST}(J)$  as being either  $J(C_2)$  or  $D_2$ . As remarked in [175, p. 1419], we can resolve this by computing the endomorphism algebras  $\text{End}(J_{K_1}) \otimes \mathbb{R}$ ,  $\text{End}(J_{K_2}) \otimes \mathbb{R}$ , and  $\text{End}(J_{K_3}) \otimes \mathbb{R}$  where  $K_1, K_2, K_3$  are the three quadratic fields unramified away from 2. In all our cases, this was always some permutation of  $\mathbb{C} \times \mathbb{C}$ ,  $\mathbb{H}$ , and  $M_2(\mathbb{R})$ , thus uniquely determining  $\text{ST}(J)$  for these curves as  $J(C_2)$ .

A summary of the number of genus 2 curves  $C/\mathbb{Q}$  found for each of the 17 Sato-Tate groups obtained in our list is given below in Table 6.12.

Table 6.12: Sato-Tate group  $\mathrm{ST}(J)$  of the Jacobian  $J$  of  $C$ 

$\mathrm{ST}(J)$	$\mathrm{USp}(4)$	$N(\mathrm{SU}(2) \times \mathrm{SU}(2))$	$N(\mathrm{U}(1) \times \mathrm{SU}(2))$	$F_{ac}$	$F_{a,b}$
<b>Num curves</b>	104	64	96	4	48
<b>Num isog classes</b>	44	24	24	2	8

$\mathrm{ST}(J)$	$E_1$	$E_2$	$J(E_1)$	$E_4$	$J(E_2)$	$J(E_4)$
<b>Num curves</b>	4	4	28	16	20	52
<b>Num isog classes</b>	4	2	14	12	5	14

$\mathrm{ST}(J)$	$C_{2,1}$	$J(C_2)$	$D_{2,1}$	$J(C_4)$	$D_{4,1}$	$D_{4,2}$
<b>Num curves</b>	12	10	24	2	4	20
<b>Num isog classes</b>	4	4	4	2	2	6

### 6.1.8 Jacobian decomposition

We recall that, given any abelian variety  $A$  over a number field  $K$ , there exists a unique set of  $K$ -simple abelian subvarieties  $B_1, \dots, B_n$  (unique up to  $K$ -isogeny and ordering) such that  $A$  is  $K$ -isogenous to  $B_1 \times \dots \times B_n$ ; this is the classical Poincaré reducibility statement [324, p. 173]. By thus using the same code of Costa–Mascot–Sijssling–Voight [120], we computed the decomposition of the Jacobian  $\mathrm{Jac}(C)$  up to isogeny.

For each curve  $C$ , we either got that  $\mathrm{Jac}(C)$  is  $\overline{\mathbb{Q}}$ -simple, or computed a number field  $E$  of minimal degree such that  $\mathrm{Jac}(C)$  splits over  $E$ . The minimal degree of a splitting field is given in Table 6.13. We remark that, whilst  $\deg(E)$  is well-defined, the field  $E$  itself is not necessarily unique (unless of course  $E = \mathbb{Q}$ ).

Table 6.13: Minimal degree of a number field  $E$  such that  $\mathrm{Jac}(C)$  splits over  $E$ 

$\deg(E)$	1	2	4	$\infty$
<b>Num curves</b>	216	100	76	120
<b>Num isog classes</b>	53	41	33	48

### 6.1.9 Isogenies

By a classical theorem of Serre (strong multiplicity one) and Faltings’ isogeny theorem [164], two abelian varieties  $A/K$  and  $B/K$  over some number field  $K$  are isogenous if and only if the trace of Frobenius  $\mathrm{tr}\rho_1(\mathrm{Frob}_{\mathfrak{p}})$  and  $\mathrm{tr}\rho_2(\mathrm{Frob}_{\mathfrak{p}})$  are the same over all but finitely primes  $\mathfrak{p}$ , where  $\rho_1$  and  $\rho_2$  denote the  $\ell$ -adic representa-

tions of  $A$  and  $B$  respectively. As discussed in Chapter 4, it was shown by Faltings and Serre that it suffices to check an effectively computable finite set of such primes  $\mathfrak{p}$ , thus giving a effective criterion to determine whether two abelian varieties are isogenous.

By a theorem of Grenié [201, p. 617], two abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2, are isogenous if and only if the traces at the primes  $p \in \{5, 7, 11, 13, 17, 19, 23, 31, 73, 137, 257, 337\}$  coincide. Therefore, we were able to group together the isogeny classes by computing the number of points in the reduction  $\#\tilde{C}_p$  of  $C$ , for all primes  $p$  in the above list. As an additional check, we also confirmed that any two curves which were deemed isogenous by Grenié’s theorem also had their trace coincide for all primes  $p < 10\,000$ .

Whilst this proves which pairs of genus 2 curves  $C/\mathbb{Q}$  have isogenous Jacobians, it doesn’t explicitly construct an isogeny  $\varphi : \text{Jac}(C) \rightarrow \text{Jac}(C')$  between any pair of isogenous Jacobians. In order to actually compute such a map  $\varphi$ , we can follow the same procedure as done in van Wamelen [461, 462] to explicitly construct isogenies between pair of isogenous curves. In particular, this enables us to compute the isogeny degree between pairs of isogenous Jacobians and construct a (partial) isogeny graph (although it cannot guarantee completeness of the isogeny graph).

The full details of such computations are given in van Wamelen [461, 462], however we shall briefly outline the algorithm here: Given a curve  $C/\mathbb{Q}$ , we computed the big period matrix  $P \in M_{2,4}(\mathbb{C})$  given as

$$P := \begin{pmatrix} \int_{B_1} \frac{dx}{y} & \int_{B_2} \frac{dx}{y} & \int_{A_1} \frac{dx}{y} & \int_{A_2} \frac{dx}{y} \\ \int_{B_1} \frac{xdx}{y} & \int_{B_2} \frac{xdx}{y} & \int_{A_1} \frac{xdx}{y} & \int_{A_2} \frac{xdx}{y} \end{pmatrix}$$

where  $A_1, A_2, B_1, B_2$  is a symplectic basis for  $H_1(C, \mathbb{Z})$ . This can be computed in Magma using the `BigPeriodMatrix` function.

Given two curves  $C_1$  and  $C_2$  with big period matrices  $P_1$  and  $P_2$ , we can numerically determine with Magma whether  $J(C_1)$  is  $\overline{\mathbb{Q}}$ -isogenous to  $J(C_2)$  (to sufficiently high precision) by searching for a nonsingular  $4 \times 4$  matrix  $M \in M_4(\mathbb{Z})$  and a  $2 \times 2$  complex matrix  $\alpha \in M_2(\mathbb{C})$  such that  $\alpha P_1 = P_2 M$ ; this can easily be accomplished with Magma’s `IsIsogenous` function.

However, to determine an explicit rational isogeny between  $J(C_1)$  and  $J(C_2)$ , we have to furthermore find such a matrix  $M \in M_4(\mathbb{Z})$  such that  $\alpha \in M_2(\mathbb{Q})$  is rational. To do this, we use Magma’s `AnalyticHomomorphisms` function which returns a  $\mathbb{Z}$ -basis for the  $\mathbb{Z}$ -module of all such matrices  $M \in M_4(\mathbb{Z})$ . By thus searching for

a suitable linear combination of these basis matrices, we hope to find a suitable rational  $\alpha \in \mathbb{M}_2(\mathbb{Q})$ ; this can be done very efficiently using the built-in LLL algorithm implemented in Magma.

Doing this for each pair of genus 2 curves  $C_1, C_2$ , we successfully found an explicit rational isogeny, where the degree of the isogeny can be read off from  $\det(M)$  (as noted in [461, p. 1688]). All computations were done to 1000 bits of precision. As expected, almost all of the isogenies  $\varphi$  were of degree a power of 2, however some were of 3-power and 5-power degree.

Out of the total of 746 pairs of isogenous Jacobians, we found exactly 13 pairs of isogenous Jacobians with an odd isogeny. Five of these had degree  $3^2$  and eight had degree  $5^2$ . We give a list of the odd-degree isogenous curves below in Table 6.14.

Table 6.14: Pairs of non-isomorphic curves  $(C_1, C_2)$  whose Jacobians are  $\mathbb{Q}$ -isogenous of odd degree.

$N$	$\mathbf{ST}(J)$	$C_1$ and $C_2$	$\Delta_{\min}$	$\det(M)$
$2^8$	$E_4$	$(x-1)(x+1)(x^2-2x-1)(x^2+1)$ $-(x-1)(x+1)(x^2+1)(239x^2+2x-239)$	$-2^9$ $-2^9 13^{12}$	$5^2$
$2^{12}$	$E_4$	$x(x^2-2x-1)(x^2+1)$ $(5x+12)(12x-5)(x^2+1)(x^2+2x-1)$	$-2^{19}$ $-2^{19} 13^{12}$	$5^2$
$2^{14}$	$E_4$	$2x(x^2+1)(x^2+2x-1)$ $-2(5x+12)(12x-5)(x^2+1)(x^2+2x-1)$	$-2^{29}$ $-2^{29} 13^{12}$	$5^2$
$2^{14}$	$E_4$	$2x(x^2-2x-1)(x^2+1)$ $2(5x+12)(12x-5)(x^2+1)(x^2+2x-1)$	$-2^{29}$ $-2^{29} 13^{12}$	$5^2$
$2^{16}$	$D_{2,1}$	$(x+44)(x^4-16x^3-164x^2+1056x-3388)$ $-(x+44)(x^4-16x^3-164x^2+1056x-3388)$	$-2^{39} 3^{12} 11^{12}$ $-2^{39} 3^{12} 11^{12}$	$3^2$
$2^{18}$	$J(E_2)$	$x(x^4+4x^3+10x^2+8x+2)$ $-x(x^4+4x^3+10x^2+8x+2)$	$2^{19}$ $2^{19}$	$3^2$
$2^{18}$	$J(E_2)$	$2x(x^4+4x^3+10x^2+8x+2)$ $-2x(x^4+4x^3+10x^2+8x+2)$	$2^{29}$ $2^{29}$	$3^2$
$2^{18}$	$J(E_4)$	$-x(x^4+2x^2+2)$ $x(x^4-478x^2+57122)$	$2^{19}$ $2^{19} 13^{12}$	$5^2$

Table 6.14 (continued).

$N$	$\mathbf{ST}(J)$	$C_1$ and $C_2$	$\Delta_{\min}$	$\mathbf{det}(M)$
$2^{18}$	$J(E_4)$	$-2x(x^4 - 2x^2 + 2)$ $2x(x^4 + 478x^2 + 57122)$	$2^{29}$ $2^{29}13^{12}$	$5^2$
$2^{18}$	$J(E_4)$	$-x(x^4 - 2x^2 + 2)$ $x(x^4 + 478x^2 + 57122)$	$2^{19}$ $2^{19}13^{12}$	$5^2$
$2^{18}$	$J(E_4)$	$-2x(x^4 + 2x^2 + 2)$ $2x(x^4 - 478x^2 + 57122)$	$2^{29}$ $2^{29}13^{12}$	$5^2$
$2^{18}$	$J(E_2)$	$(x-1)(x^4 + 4x^3 + 2x^2 - 4x - 7)$ $-(x-1)(x^4 + 4x^3 + 2x^2 - 4x - 7)$	$-2^{28}$ $-2^{28}$	$3^2$
$2^{18}$	$J(E_2)$	$x(x+1)(x^4 + 4x^2 - 4)$ $-(x-1)x(x^4 + 4x^2 - 4)$	$-2^{28}$ $-2^{28}$	$3^2$

For the 44 isogeny classes with trivial geometric endomorphism ring, we used code by van Bommel–Chidambaram–Costa–Kieffer [459] to verify that our isogeny classes were complete; i.e. any genus 2 curve  $C/\mathbb{Q}$  whose Jacobian  $J$  satisfies  $\text{End}(J_{\overline{\mathbb{Q}}}) = \mathbb{Z}$  and is isogenous to one of our 512 curves in Table 6.21 is guaranteed to also be listed in Table 6.21. For all pairs of curves within these classes, all isogenies were 2-power isogenies.

Finally, we tabulate some statistics on the size of the isogeny classes found, given in Table 6.15. We remark that, whilst many isogeny classes also contain products of elliptic curves over  $\mathbb{Q}$  and Weil restrictions of elliptic curves  $E/K$  over quadratic fields  $K$ , these numbers only count the known Jacobians in each isogeny class.

Table 6.15: Number of isogeny classes in Table 6.20 containing  $n$  known Jacobians.

$\#\mathbf{Jac}(C)$	1	2	3	4	6	8	10
<b>Num isog classes</b>	22	83	6	47	10	6	1

### 6.1.10 Rational points

For each genus 2 curve  $C/\mathbb{Q}$ , we attempted to compute a provably complete list of rational points in  $C(\mathbb{Q})$ . This was done for all the rank 0 curves and some of the rank

1 curves using Stoll's [430] implementation of Chabauty's method combined with the Mordell-Weil sieve in Magma. In summary, we were unable to prove completeness of  $C(\mathbb{Q})$  for 50 out of the 512 curves; 9 of rank 1 and all 41 of rank 2. There were also 187 curves which were not locally solvable everywhere, easily proving in these cases that  $C(\mathbb{Q}) = \emptyset$ .

For curves where Chabauty's method failed, we ran a brute force search for rational points of height up to  $10^7$  using Magma's default **RationalPoints** function. The point with largest height found was  $P = (-\frac{20}{21}, \pm\frac{64931}{21})$  lying on the rank 2 curve  $C : y^2 = x^6 - 4x^5 + 11x^4 - 16x^3 + 11x^2 - 12x + 1$ . It's worth remarking that, with the exception of  $\pm P$  and the pair of points  $(-\frac{4}{17}, \pm\frac{13392}{17})$  on the rank 2 curve  $y^2 = x^6 + 4x^5 - 40x^4 + 32x^3 + 8x^2 - 32x$ , all other rational points found had height less than 500, and so whilst we haven't proven completeness of  $C(\mathbb{Q})$  in all cases, it's reasonable to conjecture that our list of rational points is probably complete.

We give a summary of the values of  $\#C(\mathbb{Q})$  obtained in Table 6.16. We note that the number of rational points  $\#C(\mathbb{Q})$  is always even, as there are always an even number of rational Weierstrass points for all our curves, given the possible field systems that can occur, shown in Table 6.2.

Table 6.16: Number of known rational points  $\#C(\mathbb{Q})$  found on  $C$

$\#C(\mathbb{Q})$	0	2	4	6	8	10	12
<b>Num curves</b>	208	201	75	17	6	3	2

We remark that we found two curves  $C/\mathbb{Q}$  where no known rational points were found,  $C/\mathbb{Q}$  is everywhere locally soluble and Magma's **Chabauty** method failed to prove that  $C(\mathbb{Q}) = \emptyset$ . In these cases, we computed the fake 2-Selmer set using Magma's **TwoCoverDescent** function. For all such curves, we found that the fake 2-Selmer set was empty, which proved that  $C(\mathbb{Q}) = \emptyset$ , as noted by Bruin–Stoll [75].

It's worth mentioning that for bielliptic genus 2 curves of the form  $C : y^2 = f(x^2)$  where  $\text{Jac}(C)$  has rank 2, one can in principle apply the methods of Flynn–Wetherell [179] to practically compute  $C(\mathbb{Q})$ .

We'd conjecture that it should in principle be possible to provably compute  $C(\mathbb{Q})$  for all remaining curves  $C/\mathbb{Q}$  in our list, using a combination of either quadratic Chabauty and/or elliptic Chabauty. We'll leave this as an exercise for future work!

### 6.1.11 $L$ -function and BSD invariants

We computed the analytic rank and leading coefficients of the  $L$ -function  $L(C/\mathbb{Q}, s)$  using Dokchitser’s  $L$ -function calculator [145].<sup>4</sup> Recall that, by the potential modularity results of Boxer–Calegari–Gee–Pilloni [66], we have that the completed  $L$ -function  $\Lambda(s) := N^{s/2} \Gamma_{\mathbb{C}}(s)^2 L(s)$  satisfies the functional equation

$$\Lambda(s) = \varepsilon \Lambda(2 - s)$$

for  $\varepsilon = (-1)^r$  where  $r := \text{ord}_{s=1} L(s)$  is the analytic rank of  $C$ . By computing a sufficient number of Euler factors of  $L(C/\mathbb{Q}, s)$ , this allowed us to compute the leading coefficient  $L^{(r)}(C/\mathbb{Q}, 1)/r!$  to arbitrary precision. In practice, all computations were done to 100 bits of precision.

The Euler factors  $L_p(T)$  at all primes  $p$  (including  $p = 2$ ) were computed using Magma for all curves, and in particular the Euler factors for primes  $p$  of bad reduction for  $C$  was also doubled-checked via the functional equation. We remark that all computed  $L$ -functions had  $L_2(T) = 1$  as their Euler factor at 2, except for the unique conductor  $2^8$  isogeny class, whose Euler factor at 2 was  $L_2(T) = 2T^2 + 2T + 1$ .

For each genus 2 curve  $C/\mathbb{Q}$ , the regulator  $R_{C/\mathbb{Q}}$  was computed using the standard Magma function `MordellWeilGroupGenus2` which computed a set of Mordell–Weil generators for  $J(\mathbb{Q})$ . The Tamagawa numbers  $c_p$  and the real period  $\Omega_{C/\mathbb{Q}}$  was computed using Magma code by van Bommel [458, 457]. Amongst all the invariants computed for our curves, this by far took the longest amount of computation time, with several computations of  $\Omega_{C/\mathbb{Q}}$  and  $c_2$  still ongoing for some of the curves; in some rare cases this took almost 1 CPU-month to compute. In many cases, Magma was unable to compute a regular model for some of the primes  $p$  of bad reduction of  $C/\mathbb{Q}$ , resulting in either the computation failing or the real period  $\Omega_{C/\mathbb{Q}}$  being off possibly by a power of  $p$ .

As the Jacobian of  $C/\mathbb{Q}$  has good reduction at every odd prime, the Tamagawa product depends only the value  $c_2$ . As with the real period, regular models at  $p = 2$ , and thus  $c_2$ , could not always be computed successfully. We remark that in all cases where  $c_2$  could be computed, it was always a power of 2, between 1 and 16. We are unsure whether it can be shown if  $c_2$  is always a power of 2 for genus 2 curves  $C/\mathbb{Q}$  whose Jacobian is good outside 2.<sup>5</sup>

<sup>4</sup>We also note some recent work in progress of Bober–Booker–Costa–Lee–Platt–Sutherland [48] on an alternative motivic  $L$ -function calculator.

<sup>5</sup>This is not true for all genus 2 curves  $C/\mathbb{Q}$ ; for example the modular curve  $X_1(18)$  which has Weierstrass model  $y^2 + (x^3 + x + 1)y = x^5 + 2x^4 + 2x^3 + x^2$  has Tamagawa number  $c_2 = 3$ .

### Tate-Shafarevich group

We now recall the Tate-Shafarevich group  $\text{III}_{A/K}$ , first introduced by Lang–Tate [277] and Shafarevich [472]. Given an abelian variety  $A/K$ , it can be defined as

$$\text{III}_{A/K} := \ker \left( H^1(G_K, A) \rightarrow \prod_{v \in \Sigma_K} H^1(G_{K_v}, A_{K_v}) \right),$$

where  $G_K$  denotes the absolute Galois group of  $K$ . Here the product is taken over all (finite and infinite) places  $v$  of  $K$ . As remarked in [415, p. 333], one can view non-trivial elements of  $\text{III}_{A/K}$  as equivalence classes of homogeneous spaces for  $A/K$  which have a  $K_v$ -rational point for every place  $v$ , but do not have a  $K$ -rational point.<sup>6</sup> It's famously conjectured that  $\text{III}_{A/K}$  is finite, however this is still an open problem, even for elliptic curves  $E/\mathbb{Q}$ .<sup>7</sup>

Computing the Tate-Shafarevich group  $\text{III}_{A/K}$  directly is usually far from trivial. Rather, using our  $L$ -function computation, we compute the analytic order of  $\text{Sha } \text{III}_{\text{an}}(J)$  for all curves as the order of  $\text{III}_{J/\mathbb{Q}}$  predicted by the strong Birch–Swinnerton-Dyer conjecture. This is computed as

$$\text{III}_{\text{an}}(C) := \frac{L^{(r)}(C/\mathbb{Q}, 1)}{r!} \frac{|J(\mathbb{Q})_{\text{tor}}|^2}{\Omega_{C/\mathbb{Q}} \cdot R_{C/\mathbb{Q}} \cdot \prod_p c_p}.$$

To compute  $\text{III}_{\text{an}}$ , we therefore need to compute all the following invariants: the leading coefficient of the  $L$ -function  $L^{(r)}(C/\mathbb{Q}, 1)$ , the regulator  $R_{C/\mathbb{Q}}$ , the torsion subgroup  $J(\mathbb{Q})_{\text{tors}}$ , the real period  $\Omega_{C/\mathbb{Q}}$ , and the Tamagawa numbers  $c_p$ . Whilst  $L^{(r)}(C/\mathbb{Q}, 1)$ ,  $J(\mathbb{Q})_{\text{tors}}$ , and  $R_{C/\mathbb{Q}}$  were all straightforward to compute for all our curves, we were not able to successfully compute the real period and Tamagawa numbers for many of our curves, as remarked above. In total, we were able to exactly compute the real period  $\Omega_{C/\mathbb{Q}}$  for 327 genus 2 curves (and could compute  $\Omega_{C/\mathbb{Q}}$  possibly up to powers of 2, 3, 5, 7 for a further 112 curves), and the Tamagawa number  $c_2$  only for 306 genus 2 curves.

Given the above difficulties, we also undertook an unconditional computation of the 2-rank of  $\text{III}_{J/\mathbb{Q}}$  by computing the 2-Selmer group  $\text{Sel}^{(2)}(J)$  and the rank of

<sup>6</sup>It's sometimes remarked that the Tate-Shafarevich group  $\text{III}_{\text{Jac}(C)/K}$  measures (in some sense) the failure of  $C/K$  to satisfy the Hasse principle, however care should be taken here. There's no guarantee that  $|\text{III}_{J/\mathbb{Q}}|$  can indicate whether the curve  $C/\mathbb{Q}$  itself satisfies the Hasse principle; indeed we do find many curves  $C/\mathbb{Q}$  in our table for which the Hasse principle holds and where  $|\text{III}_{\text{an}}| > 1$ , and conversely find many curves  $C/\mathbb{Q}$  which violate the Hasse principle and where  $|\text{III}_{\text{an}}| = 1$ . An excellent and far more detailed discussion of the relationship between  $\text{III}_{A/K}$  and the Hasse principle is given by Mazur [312].

<sup>7</sup>It has been shown that, for any positive integer  $d \geq 1$ , there exist dimension  $d$  abelian varieties  $A/\mathbb{Q}$  such that  $|\text{III}_{A/\mathbb{Q}}[2]|$  is arbitrarily large [178].



$J(\mathbb{Q})$ . Indeed, via the following exact sequence (e.g. see [415, Theorem X.4.2])

$$0 \rightarrow J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow \text{Sel}^{(2)}(J/\mathbb{Q}) \rightarrow \text{III}_{J/\mathbb{Q}}[2] \rightarrow 0,$$

we can thus explicitly compute the 2-rank of  $\text{III}_{J/\mathbb{Q}}$  as

$$\dim_{\mathbb{F}_2} \text{III}_{J/\mathbb{Q}}[2] = \dim_{\mathbb{F}_2} \text{Sel}^{(2)}(J/\mathbb{Q}) - \text{rank} J(\mathbb{Q}) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2].$$

In the case where  $\dim_{\mathbb{F}_2} \text{III}_{J/\mathbb{Q}}[2] = 0$ , this proves unconditionally that  $|\text{III}_{J/\mathbb{Q}}|$  is odd, thereby avoiding the need to compute the exact power of 2 dividing the Tamagawa product. In the case where  $\dim_{\mathbb{F}_2} \text{III}_{J/\mathbb{Q}}[2] \geq 1$ , this gives only a lower bound for the 2-primary part of  $\text{III}_{J/\mathbb{Q}}$ .

This gave us unconditionally the 2-rank for  $\text{III}$ . For 412 curves, it was rank 0, thus proving that  $|\text{III}|$  is odd (conditional only on the assumption that  $|\text{III}|$  is finite). For 92 curves, it was rank 1; and for 5 curves it was rank 2.

We verified that this agreed with the computation of  $|\text{III}_{J/\mathbb{Q}}|$  up to squares, as predicted by Poonen–Stoll [354], who showed that the order of  $\text{III}_{J/\mathbb{Q}}$  is either a square or twice a square for Jacobians  $J$  of genus 2 curves over  $\mathbb{Q}$ , assuming  $\text{III}$  is finite.

In total, we have (unconditionally) 420 genus 2 curves where  $|\text{III}|$  is square, and 92 curves where  $|\text{III}|$  is twice a square. Amongst the curves for which we were able to deduce the analytic order  $|\text{III}_{\text{an}}|$ , it has the following distribution shown in Table 6.17.

Table 6.17: Analytic order  $|\text{III}_{\text{an}}|$  of the Tate-Shafarevich group (for curves  $C/\mathbb{Q}$  where  $|\text{III}_{\text{an}}|$  could be computed)

$\text{III}_{\text{an}}(C)$	1	2	4	9	18	25	36	49	50	98	$\square$	$2\square$	$4\square$
<b>Num curves</b>	294	49	3	23	10	9	1	6	1	3	133	33	2

### 6.1.12 Mod- $\ell$ Galois images

For a genus 2 curve  $C/\mathbb{Q}$  and positive integer  $m$ , we recall the mod- $m$  Galois representation attached to the Jacobian  $J$  of  $C$ :

$$\bar{\rho}_{C,m} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GSp}_4(\mathbb{Z}/m\mathbb{Z}).$$

By a theorem of Serre [396], if  $\text{End}(J_{\overline{\mathbb{Q}}}) = \mathbb{Z}$ , then the mod- $\ell$  representation  $\bar{\rho}_{C,\ell}$  surjects onto  $\text{GSp}_4(\mathbb{Z}/\ell\mathbb{Z})$  for all but finitely many primes  $\ell$ .

For each of our genus 2 curves  $C/\mathbb{Q}$ , we were able to compute explicitly the mod 2, mod 3, and mod 4 Galois images, i.e.  $\bar{\rho}_{C,m}(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$  for  $m = 2, 3$ , and 4, using Magma code by Shiva Chidambaram [102, 101].<sup>8</sup>

For the 104 curves with trivial geometric endomorphism ring, we also computed the set of nonmaximal primes, i.e. the primes  $\ell$  for which  $\bar{\rho}_{C,\ell}(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) \neq \text{GSp}_4(\mathbb{F}_\ell)$  using code by Banwait–Brumer–Kim–Klagsbrun–Mayle–Srinivasan–Vogt [28] building on an algorithm by Dieulefait [140]. In all our cases where  $\text{End}(J_{\bar{\mathbb{Q}}}) = \mathbb{Z}$ , the only such nonmaximal prime was  $\ell = 2$ .

The distribution of mod 2 images is shown in Table 6.18. Here, we assign the label  $Ni$  to each distinct image, where  $N$  denotes the order of  $\text{Im}(\bar{\rho}_{C,2})$  in  $\text{GSp}_4(\mathbb{F}_2)$ , and  $i$  a letter which uniquely distinguishes that mod 2 image. A full description for each of the mod 2 images is given in the appendix in Table B.1. For reference, we note that the order of  $\text{GSp}_4(\mathbb{F}_2)$  is  $720 = 2^4 \cdot 3^2 \cdot 5$ .

Table 6.18: Image of the mod 2 Galois representation  $\bar{\rho}_{C,2} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GSp}_4(\mathbb{F}_2)$

Mod 2 image	2a	2b	2c	4a	4b	4c	4d	4e
Num curves	2	6	9	12	4	19	15	64

Mod 2 image	4f	4g	8a	8b	8c	8d	8e
Num curves	29	32	68	50	102	60	40

Also using code of Chidambaram [101], we computed the mod 3 Galois image. A total of 33 different conjugacy classes within  $\text{GSp}_4(\mathbb{F}_3)$  were obtained. To save space, we tabulate below in Table 6.19 just the index of  $\text{Im}(\bar{\rho}_{C,3})$  in  $\text{GSp}_4(\mathbb{F}_3)$ , and give a detailed count of the number of genus 2 curves corresponding to each mod 3 image in the appendix in Table B.2. Here, we give a count of the number of conjugacy classes in  $\text{GSp}_4(\mathbb{F}_3)$  found with given index  $n$  and the number of genus 2 curves  $C/\mathbb{Q}$  such that  $\text{Im}(\bar{\rho}_{C,3})$  has index  $n$  in  $\text{GSp}_4(\mathbb{F}_3)$ . For reference, we note that the order of  $\text{GSp}_4(\mathbb{F}_3)$  is  $103\,680 = 2^8 \cdot 3^4 \cdot 5$ .

## 6.2 List of $\mathbb{Q}$ -isogeny classes of abelian surfaces $A/\mathbb{Q}$

We now present our table of all 234 known isogeny classes of abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2. These are ordered first by conductor  $N$ , and then

<sup>8</sup>We note that one can compute the mod 2 image from the action of  $\text{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$  on  $J[2]$ , which can be read off directly from the field system  $[M_1, M_2, \dots, M_m]$  of  $C/\mathbb{Q}$ , as presented in Table A.1. These all agreed with the computations of Chidambaram [102].

Table 6.19: Index of the image of the mod 3 Galois representation  $\bar{\rho}_{C,3} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GSp}_4(\mathbb{F}_3)$ 

$[\text{GSp}_4(\mathbb{F}_3) : \text{Im}(\bar{\rho}_{C,3})]$	<b>1</b>	<b>45</b>	<b>135</b>	<b>270</b>	<b>360</b>	<b>405</b>	<b>540</b>
<b>Num conj classes</b>	1	1	2	2	1	1	3
<b>Num curves</b>	104	32	24	108	8	8	58

$[\text{GSp}_4(\mathbb{F}_3) : \text{Im}(\bar{\rho}_{C,3})]$	<b>1080</b>	<b>1296</b>	<b>1620</b>	<b>2160</b>	<b>3240</b>	<b>6480</b>	<b>12960</b>
<b>Num conj classes</b>	3	1	3	1	6	6	2
<b>Num curves</b>	30	4	72	4	32	24	4











by the degree of a minimal splitting field for  $A/\mathbb{Q}$ . There are eleven columns giving the following information:

1. A positive integer from 1 to 234 uniquely identifying this isogeny class. A link to the corresponding L-function page on the LMFDB [290] for the 111 degree 4 motivic weight 1 rational 2-power conductor L-functions on the LMFDB.
2. The isogeny decomposition of  $A$  over  $\bar{\mathbb{Q}}$ . We give a decomposition over the smallest possible degree number field. Otherwise we say that  $A$  is  $\bar{\mathbb{Q}}$ -simple. We use the LMFDB isogeny class labels for all elliptic curves  $E$  on the LMFDB occurring as isogeny factors of  $A/\mathbb{Q}$ ; otherwise an asterisk indicates an elliptic curve not on the LMFDB.
3. A list of minimal degree number fields over which  $A$  splits.<sup>9</sup> This is empty if  $A$  is  $\bar{\mathbb{Q}}$ -simple.
4. The conductor  $N$  of  $A/\mathbb{Q}$ .
5. The rank of  $A(\mathbb{Q})$ . If we were unable to unconditionally compute the rank, an asterisk indicates that this is only the analytic rank. In all cases, the algebraic rank is unconditionally at most 2.
6. The  $\mathbb{Q}$ -endomorphism algebra  $\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$ . A question mark indicates that we were unable to compute this for a given isogeny class.
7. The geometric  $\bar{\mathbb{Q}}$ -endomorphism algebra  $\text{End}(A_{\bar{\mathbb{Q}}}) \otimes \mathbb{Q}$ .

<sup>9</sup>To save space, we only give a complete list if  $A$  splits over  $\mathbb{Q}$  or a quadratic field. Otherwise, we give one example of a minimal degree splitting field, with three dots (...) indicating this field is not unique.

8. The endomorphism field  $A_{\text{endo}}$ ; i.e. the minimal number field over which  $A$  attains all its endomorphisms over  $\overline{\mathbb{Q}}$ .
9. The Sato-Tate group  $\text{ST}(A)$  of  $A/\mathbb{Q}$ , with links to the corresponding LMFDB pages. To save space, we adopt the same shorthand notation as given in Fité–Kedlaya–Rotger–Sutherland [175, p. 1425], identifying  $G_{1,3}$  and  $G_{3,3}$  with the Sato-Tate groups  $\text{U}(1) \times \text{SU}(2)$  and  $\text{SU}(2) \times \text{SU}(2)$  respectively.
10. The number of known genus 2 curves  $C/\mathbb{Q}$  whose Jacobian  $\text{Jac}(C)$  is  $\mathbb{Q}$ -isogenous to  $A/\mathbb{Q}$ .
11. The leading coefficient at  $s = 1$  of the  $L$ -function  $L(A/\mathbb{Q}, s)$  (given to 9 decimal places).

Table 6.20: A list of the 234 known isogeny classes of abelian surfaces  $A/\mathbb{Q}$  with good reduction away from 2.

Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	# Jac( $C$ )	$L^{(r)}(C, 1)/r!$
 1	$(4.4.2048.1-1.1-a)^2$	$L_4$	$2^8$	0	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	2	0.1344899147
 2	$32a \times 32a$	$\mathbb{Q}$	$2^{10}$	0	$M_2(\mathbb{Q})$	$M_2(K_1)$	$K_1$	$C_{2,1}$	4	0.429699114
 3	$32a \times 64a$	$\mathbb{Q}$	$2^{11}$	0	$\mathbb{Q} \times \mathbb{Q}$	$M_2(K_1)$	$L_1$	$D_{2,1}$	10	0.607486314
 4	$32a \times 128a$	$\mathbb{Q}$	$2^{12}$	1	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	6	0.571965202
 5	$32a \times 128b$	$\mathbb{Q}$	$2^{12}$	0	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	6	0.636924875
 6	$32a \times 128c$	$\mathbb{Q}$	$2^{12}$	0	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	6	0.900464954
 7	$32a \times 128d$	$\mathbb{Q}$	$2^{12}$	0	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	6	0.935487667
 8	$64a \times 64a$	$\mathbb{Q}$	$2^{12}$	0	$M_2(\mathbb{Q})$	$M_2(K_1)$	$K_1$	$C_{2,1}$	4	0.859398227
 9	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-64.1-a)$	$K_3$	$2^{12}$	0	$K_1$	$M_2(K_2)$	$L_1$	$J(C_2)$	3	0.793124183
 10	$(4.4.2048.1-16.1-a)^2$	$L_4$	$2^{12}$	0	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	2	0.925318042
11	$32a \times 256a$	$\mathbb{Q}$	$2^{13}$	1	$\mathbb{Q} \times \mathbb{Q}$	$K_1 \times K_2$	$L_1$	$F_{a,b}$	8	0.792780319
12	$32a \times 256b$	$\mathbb{Q}$	$2^{13}$	1	$\mathbb{Q} \times \mathbb{Q}$	$M_2(K_1)$	$M_2$	$D_{4,2}$	4	0.87978529
13	$32a \times 256c$	$\mathbb{Q}$	$2^{13}$	0	$\mathbb{Q} \times \mathbb{Q}$	$M_2(K_1)$	$M_2$	$D_{4,2}$	4	1.022002486
14	$32a \times 256d$	$\mathbb{Q}$	$2^{13}$	0	$\mathbb{Q} \times \mathbb{Q}$	$K_1 \times K_2$	$L_1$	$F_{a,b}$	8	1.167569713

Draft of 4822 pm, 7:34 Sunday, April 13  
(0822 0073 2273 3019 5346)

---

195

Table 6.20 (continued).






Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(C, 1)/r!$
31	64a $\times$ 256a	$\mathbb{Q}$	$2^{14}$	1	$\mathbb{Q} \times \mathbb{Q}$	$K_1 \times K_2$	$L_1$	$F_{a,b}$	8	1.121460679
32	64a $\times$ 256b	$\mathbb{Q}$	$2^{14}$	1	$\mathbb{Q} \times \mathbb{Q}$	$M_2(K_1)$	$M_2$	$D_{4,2}$	4	1.244204288
33	64a $\times$ 256c	$\mathbb{Q}$	$2^{14}$	0	$\mathbb{Q} \times \mathbb{Q}$	$M_2(K_1)$	$M_2$	$D_{4,2}$	4	1.445329777
34	64a $\times$ 256d	$\mathbb{Q}$	$2^{14}$	0	$\mathbb{Q} \times \mathbb{Q}$	$K_1 \times K_2$	$L_1$	$F_{a,b}$	8	1.651192923
 35	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-1024.1\text{-CMb})$	$K_1, K_3$	$2^{14}$	0	$K_1$	$M_2(K_1)$	$L_1$	$J(C_2)$	2	1.215372628
 36	$\text{Res}_{K_2/\mathbb{Q}}(2.0.8.1-256.1\text{-CMb})$	$K_2, K_3$	$2^{14}$	0	$K_2$	$M_2(K_2)$	$L_1$	$J(C_2)$	3	1.121846977
 37	$(4.4.2048.1-1.1\text{-a})^2$	$L_4$	$2^{14}$	0	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	2	1.67761434
 38	$(4.4.2048.1-16.1\text{-a})^2$	$L_4$	$2^{14}$	0	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	2	0.925318042
 39	4.2.2048.1-32.1-a* $\times$ 4.2.2048.1-32.1-b*	$L_2, \dots$	$2^{14}$	0	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_2$	$J(E_4)$	8	1.053463345
40	128a $\times$ 256a	$\mathbb{Q}$	$2^{15}$	2	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_2$	$K_2$	$N(G_{1,3})$	4	1.055256435
41	128a $\times$ 256b	$\mathbb{Q}$	$2^{15}$	2	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	2	1.171067276
42	128a $\times$ 256c	$\mathbb{Q}$	$2^{15}$	1	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	2	1.360370175
43	128a $\times$ 256d	$\mathbb{Q}$	$2^{15}$	1	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_2$	$K_2$	$N(G_{1,3})$	4	1.55413224
44	128b $\times$ 256a	$\mathbb{Q}$	$2^{15}$	1	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_2$	$K_2$	$N(G_{1,3})$	4	1.17473584
45	128b $\times$ 256b	$\mathbb{Q}$	$2^{15}$	1	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	2	1.303659143
46	128b $\times$ 256c	$\mathbb{Q}$	$2^{15}$	0	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	2	1.514395503
47	128b $\times$ 256d	$\mathbb{Q}$	$2^{15}$	0	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_2$	$K_2$	$N(G_{1,3})$	4	1.730095911

Table 6.20 (continued).






Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(1)/r!$
48	128c $\times$ 256a	$\mathbb{Q}$	$2^{15}$	1	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_2$	$K_2$	$N(G_{1,3})$	4	1.661827358
49	128c $\times$ 256b	$\mathbb{Q}$	$2^{15}$	1	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	2	1.843652441
50	128c $\times$ 256c	$\mathbb{Q}$	$2^{15}$	0	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	2	2.141678659
51	128c $\times$ 256d	$\mathbb{Q}$	$2^{15}$	0	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_2$	$K_2$	$N(G_{1,3})$	4	2.446225101
52	128d $\times$ 256a	$\mathbb{Q}$	$2^{15}$	1	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_2$	$K_2$	$N(G_{1,3})$	4	1.725943079
53	128d $\times$ 256b	$\mathbb{Q}$	$2^{15}$	1	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	2	1.91355952
54	128d $\times$ 256c	$\mathbb{Q}$	$2^{15}$	0	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_1$	$K_1$	$N(G_{1,3})$	2	2.22497718
55	128d $\times$ 256d	$\mathbb{Q}$	$2^{15}$	0	$\mathbb{Q} \times \mathbb{Q}$	$\mathbb{Q} \times K_2$	$K_2$	$N(G_{1,3})$	4	2.54188108
 56	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-512.1-a)$	$K_3$	$2^{15}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	4	1.426909103
 57	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-512.1-b)$	$K_3$	$2^{15}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	4	1.544248813
 58	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-512.1-e)$	$K_3$	$2^{15}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	4	1.641881001
 59	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-512.1-f)$	$K_3$	$2^{15}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	4	1.169557754
60	4.0.512.1-4096.1-a* $\times$ 4.0.512.1-4096.1-b*	$L_7, \dots$	$2^{15}$	0	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_3$	$J(E_4)$	4	1.924003071
61	4.0.512.1-4096.1-a* $\times$ 4.0.512.1-4096.1-b*	$L_7, \dots$	$2^{15}$	1	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_3$	$J(E_4)$	4	1.338415595
 62	256a $\times$ 256a	$\mathbb{Q}$	$2^{16}$	2	$M_2(\mathbb{Q})$	$M_2(K_2)$	$K_2$	$C_{2,1}$	2	1.462652852
63	256a $\times$ 256b	$\mathbb{Q}$	$2^{16}$	2	$\mathbb{Q} \times \mathbb{Q}$	$K_1 \times K_2$	$L_1$	$F_{a,b}$	4	1.623174078
64	256a $\times$ 256c	$\mathbb{Q}$	$2^{16}$	1	$\mathbb{Q} \times \mathbb{Q}$	$K_1 \times K_2$	$L_1$	$F_{a,b}$	4	1.885559992



Table 6.20 (continued).















Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(1)/r!$
 65	256a $\times$ 256d	$\mathbb{Q}$	$2^{16}$	1	$\mathbb{Q} \times \mathbb{Q}$	$M_2(K_2)$	$L_1$	$D_{2,1}$	6	2.1544226597
 66	256b $\times$ 256b	$\mathbb{Q}$	$2^{16}$	2	$M_2(\mathbb{Q})$	$M_2(K_1)$	$K_1$	$C_{2,1}$	0	1.8014211967
 67	256b $\times$ 256c	$\mathbb{Q}$	$2^{16}$	1	$\mathbb{Q} \times \mathbb{Q}$	$M_2(K_1)$	$L_1$	$D_{2,1}$	4	2.0924693852
	256b $\times$ 256d	$\mathbb{Q}$	$2^{16}$	1	$\mathbb{Q} \times \mathbb{Q}$	$K_1 \times K_2$	$L_1$	$F_{a,b}$	4	2.390344738
 69	256c $\times$ 256c	$\mathbb{Q}$	$2^{16}$	0	$M_2(\mathbb{Q})$	$M_2(K_1)$	$K_1$	$C_{2,1}$	0	2.430145257
	256c $\times$ 256d	$\mathbb{Q}$	$2^{16}$	0	$\mathbb{Q} \times \mathbb{Q}$	$K_1 \times K_2$	$L_1$	$F_{a,b}$	4	2.77656442
 71	256d $\times$ 256d	$\mathbb{Q}$	$2^{16}$	0	$M_2(\mathbb{Q})$	$M_2(K_2)$	$K_2$	$C_{2,1}$	2	3.172496734
 72	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-4096.1-\text{CMb})$	$K_1, K_3$	$2^{16}$	0	$K_1$	$M_2(K_1)$	$L_1$	$J(C_2)$	2	1.718796455
 73	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-4096.1-\text{b})$	$K_1, K_3$	$2^{16}$	0	$K_3$	$M_2(K_2)$	$L_1$	$D_{2,1}$	4	1.586248367
 74	$\text{Res}_{K_2/\mathbb{Q}}(2.0.8.1-1024.1-\text{a})$	$K_2, K_3$	$2^{16}$	0	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$L_1$	$J(E_2)$	4	1.386198503
 75	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-1024.1-\text{a})$	$K_3$	$2^{16}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	4	1.654004438
 76	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-1024.1-\text{b})$	$K_3$	$2^{16}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	4	2.082145936
 77	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-1024.1-\text{e})$	$K_3$	$2^{16}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	4	2.022823243
 78	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-1024.1-\text{h})$	$K_3$	$2^{16}$	0	$K_1$	$M_2(\mathbb{Q})$	$K_3$	$E_2$	2	0.943494072
 79	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-1024.1-\text{j})$	$K_3$	$2^{16}$	0	$K_1$	$M_2(\mathbb{Q})$	$K_3$	$E_2$	2	2.036627835
 80	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-1024.1-\text{l})$	$K_3$	$2^{16}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	4	1.790018989
	4.2.1024.1-4096.1-a* $\times$ 4.2.1024.1-4096.1-b*	$L_6, \dots$	$2^{16}$	0	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_3$	$J(E_4)$	4	2.140426323

Table 6.20 (continued).
















Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(C, 1)/r!$
82	$4.2.1024.1-4096.1-a^* \times 4.2.1024.1-4096.1-b^*$	$L_6, \dots$	$2^{16}$	1	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_3$	$J(E_4)$	4	$1.671844993$
 83	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-8192.1-a)$	$K_1$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_1$	$N(G_{3,3})$	2	$2.412492259$
 84	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-8192.1-b)$	$K_1$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_1$	$N(G_{3,3})$	2	$2.490336883$
 85	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-8192.1-e)$	$K_1$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_1$	$N(G_{3,3})$	2	$2.852066328$
 86	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-8192.1-f)$	$K_1$	$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_1$	$N(G_{3,3})$	2	$2.139449425$
 87	$\text{Res}_{K_2/\mathbb{Q}}(2.0.8.1-2048.1-a)$	$K_2$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_2$	$N(G_{3,3})$	2	$1.75451665$
 88	$\text{Res}_{K_2/\mathbb{Q}}(2.0.8.1-2048.1-b)$	$K_2$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_2$	$N(G_{3,3})$	2	$1.866388473$
 89	$\text{Res}_{K_2/\mathbb{Q}}(2.0.8.1-2048.1-e)$	$K_2$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_2$	$N(G_{3,3})$	2	$3.395306422$
 90	$\text{Res}_{K_2/\mathbb{Q}}(2.0.8.1-2048.1-f)$	$K_2$	$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_2$	$N(G_{3,3})$	2	$2.422379626$
 91	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-2048.1-a)$	$K_3$	$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	2	$1.621149711$
 92	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-2048.1-b)$	$K_3$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	2	$2.414964091$
 93	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-2048.1-c)$	$K_3$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	2	$2.627281319$
 94	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-2048.1-d)$	$K_3$	$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	2	$1.375597308$
 95	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-2048.1-e)$	$K_3$	$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	2	$2.197291476$
 96	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-2048.1-f)$	$K_3$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	2	$2.611031462$
 97	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-2048.1-g)$	$K_3$	$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	2	$1.945388369$

Table 6.20 (continued).













Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(C, 1)/r!$
 98	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-2048.1-h)$	$K_3$	$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	2	2.746768338
 99	$\overline{\mathbb{Q}}$ -simple		$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	4	2.720237481
 100	$\overline{\mathbb{Q}}$ -simple		$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	4	1.34573784
 101	$\overline{\mathbb{Q}}$ -simple		$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	4	2.69147569
 102	$\overline{\mathbb{Q}}$ -simple		$2^{17}$	2	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	4	2.123919348
103	$\overline{\mathbb{Q}}$ -simple		$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	4	2.213176835
104	$\overline{\mathbb{Q}}$ -simple		$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	4	1.192999398
105	$\overline{\mathbb{Q}}$ -simple		$2^{17}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	4	3.516318419
106	$\overline{\mathbb{Q}}$ -simple		$2^{17}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	4	1.763521561
 107	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-16384.1-\text{CMc})$	$K_1$	$2^{18}$	2	?	$M_2(K_1)$	?	?	0	3.142787775
 108	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-16384.1-\text{CMd})$	$K_1$	$2^{18}$	0	?	$M_2(K_1)$	?	?	0	2.890659554
 109	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-16384.1-\text{CMf})$	$K_1$	$2^{18}$	0	?	$M_2(K_1)$	?	?	0	2.044004973
 110	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-16384.1-\text{CMh})$	$K_1$	$2^{18}$	0	?	$M_2(K_1)$	?	?	0	2.044004973
 111	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-16384.1-a)$	$K_1$	$2^{18}$	2	$K_3$	$M_2(\mathbb{Q})$	$K_1$	$J(E_1)$	1	3.267072692
 112	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-16384.1-b)$	$K_1$	$2^{18}$	0	?	$M_2(\mathbb{Q})$	?	?	0	1.924003071
 113	$\text{Res}_{K_1/\mathbb{Q}}(2.0.4.1-16384.1-d)$	$K_1$	$2^{18}$	0	$K_3$	$M_2(\mathbb{Q})$	$K_1$	$J(E_1)$	1	2.720951237

Table 6.20 (continued).

















Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(1)/r!$
 114	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-4096.1-a)$	$K_3$	$2^{18}$	0	$K_3$	$M_2(\mathbb{Q})$	$K_3$	$J(E_1)$	1	2.297820699
 115	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-4096.1-b)$	$K_3$	$2^{18}$	0	?	$M_2(\mathbb{Q})$	?	?	0	0.812402299
 116	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-4096.1-c)$	$K_3$	$2^{18}$	0	?	$M_2(\mathbb{Q})$	?	?	0	2.140426323
 117	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-4096.1-d)$	$K_3$	$2^{18}$	0	?	$M_2(\mathbb{Q})$	?	?	0	1.513609967
 118	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-4096.1-e)$	$K_3$	$2^{18}$	1	?	$M_2(K_1)$	?	?	0	3.260282435
 119	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-4096.1-f)$	$K_3$	$2^{18}$	0	?	$M_2(K_1)$	?	?	0	1.718796455
 120	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-4096.1-i)$	$K_3$	$2^{18}$	2	$K_3$	$M_2(\mathbb{Q})$	$K_3$	$J(E_1)$	1	3.433425964
 121	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-4096.1-j)$	$K_3$	$2^{18}$	0	?	$M_2(\mathbb{Q})$	?	?	0	2.819677424
 122	$(4.0.256.1-1048576.1-a^*)^2$	$L_1$	$2^{18}$	1	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$L_1$	$J(E_2)$	2	3.057022756
 123	$(4.2.1024.1-65536.1-a^*)^2$	$L_6, \dots$	$2^{18}$	0	$K_3$	$M_2(K_2)$	$M_3$	$D_{4,2}$	2	4.486587907
 124	$(4.2.1024.1-65536.1-a^*)^2$	$L_6, \dots$	$2^{18}$	2	$K_3$	$M_2(K_2)$	$M_3$	$D_{4,2}$	2	2.342106676
 125	$(4.4.2048.1-16384.1-a^*)^2$	$L_4$	$2^{18}$	2	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	1	2.077318732
 126	$(4.4.2048.1-16384.1-a^*)^2$	$L_4$	$2^{18}$	0	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	1	5.146086025
 127	$(4.4.2048.1-16384.1-b^*)^2$	$L_4$	$2^{18}$	0	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	1	0.862624538
 128	$(4.4.2048.1-16384.1-b^*)^2$	$L_4$	$2^{18}$	$0^*$	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	1	3.450498151
 129	$4.2.2048.1-16384.1-a^* \times 4.2.2048.1-16384.1-b^*$	$L_2, \dots$	$2^{18}$	1	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_2$	$J(E_4)$	4	3.418554923

Table 6.20 (continued).



Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(1)/r!$
 130	4.2.2048.1-16384.1-a* $\times$ 4.2.2048.1-16384.1-b*	$L_2, \dots$	$2^{18}$	1	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_2$	$J(E_4)$	4	2.675411424
 131	$\overline{\mathbb{Q}}$ -simple		$2^{18}$	1	$\mathbb{Q}$	$B_6(\mathbb{Q})$	$L_1$	$J(E_2)$	4	3.198880541
132	$\overline{\mathbb{Q}}$ -simple		$2^{18}$	1	$\mathbb{Q}$	$B_6(\mathbb{Q})$	$L_1$	$J(E_2)$	4	3.187666868
133	$\overline{\mathbb{Q}}$ -simple		$2^{18}$	2	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.60831632
134	$\overline{\mathbb{Q}}$ -simple		$2^{18}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.344591613
135	$\overline{\mathbb{Q}}$ -simple		$2^{18}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.787344584
136	$\overline{\mathbb{Q}}$ -simple		$2^{18}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.661205084
137	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-G^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.904270707
138	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-H^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.798503809
139	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-I^*)$	$K_3$	$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	2.390466408
140	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-J^*)$	$K_3$	$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	0.93603293
141	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-K^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.850801484
142	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-L^*)$	$K_3$	$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	1.549178897
143	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-M^*)$	$K_3$	$2^{19}$	0*	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	2.64750093
144	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-N^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.24099914
145	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-a^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	4.166533159
146	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-b^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.990289603

Table 6.20 (continued).




Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(1)/r!$
147	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-c^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.703542657
148	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-d^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.349469815
149	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-e^*)$	$K_3$	$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	2.30393918
150	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-f^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.896395552
151	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-g^*)$	$K_3$	$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	1.92669986
152	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-j^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.477543788
153	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-q^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.195374002
154	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-r^*)$	$K_3$	$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	2.267833394
155	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-s^*)$	$K_3$	$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	2.971739467
156	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-t^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.279011096
157	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-u^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.922064359
158	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-v^*)$	$K_3$	$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	4.229358371
159	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-w^*)$	$K_3$	$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	2.797071252
160	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-8192.1-x^*)$	$K_3$	$2^{19}$	2	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	4.370886924
 161	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	1.621349005
 162	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.318517443
 163	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.693566774

Table 6.20 (continued).

Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(1)/r!$
<a href="#">lmf db</a> 164	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.512884023
165	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.573458344
166	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	2	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.315945199
167	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	2	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.387600006
168	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.24269801
169	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.157607096
170	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.205176928
171	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	5.271861469
172	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	1.250448067
173	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.424547122
174	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.500896135
175	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	2	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.466411345
176	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.44025885
177	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	2	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.211994296
178	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.019496046
179	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.828713219
180	$\overline{\mathbb{Q}}$ -simple		$2^{19}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.804854188

Draft of 5554  
(422 9m, Sunday, 1555  
3521  
1714  
5512  
3503  
069  
6049  
898  
3883  
099  
9379  
5519  
5217  
2094  
2520  
203










Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	# Jac( $C$ )	$L^{(r)}(A, 1)/r!$
 181	$\text{Res}_{K_2/\mathbb{Q}}(2.0.8.1-16384.1-a)$	$K_2, K_3$	$2^{20}$	2	?	$M_2(K_1)$	?	?	0	$5.85545308$
 182	$\text{Res}_{K_2/\mathbb{Q}}(2.0.8.1-16384.1-b)$	$K_2, K_3$	$2^{20}$	0	?	$M_2(K_1)$	?	?	0	$2.04404973$
183	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-B^*)$	$K_3$	$2^{20}$	1	?	$M_2(\mathbb{Q})$	?	?	0	$4.735216952$
 184	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-C^*)$	$K_3$	$2^{20}$	2	$K_3$	$M_2(\mathbb{Q})$	$K_3$	$J(E_1)$	1	$5.61558684$
 185	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-E^*)$	$K_3$	$2^{20}$	0	$K_3$	$M_2(\mathbb{Q})$	$K_3$	$J(E_1)$	1	$2.617194648$
 186	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-F^*)$	$K_3$	$2^{20}$	0	?	$M_2(\mathbb{Q})$	?	?	0	$3.35522868$
 187	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-G^*)$	$K_3$	$2^{20}$	2	?	$M_2(\mathbb{Q})$	?	?	0	$5.185032858$
188	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-H^*)$	$K_3$	$2^{20}$	0	?	$M_2(\mathbb{Q})$	?	?	0	$2.10692669$
 189	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-I^*)$	$K_3$	$2^{20}$	$0^*$	?	$M_2(\mathbb{Q})$	?	?	0	$3.450498151$
190	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-K^*)$	$K_3$	$2^{20}$	0	?	$M_2(\mathbb{Q})$	?	?	0	$1.48982215$
 191	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-L^*)$	$K_3$	$2^{20}$	0	$K_3$	$M_2(\mathbb{Q})$	$K_3$	$J(E_1)$	1	$3.638832325$
 192	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-N^*)$	$K_3$	$2^{20}$	0	$K_3$	$M_2(\mathbb{Q})$	$K_3$	$J(E_1)$	1	$0.60996766$
193	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-a^*)$	$K_3$	$2^{20}$	2	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	$5.393798017$
194	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-b^*)$	$K_3$	$2^{20}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	$2.765192056$
195	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-c^*)$	$K_3$	$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	$5.152174972$
196	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-d^*)$	$K_3$	$2^{20}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	$3.020943646$
197	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-e^*)$	$K_3$	$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	$4.825209324$



Table 6.20 (continued).










Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(1)/r!$
198	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-f^*)$	$K_3$	$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	3.263371437
199	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-g^*)$	$K_3$	$2^{20}$	0	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	1.955586054
200	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-h^*)$	$K_3$	$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q} \times \mathbb{Q}$	$K_3$	$N(G_{3,3})$	0	4.444648275
201	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-q^*)$	$K_3$	$2^{20}$	1	?	$M_2(K_1)$	?	?	0	4.509133116
202	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-s^*)$	$K_3$	$2^{20}$	1	?	$M_2(K_1)$	?	?	0	4.393484679
 203	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-u^*)$	$K_3$	$2^{20}$	0	?	$M_2(K_1)$	?	?	0	2.044604973
 204	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-v^*)$	$K_3$	$2^{20}$	0	?	$M_2(K_1)$	?	?	0	2.890659554
205	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-y^*)$	$K_3$	$2^{20}$	1	?	$M_2(\mathbb{Q})$	?	?	0	3.90653201
 206	$\text{Res}_{K_3/\mathbb{Q}}(2.2.8.1-16384.1-z^*)$	$K_3$	$2^{20}$	0	?	$M_2(\mathbb{Q})$	?	?	0	1.850636083
207	$(4.2.2048.1-262144.1-c^*)^2$	$L_2, \dots$	$2^{20}$	1	$\mathbb{Q}$	$M_2(K_2)$	$M_2$	$D_{4,1}$	2	4.711863357
 208	$(4.4.2048.1-262144.1-a^*)^2$	$L_4$	$2^{20}$	0	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	1	1.624804598
 209	$(4.4.2048.1-262144.1-a^*)^2$	$L_4$	$2^{20}$	$0^*$	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	1	3.249609196
 210	$(4.4.2048.1-262144.1-b^*)^2$	$L_4$	$2^{20}$	2	$K_1$	$M_2(K_2)$	$M_1$	$J(C_4)$	1	3.457413594
 211	$(4.4.2048.1-262144.1-b^*)^2$	$L_4$	$2^{20}$	0	$K_1$	$M_2(K_2)$	$M_1$	$J(C_4)$	1	4.486587907
 212	$(4.4.2048.1-262144.1-c^*)^2$	$L_4$	$2^{20}$	2	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	1	3.828014111
 213	$(4.4.2048.1-262144.1-c^*)^2$	$L_4$	$2^{20}$	0	$K_1$	$M_2(\mathbb{Q})$	$L_4$	$E_4$	1	5.639354847
214	$4.0.2048.1-262144.1-a^* \times 4.0.2048.1-262144.1-b^*$	$L_3, \dots$	$2^{20}$	1	$\mathbb{Q}$	$M_2(K_2)$	$M_2$	$D_{4,1}$	2	4.192678169

Table 6.20 (continued).

Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(1)/r!$
215	4.2.1024.1-1048576.1-a* $\times$ 4.2.1024.1-1048576.1-b*	$L_6, \dots$	$2^{20}$	1	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_3$	$J(E_4)$	2	6.432872755
216	4.2.1024.1-1048576.1-a* $\times$ 4.2.1024.1-1048576.1-b*	$L_6, \dots$	$2^{20}$	1	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_3$	$J(E_4)$	2	2.8228417
217	4.2.1024.1-1048576.1-c* $\times$ 4.2.1024.1-1048576.1-d*	$L_6, \dots$	$2^{20}$	1	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_3$	$J(E_4)$	2	2.094887677
218	4.2.1024.1-1048576.1-c* $\times$ 4.2.1024.1-1048576.1-d*	$L_6, \dots$	$2^{20}$	1	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_3$	$J(E_4)$	2	8.422556632
219	4.2.2048.1-262144.1-a* $\times$ 4.2.2048.1-262144.1-b*	$L_2, \dots$	$2^{20}$	0	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_2$	$J(E_4)$	2	3.027019935
220	4.2.2048.1-262144.1-a* $\times$ 4.2.2048.1-262144.1-b*	$L_2, \dots$	$2^{20}$	2	$\mathbb{Q}$	$M_2(\mathbb{Q})$	$M_2$	$J(E_4)$	2	4.857483713
221	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.437194136
222	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	1	$\mathbb{Q}$	$L_5$	$L_5$	$F_{ac}$	2	5.11088886
223	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	6.583267814
224	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	2	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	3.181370747
225	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.858417663
226	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.847463254
227	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	1	$\mathbb{Q}$	$L_5$	$L_5$	$F_{ac}$	2	3.58110746
228	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	2	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.375110587
229	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.126613658
230	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	4.052689859
231	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.179041063

Table 6.20 (continued).

Label	Isogeny decomposition	$A_{\text{split}}$	$N$	Rank	$\text{End}(A_{\mathbb{Q}}) \otimes \mathbb{Q}$	$\text{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$A_{\text{endo}}$	$\text{ST}(A)$	$\# \text{Jac}(C)$	$L^{(r)}(C, 1)/r!$
232	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	1.925520147
233	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	1	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	5.607970431
234	$\overline{\mathbb{Q}}$ -simple		$2^{20}$	0	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\text{USp}(4)$	2	2.179041063

### 6.3 List of genus 2 curves $C/\mathbb{Q}$

We now finally arrive at the *pièce de résistance* of this chapter! In a similar spirit to Smart's [418] original list of 366 genus 2 curves  $C/\mathbb{Q}$  with good reduction away from 2, we present our final table of all 512 known genus 2 curves  $C/\mathbb{Q}$  whose Jacobian has good reduction away from 2.

As with Table 6.20, we have ordered all curves by their conductor  $N$  and are grouped together into each of their 175  $\mathbb{Q}$ -isogeny classes. Within each isogeny class, the curves are ordered by absolute discriminant  $|\Delta_{\min}|$ . There are ten columns giving the following information:

1. A number giving the unique label for the isogeny class of  $C/\mathbb{Q}$ , which corresponds to the label of the isogeny class given in Table 6.20.<sup>10</sup>
2. A polynomial  $f(x)$  giving a simplified Weierstrass model  $C : y^2 = f(x)$ , which is also a minimal Weierstrass model wherever possible. If a globally minimal and simplified Weierstrass model for  $C/\mathbb{Q}$  does not exist, a footnote is given with a globally minimal model. Links to the corresponding LMFDB [290] pages are given for the 29 genus 2 curves  $C/\mathbb{Q}$  where  $|\Delta_{\min}| \leq 10^6$ .
3. The field system for  $C/\mathbb{Q}$ .
4. The discriminant  $\Delta_{\min}$  of a globally minimal Weierstrass model for  $C/\mathbb{Q}$ .
5. A unique label corresponding to the  $\overline{\mathbb{Q}}$ -isomorphism class of  $C/\mathbb{Q}$ , as given in Table 6.22.
6. The conductor  $N$  of the Jacobian  $J = \text{Jac}(C)$ .
7. The rank of  $J(\mathbb{Q})$ . If we were unable to unconditionally compute the rank, an asterisk indicates that this is only the analytic rank. In all cases, the algebraic rank is unconditionally at most 2.
8. The torsion subgroup  $J(\mathbb{Q})_{\text{tors}}$  of the Jacobian  $J$  (to save space, we adopt the common shorthand  $\mathbb{Z}/N$  to mean the order  $N$  cyclic group  $\mathbb{Z}/N\mathbb{Z}$ ).
9. The number of rational points in  $C(\mathbb{Q})$ . For curves where completeness has not been proven, an asterisk indicates these are all the known points of height up to  $10^7$ . In the case where there are no known rational points, a subscript <sub>LS</sub> indicates whether the curve is locally solvable everywhere (e.g.  $0_{\text{LS}}$  indicates a curve which violates the Hasse principle).


---

<sup>10</sup>Using the digital version of this thesis, these numbers are all hyperlinked and will take you to the corresponding isogeny class listed in Table 6.20.

10. The automorphism group of  $C$  (over  $\mathbb{Q}$ ).

DRAFT

Table 6.21: A list of 512 known genus 2 curves  $C/\mathbb{Q}$  whose Jacobian has good reduction away from 2.

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut( $C$ )
<b>1</b>	 $(x-1)(x+1)(x^2-2x-1)(x^2+1)^{\text{a}}$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^9$	<b>2a</b>	$2^8$	0	$\mathbb{Z}/2 \times \mathbb{Z}/10$	6	$C_4^2$
	$-(x-1)(x+1)(x^2+1)(239x^2+2x-239)^{\text{b}}$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^9 13^{12}$	<b>26a</b>	$2^8$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2^4$
<b>2</b>	$-(2x-1)(x^2-2x+3)(x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, K_2, K_2]$	$2^{16} 3^{12}$	<b>6a</b>	$2^{10}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_4^2$
	$-3(x^2-2)(x^2+1)(2x^2-1)$	$[K_1, K_3, K_3]$	$-2^{16} 3^{22}$	<b>6a</b>	$2^{10}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$D_{16}^2$
	$3(x^2-2)(x^2+1)(2x^2-1)$	$[K_1, K_3, K_3]$	$-2^{16} 3^{22}$	<b>6a</b>	$2^{10}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/4$	0	$D_{16}^2$
	$-2x(x^4-14x^2+81)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{36} 3^{12}$	<b>6a</b>	$2^{10}$	0	$\mathbb{Z}/4$	2	$C_2^4$
<b>3</b>	$x(x+4)(2x-1)(x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_2]$	$-2^{21} 3^{12}$	<b>6a</b>	$2^{11}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2^2$
	$-x(x+4)(2x-1)(x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_2]$	$-2^{21} 3^{12}$	<b>6a</b>	$2^{11}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2^2$
	$3(x^2-2)(x^2+1)(x^2+4)$	$[K_1, K_1, K_3]$	$2^{21} 3^{22}$	<b>6a</b>	$2^{11}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2^2$
	$-3(x^2-2)(x^2+1)(x^2+4)$	$[K_1, K_1, K_3]$	$2^{21} 3^{22}$	<b>6a</b>	$2^{11}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/4$	0	$C_2^2$
	$-(x^2-2)(x^2+2)(7x^2-16x-14)$	$[K_2, K_3, K_3]$	$-2^{51} 3^{12}$	<b>6a</b>	$2^{11}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0 <sub>LS</sub>	$C_2^2$
	$(x^2-2)(x^2+2)(7x^2+16x-14)$	$[K_2, K_3, K_3]$	$-2^{51} 3^{12}$	<b>6a</b>	$2^{11}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/4$	0	$C_2^2$
	$3(x^2-2)(x^4+68x^2+4)$	$[K_3, L_1]$	$2^{51} 3^{22}$	<b>6a</b>	$2^{11}$	0	$\mathbb{Z}/4$	0	$C_2^2$

<sup>a</sup>A globally minimal model for this curve is  $y^2 + (x^3 + x^2 + x + 1)y = -x^5 - x^4 - x^3 - x^2$ .

<sup>b</sup>A globally minimal model for this curve is  $y^2 + (x^3 + x^2 + x + 1)y = -60x^6 - x^5 + 59x^4 - x^3 + 59x^2 - 60$ .

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
4	$-3(x^2 - 2)(x^4 + 68x^2 + 4)$	$[K_3, L_1]$	$2^{51}3^{22}$	6a	$2^{11}$	0	$\mathbb{Z}/4$	0	$C_2^2$
	$(3x^2 + 2x + 1)(x^4 - 4x^3 - 254x^2 - 252x - 2047)$	$[K_2, L_2]$	$2^{54}3^{12}11^{12}$	66a	$2^{11}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2^2$
	$-(3x^2 + 2x + 1)(x^4 - 4x^3 - 254x^2 - 252x - 2047)$	$[K_2, L_2]$	$2^{54}3^{12}11^{12}$	66a	$2^{11}$	0	$\mathbb{Z}/4$	0	$C_2^2$
	$\text{lmf}_{\text{db}} (x - 2)(x + 2)(x^4 - 4x^2 - 4)^{\text{c}}$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{16}$	2b	$2^{12}$	1	$\mathbb{Z}/8$	6	$C_2^2$
	$-(x^2 - 2)(x^4 - 2x^2 + 2)$	$[K_3, L_7]$	$2^{24}$	2c	$2^{12}$	1	$\mathbb{Z}/8$	6	$C_2^2$
	$(x^2 + 2)(x^4 + 2x^2 + 2)$	$[K_2, L_7]$	$-2^{24}$	2c	$2^{12}$	1	$\mathbb{Z}/4$	4	$C_2^2$
	$(x^2 + 1)(x^4 - 4x^2 - 4)$	$[K_1, L_6]$	$2^{26}$	2b	$2^{12}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$(x^2 + 4)(x^4 + 8x^3 + 4x^2 - 16x + 28)^{\text{d}}$	$[K_1, L_6]$	$2^{16}5^{12}$	10a	$2^{12}$	1	$\mathbb{Z}/4$	4	$C_2^2$
	$-(2x + 1)(x^4 + 4x^3 - 14x^2 - 4x + 41)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{26}5^{12}$	10a	$2^{12}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$\text{lmf}_{\text{db}} (x - 2)(x + 2)(x^4 - 4x^2 + 8)^{\text{e}}$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{19}$	2c	$2^{12}$	0	$\mathbb{Z}/8$	4	$C_2^2$
5	$-(x^2 - 2)(x^4 - 2x^2 - 1)$	$[K_3, L_6]$	$-2^{21}$	2b	$2^{12}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$(x^2 + 2)(x^4 + 2x^2 - 1)$	$[K_2, L_6]$	$2^{21}$	2b	$2^{12}$	0	$\mathbb{Z}/4$	2	$C_2^2$
	$-2(x^2 + 1)(x^4 + 2x^2 + 2)$	$[K_1, L_7]$	$-2^{29}$	2c	$2^{12}$	0	$\mathbb{Z}/4$	0	$C_2^2$
	$-5(x^2 + 2)(x^4 + 14x^2 - 1)$	$[K_2, L_6]$	$2^{21}5^{22}$	10a	$2^{12}$	0	$\mathbb{Z}/2$	0	$C_2^2$

<sup>c</sup> A globally minimal model for this curve is  $y^2 + (x^3)y = -2x^4 + 3x^2 + 4$ .<sup>d</sup> A globally minimal model for this curve is  $y^2 + (x^3)y = 2x^5 + 2x^4 + 4x^3 + 11x^2 - 16x + 28$ .<sup>e</sup> A globally minimal model for this curve is  $y^2 + (x^3)y = -2x^4 + 6x^2 - 8$ .

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
6	$5(x^2 - 2)(x^4 - 14x^2 - 1)$	$[K_3, L_6]$	$-2^{21}5^{22}$	10a	$2^{12}$	0	$\mathbb{Z}/8$	0	$C_2^2$
	$\text{Imf}_{\text{db}} (x^2 + 4)(x^4 + 4x^2 - 4)^{\text{f}}$	$[K_1, L_6]$	$2^{16}$	2b	$2^{12}$	0	$\mathbb{Z}/4$	2	$C_2^2$
	$-(x^2 + 2)(x^4 + 2x^2 + 2)$	$[K_2, L_7]$	$-2^{24}$	2c	$2^{12}$	0	$\mathbb{Z}/8$	0	$C_2^2$
	$(x^2 - 2)(x^4 - 2x^2 + 2)$	$[K_3, L_7]$	$2^{24}$	2c	$2^{12}$	0	$\mathbb{Z}/4$	2	$C_2^2$
	$-(x - 1)(x + 1)(x^4 + 4x^2 - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{26}$	2b	$2^{12}$	0	$\mathbb{Z}/2$	2	$C_2^2$
	$(4x - 1)(4x^4 - 20x^2 + 16x + 7)^{\text{g}}$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{16}5^{12}$	10a	$2^{12}$	0	$\mathbb{Z}/8$	2	$C_2^2$
	$-(x^2 + 1)(4x^4 - 16x^3 + 4x^2 + 8x + 7)$	$[K_1, L_6]$	$2^{26}5^{12}$	10a	$2^{12}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2^2$
7	$\text{Imf}_{\text{db}} (x^2 + 4)(x^4 + 4x^2 + 8)^{\text{h}}$	$[K_1, L_7]$	$-2^{19}$	2c	$2^{12}$	0	$\mathbb{Z}/8$	2	$C_2^2$
	$-(x^2 + 2)(x^4 + 2x^2 - 1)$	$[K_2, L_6]$	$2^{21}$	2b	$2^{12}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$(x^2 - 2)(x^4 - 2x^2 - 1)$	$[K_3, L_6]$	$-2^{21}$	2b	$2^{12}$	0	$\mathbb{Z}/8$	2	$C_2^2$
	$2(x - 1)(x + 1)(x^4 - 2x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}$	2c	$2^{12}$	0	$\mathbb{Z}/4$	2	$C_2^2$
	$-5(x^2 - 2)(x^4 - 14x^2 - 1)$	$[K_3, L_6]$	$-2^{21}5^{22}$	10a	$2^{12}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$5(x^2 + 2)(x^4 + 14x^2 - 1)$	$[K_2, L_6]$	$2^{21}5^{22}$	10a	$2^{12}$	0	$\mathbb{Z}/4$	0	$C_2^2$

<sup>f</sup> A globally minimal model for this curve is  $y^2 + (x^3)y = 2x^4 + 3x^2 - 4$ .<sup>g</sup> A globally minimal model for this curve is  $y^2 + y = 4x^5 - x^4 - 20x^3 + 21x^2 + 3x - 2$ .<sup>h</sup> A globally minimal model for this curve is  $y^2 + (x^3)y = 2x^4 + 6x^2 + 8$ .



Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
8	$-x(x^4 - 14x^2 + 81)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{26}3^{12}$	6a	$2^{12}$	0	$\mathbb{Z}/4$	2	$C_2^2$
	$-2(2x - 1)(x^2 - 2x + 3)(x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, K_2, K_2]$	$2^{26}3^{12}$	6a	$2^{12}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2^2$
	$-6(x^2 - 2)(x^2 + 1)(2x^2 - 1)$	$[K_1, K_3, K_3]$	$-2^{26}3^{22}$	6a	$2^{12}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$D_4$
	$6(x^2 - 2)(x^2 + 1)(2x^2 - 1)$	$[K_1, K_3, K_3]$	$-2^{26}3^{22}$	6a	$2^{12}$	0	$\mathbb{Z}/4 \times \mathbb{Z}/4$	0	$D_4$
9	$\frac{\text{Imf}}{\text{db}} (x - 1)x(x + 1)(x^2 + 1)$	$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_1]$	$-2^{16}$	2d	$2^{12}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2^4$
	$5(3x^2 + 2x + 1)(x^4 + 28x^3 - 30x^2 + 36x - 31)$	$[K_2, L_6]$	$2^{51}5^{22}$	10b	$2^{12}$	0	$\mathbb{Z}/2$	0	$C_2^3$
	$-5(3x^2 - 2x + 1)(x^4 - 28x^3 - 30x^2 - 36x - 31)$	$[K_2, L_6]$	$2^{51}5^{22}$	10b	$2^{12}$	0	$\mathbb{Z}/4$	0	$C_2^3$
10	$\frac{\text{Imf}}{\text{db}} x(x^2 - 2x - 1)(x^2 + 1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{19}$	2a	$2^{12}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_4$
	$(5x + 12)(12x - 5)(x^2 + 1)(x^2 + 2x - 1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{19}13^{12}$	26a	$2^{12}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_4$
11	$-(x^2 + 2)(2x^4 + 4x^2 + 1)$	$[K_2, L_5]$	$-2^{22}$	2e	$2^{13}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$(x^2 - 2)(2x^4 - 4x^2 + 1)$	$[K_3, L_4]$	$2^{22}$	2e	$2^{13}$	1	$\mathbb{Z}/4$	4	$C_2^2$
	$(x - 1)(x + 1)(x^4 - 8x^2 + 8)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{27}$	2e	$2^{13}$	1	$\mathbb{Z}/2$	4	$C_2^2$
	$(x^2 + 1)(x^4 + 8x^2 + 8)$	$[K_1, L_5]$	$-2^{27}$	2e	$2^{13}$	1	$\mathbb{Z}/4$	2	$C_2^2$
	$-(x^2 - 2x - 1)(2x^4 + 8x^3 + 8x^2 - 8x + 7)$	$[K_3, L_5]$	$2^{22}7^{12}$	14a	$2^{13}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$-(2x - 1)(x^4 - 8x^2 + 32x + 136)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{27}7^{12}$	14a	$2^{13}$	1	$\mathbb{Z}/4$	2	$C_2^2$
									$C_{14}^2$

Draft of 4:22 pm, Sunday, April 13, 2025

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>12</b>	$-7(x^2 + 2)(2x^4 - 20x^2 + 1)$	$[K_2, L_4]$	$-2^{22}7^{22}$	14a	$2^{13}$	1	$\mathbb{Z}/4$	0	$C_2^2$
	$7(x^2 + 1)(x^4 - 40x^2 + 8)$	$[K_1, L_4]$	$-2^{27}7^{22}$	14a	$2^{13}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$-(x^2 + 2)(x^4 - 4x^3 + 2x^2 - 4x + 7)$	$[K_2, L_2]$	$2^{22}3^{12}$	6b	$2^{13}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$(x^2 + 2)(x^4 - 4x^3 + 2x^2 - 4x + 7)$	$[K_2, L_2]$	$2^{22}3^{12}$	6b	$2^{13}$	1	$\mathbb{Z}/4$	4	$C_2^2$
	$-3(x^2 - 2)(2x^4 - 8x^2 - 1)$	$[K_3, L_2]$	$-2^{22}3^{22}$	6b	$2^{13}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$3(x^2 - 2)(2x^4 - 8x^2 - 1)$	$[K_3, L_2]$	$-2^{22}3^{22}$	6b	$2^{13}$	1	$\mathbb{Z}/4$	0	$C_2^2$
	$-(2x + 1)(x^4 + 8x^3 - 8x^2 + 8)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{27}3^{12}$	6b	$2^{13}$	0	$\mathbb{Z}/2$	2	$C_2^2$
	$-(2x - 1)(x^4 - 8x^3 - 8x^2 + 8)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{27}3^{12}$	6b	$2^{13}$	0	$\mathbb{Z}/4$	2	$C_2^2$
<b>13</b>	$3(x^2 + 1)(x^4 - 16x^2 - 8)$	$[K_1, L_2]$	$2^{27}3^{22}$	6b	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-3(x^2 + 1)(x^4 - 16x^2 - 8)$	$[K_1, L_2]$	$2^{27}3^{22}$	6b	$2^{13}$	0	$\mathbb{Z}/4$	0	$C_2^2$
	$-(x^2 - 2)(2x^4 - 4x^2 + 1)$	$[K_3, L_4]$	$2^{22}$	2e	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$(x^2 + 2)(2x^4 + 4x^2 + 1)$	$[K_2, L_5]$	$-2^{22}$	2e	$2^{13}$	0	$\mathbb{Z}/4$	0	$C_2^2$
<b>14</b>	$-(x^2 + 1)(x^4 + 8x^2 + 8)$	$[K_1, L_5]$	$-2^{27}$	2e	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-(x - 1)(x + 1)(x^4 - 8x^2 + 8)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{27}$	2e	$2^{13}$	0	$\mathbb{Z}/4$	2	$C_2^2$
	$(x^2 - 2x - 1)(2x^4 + 8x^3 + 8x^2 - 8x + 7)$	$[K_3, L_5]$	$2^{22}7^{12}$	14a	$2^{13}$	0	$\mathbb{Z}/4$	0 <sub>LS</sub>	$C_2^2$
									$C_2^{215}$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
15	$(2x-1)(x^4-8x^2+32x+136)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{27}7^{12}$	14a	$2^{13}$	0	$\mathbb{Z}/2$	2	$C_2^2$
	$7(x^2+2)(2x^4-20x^2+1)$	$[K_2, L_4]$	$-2^{22}7^{22}$	14a	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-7(x^2+1)(x^4-40x^2+8)$	$[K_1, L_4]$	$-2^{27}7^{22}$	14a	$2^{13}$	0	$\mathbb{Z}/4$	0	$C_2^2$
	$\text{lmf}_{\text{db}} (x-1)(x+1)(x^4-2x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{19}$	2c	$2^{13}$	1	$\mathbb{Z}/2$	4	$C_2^2$
	$\text{lmf}_{\text{db}} (x^2+1)(x^4+2x^2+2)$	$[K_1, L_7]$	$-2^{19}$	2c	$2^{13}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$(x^2+6x+1)(x^4+4x^3-2x^2+4x+1)^{\text{i}}$	$[K_3, L_6]$	$-2^{21}$	2b	$2^{13}$	1	$\mathbb{Z}/4$	6	$C_2^2$
	$-(3x^2-2x+3)(x^4+4x^3-2x^2+4x+1)^{\text{j}}$	$[K_2, L_6]$	$2^{21}$	2b	$2^{13}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$5(3x^2+2x+3)(7x^4-4x^3-14x^2-4x+7)^{\text{k}}$	$[K_2, L_6]$	$2^{21}5^{22}$	10a	$2^{13}$	1	$\mathbb{Z}/4$	0	$C_2^2$
	$-5(x^2-6x+1)(7x^4-4x^3-14x^2-4x+7)^{\text{l}}$	$[K_3, L_6]$	$-2^{21}5^{22}$	10a	$2^{13}$	1	$\mathbb{Z}/2$	0	$C_2^2$
16	$-2(x^2+2)(x^4+2x^2+2)$	$[K_2, L_7]$	$-2^{34}$	2c	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$2(x^2-2)(x^4-2x^2+2)$	$[K_3, L_7]$	$2^{34}$	2c	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-2(x-1)(x+1)(x^4+4x^2-4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{36}$	2b	$2^{13}$	0	$\mathbb{Z}/2$	2	$C_2^2$
	$-2(x^2+1)(x^4-4x^2-4)$	$[K_1, L_6]$	$2^{36}$	2b	$2^{13}$	0	$\mathbb{Z}/4$	0	$C_2^2$

<sup>i</sup>A globally minimal model for this curve is  $y^2 + (x^3 + x^2 + x + 1)y = 2x^5 + 5x^4 - 2x^3 + 5x^2 + 2x$ .

<sup>j</sup>A globally minimal model for this curve is  $y^2 + (x^3 + x^2 + x + 1)y = -x^6 - 3x^5 + 2x^4 - 8x^3 + 2x^2 - 3x - 1$ .

<sup>k</sup>A globally minimal model for this curve is  $y^2 + (x^3 + x^2 + x + 1)y = 26x^6 + 2x^5 - 37x^4 - 66x^3 - 37x^2 + 2x + 26$ .

<sup>l</sup>A globally minimal model for this curve is  $y^2 + (x^3 + x^2 + x + 1)y = -9x^6 + 57x^5 - 22x^4 - 96x^3 - 22x^2 + 57x - 9$ .

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
17	$-2(2x-1)(x^4-4x^3-14x^2+4x+41)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{36}5^{12}$	10a	$2^{13}$	0	$\mathbb{Z}/4$	2	$C_2^2$
	$-2(x^2+1)(4x^4-16x^3+4x^2+8x+7)$	$[K_1, L_6]$	$2^{36}5^{12}$	10a	$2^{13}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2^2$
	$\text{Imf}_{\text{db}} -(x^2+1)(x^4+2x^2+2)$	$[K_1, L_7]$	$-2^{19}$	2c	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$\text{Imf}_{\text{db}} -(x-1)(x+1)(x^4-2x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{19}$	2c	$2^{13}$	0	$\mathbb{Z}/2$	2	$C_2^2$
	$-2(x^2-2)(x^4-2x^2-1)$	$[K_3, L_6]$	$-2^{31}$	2b	$2^{13}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2^2$
	$2(x^2+2)(x^4+2x^2-1)$	$[K_2, L_6]$	$2^{31}$	2b	$2^{13}$	0	$\mathbb{Z}/4$	0	$C_2^2$
	$-10(x^2+2)(x^4+14x^2-1)$	$[K_2, L_6]$	$2^{31}5^{22}$	10a	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$10(x^2-2)(x^4-14x^2-1)$	$[K_3, L_6]$	$-2^{31}5^{22}$	10a	$2^{13}$	0	$\mathbb{Z}/4$	0	$C_2^2$
18	$-2(x^2-2)(x^4-2x^2+2)$	$[K_3, L_7]$	$2^{34}$	2c	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$2(x^2+2)(x^4+2x^2+2)$	$[K_2, L_7]$	$-2^{34}$	2c	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$2(x-1)(x+1)(x^4+4x^2-4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{36}$	2b	$2^{13}$	0	$\mathbb{Z}/4$	2	$C_2^2$
	$2(x^2+1)(x^4-4x^2-4)$	$[K_1, L_6]$	$2^{36}$	2b	$2^{13}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2^2$
	$2(2x-1)(x^4-4x^3-14x^2+4x+41)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{36}5^{12}$	10a	$2^{13}$	0	$\mathbb{Z}/2$	2	$C_2^2$
	$2(x^2+1)(4x^4-16x^3+4x^2+8x+7)$	$[K_1, L_6]$	$2^{36}5^{12}$	10a	$2^{13}$	0	$\mathbb{Z}/4$	0	$C_2^2$
19	$\text{Imf}_{\text{db}} -(x-1)x(x+1)(x^2-2x-1)$	$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_3]$	$2^{17}$	2f	$2^{13}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2^{17}$

Draft of 4:22 pm, Sunday, April 13, 2025

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
	$x(x^4 - 8x^3 + 18x^2 + 8x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{25}$	2g	$2^{13}$	0	$\mathbb{Z}/4$	2	$C_2$
	$2x(x^4 - 8x^3 + 18x^2 + 8x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{35}$	2g	$2^{13}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 - 2x - 1)(x^2 - 2x + 3)(3x^2 + 2x + 1)$	$[K_2, K_2, K_3]$	$2^{47}$	2f	$2^{13}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$-7(x^2 + 2x + 3)(31x^4 - 100x^3 + 30x^2 + 36x - 1)$	$[K_2, L_4]$	$-2^{52}7^{22}$	14b	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2$
	$7(x^2 + 2x + 3)(31x^4 - 100x^3 + 30x^2 + 36x - 1)$	$[K_2, L_4]$	$-2^{52}7^{22}$	14b	$2^{13}$	0	$\mathbb{Z}/4$	0	$C_2$
20	$\text{Imf}_{\text{db}} -(x-1)x(x+1)(x^2-2)$	$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_3]$	$2^{15}$	2h	$2^{13}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2$
	$\text{Imf}_{\text{db}} x(x+4)(x^4-12x^2+16x-4)^{\text{m}}$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{17}$	2i	$2^{13}$	0	$\mathbb{Z}/8$	4	$C_2$
	$-2x(x^2+1)(x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_2]$	$2^{25}$	2h	$2^{13}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$-(2x-3)(x^4+4x^3-6x^2-4x+1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{27}$	2i	$2^{13}$	0	$\mathbb{Z}/2$	2	$C_2$
	$3(x^2-2x-1)(x^2-2x+2)(x^2+4x+2)$	$[K_1, K_3, K_3]$	$-2^{22}3^{22}$	6c	$2^{13}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$-3(x^2-4x+2)(x^2+2x-1)(x^2+2x+2)$	$[K_1, K_3, K_3]$	$-2^{22}3^{22}$	6c	$2^{13}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/4$	0	$C_2$
	$21(x^2+4x+8)(17x^4-32x^3-44x^2+80x-4)^{\text{n}}$	$[K_1, L_4]$	$-2^{17}3^{22}7^{22}$	42a	$2^{13}$	0	$\mathbb{Z}/4$	0	$C_2$
	$21(2x^2-2x+1)(x^4+40x^3+44x^2-64x-68)$	$[K_1, L_4]$	$-2^{27}3^{22}7^{22}$	42a	$2^{13}$	0	$\mathbb{Z}/2$	0	$C_2$

<sup>m</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = x^5 - 3x^4 - 8x^3 + 15x^2 - 4x$ .

<sup>n</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = 89x^6 + 189x^5 - 189x^4 - 1848x^3 - 189x^2 + 3276x - 168$ .

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>21</b>	$(x^2 + 1)(x^4 + 1)$	$[K_1, L_1]$	$-2^{22}$	2f	$2^{14}$	2	$\mathbb{Z}/2$	$8^*$	$D_4$
<b>22</b>	$(x^2 - 2x + 2)(x^2 - 2)(x^2 + 2x + 2)$	$[K_1, K_1, K_3]$	$2^{37}$	2f	$2^{14}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$(x^2 - 4x + 2)(x^2 - 2)(x^2 + 4x + 2)$	$[K_3, K_3, K_3]$	$2^{47}$	2f	$2^{14}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$-(x - 1)(x^4 + 40x^3 + 20x^2 + 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{31}3^{12}$	6d	$2^{14}$	1	$\mathbb{Z}/2$	4	$C_2$
	$2(x - 1)(x^4 + 40x^3 + 20x^2 + 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{41}3^{12}$	6d	$2^{14}$	1	$\mathbb{Z}/2$	$2^*$	$C_2$
<b>23</b>	$-x(x^2 - 2x - 1)(x^2 + 2x - 1)$	$[\mathbb{Q}, \mathbb{Q}, K_3, K_3]$	$2^{22}$	2f	$2^{14}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2$
	$(x - 1)(x + 1)(x^4 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{22}$	2f	$2^{14}$	1	$\mathbb{Z}/2$	4	$C_2^2$
	$-(x^2 - 2x - 1)(x^4 - 8x^3 + 18x^2 + 8x + 1)$	$[K_3, L_7]$	$2^{40}$	2g	$2^{14}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>24</b>	$(x^2 - 2x + 2)(x^2 + 2)(x^2 + 2x + 2)$	$[K_1, K_1, K_2]$	$-2^{37}$	2f	$2^{14}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2^2$
	$(x^2 + 2)(x^4 + 12x^2 + 4)$	$[K_2, L_1]$	$-2^{47}$	2f	$2^{14}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$(x^2 - 2x - 1)(x^4 + 4x^3 + 66x^2 - 4x + 577)$	$[K_3, L_5]$	$2^{52}7^{12}$	14b	$2^{14}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>25</b>	$-2(x^2 + 1)(x^4 + 1)$	$[K_1, L_1]$	$-2^{32}$	2f	$2^{14}$	0	$\mathbb{Z}/2$	0	$D_4$
<b>26</b>	$-(x^2 - 2x + 2)(x^2 + 2)(x^2 + 2x + 2)$	$[K_1, K_1, K_2]$	$-2^{37}$	2f	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2^2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut( $C$ )
<b>27</b>	$-(x^2 + 2)(x^4 + 12x^2 + 4)$	$[K_2, L_1]$	$-2^{47}$	2f	$2^{14}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-(x^2 - 2x - 1)(x^4 + 4x^3 + 66x^2 - 4x + 577)$	$[K_3, L_5]$	$2^{52}7^{12}$	14b	$2^{14}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2^2$
	$-x(x^4 + 6x^2 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{22}$	2f	$2^{14}$	0	$\mathbb{Z}/2$	2	$C_2^2$
	$-2x(x^2 - 2x - 1)(x^2 + 2x - 1)$	$[\mathbb{Q}, \mathbb{Q}, K_3, K_3]$	$2^{32}$	2f	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2^2$
	$-(x^2 + 2x - 1)(5x^4 + 8x^3 - 6x^2 - 8x + 5)$	$[K_3, L_7]$	$2^{40}$	2g	$2^{14}$	0	$\mathbb{Z}/4$	0	$C_2^2$
<b>28</b>	$-(x^2 + 1)(x^4 + 1)$	$[K_1, L_1]$	$-2^{22}$	2f	$2^{14}$	0	$\mathbb{Z}/2$	0	$D_4$
<b>29</b>	$-(x^2 - 2x + 2)(x^2 - 2)(x^2 + 2x + 2)$	$[K_1, K_1, K_3]$	$2^{37}$	2f	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2^2$
	$-(x^2 - 4x + 2)(x^2 - 2)(x^2 + 4x + 2)$	$[K_3, K_3, K_3]$	$2^{47}$	2f	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2^2$
	$(x - 1)(x^4 + 40x^3 + 20x^2 + 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{31}3^{12}$	6d	$2^{14}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-2(x - 1)(x^4 + 40x^3 + 20x^2 + 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{41}3^{12}$	6d	$2^{14}$	0	$\mathbb{Z}/2$	2	$C_2$
<b>30</b>	$2(x^2 + 1)(x^4 + 1)$	$[K_1, L_1]$	$-2^{32}$	2f	$2^{14}$	0	$\mathbb{Z}/2$	0	$D_4$
<b>31</b>	$(x^2 + 8)(x^4 + 8x^2 + 8)^{\circ}$	$[K_2, L_5]$	$-2^{22}$	2e	$2^{14}$	1	$\mathbb{Z}/4$	4	$C_2^2$

<sup>◦</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = 4x^4 + 18x^2 + 16$ .

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>32</b>	$-(x^2 + 4)(x^4 + 4x^2 + 2)$	$[K_1, L_5]$	$-2^{27}$	2e	$2^{14}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$(x - 2)(x + 2)(x^4 - 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{27}$	2e	$2^{14}$	1	$\mathbb{Z}/8$	4	$C_2^2$
	$-2(x^2 - 2)(2x^4 - 4x^2 + 1)$	$[K_3, L_4]$	$2^{32}$	2e	$2^{14}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$(x^2 - 4x - 4)(x^4 + 8x^3 + 16x^2 - 32x + 56)^{\text{p}}$	$[K_3, L_5]$	$2^{22}7^{12}$	14a	$2^{14}$	1	$\mathbb{Z}/4$	4	$C_2^2$
	$-(4x + 1)(2x^4 - 4x^2 - 8x + 17)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{27}7^{12}$	14a	$2^{14}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$-7(x^2 + 4)(x^4 - 20x^2 + 2)$	$[K_1, L_4]$	$-2^{27}7^{22}$	14a	$2^{14}$	1	$\mathbb{Z}/8$	0	$C_2^2$
	$14(x^2 + 2)(2x^4 - 20x^2 + 1)$	$[K_2, L_4]$	$-2^{32}7^{22}$	14a	$2^{14}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$-x(x + 4)(x^4 - 4x^2 + 8x + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{27}3^{12}$	6b	$2^{14}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$(x - 4)x(x^4 - 4x^2 - 8x + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{27}3^{12}$	6b	$2^{14}$	1	$\mathbb{Z}/4$	6	$C_2^2$
	$3(x^2 + 4)(x^4 + 8x^2 - 2)$	$[K_1, L_2]$	$2^{27}3^{22}$	6b	$2^{14}$	1	$\mathbb{Z}/4$	0	$C_2^2$
	$-3(x^2 + 4)(x^4 + 8x^2 - 2)$	$[K_1, L_2]$	$2^{27}3^{22}$	6b	$2^{14}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$-(3x^2 + 4x + 4)(x^4 - 8x^3 - 8x^2 + 8)^{\text{q}}$	$[K_2, L_2]$	$2^{22}3^{12}$	6b	$2^{14}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$2(x^2 + 2)(x^4 - 4x^3 + 2x^2 - 4x + 7)$	$[K_2, L_2]$	$2^{32}3^{12}$	6b	$2^{14}$	0	$\mathbb{Z}/4$	0	$C_2^2$
	$-3(x^2 - 8)(x^4 - 16x^2 - 8)^{\text{r}}$	$[K_3, L_2]$	$-2^{22}3^{22}$	6b	$2^{14}$	0	$\mathbb{Z}/2$	0	$C_2^2$

<sup>p</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = x^5 - 5x^4 - 32x^3 + 30x^2 - 24x - 56$ .<sup>q</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = -x^6 + 5x^5 + 13x^4 + 16x^3 + 2x^2 - 8x - 8$ .<sup>r</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = -x^6 + 18x^4 - 90x^2 - 48$ .



Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>34</b>	$6(x^2 - 2)(2x^4 - 8x^2 - 1)$	$[K_3, L_2]$	$-2^{32}3^{22}$	6b	$2^{14}$	0	$\mathbb{Z}/4$	0	$C_2$
	$(x^2 - 8)(x^4 - 8x^2 + 8)^s$	$[K_3, L_4]$	$2^{22}$	2e	$2^{14}$	0	$\mathbb{Z}/8$	2	$C_2$
	$(x^2 + 4)(x^4 + 4x^2 + 2)$	$[K_1, L_5]$	$-2^{27}$	2e	$2^{14}$	0	$\mathbb{Z}/4$	2	$C_2$
	$-(x - 2)(x + 2)(x^4 - 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{27}$	2e	$2^{14}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-2(x^2 + 2)(2x^4 + 4x^2 + 1)$	$[K_2, L_5]$	$-2^{32}$	2e	$2^{14}$	0	$\mathbb{Z}/2$	0	$C_2$
	$-(4x - 1)(2x^4 - 4x^2 + 8x + 17)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{27}7^{12}$	14a	$2^{14}$	0	$\mathbb{Z}/4$	2	$C_2$
	$-2(x^2 + 2x - 1)(2x^4 - 8x^3 + 8x^2 + 8x + 7)$	$[K_3, L_5]$	$2^{32}7^{12}$	14a	$2^{14}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2^2$
	$-7(x^2 + 8)(x^4 - 40x^2 + 8)^t$	$[K_2, L_4]$	$-2^{22}7^{22}$	14a	$2^{14}$	0	$\mathbb{Z}/8$	0	$C_2^2$
<b>35</b>	$7(x^2 + 4)(x^4 - 20x^2 + 2)$	$[K_1, L_4]$	$-2^{27}7^{22}$	14a	$2^{14}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-3(x^2 - 2x - 1)(x^2 + 4x + 5)(5x^2 - 4x + 1)$	$[K_1, K_1, K_3]$	$2^{41}3^{22}$	6a	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
<b>36</b>	$3(x^2 - 2x - 1)(17x^4 + 4x^3 + 34x^2 - 4x + 17)$	$[K_3, L_1]$	$2^{51}3^{22}$	6a	$2^{14}$	0	$\mathbb{Z}/2$	0	$C_2$
	$-x(x^2 - 2x + 2)(x^2 + 2x + 2)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_1]$	$2^{26}$	2d	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$-5(x^2 - 4x + 2)(x^4 + 32x^3 + 60x^2 + 64x + 4)$	$[K_3, L_6]$	$-2^{51}5^{22}$	10b	$2^{14}$	0	$\mathbb{Z}/4$	0	$C_2$

<sup>s</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = -4x^4 + 18x^2 - 16$ .

<sup>t</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = -2x^6 + 56x^4 + 546x^2 - 112$ .

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
	$5(x^2 - 4x + 2)(x^4 + 32x^3 + 60x^2 + 64x + 4)$	$[K_3, L_6]$	$-2^{51}5^{22}$	10b	$2^{14}$	0	$\mathbb{Z}/2$	0	$C_2$
37	$2x(x^2 + 1)(x^2 + 2x - 1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{29}$	2a	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$-2(5x + 12)(12x - 5)(x^2 + 1)(x^2 + 2x - 1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{29}13^{12}$	26a	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
38	$2x(x^2 - 2x - 1)(x^2 + 1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{29}$	2a	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$2(5x + 12)(12x - 5)(x^2 + 1)(x^2 + 2x - 1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{29}13^{12}$	26a	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
39	$\frac{\text{Inf}}{\text{db}} -x(x^2 + 1)(x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_2]$	$2^{15}$	2h	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$-2(x - 1)x(x + 1)(x^2 - 2)$	$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_3]$	$2^{25}$	2h	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2$
	$-2(2x - 3)(x^4 + 4x^3 - 6x^2 - 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{37}$	2i	$2^{14}$	0	$\mathbb{Z}/2$	2	$C_2$
	$2(2x - 3)(x^4 + 4x^3 - 6x^2 - 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{37}$	2i	$2^{14}$	0	$\mathbb{Z}/4$	2	$C_2$
	$6(x^2 - 2x - 1)(x^2 - 2x + 2)(x^2 + 4x + 2)$	$[K_1, K_3, K_3]$	$-2^{32}3^{22}$	6c	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$-6(x^2 - 4x + 2)(x^2 + 2x - 1)(x^2 + 2x + 2)$	$[K_1, K_3, K_3]$	$-2^{32}3^{22}$	6c	$2^{14}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$42(2x^2 - 2x + 1)(x^4 + 40x^3 + 44x^2 - 64x - 68)$	$[K_1, L_4]$	$-2^{37}3^{22}7^{22}$	42a	$2^{14}$	0	$\mathbb{Z}/2$	0	$C_2$
	$-42(2x^2 - 2x + 1)(x^4 + 40x^3 + 44x^2 - 64x - 68)$	$[K_1, L_4]$	$-2^{37}3^{22}7^{22}$	42a	$2^{14}$	0	$\mathbb{Z}/4$	0	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>40</b>	$(x^2 + 4)(x^4 - 8)^{\text{u}}$	$[K_1, L_2]$	$2^{21}$	<b>2j</b>	$2^{15}$	2	$\mathbb{Z}/2$	$6^*$	$C_2^2$
	$(x^2 - 2)(x^4 - 2)$	$[K_3, L_2]$	$-2^{26}$	<b>2j</b>	$2^{15}$	2	$\mathbb{Z}/2$	$12^*$	$C_2^2$
	$(x - 4)x(x^4 + 8x^3 - 8x^2 + 8)^{\text{v}}$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}3^{12}$	<b>6e</b>	$2^{15}$	2	$\mathbb{Z}/2$	$10^*$	$C_2^2$
	$(x^2 + 2)(x^4 - 4x^2 - 8x + 2)$	$[K_2, L_2]$	$2^{26}3^{12}$	<b>6e</b>	$2^{15}$	2	$\mathbb{Z}/2$	$8^*$	$C_2^2$
<b>41</b>	$(x^2 - 2)(x^4 - 4x^2 + 2)$	$[K_3, L_4]$	$2^{26}$	<b>2k</b>	$2^{15}$	2	$\mathbb{Z}/2$	$10^*$	$C_2^2$
	$(x^2 + 2)(x^4 + 4x^2 + 2)$	$[K_2, L_5]$	$-2^{26}$	<b>2k</b>	$2^{15}$	2	$\mathbb{Z}/2$	$8^*$	$C_2^2$
<b>42</b>	$(x - 2)(x + 2)(x^4 - 8x^2 + 8)^{\text{w}}$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	<b>2k</b>	$2^{15}$	1	$\mathbb{Z}/2$	4	$C_2^2$
	$(x^2 + 4)(x^4 + 8x^2 + 8)^{\text{x}}$	$[K_1, L_5]$	$-2^{21}$	<b>2k</b>	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2^2$
<b>43</b>	$(x - 2)(x + 2)(x^4 - 8)^{\text{y}}$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}$	<b>2j</b>	$2^{15}$	1	$\mathbb{Z}/2$	4	$C_2^2$
	$(x^2 + 2)(x^4 - 2)$	$[K_2, L_2]$	$2^{26}$	<b>2j</b>	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$-3(x^2 + 4)(x^4 - 16x^2 - 8)^{\text{z}}$	$[K_1, L_2]$	$2^{21}3^{22}$	<b>6e</b>	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2^2$

<sup>u</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = x^4 - 2x^2 - 8$ .<sup>v</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = x^5 - 10x^4 + 8x^3 + 2x^2 - 8x$ .<sup>w</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = -3x^4 + 10x^2 - 8$ .<sup>x</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = 3x^4 + 10x^2 + 8$ .<sup>y</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = -x^4 - 2x^2 + 8$ .<sup>z</sup>A globally minimal model for this curve is  $y^2 + (x^3)y = -x^6 + 9x^4 + 54x^2 + 24$ .

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>44</b>	$-3(x^2 - 2)(x^4 + 8x^2 - 2)$	$[K_3, L_2]$	$-2^{26}3^{22}$	6e	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$(x^2 + 1)(x^4 - 2)$	$[K_1, L_2]$	$2^{21}$	2j	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$-2(x^2 - 2)(x^4 - 2)$	$[K_3, L_2]$	$-2^{36}$	2j	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$-(2x + 1)(x^4 - 4x^2 - 8x + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}3^{12}$	6e	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$-2(x^2 + 2)(x^4 - 4x^2 - 8x + 2)$	$[K_2, L_2]$	$2^{36}3^{12}$	6e	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2^2$
<b>45</b>	$-(x^2 + 1)(x^4 + 4x^2 + 2)$	$[K_1, L_5]$	$-2^{21}$	2k	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$(x - 1)(x + 1)(x^4 - 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	2k	$2^{15}$	1	$\mathbb{Z}/2$	4	$C_2^2$
<b>46</b>	$-2(x^2 + 2)(x^4 + 4x^2 + 2)$	$[K_2, L_5]$	$-2^{36}$	2k	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-2(x^2 - 2)(x^4 - 4x^2 + 2)$	$[K_3, L_4]$	$2^{36}$	2k	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
<b>47</b>	$-(x - 1)(x + 1)(x^4 - 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}$	2j	$2^{15}$	0	$\mathbb{Z}/2$	2	$C_2^2$
	$-2(x^2 + 2)(x^4 - 2)$	$[K_2, L_2]$	$2^{36}$	2j	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-3(x^2 + 1)(x^4 + 8x^2 - 2)$	$[K_1, L_2]$	$2^{21}3^{22}$	6e	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$6(x^2 - 2)(x^4 + 8x^2 - 2)$	$[K_3, L_2]$	$-2^{36}3^{22}$	6e	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>48</b>	$-(x^2 + 2)(x^4 - 2)$	$[K_2, L_2]$	$2^{26}$	<b>2j</b>	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$-2(x - 1)(x + 1)(x^4 - 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{31}$	<b>2j</b>	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$3(x^2 - 2)(x^4 + 8x^2 - 2)$	$[K_3, L_2]$	$-2^{26}3^{22}$	<b>6e</b>	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$-6(x^2 + 1)(x^4 + 8x^2 - 2)$	$[K_1, L_2]$	$2^{31}3^{22}$	<b>6e</b>	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2^2$
<b>49</b>	$-(x^2 + 2)(x^4 + 4x^2 + 2)$	$[K_2, L_5]$	$-2^{26}$	<b>2k</b>	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2^2$
	$-(x^2 - 2)(x^4 - 4x^2 + 2)$	$[K_3, L_4]$	$2^{26}$	<b>2k</b>	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2^2$
<b>50</b>	$-2(x^2 + 1)(x^4 + 4x^2 + 2)$	$[K_1, L_5]$	$-2^{31}$	<b>2k</b>	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$2(x - 1)(x + 1)(x^4 - 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{31}$	<b>2k</b>	$2^{15}$	0	$\mathbb{Z}/2$	2	$C_2^2$
<b>51</b>	$-(x^2 - 2)(x^4 - 2)$	$[K_3, L_2]$	$-2^{26}$	<b>2j</b>	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$2(x^2 + 1)(x^4 - 2)$	$[K_1, L_2]$	$2^{31}$	<b>2j</b>	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-(x^2 + 2)(x^4 - 4x^2 - 8x + 2)$	$[K_2, L_2]$	$2^{26}3^{12}$	<b>6e</b>	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$-2(2x + 1)(x^4 - 4x^2 - 8x + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{31}3^{12}$	<b>6e</b>	$2^{15}$	0	$\mathbb{Z}/2$	2	$C_2^2$
<b>52</b>	$(x - 1)(x + 1)(x^4 - 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}$	<b>2j</b>	$2^{15}$	1	$\mathbb{Z}/2$	4	$C_2^2$
	$2(x^2 + 2)(x^4 - 2)$	$[K_2, L_2]$	$2^{36}$	<b>2j</b>	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2^2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>53</b>	$3(x^2 + 1)(x^4 + 8x^2 - 2)$	$[K_1, L_2]$	$2^{21}3^{22}$	6e	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2$
	$-6(x^2 - 2)(x^4 + 8x^2 - 2)$	$[K_3, L_2]$	$-2^{36}3^{22}$	6e	$2^{15}$	1	$\mathbb{Z}/2$	0	$C_2$
	$(x^2 + 1)(x^4 + 4x^2 + 2)$	$[K_1, L_5]$	$-2^{21}$	2k	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x - 1)(x + 1)(x^4 - 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	2k	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>54</b>	$2(x^2 + 2)(x^4 + 4x^2 + 2)$	$[K_2, L_5]$	$-2^{36}$	2k	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2$
	$2(x^2 - 2)(x^4 - 4x^2 + 2)$	$[K_3, L_4]$	$2^{36}$	2k	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>55</b>	$-(x^2 + 1)(x^4 - 2)$	$[K_1, L_2]$	$2^{21}$	2j	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$2(x^2 - 2)(x^4 - 2)$	$[K_3, L_2]$	$-2^{36}$	2j	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
	$(2x + 1)(x^4 - 4x^2 - 8x + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}3^{12}$	6e	$2^{15}$	0	$\mathbb{Z}/2$	2	$C_2^2$
	$2(x^2 + 2)(x^4 - 4x^2 - 8x + 2)$	$[K_2, L_2]$	$2^{36}3^{12}$	6e	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2^2$
<b>56</b>	$(x + 1)(x^2 - 2x - 1)(x^2 + 1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{23}$	2l	$2^{15}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 1)(x^4 + 4x^3 - 6x^2 + 12x - 7)$	$[K_1, L_6]$	$2^{42}$	2m	$2^{15}$	0	$\mathbb{Z}/4$	0	$C_2$
	$-(x^2 - 2x - 1)(x^4 - 12x^3 + 18x^2 + 44x + 17)$	$[K_3, L_4]$	$2^{50}$	2n	$2^{15}$	0	$\mathbb{Z}/4$	$0_{\text{LS}}$	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>57</b>	$-(2x^2 + 1)(4x^4 - 4x^2 + 32x - 31)$	$[K_2, L_2]$	$2^{50}3^{12}$	6f	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2$
	$x(x^2 - 2x + 2)(x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_2]$	$2^{23}$	2l	$2^{15}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$-x(x^4 - 8x^3 + 12x^2 - 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{32}$	2m	$2^{15}$	0	$\mathbb{Z}/4$	2	$C_2$
	$(x^2 + 2)(7x^4 - 16x^3 + 36x^2 - 32x + 28)$	$[K_2, L_5]$	$-2^{50}$	2n	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>58</b>	$3(x^2 + 4x + 2)(x^4 - 16x^3 - 4x^2 - 32x + 4)$	$[K_3, L_2]$	$-2^{50}3^{22}$	6f	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2$
	$(x - 1)(x^2 + 1)(x^2 + 2x - 1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{23}$	2l	$2^{15}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2$
	$(x^2 + 1)(x^4 + 4x^3 - 6x^2 + 12x - 7)$	$[K_1, L_6]$	$2^{42}$	2m	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2$
	$(x^2 - 2x - 1)(x^4 - 12x^3 + 18x^2 + 44x + 17)$	$[K_3, L_4]$	$2^{50}$	2n	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>59</b>	$(2x^2 + 1)(4x^4 - 4x^2 - 32x - 31)$	$[K_2, L_2]$	$2^{50}3^{12}$	6f	$2^{15}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-x(x^2 - 2x + 2)(x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_2]$	$2^{23}$	2l	$2^{15}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$x(x^4 - 8x^3 + 12x^2 - 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{32}$	2m	$2^{15}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 2)(7x^4 + 16x^3 + 36x^2 + 32x + 28)$	$[K_2, L_5]$	$-2^{50}$	2n	$2^{15}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>60</b>	$-3(x^2 - 4x + 2)(x^4 + 16x^3 - 4x^2 + 32x + 4)$	$[K_3, L_2]$	$-2^{50}3^{22}$	6f	$2^{15}$	0	$\mathbb{Z}/4$	0	$C_2$
	$-(x - 1)(x^2 - 2x - 1)(x^2 + 1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{23}$	2o	$2^{15}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>61</b>	$(x-1)(x^4+8x^3+4x^2-16x+4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2p	$2^{15}$	0	$\mathbb{Z}/4$	2	$C_4$
	$-2(x-1)(x^4+8x^3+4x^2-16x+4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{39}$	2p	$2^{15}$	0	$\mathbb{Z}/2$	2	$C_4$
	$-(x^2-2x-1)(x^2+2x-1)(x^2+2x+3)$	$[K_2, K_3, K_3]$	$-2^{43}$	2o	$2^{15}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$-(x+1)(x^2+1)(x^2+2x-1)$	$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$-2^{23}$	2o	$2^{15}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_4$
	$-(x-1)(x^4+8x^3+4x^2-16x+4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2p	$2^{15}$	1	$\mathbb{Z}/2$	4	$C_4$
	$2(x-1)(x^4+8x^3+4x^2-16x+4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{39}$	2p	$2^{15}$	1	$\mathbb{Z}/4$	4	$C_4$
	$(x^2-2x-1)(x^2+2x-1)(x^2+2x+3)$	$[K_2, K_3, K_3]$	$-2^{43}$	2o	$2^{15}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
<b>62</b>	$(x^2-2x-1)(x^2+1)(x^2+2x-1)$	$[K_1, K_3, K_3]$	$-2^{36}$	2d	$2^{16}$	2	$\mathbb{Z}/2 \times \mathbb{Z}/2$	$4^*$	$D_4$
	$(x^2-2)(x^4+12x^2+4)$	$[K_3, L_1]$	$2^{51}$	2d	$2^{16}$	2	$\mathbb{Z}/2$	$2^*$	$C_2^2$
<b>63</b>	$-(x^2+1)(x^4-2x^2-1)$	$[K_1, L_6]$	$2^{24}$	2q	$2^{16}$	2	$\mathbb{Z}/2$	$6^*$	$C_2^2$
	$(x-1)(x+1)(x^4+2x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{24}$	2q	$2^{16}$	2	$\mathbb{Z}/2$	$10^*$	$C_2^2$
	$-(x^2-2)(x^4+4x^2-4)$	$[K_3, L_6]$	$-2^{39}$	2q	$2^{16}$	2	$\mathbb{Z}/2$	$4^*$	$C_2^2$
	$(x^2+2)(x^4-4x^2-4)$	$[K_2, L_6]$	$2^{39}$	2q	$2^{16}$	2	$\mathbb{Z}/2$	$2^*$	$C_2^2$
<b>64</b>	$x(x^4-4x^3-2x^2-4x+1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{24}$	2q	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2^2$



Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
65	$2(x^2 + 1)(x^4 - 2x^2 - 1)$	$[K_1, L_6]$	$2^{34}$	2q	$2^{16}$	1	$\mathbb{Z}/2$	0	$C_2$
	$(x^2 + 2)(x^4 + 4x^2 - 4)$	$[K_2, L_6]$	$2^{39}$	2q	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2$
	$(x^2 - 2)(x^4 - 4x^2 - 4)$	$[K_3, L_6]$	$-2^{39}$	2q	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2$
	$\text{Imf}_{\text{db}} x(x^4 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{16}$	2d	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-2x(x^4 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{26}$	2d	$2^{16}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-(x^2 - 4x + 2)(x^2 + 2)(x^2 + 4x + 2)$	$[K_2, K_3, K_3]$	$-2^{51}$	2d	$2^{16}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$(x^2 - 4x + 2)(x^2 + 2)(x^2 + 4x + 2)$	$[K_2, K_3, K_3]$	$-2^{51}$	2d	$2^{16}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$(2x^2 - 2x + 1)(4x^4 - 16x^3 - 12x^2 - 8x - 47)$	$[K_1, L_6]$	$2^{46}5^{12}$	10b	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(2x^2 - 2x + 1)(4x^4 - 16x^3 - 12x^2 - 8x - 47)$	$[K_1, L_6]$	$2^{46}5^{12}$	10b	$2^{16}$	1	$\mathbb{Z}/2$	0	$C_2$
67	$-x(2x^2 - 8x + 9)(2x^2 + 8x + 9)$	$[\mathbb{Q}, \mathbb{Q}, K_2, K_2]$	$2^{36}3^{12}$	6a	$2^{16}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	$2^*$	$C_2$
	$-x(4x^4 + 28x^2 + 81)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{36}3^{12}$	6a	$2^{16}$	1	$\mathbb{Z}/2$	$2^*$	$C_2$
	$(x + 44)(x^4 - 16x^3 - 164x^2 + 1056x - 3388)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{39}3^{12}11^{12}$	66a	$2^{16}$	1	$\mathbb{Z}/2$	$2^*$	$C_2$
	$-(x + 44)(x^4 - 16x^3 - 164x^2 + 1056x - 3388)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{39}3^{12}11^{12}$	66a	$2^{16}$	1	$\mathbb{Z}/4$	$2^*$	$C_2$
68	$-(x - 1)(x + 1)(x^4 + 2x^2 - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{24}$	2q	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2^2$
	$(x^2 + 1)(x^4 - 2x^2 - 1)$	$[K_1, L_6]$	$2^{24}$	2q	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2^2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>70</b>	$-(x^2 + 2)(x^4 - 4x^2 - 4)$	$[K_2, L_6]$	$2^{39}$	2q	$2^{16}$	1	$\mathbb{Z}/2$	0	$C_2$
	$(x^2 - 2)(x^4 + 4x^2 - 4)$	$[K_3, L_6]$	$-2^{39}$	2q	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2$
	$x(x^4 + 4x^3 - 2x^2 + 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{24}$	2q	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-2(x^2 + 1)(x^4 - 2x^2 - 1)$	$[K_1, L_6]$	$2^{34}$	2q	$2^{16}$	0	$\mathbb{Z}/2$	0	$C_2$
	$-(x^2 - 2)(x^4 - 4x^2 - 4)$	$[K_3, L_6]$	$-2^{39}$	2q	$2^{16}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2$
	$-(x^2 + 2)(x^4 + 4x^2 - 4)$	$[K_2, L_6]$	$2^{39}$	2q	$2^{16}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>71</b>	$-(x^2 - 2x - 1)(x^2 + 1)(x^2 + 2x - 1)$	$[K_1, K_3, K_3]$	$-2^{36}$	2d	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$D_4$
	$-(x^2 - 2)(x^4 + 12x^2 + 4)$	$[K_3, L_1]$	$2^{51}$	2d	$2^{16}$	0	$\mathbb{Z}/2$	0	$C_2^2$
<b>72</b>	$-3(x^2 - 6x + 7)(x^2 + 1)(7x^2 + 6x + 1)$	$[K_1, K_3, K_3]$	$-2^{46}3^{22}$	6a	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_4$
	$3(x^2 + 1)(x^2 + 6x + 7)(7x^2 - 6x + 1)$	$[K_1, K_3, K_3]$	$-2^{46}3^{22}$	6a	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_4$
<b>73</b>	$x(x^2 - 2)(x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, K_2, K_3]$	$-2^{26}$	2d	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$(x^2 - 2x - 1)(x^2 + 2x + 3)(3x^2 - 2x + 1)$	$[K_2, K_2, K_3]$	$2^{51}$	2d	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$(x - 3)(4x^4 + 16x^3 - 12x^2 + 8x - 47)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{36}5^{12}$	10b	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
	$-(x-3)(4x^4+16x^3-12x^2+8x-47)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{36}5^{12}$	10b	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$
74	$-x(x^2-4x+2)(x^2+4x+2)$	$[\mathbb{Q}, \mathbb{Q}, K_3, K_3]$	$2^{32}$	2f	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$-x(x^4+12x^2+4)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{32}$	2f	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-7(x^2+2x+2)(x^4+32x^3-132x^2+64x+4)$	$[K_1, L_4]$	$-2^{47}7^{22}$	14b	$2^{16}$	0	$\mathbb{Z}/4$	0	$C_2$
	$7(x^2-2x+2)(x^4-32x^3-132x^2-64x+4)$	$[K_1, L_4]$	$-2^{47}7^{22}$	14b	$2^{16}$	0	$\mathbb{Z}/2$	0	$C_2$
75	$-(x^2-2x+3)(x^2+1)(x^2+2x-1)$	$[K_1, K_2, K_3]$	$2^{38}$	2l	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$-(x^2+1)(7x^4+12x^3+30x^2+20x+23)$	$[K_1, L_5]$	$-2^{45}$	2n	$2^{16}$	0	$\mathbb{Z}/2$	0	$C_2$
	$-(x^2+2x-1)(x^4+4x^3-6x^2+12x-7)$	$[K_3, L_6]$	$-2^{47}$	2m	$2^{16}$	0	$\mathbb{Z}/2$	0 <sub>LS</sub>	$C_2$
	$-(x+1)(4x^4-16x^3+20x^2-40x+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{35}3^{12}$	6f	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$
76	$x(x^2-4x+2)(x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, K_2, K_3]$	$-2^{28}$	2l	$2^{16}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2$
	$-x(x^4-16x^3+60x^2-32x+4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{35}$	2n	$2^{16}$	1	$\mathbb{Z}/4$	2	$C_2$
	$(x^2+2)(x^4-8x^3+12x^2-16x+4)$	$[K_2, L_6]$	$2^{47}$	2m	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-3(x^2+2x+2)(x^4+16x^3-4x^2+32x+4)$	$[K_1, L_2]$	$2^{45}3^{22}$	6f	$2^{16}$	1	$\mathbb{Z}/4$	0	$C_2$
77	$(x^2-2x+3)(x^2+1)(x^2+2x-1)$	$[K_1, K_2, K_3]$	$2^{38}$	2l	$2^{16}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>78</b>	$(x^2 + 1)(7x^4 - 12x^3 + 30x^2 - 20x + 23)$	$[K_1, L_5]$	$-2^{45}$	2n	$2^{16}$	1	$\mathbb{Z}/2$	0	$C_2$
	$(x^2 + 2x - 1)(x^4 + 4x^3 - 6x^2 + 12x - 7)$	$[K_3, L_6]$	$-2^{47}$	2m	$2^{16}$	1	$\mathbb{Z}/2$	2	$C_2$
	$(x + 1)(4x^4 - 16x^3 + 20x^2 - 40x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{35}3^{12}$	6f	$2^{16}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-(x^2 - 2x + 3)(x^2 + 1)(3x^2 + 2x + 1)$	$[K_1, K_2, K_2]$	$-2^{42}$	2f	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$(x - 3)(4x^4 + 16x^3 + 84x^2 + 200x + 289)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{37}7^{12}$	14b	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$
<b>79</b>	$(x^2 + 1)(x^2 + 2x + 3)(3x^2 - 2x + 1)$	$[K_1, K_2, K_2]$	$-2^{42}$	2f	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$(x + 3)(4x^4 - 16x^3 + 84x^2 - 200x + 289)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{37}7^{12}$	14b	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$
<b>80</b>	$-x(x^2 - 4x + 2)(x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, K_2, K_3]$	$-2^{28}$	2l	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$x(x^4 - 16x^3 + 60x^2 - 32x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{35}$	2n	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 2)(x^4 - 8x^3 + 12x^2 - 16x + 4)$	$[K_2, L_6]$	$2^{47}$	2m	$2^{16}$	0	$\mathbb{Z}/2$	0	$C_2$
	$3(x^2 - 2x + 2)(x^4 - 16x^3 - 4x^2 - 32x + 4)$	$[K_1, L_2]$	$2^{45}3^{22}$	6f	$2^{16}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>81</b>	$-(x - 1)(x^4 + 4x^2 - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{24}$	2s	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$
	$(x - 1)(x^2 - 2x - 1)(x^2 + 2x - 1)$	$[\mathbb{Q}, \mathbb{Q}, K_3, K_3]$	$2^{26}$	2r	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
	$2(x - 1)(x^4 + 4x^2 - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{34}$	2s	$2^{16}$	0	$\mathbb{Z}/2$	2	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>82</b>	$-(x^2 + 1)(x^2 + 2x - 1)(x^2 + 2x + 3)$	$[K_1, K_2, K_3]$	$2^{36}$	2r	$2^{16}$	0	$\mathbb{Z}/2 \times \mathbb{Z}/2$	0	$C_2$
	$(x - 1)(x^4 + 4x^2 - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{24}$	2s	$2^{16}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-(x - 1)(x^2 - 2x - 1)(x^2 + 2x - 1)$	$[\mathbb{Q}, \mathbb{Q}, K_3, K_3]$	$2^{26}$	2r	$2^{16}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	4	$C_2$
	$-2(x - 1)(x^4 + 4x^2 - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{34}$	2s	$2^{16}$	1	$\mathbb{Z}/2$	4	$C_2$
	$(x^2 + 1)(x^2 + 2x - 1)(x^2 + 2x + 3)$	$[K_1, K_2, K_3]$	$2^{36}$	2r	$2^{16}$	1	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	$C_2$
<b>83</b>	$-(x^2 - 2x - 1)(x^4 - 4x^3 - 6x^2 + 4x + 1)$	$[K_3, L_4]$	$2^{40}$	2t	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 - 2x - 1)(x^4 - 4x^3 + 10x^2 + 4x + 1)$	$[K_3, L_3]$	$2^{40}$	2u	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>84</b>	$x(x^4 - 4x^3 - 6x^2 + 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{25}$	2t	$2^{17}$	1	$\mathbb{Z}/2$	4	$C_2$
	$2x(x^4 + 4x^3 + 10x^2 - 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_3]$	$2^{35}$	2u	$2^{17}$	1	$\mathbb{Z}/2$	4	$C_2$
<b>85</b>	$(x^2 + 2x - 1)(x^4 - 4x^3 - 6x^2 + 4x + 1)$	$[K_3, L_4]$	$2^{40}$	2t	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 - 2x - 1)(3x^4 - 4x^3 - 2x^2 + 4x + 3)$	$[K_3, L_3]$	$2^{40}$	2u	$2^{17}$	1	$\mathbb{Z}/2$	0	$C_2$
<b>86</b>	$-x(x^4 - 4x^3 + 10x^2 + 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_3]$	$2^{25}$	2u	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>87</b>	$-2x(x^4 + 4x^3 - 6x^2 - 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{35}$	2t	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$x(x^4 + 8x^3 + 4x^2 - 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{33}$	2w	$2^{17}$	1	$\mathbb{Z}/2$	4	$C_2$
	$(x^2 - 2)(x^4 + 4x^3 + 4x^2 - 8x + 4)$	$[K_3, L_7]$	$2^{44}$	2v	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>88</b>	$-x(x^4 + 4x^3 + 4x^2 - 8x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}$	2v	$2^{17}$	1	$\mathbb{Z}/2$	4	$C_2$
	$(x^2 - 2)(x^4 + 8x^3 + 4x^2 - 16x + 4)$	$[K_3, L_4]$	$2^{48}$	2w	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>89</b>	$x(x^4 + 4x^3 + 4x^2 - 8x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}$	2v	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 - 2)(x^4 + 8x^3 + 4x^2 - 16x + 4)$	$[K_3, L_4]$	$2^{48}$	2w	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>90</b>	$-x(x^4 + 8x^3 + 4x^2 - 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{33}$	2w	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 - 2)(x^4 + 4x^3 + 4x^2 - 8x + 4)$	$[K_3, L_7]$	$2^{44}$	2v	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>91</b>	$-x(x^4 - 8x^3 + 28x^2 - 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_3]$	$2^{33}$	2y	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 2)(x^4 - 4x^3 + 12x^2 - 8x + 4)$	$[K_2, L_7]$	$-2^{44}$	2x	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>92</b>	$(x^2 + 1)(3x^4 + 4x^3 + 14x^2 + 12x + 11)$	$[K_1, L_3]$	$-2^{43}$	2y	$2^{17}$	1	$\mathbb{Z}/2$	0	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>93</b>	$(x^2 + 2x - 1)(x^4 + 6x^2 - 8x + 5)$	$[K_3, L_7]$	$2^{44}$	2x	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
	$(x^2 + 1)(x^4 + 6x^2 - 8x + 5)$	$[K_1, L_7]$	$-2^{39}$	2x	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
	$(x^2 - 2x - 1)(x^4 - 4x^3 + 10x^2 + 20x + 9)$	$[K_3, L_3]$	$2^{48}$	2y	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>94</b>	$-x(x^4 - 4x^3 + 12x^2 - 8x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}$	2x	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 2)(3x^4 - 8x^3 + 20x^2 - 16x + 12)$	$[K_2, L_3]$	$-2^{48}$	2y	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>95</b>	$x(x^4 - 4x^3 + 12x^2 - 8x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}$	2x	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$(x^2 + 2)(3x^4 + 8x^3 + 20x^2 + 16x + 12)$	$[K_2, L_3]$	$-2^{48}$	2y	$2^{17}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2$
<b>96</b>	$-(x^2 + 1)(x^4 + 6x^2 - 8x + 5)$	$[K_1, L_7]$	$-2^{39}$	2x	$2^{17}$	1	$\mathbb{Z}/2$	0	$C_2$
	$-(x^2 - 2x - 1)(x^4 - 4x^3 + 10x^2 + 20x + 9)$	$[K_3, L_3]$	$2^{48}$	2y	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>97</b>	$-(x^2 + 1)(3x^4 - 4x^3 + 14x^2 - 12x + 11)$	$[K_1, L_3]$	$-2^{43}$	2y	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
	$-(x^2 + 2x - 1)(x^4 + 6x^2 - 8x + 5)$	$[K_3, L_7]$	$2^{44}$	2x	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>98</b>	$x(x^4 - 8x^3 + 28x^2 - 16x + 4)$	$[\mathbb{Q}, \mathbb{Q}, L_3]$	$2^{33}$	2y	$2^{17}$	1	$\mathbb{Z}/2$	4	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
99	$(x^2 + 2)(x^4 - 4x^3 + 12x^2 - 8x + 4)$	$[K_2, L_7]$	$-2^{44}$	2x	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
	$\text{Imf}_{\text{db}} -x(x^4 + 4x^3 + 4x^2 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{17}$	2z	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-x(x^4 + 4x^3 - 2x^2 - 12x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{25}$	2B	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-2(x - 1)(x^4 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{28}$	2A	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$2(x^2 + 1)(x^4 + 4x^3 + 6x^2 + 4x + 3)$	$[K_1, L_3]$	$-2^{35}$	2C	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
100	$\text{Imf}_{\text{db}} x(x^4 + 4x^3 + 4x^2 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{17}$	2z	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$x(x^4 + 4x^3 - 2x^2 - 12x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{25}$	2B	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$2(x - 1)(x^4 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{28}$	2A	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-2(x^2 + 1)(x^4 + 4x^3 + 6x^2 + 4x + 3)$	$[K_1, L_3]$	$-2^{35}$	2C	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
101	$\text{Imf}_{\text{db}} -(x + 1)(x^4 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{18}$	2A	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-x(x + 2)(x^4 - 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{25}$	2B	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 1)(x^4 + 4x^3 + 6x^2 + 4x + 3)$	$[K_1, L_3]$	$-2^{25}$	2C	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
	$2x(x^4 + 4x^3 + 4x^2 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{27}$	2z	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
102	$\text{Imf}_{\text{db}} -(x - 1)(x^4 + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{18}$	2A	$2^{17}$	2	$\mathbb{Z}/2$	6*	$C_2$



Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>103</b>	$x(x+2)(x^4-4x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{25}$	<b>2B</b>	$2^{17}$	2	$\mathbb{Z}/2$	$12^*$	$C_2$
	$(x^2+1)(x^4+4x^3+6x^2+4x+3)$	$[K_1, L_3]$	$-2^{25}$	<b>2C</b>	$2^{17}$	2	$\mathbb{Z}/2$	$6^*$	$C_2$
	$-2x(x^4+4x^3+4x^2+1)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{27}$	<b>2z</b>	$2^{17}$	2	$\mathbb{Z}/2$	$8^*$	$C_2$
	$(x-1)(x^4-4x^3-14x^2+4x+17)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{33}$	<b>2D</b>	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2+2)(5x^4+4x^3+4x^2+8x+4)$	$[K_2, L_7]$	$-2^{44}$	<b>2E</b>	$2^{17}$	1	$\mathbb{Z}/2$	0	$C_2$
	$-(x^2-2)(3x^4+8x^3-12x^2-16x+44)$	$[K_3, L_3]$	$2^{54}$	<b>2F</b>	$2^{17}$	1	$\mathbb{Z}/2$	0	$C_2$
	$-(3x^2+4x+2)(x^4+12x^2+4)$	$[K_2, L_1]$	$-2^{57}$	<b>2G</b>	$2^{17}$	1	$\mathbb{Z}/2$	0	$C_2$
<b>104</b>	$x(4x^4-20x^2-16x+1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{33}$	<b>2D</b>	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2+2x+3)(x^4-2x^2-8x+13)$	$[K_2, L_7]$	$-2^{44}$	<b>2E</b>	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
	$(x^2-2)(11x^4+8x^3-12x^2-16x+12)$	$[K_3, L_3]$	$2^{54}$	<b>2F</b>	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
	$-(x^2+2x+3)(x^4-4x^3+18x^2-28x+17)$	$[K_2, L_1]$	$-2^{57}$	<b>2G</b>	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>105</b>	$-(x-1)(x^4-4x^3-14x^2+4x+17)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{33}$	<b>2D</b>	$2^{17}$	0	$\mathbb{Z}/2$	2	$C_2$
	$(x^2+2)(5x^4+4x^3+4x^2+8x+4)$	$[K_2, L_7]$	$-2^{44}$	<b>2E</b>	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$
	$(x^2-2)(3x^4+8x^3-12x^2-16x+44)$	$[K_3, L_3]$	$2^{54}$	<b>2F</b>	$2^{17}$	0	$\mathbb{Z}/2$	0	$C_2$

Draft of 4:22 pm, Sunday, April 13, 2025

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
	$(3x^2 + 4x + 2)(x^4 + 12x^2 + 4)$	$[K_2, L_1]$	$-2^{57}$	2G	$2^{17}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2$
106	$x(4x^4 - 20x^2 + 16x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{33}$	2D	$2^{17}$	1	$\mathbb{Z}/2$	4	$C_2$
	$(x^2 + 2x + 3)(x^4 - 2x^2 - 8x + 13)$	$[K_2, L_7]$	$-2^{44}$	2E	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 - 2)(11x^4 + 8x^3 - 12x^2 - 16x + 12)$	$[K_3, L_3]$	$2^{54}$	2F	$2^{17}$	1	$\mathbb{Z}/2$	0	$C_2$
	$(x^2 + 2x + 3)(x^4 - 4x^3 + 18x^2 - 28x + 17)$	$[K_2, L_1]$	$-2^{57}$	2G	$2^{17}$	1	$\mathbb{Z}/2$	2	$C_2$
111	$-x(x^4 + 4x^2 - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{28}$	2o	$2^{18}$	2	$\mathbb{Z}/2$	$4^*$	$C_2$
113	$-x(x^4 - 4x^2 - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{28}$	2o	$2^{18}$	0	$\mathbb{Z}/2$	2	$C_2$
114	$-(x^2 + 2)(x^4 + 4x^3 + 4x^2 - 8x + 4)$	$[K_2, L_7]$	$-2^{46}$	2r	$2^{18}$	0	$\mathbb{Z}/2$	0	$C_2$
120	$(x^2 + 2)(x^4 + 4x^3 + 4x^2 - 8x + 4)$	$[K_2, L_7]$	$-2^{46}$	2r	$2^{18}$	2	$\mathbb{Z}/2$	$4^*$	$C_2$
122	$x(x^4 + 2x^2 - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{18}$	2o	$2^{18}$	1	$\mathbb{Z}/2$	2	$C_2$
	$2x(x^4 + 2x^2 - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{28}$	2o	$2^{18}$	1	$\mathbb{Z}/2$	4	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>123</b>	$-(x^2 + 2x - 1)(x^4 + 6x^2 + 8x + 5)$	$[K_3, L_7]$	$2^{46}$	2d	$2^{18}$	0	$\mathbb{Z}/2$	0	$C_4$
	$-(x^2 + 2x - 1)(x^4 - 4x^3 - 6x^2 - 12x - 7)$	$[K_3, L_6]$	$-2^{51}$	2d	$2^{18}$	0	$\mathbb{Z}/2$	0	$C_4$
<b>124</b>	$(x^2 - 2x - 1)(x^4 + 6x^2 - 8x + 5)$	$[K_3, L_7]$	$2^{46}$	2d	$2^{18}$	2	$\mathbb{Z}/2$	$4^*$	$C_4$
	$(x^2 + 2x - 1)(x^4 - 4x^3 - 6x^2 - 12x - 7)$	$[K_3, L_6]$	$-2^{51}$	2d	$2^{18}$	2	$\mathbb{Z}/2$	$2^*$	$C_4$
<b>125</b>	$(x^2 + 1)(x^4 - 8x^3 + 18x^2 + 8x + 1)$	$[K_1, L_7]$	$-2^{45}$	2h	$2^{18}$	2	$\mathbb{Z}/2$	$4^*$	$C_4$
<b>126</b>	$(x^2 + 1)(5x^4 - 8x^3 - 6x^2 + 8x + 5)$	$[K_1, L_7]$	$-2^{45}$	2h	$2^{18}$	0	$\mathbb{Z}/2$	0	$C_4$
<b>127</b>	$-(x^2 + 1)(5x^4 + 8x^3 - 6x^2 - 8x + 5)$	$[K_1, L_7]$	$-2^{45}$	2h	$2^{18}$	0	$\mathbb{Z}/2$	0	$C_4$
<b>128</b>	$-(x^2 + 1)(x^4 + 8x^3 + 18x^2 - 8x + 1)$	$[K_1, L_7]$	$-2^{45}$	2h	$2^{18}$	$0^*$	$\mathbb{Z}/2$	0	$C_4$
<b>129</b>	$\text{Imf}_{\text{db}} -x(x^4 + 2x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{19}$	2a	$2^{18}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-2x(x^4 - 2x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}$	2a	$2^{18}$	1	$\mathbb{Z}/2$	4	$C_2$
	$x(x^4 - 478x^2 + 57122)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{19}13^{12}$	26a	$2^{18}$	1	$\mathbb{Z}/2$	$2^*$	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
130	$2x(x^4 + 478x^2 + 57122)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}13^{12}$	26a	$2^{18}$	1	$\mathbb{Z}/2$	$2^*$	$C_2$
	$\text{Imf}_{\text{db}} -x(x^4 - 2x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{19}$	2a	$2^{18}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-2x(x^4 + 2x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}$	2a	$2^{18}$	1	$\mathbb{Z}/2$	2	$C_2$
	$x(x^4 + 478x^2 + 57122)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{19}13^{12}$	26a	$2^{18}$	1	$\mathbb{Z}/2$	$2^*$	$C_2$
	$2x(x^4 - 478x^2 + 57122)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}13^{12}$	26a	$2^{18}$	1	$\mathbb{Z}/2$	$2^*$	$C_2$
131	$\text{Imf}_{\text{db}} x(x^4 + 4x^3 + 10x^2 + 8x + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{19}$	2H	$2^{18}$	1	$\mathbb{Z}/2$	4	$C_2$
	$\text{Imf}_{\text{db}} -x(x^4 + 4x^3 + 10x^2 + 8x + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{19}$	2H	$2^{18}$	1	$\mathbb{Z}/2$	4	$C_2$
	$2x(x^4 + 4x^3 + 10x^2 + 8x + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}$	2H	$2^{18}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-2x(x^4 + 4x^3 + 10x^2 + 8x + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_7]$	$2^{29}$	2H	$2^{18}$	1	$\mathbb{Z}/2$	4	$C_2$
132	$(x-1)(x^4 + 4x^3 + 2x^2 - 4x - 7)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{28}$	2I	$2^{18}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-(x-1)(x^4 + 4x^3 + 2x^2 - 4x - 7)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{28}$	2I	$2^{18}$	1	$\mathbb{Z}/2$	2	$C_2$
	$x(x+1)(x^4 + 4x^2 - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{28}$	2I	$2^{18}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-(x-1)x(x^4 + 4x^2 - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{28}$	2I	$2^{18}$	1	$\mathbb{Z}/2$	2	$C_2$
133	$(x^2 + 2x + 3)(x^4 + 6x^2 - 8x + 5)$	$[K_2, L_7]$	$-2^{46}$	2J	$2^{18}$	2	$\mathbb{Z}/2$	$4^*$	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
	$(x^2 - 2x - 1)(x^4 + 8x^3 + 22x^2 + 16x + 5)$	$[K_3, L_7]$	$2^{46}$	2K	$2^{18}$	2	$\mathbb{Z}/2$	$4^*$	$C_2$
134	$(x^2 + 2x + 3)(5x^4 + 8x^3 + 6x^2 + 1)$	$[K_2, L_7]$	$-2^{46}$	2J	$2^{18}$	1	$\mathbb{Z}/2$	0	$C_2$
	$(x^2 + 2x - 1)(x^4 - 2x^2 - 8x + 13)$	$[K_3, L_7]$	$2^{46}$	2K	$2^{18}$	1	$\mathbb{Z}/2$	2	$C_2$
135	$-(x^2 + 2x + 3)(5x^4 + 8x^3 + 6x^2 + 1)$	$[K_2, L_7]$	$-2^{46}$	2J	$2^{18}$	1	$\mathbb{Z}/2$	0	$C_2$
	$-(x^2 + 2x - 1)(x^4 - 2x^2 - 8x + 13)$	$[K_3, L_7]$	$2^{46}$	2K	$2^{18}$	1	$\mathbb{Z}/2$	0	$C_2$
136	$-(x^2 - 2x + 3)(x^4 + 6x^2 + 8x + 5)$	$[K_2, L_7]$	$-2^{46}$	2J	$2^{18}$	0	$\mathbb{Z}/2$	0	$C_2$
	$-(x^2 - 2x - 1)(x^4 + 8x^3 + 22x^2 + 16x + 5)$	$[K_3, L_7]$	$2^{46}$	2K	$2^{18}$	0	$\mathbb{Z}/2$	0	$C_2$
161	$\text{Imf}_{\text{db}}(x+1)(x^4-2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{19}$	2L	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-2(x-1)(x^4-2x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{30}$	2M	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
162	$\text{Imf}_{\text{db}}(x-1)(x^4-2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{19}$	2L	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
	$2(x-1)(x^4-2x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{30}$	2M	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
163	$\text{Imf}_{\text{db}}x(x^4+4x^3+2x^2-4x-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{19}$	2N	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
	$2(x-1)(x^4+2x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{30}$	2O	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
164	$\text{db} -x(x^4+4x^3+2x^2-4x-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{19}$	2N	$2^{19}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-2(x-1)(x^4+2x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{30}$	2O	$2^{19}$	1	$\mathbb{Z}/2$	4	$C_2$
165	$-(x-1)(x^4+2x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{20}$	2O	$2^{19}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-2x(x^4+4x^3+2x^2-4x-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2N	$2^{19}$	1	$\mathbb{Z}/2$	4	$C_2$
166	$(x-1)(x^4+2x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{20}$	2O	$2^{19}$	2	$\mathbb{Z}/2$	$6^*$	$C_2$
	$2x(x^4+4x^3+2x^2-4x-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2N	$2^{19}$	2	$\mathbb{Z}/2$	$6^*$	$C_2$
167	$(x-1)(x^4-2x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{20}$	2M	$2^{19}$	2	$\mathbb{Z}/2$	$6^*$	$C_2$
	$-2(x+1)(x^4-2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{29}$	2L	$2^{19}$	2	$\mathbb{Z}/2$	$8^*$	$C_2$
168	$-(x-1)(x^4-2x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$-2^{20}$	2M	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
	$2(x+1)(x^4-2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{29}$	2L	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
169	$-(x+4)(x^4-12x^2+16x-4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2P	$2^{19}$	1	$\mathbb{Z}/2$	4	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
	$(2x^2 - 2x + 1)(4x^4 + 32x^3 + 76x^2 + 32x - 41)$	$[K_1, L_6]$	$2^{40}5^{12}$	10c	$2^{19}$	1	$\mathbb{Z}/2$	0	$C_2$
170	$-(x+1)(x^4 - 4x^3 - 6x^2 + 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2Q	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 1)(x^4 - 4x^3 + 2x^2 + 4x - 7)$	$[K_1, L_6]$	$2^{40}$	2R	$2^{19}$	0	$\mathbb{Z}/2$	0	$C_2$
171	$-(x+2)(4x^4 - 12x^2 + 8x - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2P	$2^{19}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 2x + 2)(23x^4 - 24x^3 - 52x^2 + 80x - 28)$	$[K_1, L_6]$	$2^{40}5^{12}$	10c	$2^{19}$	1	$\mathbb{Z}/2$	2	$C_2$
172	$(x+2)(4x^4 - 12x^2 + 8x - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2P	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
	$(x^2 - 2x + 2)(23x^4 + 24x^3 - 52x^2 - 80x - 28)$	$[K_1, L_6]$	$2^{40}5^{12}$	10c	$2^{19}$	0	$\mathbb{Z}/2$	0	$C_2$
173	$-(x-1)(x^4 + 4x^3 - 6x^2 - 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2Q	$2^{19}$	1	$\mathbb{Z}/2$	4	$C_2$
	$(x^2 + 1)(x^4 - 4x^3 + 2x^2 + 4x - 7)$	$[K_1, L_6]$	$2^{40}$	2R	$2^{19}$	1	$\mathbb{Z}/2$	2	$C_2$
174	$(x+4)(x^4 - 12x^2 + 16x - 4)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2P	$2^{19}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(2x^2 - 2x + 1)(4x^4 + 32x^3 + 76x^2 + 32x - 41)$	$[K_1, L_6]$	$2^{40}5^{12}$	10c	$2^{19}$	0	$\mathbb{Z}/2$	0 <sub>LS</sub>	$C_2$
175	$(x+1)(x^4 + 4x^3 - 6x^2 - 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2Q	$2^{19}$	2	$\mathbb{Z}/2$	6*	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
176	$(x^2 + 1)(x^4 - 4x^3 + 10x^2 - 12x + 1)$	$[K_1, L_6]$	$2^{40}$	2R	$2^{19}$	2	$\mathbb{Z}/2$	$6^*$	$C_2$
	$-(x + 1)(x^4 + 4x^3 - 6x^2 - 4x + 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{29}$	2Q	$2^{19}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 1)(x^4 - 4x^3 + 10x^2 - 12x + 1)$	$[K_1, L_6]$	$2^{40}$	2R	$2^{19}$	1	$\mathbb{Z}/2$	0	$C_2$
177	$-(x^2 - 2x - 1)(x^4 + 12x^3 + 34x^2 + 20x + 1)$	$[K_3, L_4]$	$2^{52}$	2S	$2^{19}$	2	$\mathbb{Z}/2$	$4^*$	$C_2$
	$(x^2 - 2x + 3)(x^4 - 4x^3 - 6x^2 - 12x - 7)$	$[K_2, L_6]$	$2^{53}$	2T	$2^{19}$	2	$\mathbb{Z}/2$	$2^*$	$C_2$
178	$(x^2 + 2x - 1)(x^4 + 4x^3 - 14x^2 - 4x + 17)$	$[K_3, L_4]$	$2^{52}$	2S	$2^{19}$	1	$\mathbb{Z}/2$	2	$C_2$
	$(x^2 - 2x + 3)(7x^4 - 12x^3 + 6x^2 - 4x - 1)$	$[K_2, L_6]$	$2^{53}$	2T	$2^{19}$	1	$\mathbb{Z}/2$	0	$C_2$
179	$-(x^2 + 2x - 1)(x^4 + 4x^3 - 14x^2 - 4x + 17)$	$[K_3, L_4]$	$2^{52}$	2S	$2^{19}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2$
	$-(x^2 - 2x + 3)(7x^4 - 12x^3 + 6x^2 - 4x - 1)$	$[K_2, L_6]$	$2^{53}$	2T	$2^{19}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2$
180	$(x^2 - 2x - 1)(x^4 + 12x^3 + 34x^2 + 20x + 1)$	$[K_3, L_4]$	$2^{52}$	2S	$2^{19}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 2x + 3)(x^4 + 4x^3 - 6x^2 + 12x - 7)$	$[K_2, L_6]$	$2^{53}$	2T	$2^{19}$	1	$\mathbb{Z}/2$	0	$C_2$



Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut( $C$ )
<b>184</b>	$(x^2 + 2)(x^4 - 8x^3 + 4x^2 + 16x + 4)$	$[K_2, L_4]$	$-2^{54}$	<b>2a</b>	$2^{20}$	2	$\mathbb{Z}/2$	$2^*$	$C_4$
<b>185</b>	$-(x^2 + 2)(x^4 + 8x^3 + 4x^2 - 16x + 4)$	$[K_2, L_4]$	$-2^{54}$	<b>2a</b>	$2^{20}$	0	$\mathbb{Z}/2$	0	$C_4$
<b>191</b>	$(x^2 + 2)(3x^4 + 16x^3 + 12x^2 - 32x + 12)$	$[K_2, L_3]$	$-2^{60}$	<b>2h</b>	$2^{20}$	0	$\mathbb{Z}/2$	0	$C_4$
<b>192</b>	$-(x^2 + 2)(3x^4 + 16x^3 + 12x^2 - 32x + 12)$	$[K_2, L_3]$	$-2^{60}$	<b>2h</b>	$2^{20}$	0	$\mathbb{Z}/2$	0	$C_4$
<b>207</b>	$-x(x^4 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_3]$	$2^{21}$	<b>2d</b>	$2^{20}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-2x(x^4 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_3]$	$2^{31}$	<b>2d</b>	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>208</b>	$-(x^2 + 1)(3x^4 + 4x^3 - 2x^2 - 4x + 3)$	$[K_1, L_3]$	$-2^{41}$	<b>2r</b>	$2^{20}$	0	$\mathbb{Z}/2$	0	$C_4$
<b>209</b>	$-(x^2 + 1)(x^4 + 4x^3 + 10x^2 - 4x + 1)$	$[K_1, L_3]$	$-2^{41}$	<b>2r</b>	$2^{20}$	$0^*$	$\mathbb{Z}/2$	0	$C_4$
<b>210</b>	$(x^2 + 1)(x^4 - 4x^3 - 6x^2 + 4x + 1)$	$[K_1, L_4]$	$-2^{41}$	<b>2d</b>	$2^{20}$	2	$\mathbb{Z}/2$	$4^*$	$C_4$
<b>211</b>	$-(x^2 + 1)(x^4 + 4x^3 - 6x^2 - 4x + 1)$	$[K_1, L_4]$	$-2^{41}$	<b>2d</b>	$2^{20}$	0	$\mathbb{Z}/2$	0	$C_4$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
<b>212</b>	$(x^2 + 1)(x^4 - 4x^3 + 10x^2 + 4x + 1)$	$[K_1, L_3]$	$-2^{41}$	<b>2r</b>	$2^{20}$	2	$\mathbb{Z}/2$	$4^*$	$C_2$
<b>213</b>	$(x^2 + 1)(3x^4 - 4x^3 - 2x^2 + 4x + 3)$	$[K_1, L_3]$	$-2^{41}$	<b>2r</b>	$2^{20}$	0	$\mathbb{Z}/2$	0	$C_2$
<b>214</b>	$x(x^4 - 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}$	<b>2d</b>	$2^{20}$	1	$\mathbb{Z}/2$	4	$C_2$
	$2x(x^4 - 2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{31}$	<b>2d</b>	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
<b>215</b>	$-(x^2 - 2x - 1)(x^4 + 4x^3 + 10x^2 - 20x + 9)$	$[K_3, L_3]$	$2^{54}$	<b>2a</b>	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-(x^2 + 2x - 1)(3x^4 + 4x^3 + 14x^2 + 12x + 11)$	$[K_3, L_3]$	$2^{54}$	<b>2a</b>	$2^{20}$	1	$\mathbb{Z}/2$	0	$C_2$
<b>216</b>	$(x^2 - 2x - 1)(x^4 + 4x^3 + 10x^2 - 20x + 9)$	$[K_3, L_3]$	$2^{54}$	<b>2a</b>	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
	$(x^2 + 2x - 1)(3x^4 + 4x^3 + 14x^2 + 12x + 11)$	$[K_3, L_3]$	$2^{54}$	<b>2a</b>	$2^{20}$	1	$\mathbb{Z}/2$	0	$C_2$
<b>217</b>	$(x^2 - 2x - 1)(x^4 + 12x^3 + 18x^2 - 44x + 17)$	$[K_3, L_4]$	$2^{60}$	<b>2h</b>	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
	$(x^2 + 2x - 1)(7x^4 + 12x^3 + 30x^2 + 20x + 23)$	$[K_3, L_5]$	$2^{60}$	<b>2h</b>	$2^{20}$	1	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2$
<b>218</b>	$-(x^2 - 2x - 1)(x^4 + 12x^3 + 18x^2 - 44x + 17)$	$[K_3, L_4]$	$2^{60}$	<b>2h</b>	$2^{20}$	1	$\mathbb{Z}/2$	0	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
	$-(x^2 + 2x - 1)(7x^4 + 12x^3 + 30x^2 + 20x + 23)$	$[K_3, L_5]$	$2^{60}$	2h	$2^{20}$	1	$\mathbb{Z}/2$	0	$C_2$
219	$-x(x^4 + 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{21}$	2r	$2^{20}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-2x(x^4 - 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{31}$	2r	$2^{20}$	0	$\mathbb{Z}/2$	2	$C_2$
220	$-x(x^4 - 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	2r	$2^{20}$	2	$\mathbb{Z}/2$	6*	$C_2$
	$-2x(x^4 + 4x^2 + 2)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{31}$	2r	$2^{20}$	2	$\mathbb{Z}/2$	4*	$C_2$
221	$(x - 1)(2x^4 - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}$	2U	$2^{20}$	1	$\mathbb{Z}/2$	4	$C_2$
	$2x(2x^4 + 8x^3 + 8x^2 - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{31}$	2V	$2^{20}$	1	$\mathbb{Z}/2$	4	$C_2$
222	$-(x + 1)(x^4 - 4x^3 + 2x^2 + 4x - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	2W	$2^{20}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-2(x + 1)(x^4 - 4x^3 + 2x^2 + 4x - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{31}$	2W	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
223	$x(2x^4 + 8x^3 + 8x^2 - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	2V	$2^{20}$	1	$\mathbb{Z}/2$	4	$C_2$
	$-2(x + 1)(2x^4 - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{31}$	2U	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
224	$-(x + 1)(x^4 - 4x^3 - 2x^2 + 4x - 1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	2X	$2^{20}$	2	$\mathbb{Z}/2$	8*	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
225	$-2(x-2)(2x^4+8x^3-4x^2+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{31}3^{12}$	6g	$2^{20}$	2	$\mathbb{Z}/2$	$6^*$	$C_2$
	$-(x-1)(x^4+4x^3-2x^2-4x-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	2X	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
	$2(x-2)(2x^4+8x^3-4x^2+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{31}3^{12}$	6g	$2^{20}$	1	$\mathbb{Z}/2$	4	$C_2$
226	$(x+1)(2x^4-1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}$	2U	$2^{20}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-2x(2x^4+8x^3+8x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{31}$	2V	$2^{20}$	0	$\mathbb{Z}/2$	2	$C_2$
227	$-(x-1)(x^4+4x^3+2x^2-4x-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	2W	$2^{20}$	1	$\mathbb{Z}/2$	4	$C_2$
	$2(x+1)(x^4-4x^3+2x^2+4x-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{31}$	2W	$2^{20}$	1	$\mathbb{Z}/2$	4	$C_2$
228	$-x(2x^4+8x^3+8x^2-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{21}$	2V	$2^{20}$	2	$\mathbb{Z}/2$	$6^*$	$C_2$
	$2(x+1)(2x^4-1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{31}$	2U	$2^{20}$	2	$\mathbb{Z}/2$	$4^*$	$C_2$
229	$-2(x+1)(x^4-4x^3-2x^2+4x-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{31}$	2X	$2^{20}$	0	$\mathbb{Z}/2$	2	$C_2$
	$-(x-2)(2x^4+8x^3-4x^2+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}3^{12}$	6g	$2^{20}$	0	$\mathbb{Z}/2$	2	$C_2$
230	$2(x+1)(x^4-4x^3-2x^2+4x-1)$	$[\mathbb{Q}, \mathbb{Q}, L_4]$	$2^{31}$	2X	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$

Table 6.21 (continued).

Isog Label	Simplified Weierstrass equation	Field system	$\Delta_{\min}$	$\overline{\mathbb{Q}}$ label	$N$	Rank	$J(\mathbb{Q})_{\text{tors}}$	$\#C(\mathbb{Q})$	Aut
	$(x-2)(2x^4+8x^3-4x^2+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$-2^{21}3^{12}$	6g	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
231	$-(2x^2-1)(4x^4-36x^2+32x+17)$	$[K_3, L_4]$	$2^{60}$	2Y	$2^{20}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2$
	$3(x^2-6x+7)(x^4-12x^3-46x^2-84x-47)$	$[K_3, L_2]$	$-2^{60}3^{22}$	6h	$2^{20}$	0	$\mathbb{Z}/2$	0	$C_2$
232	$(x^2-2x-1)(x^4-4x^3-30x^2+4x+97)$	$[K_3, L_4]$	$2^{60}$	2Y	$2^{20}$	1	$\mathbb{Z}/2$	2	$C_2$
	$-3(2x^2+4x+1)(4x^4+16x^3-76x^2+104x-47)$	$[K_3, L_2]$	$-2^{60}3^{22}$	6h	$2^{20}$	1	$\mathbb{Z}/2$	0	$C_2$
233	$(2x^2-1)(4x^4-36x^2+32x+17)$	$[K_3, L_4]$	$2^{60}$	2Y	$2^{20}$	1	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2$
	$-3(x^2-6x+7)(x^4-12x^3-46x^2-84x-47)$	$[K_3, L_2]$	$-2^{60}3^{22}$	6h	$2^{20}$	1	$\mathbb{Z}/2$	0	$C_2$
234	$-(x^2-2x-1)(x^4-4x^3-30x^2+4x+97)$	$[K_3, L_4]$	$2^{60}$	2Y	$2^{20}$	0	$\mathbb{Z}/2$	$0_{\text{LS}}$	$C_2$
	$3(2x^2+4x+1)(4x^4+16x^3-76x^2+104x-47)$	$[K_3, L_2]$	$-2^{60}3^{22}$	6h	$2^{20}$	0	$\mathbb{Z}/2$	0	$C_2$

## 6.4 List of $\overline{\mathbb{Q}}$ -isomorphism classes of genus 2 curves

Finally, we present a table of the 67  $\overline{\mathbb{Q}}$ -isomorphism classes found in the above list of genus 2 curves  $C/\mathbb{Q}$ . These are ordered first by the product of the primes of geometric bad reduction, and then by the order in which they first appear in Table 6.21. There are seven columns giving the following information:

1. A label for the  $\overline{\mathbb{Q}}$ -isomorphism class given in the format  $\mathbb{N}i$ . Here,  $\mathbb{N}$  is the product of the geometric bad primes for  $C/\mathbb{Q}$ , and  $i$  is a letter that distinguishes this  $\overline{\mathbb{Q}}$ -isomorphism class amongst those with the same set of geometric bad primes.
2. The  $G_2$ -invariants, as defined in (1.19).
3. The set of geometric bad primes for  $C/\mathbb{Q}$ .
4. The geometric automorphism group  $\text{Aut}(C_{\overline{\mathbb{Q}}})$ .
5. The identity component  $\text{ST}^0(J)$  of the Sato-Tate group  $\text{ST}(J)$  of the Jacobian  $J$  of  $C/\mathbb{Q}$ .
6. A checkmark indicating whether  $C/\mathbb{Q}$  has  $\text{GL}_2$ -type over  $\overline{\mathbb{Q}}$ .
7. Two numbers; the first indicating the number of genus 2 curves  $C/\mathbb{Q}$  listed in Table 6.21 which are contained in this  $\overline{\mathbb{Q}}$ -isomorphism class, and the second (in brackets) indicating the number of  $\mathbb{Q}$ -isogeny classes this  $\overline{\mathbb{Q}}$ -isomorphism class hits.

Table 6.22: The 67 known  $\overline{\mathbb{Q}}$ -isomorphism classes of genus 2 curves  $C/\mathbb{Q}$  whose Jacobian has good reduction away from 2.

$\overline{\mathbb{Q}}$ label	G2-invariants $(g_1, g_2, g_3)$	Bad primes	$\text{Aut}(C_{\overline{\mathbb{Q}}})$	$\text{ST}^0(J)$	$\text{GL}_2/\overline{\mathbb{Q}}?$	$\#C/\mathbb{Q}$ (iso)
2a	$(2 \cdot 13^5, \frac{13^3 \cdot 59}{2^2}, \frac{-3^2 \cdot 13^2}{2^3})$	{2}	$D_4$	$\text{SU}(2)$		14 (10)
2b	$(2^9 \cdot 3^{10}, -2^5 \cdot 3^6 \cdot 5 \cdot 19, -2^7 \cdot 3^4 \cdot 113)$	{2}	$C_2^2$	$\text{U}(1) \times \text{SU}(2)$		16 (8)
2c	$(2^{11} \cdot 3^5 \cdot 7^5, 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 23, 2^8 \cdot 3^2 \cdot 7^3 \cdot 23)$	{2}	$C_2^2$	$\text{U}(1) \times \text{SU}(2)$		16 (8)
2d	$(2^4 \cdot 5^5, 2 \cdot 3 \cdot 5^4, -5^3)$	{2}	$\text{GL}_2(\mathbb{F}_3)$	$\text{U}(1)$		22 (12)
2e	$(2^{13} \cdot 3^5 \cdot 11^5, 2^7 \cdot 3^3 \cdot 11^3 \cdot 2689, 2^9 \cdot 3^2 \cdot 11^2 \cdot 1087)$	{2}	$C_2^2$	$\text{U}(1) \times \text{U}(1)$		16 (4)
2f	$(2^{23}, 2^{14} \cdot 3 \cdot 5, 2^{12})$	{2}	$D_4$	$\text{SU}(2)$		22 (14)
2g	$(2^{10} \cdot 47^5, 2^5 \cdot 5 \cdot 19 \cdot 31 \cdot 47^3, 2^8 \cdot 7 \cdot 47^2 \cdot 137)$	{2}	$C_2^2$	$\text{SU}(2)$		4 (3)
2h	$(\frac{67^5}{2^5}, \frac{3 \cdot 67^3 \cdot 353}{2^8}, \frac{-31 \cdot 67^2}{2^9})$	{2}	$D_4$	$\text{SU}(2)$		14 (10)
2i	$(2^8 \cdot 59^5, 2^4 \cdot 59^3 \cdot 997, 2^3 \cdot 7 \cdot 59^2 \cdot 127)$	{2}	$C_2$	$\text{SU}(2)$		4 (2)
2j	$(2^{29}, 2^{17} \cdot 3 \cdot 43, -2^{15})$	{2}	$C_2^2$	$\text{U}(1) \times \text{SU}(2)$		16 (8)
2k	$(2^{14} \cdot 3^5 \cdot 5^5, 2^8 \cdot 3^3 \cdot 5^3 \cdot 577, 2^9 \cdot 3^2 \cdot 5^2 \cdot 223)$	{2}	$C_2^2$	$\text{U}(1) \times \text{SU}(2)$		16 (8)

Table 6.22 (continued).

$\overline{\mathbb{Q}}$ label	G2-invariants $(g_1, g_2, g_3)$	Bad primes	$\text{Aut}(C_{\overline{\mathbb{Q}}})$	$\text{ST}^0(J)$	$\text{GL}_2/\overline{\mathbb{Q}}?$	$\#C/\mathbb{Q}$ (iso)
<b>2l</b>	$(2^{17}, 2^{11} \cdot 3, -2^9)$	$\{2\}$	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	8 (8)
<b>2m</b>	$(2^{23}, 2^{14} \cdot 17, -2^{12})$	$\{2\}$	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	8 (8)
<b>2n</b>	$(2^{10} \cdot 53^5, 2^5 \cdot 47 \cdot 53^3 \cdot 79, 2^8 \cdot 17 \cdot 53^2 \cdot 79)$	$\{2\}$	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	8 (8)
<b>2o</b>	$(2^7, 2^4 \cdot 5, -2^3 \cdot 3)$	$\{2\}$	$D_4$	$\text{SU}(2)$		8 (5)
<b>2p</b>	$(2^6 \cdot 7^{10}, 2^4 \cdot 7^6 \cdot 367, 2^3 \cdot 3 \cdot 5 \cdot 7^4 \cdot 113)$	$\{2\}$	$C_2$	$\text{SU}(2)$		4 (2)
<b>2q</b>	$(2^{11} \cdot 3^5, 2^7 \cdot 3^3, -2^7 \cdot 3^2 \cdot 5)$	$\{2\}$	$C_2^2$	$\text{U}(1) \times \text{U}(1)$		16 (4)
<b>2r</b>	$(2^4 \cdot 11^5, 2 \cdot 11^3 \cdot 23, -3 \cdot 11^2)$	$\{2\}$	$D_4$	$\text{SU}(2)$		14 (10)
<b>2s</b>	$(2^{16}, 2^{10} \cdot 19, -2^8 \cdot 3)$	$\{2\}$	$C_2$	$\text{SU}(2)$		4 (2)
<b>2t</b>	$(2^{25}, 2^{15} \cdot 31, 2^{13})$	$\{2\}$	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	4 (4)
<b>2u</b>	$(2^{15} \cdot 7^5, 2^9 \cdot 3 \cdot 7^3 \cdot 43, 2^9 \cdot 7^2 \cdot 47)$	$\{2\}$	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	4 (4)
<b>2v</b>	$(2^{16} \cdot 3^5, 2^{10} \cdot 3^3 \cdot 5^2, 2^9 \cdot 3^2 \cdot 7)$	$\{2\}$	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	4 (4)
<b>2w</b>	$(2^{12} \cdot 3^{10}, 2^7 \cdot 3^6 \cdot 5 \cdot 19, 2^8 \cdot 3^4 \cdot 17)$	$\{2\}$	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	4 (4)



Table 6.22 (continued).

$\overline{\mathbb{Q}}$ label	G2-invariants $(g_1, g_2, g_3)$	Bad primes	$\text{Aut}(C_{\overline{\mathbb{Q}}})$	$\text{ST}^0(J)$	$\text{GL}_2/\overline{\mathbb{Q}}?$	$\#C/\mathbb{Q}$ (iso)
<b>2x</b>	$(2^{21}, 2^{13} \cdot 7, 2^{11})$	{2}	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	8 (8)
<b>2y</b>	$(2^{12} \cdot 11^5, 2^7 \cdot 3 \cdot 11^3 \cdot 53, 2^8 \cdot 7^2 \cdot 11^2)$	{2}	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	8 (8)
<b>2z</b>	$(2^3 \cdot 17^5, 7 \cdot 17^4, \frac{3^2 \cdot 17^2 \cdot 31}{2})$	{2}	$C_2$	$\text{USp}(4)$		4 (4)
<b>2A</b>	$(2^2 \cdot 5^5, \frac{5^3 \cdot 11}{2}, \frac{3 \cdot 5^3}{2^2})$	{2}	$C_2$	$\text{USp}(4)$		4 (4)
<b>2B</b>	$(2^{10} \cdot 13^5, 2^6 \cdot 13^3 \cdot 79, 2^5 \cdot 3 \cdot 13^2 \cdot 17)$	{2}	$C_2$	$\text{USp}(4)$		4 (4)
<b>2C</b>	$(2^{10} \cdot 11^5, 2^6 \cdot 11^3 \cdot 37, 2^5 \cdot 3 \cdot 7 \cdot 11^2)$	{2}	$C_2$	$\text{USp}(4)$		4 (4)
<b>2D</b>	$(2^{17} \cdot 5^5, 2^{10} \cdot 5^4 \cdot 7, 2^8 \cdot 3 \cdot 5^2)$	{2}	$C_2$	$\text{USp}(4)$		4 (4)
<b>2E</b>	$(2^{26}, 2^{16}, 0)$	{2}	$C_2$	$\text{USp}(4)$		4 (4)
<b>2F</b>	$(2 \cdot 97^5, \frac{13 \cdot 97^3 \cdot 251}{2^2}, \frac{3 \cdot 11 \cdot 97^2 \cdot 1151}{2^3})$	{2}	$C_2$	$\text{USp}(4)$		4 (4)
<b>2G</b>	$(\frac{11^5}{2^2}, \frac{-11^3 \cdot 13}{2^5}, \frac{3 \cdot 5 \cdot 7 \cdot 11^2}{2^6})$	{2}	$C_2$	$\text{USp}(4)$		4 (4)
<b>2H</b>	$(2 \cdot 3^5 \cdot 7^5, \frac{3^5 \cdot 7^3 \cdot 19}{2^2}, \frac{3^4 \cdot 7^2 \cdot 71}{2^3})$	{2}	$C_2$	$\text{SU}(2)$		4 (1)

Table 6.22 (continued).

$\overline{\mathbb{Q}}$ label	G2-invariants $(g_1, g_2, g_3)$	Bad primes	$\text{Aut}(C_{\overline{\mathbb{Q}}})$	$\text{ST}^0(J)$	$\text{GL}_2/\overline{\mathbb{Q}}?$	$\#C/\mathbb{Q}$ (iso)
2I	$(-2^7 \cdot 3^5, 2^4 \cdot 3^4, -2^3 \cdot 3^3 \cdot 13)$	{2}	$C_2$	SU(2)		4 (1)
2J	$(2^4 \cdot 11^5, 2 \cdot 3 \cdot 5 \cdot 11^3, 3 \cdot 7 \cdot 11^2)$	{2}	$C_2$	USp(4)		4 (4)
2K	$(2^4 \cdot 13^5, 2 \cdot 13^3 \cdot 71, 5 \cdot 13^2 \cdot 31)$	{2}	$C_2$	USp(4)		4 (4)
2L	$(2^6 \cdot 5^5, 2^3 \cdot 5^3 \cdot 17, -2^2 \cdot 3 \cdot 5^3)$	{2}	$C_2$	USp(4)		4 (4)
2M	$(-2^5, 2^2, -2 \cdot 3 \cdot 5)$	{2}	$C_2$	USp(4)		4 (4)
2N	$(2^6 \cdot 3^5 \cdot 5^5, 2^3 \cdot 3^4 \cdot 5^3 \cdot 19, 2^2 \cdot 3^3 \cdot 5^2 \cdot 17)$	{2}	$C_2$	USp(4)		4 (4)
2O	$(2^5 \cdot 3^5, 2^2 \cdot 3^4 \cdot 5, -2 \cdot 3^3)$	{2}	$C_2$	USp(4)		4 (4)
2P	$(2^6 \cdot 83^5, 2^3 \cdot 3 \cdot 83^3 \cdot 631, 2^2 \cdot 3 \cdot 7 \cdot 17 \cdot 31 \cdot 83^2)$	{2}	$C_2$	USp(4)		4 (4)
2Q	$(2^6 \cdot 11^5, 2^3 \cdot 3 \cdot 7 \cdot 11^3, 2^2 \cdot 3 \cdot 11^2)$	{2}	$C_2$	USp(4)		4 (4)
2R	$(2^5 \cdot 5^5, -2^2 \cdot 5^3, -2 \cdot 5^3)$	{2}	$C_2$	USp(4)		4 (4)
2S	$(2^3 \cdot 23^5, 11 \cdot 13 \cdot 23^3, \frac{7 \cdot 23^2 \cdot 31}{2})$	{2}	$C_2$	USp(4)		4 (4)
2T	$(2^2 \cdot 11^5, \frac{3^3 \cdot 11^3}{2}, \frac{-3 \cdot 5 \cdot 11^2}{2^2})$	{2}	$C_2$	USp(4)		4 (4)

Table 6.22 (continued).

$\overline{\mathbb{Q}}$ label	<b>G2-invariants</b> $(g_1, g_2, g_3)$	<b>Bad primes</b>	$\text{Aut}(C_{\overline{\mathbb{Q}}})$	$\text{ST}^0(J)$	$\text{GL}_2/\overline{\mathbb{Q}}?$	$\#C/\mathbb{Q}$ (iso)
<b>2U</b>	$(2^4 \cdot 5^5, 2 \cdot 5^3 \cdot 23, -3^2 \cdot 5^3)$	{2}	$C_2$	USp(4)		4 (4)
<b>2V</b>	$(2^4 \cdot 19^5, 2 \cdot 5 \cdot 19^4, 3 \cdot 19^2 \cdot 31)$	{2}	$C_2$	USp(4)		4 (4)
<b>2W</b>	$(2^4 \cdot 3^{15}, 2 \cdot 3^{10} \cdot 61, 3^7 \cdot 47)$	{2}	$C_2$	$\text{U}(1) \times \text{U}(1)$		4 (2)
<b>2X</b>	$(2^4 \cdot 3^{15}, 2 \cdot 3^9 \cdot 47, 3^6 \cdot 5)$	{2}	$C_2$	USp(4)		4 (4)
<b>2Y</b>	$(\frac{139^5}{2^5}, \frac{139^3 \cdot 5171}{2^8}, \frac{17 \cdot 23 \cdot 79 \cdot 139^2}{2^9})$	{2}	$C_2$	USp(4)		4 (4)
<b>6a</b>	$(\frac{2^9 \cdot 23^5}{3^7}, \frac{2^4 \cdot 5 \cdot 11 \cdot 23^3 \cdot 37}{3^8}, \frac{-2^8 \cdot 23^2 \cdot 89}{3^{10}})$	{2, 3}	$D_4$	U(1)		22 (6)
<b>6b</b>	$(\frac{-2^{18} \cdot 5^5}{3^7}, \frac{2^{10} \cdot 5^3 \cdot 1549}{3^8}, \frac{-2^{11} \cdot 5^2 \cdot 3673}{3^{10}})$	{2, 3}	$C_2^2$	U(1)		16 (4)
<b>6c</b>	$(\frac{-5^5 \cdot 13^5}{2^2 \cdot 3^7}, \frac{-5^3 \cdot 13^4 \cdot 829}{2^5 \cdot 3^8}, \frac{-5^3 \cdot 13^2 \cdot 29 \cdot 163 \cdot 179}{2^6 \cdot 3^{10}})$	{2, 3}	$C_2$	SU(2)		4 (2)
<b>6d</b>	$(\frac{-2^4 \cdot 23^5}{3^7}, \frac{-2^6 \cdot 23^3 \cdot 239}{3^8}, \frac{-2^2 \cdot 5 \cdot 23^2 \cdot 29 \cdot 1451}{3^{10}})$	{2, 3}	$C_2$	SU(2)		4 (2)
<b>6e</b>	$(\frac{-2^{19}}{3^7}, \frac{2^{11} \cdot 13}{3^8}, \frac{-2^{11} \cdot 11 \cdot 107}{3^{10}})$	{2, 3}	$C_2^2$	$\text{U}(1) \times \text{SU}(2)$		16 (8)

Table 6.22 (continued).

$\overline{\mathbb{Q}}$ label	<b>G2-invariants</b> $(g_1, g_2, g_3)$	<b>Bad primes</b>	$\text{Aut}(C_{\overline{\mathbb{Q}}})$	$\text{ST}^0(J)$	$\text{GL}_2/\overline{\mathbb{Q}}?$	$\#C/\mathbb{Q}$ (iso)
<b>6f</b>	$\left(\frac{2^{10} \cdot 13^5}{3^7}, \frac{2^5 \cdot 13^3 \cdot 883}{3^8}, \frac{-2^8 \cdot 13^2 \cdot 281}{3^{10}}\right)$	$\{2, 3\}$	$C_2^2$	$\text{SU}(2) \times \text{SU}(2)$	✓	8 (8)
<b>6g</b>	$\left(\frac{-2^4 \cdot 41^5}{3^7}, \frac{-2 \cdot 41^3 \cdot 1789}{3^8}, \frac{-5 \cdot 17 \cdot 41^2 \cdot 281}{3^{10}}\right)$	$\{2, 3\}$	$C_2$	$\text{USp}(4)$		4 (4)
<b>6h</b>	$\left(\frac{-97^5}{2^5 \cdot 3^7}, \frac{-11 \cdot 97^3 \cdot 1667}{2^8 \cdot 3^8}, \frac{-97^2 \cdot 113 \cdot 45137}{2^9 \cdot 3^{10}}\right)$	$\{2, 3\}$	$C_2$	$\text{USp}(4)$		4 (4)
<b>10a</b>	$\left(\frac{-2^9 \cdot 3^5 \cdot 67^5}{5^{12}}, \frac{-2^5 \cdot 3^3 \cdot 23 \cdot 67^3 \cdot 383}{5^{12}}, \frac{-2^7 \cdot 3^2 \cdot 13^2 \cdot 67^2 \cdot 113}{5^{12}}\right)$	$\{2, 5\}$	$C_2^2$	$\text{U}(1) \times \text{SU}(2)$		16 (8)
<b>10b</b>	$\left(\frac{-2^9 \cdot 29^5}{5^{12}}, \frac{2^4 \cdot 29^3 \cdot 61 \cdot 67}{5^{12}}, \frac{-2^8 \cdot 29^2 \cdot 27529}{5^{12}}\right)$	$\{2, 5\}$	$C_2^2$	$\text{U}(1)$		8 (4)
<b>10c</b>	$\left(\frac{2^5 \cdot 13^5 \cdot 137^5}{5^{12}}, \frac{2^2 \cdot 13^4 \cdot 137^3 \cdot 193 \cdot 443}{5^{12}}, \frac{2 \cdot 7 \cdot 13^2 \cdot 89 \cdot 137^2 \cdot 390821}{5^{12}}\right)$	$\{2, 5\}$	$C_2$	$\text{USp}(4)$		4 (4)
<b>14a</b>	$\left(\frac{2^{13} \cdot 3^{10} \cdot 19^5}{7^{12}}, \frac{2^7 \cdot 3^6 \cdot 19^3 \cdot 59 \cdot 2339}{7^{12}}, \frac{-2^9 \cdot 3^4 \cdot 17 \cdot 19^2 \cdot 6337}{7^{12}}\right)$	$\{2, 7\}$	$C_2^2$	$\text{U}(1) \times \text{U}(1)$		16 (4)
<b>14b</b>	$\left(\frac{-2^8 \cdot 151^5}{7^{12}}, \frac{2^3 \cdot 5 \cdot 41 \cdot 43 \cdot 151^3}{7^{12}}, \frac{-2^8 \cdot 71 \cdot 151^2 \cdot 2663}{7^{12}}\right)$	$\{2, 7\}$	$C_2^2$	$\text{SU}(2)$		8 (6)

Table 6.22 (continued).

$\overline{\mathbb{Q}}$ label	<b>G2-invariants</b> $(g_1, g_2, g_3)$	<b>Bad primes</b>	$\text{Aut}(C_{\overline{\mathbb{Q}}})$	$\text{ST}^0(J)$	$\text{GL}_2/\overline{\mathbb{Q}}?$	$\#C/\mathbb{Q}$ (iso)
<b>26a</b>	$\left(\frac{2 \cdot 11^5 \cdot 41543^5}{13^{12}}, \frac{11^3 \cdot 47 \cdot 28703 \cdot 38699 \cdot 41543^3}{2^2 \cdot 13^{12}}, \frac{-3 \cdot 11^2 \cdot 41543^2 \cdot 76163}{2^3 \cdot 13^{12}}\right)$	$\{2, 13\}$	$D_4$	$\text{SU}(2)$		8 (6)
<b>42a</b>	$\left(\frac{-2^8 \cdot 2281^5}{3^7 \cdot 7^{12}}, \frac{-2^4 \cdot 353 \cdot 2281^3 \cdot 36151}{3^8 \cdot 7^{12}}, \frac{-2^3 \cdot 2281^2 \cdot 3697 \cdot 24726833}{3^{10} \cdot 7^{12}}\right)$	$\{2, 3, 7\}$	$C_2$	$\text{SU}(2)$		4 (2)
<b>66a</b>	$\left(\frac{-2^6 \cdot 19^5 \cdot 617^5}{3^7 \cdot 11^{12}}, \frac{-2 \cdot 5^2 \cdot 13 \cdot 19^3 \cdot 109 \cdot 617^3 \cdot 11467}{3^8 \cdot 11^{12}}, \frac{-2^8 \cdot 19^2 \cdot 577 \cdot 617^2 \cdot 2301569}{3^{10} \cdot 11^{12}}\right)$	$\{2, 3, 11\}$	$C_2^2$	$\text{U}(1)$		4 (2)

*“Goodbye..? Oh no, please. Can’t we go back to page one and do it all over again?”*  
- A.A. Milne, Winnie-the-Pooh

# Appendix A

## Field systems of genus 2 curves

Here, we tabulate a full list of all 48 possible field systems, as defined in Definition 5.8, of a genus 2 curve  $C : y^2 = f(x)$  over  $\mathbb{Q}$  whose Jacobian has good reduction away from 2. We recall that  $K_1, K_2, K_3$  denote the three quadratic fields unramified away from 2, namely  $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2})$  respectively;  $L_1, L_2, \dots, L_7$  denote the seven quartic fields unramified away from 2, namely  $\mathbb{Q}(\sqrt[4]{-1}), \mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt[4]{-2}), \mathbb{Q}(\sqrt{2 + \sqrt{2}}), \mathbb{Q}(\sqrt{-2 - \sqrt{2}}), \mathbb{Q}(\sqrt{1 + \sqrt{2}}), \mathbb{Q}(\sqrt{1 + \sqrt{-1}})$  respectively; and  $M_1, M_2, M_3$  denote the three octic fields  $\mathbb{Q}(\sqrt[8]{-1}), \mathbb{Q}(\zeta_8, \sqrt[4]{2}), \mathbb{Q}(\sqrt[4]{2\sqrt{2} - 3})$  respectively. These are also defined in Tables 5.4 and 5.6 given in Chapter 5.

Table A.1: List of all 48 possible field systems  $[M_1, M_2, \dots, M_m]$  of genus 2 curves  $C : y^2 = f(x)$  over  $\mathbb{Q}$  whose Jacobian has good reduction away from 2. For each field system, we give the corresponding field of 2-torsion  $\mathbb{Q}(J[2])$  and its Galois group. We also give the number of rational 2-torsion points  $\#J(\mathbb{Q})[2]$ , the mod 2 Galois image  $\text{Im}(\bar{\rho}_{C,2})$ , and the number of known genus 2 curves  $C/\mathbb{Q}$  with 2-power conductor with this field system.

Field System	$\mathbb{Q}(J[2])$	$\text{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$	$\#J(\mathbb{Q})[2]$	$\text{Im}(\bar{\rho}_{C,2})$	Num curves
$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}]$	$\mathbb{Q}$	$C_1$	16	$\{I\}$	0
$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_1]$	$K_1$	$C_2$	8	2b	1
$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_2]$	$K_2$	$C_2$	8	2b	2
$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_3]$	$K_3$	$C_2$	8	2b	3
$[\mathbb{Q}, \mathbb{Q}, K_1, K_1]$	$K_1$	$C_2$	4	2c	1
$[\mathbb{Q}, \mathbb{Q}, K_1, K_2]$	$L_1$	$C_2^2$	4	4c	4

Table A.1 (continued).

Field System	$\mathbb{Q}(J[2])$	$\text{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$	$\#J(\mathbb{Q})[2]$	$\text{Im}(\bar{\rho}_{C,2})$	Num curves
$[\mathbb{Q}, \mathbb{Q}, K_1, K_3]$	$L_1$	$C_2^2$	4	4c	12
$[\mathbb{Q}, \mathbb{Q}, K_2, K_2]$	$K_2$	$C_2$	4	2c	3
$[\mathbb{Q}, \mathbb{Q}, K_2, K_3]$	$L_1$	$C_2^2$	4	4c	3
$[\mathbb{Q}, \mathbb{Q}, K_3, K_3]$	$K_3$	$C_2$	4	2c	5
$[\mathbb{Q}, \mathbb{Q}, L_1]$	$L_1$	$C_2^2$	2	4a	12
$[\mathbb{Q}, \mathbb{Q}, L_2]$	$M_2$	$D_4$	2	8c	34
$[\mathbb{Q}, \mathbb{Q}, L_3]$	$M_2$	$D_4$	2	8c	6
$[\mathbb{Q}, \mathbb{Q}, L_4]$	$L_4$	$C_4$	2	4e	56
$[\mathbb{Q}, \mathbb{Q}, L_5]$	$L_5$	$C_4$	2	4e	8
$[\mathbb{Q}, \mathbb{Q}, L_6]$	$M_3$	$D_4$	2	8c	36
$[\mathbb{Q}, \mathbb{Q}, L_7]$	$M_3$	$D_4$	2	8c	26
$[K_1, K_1, K_1]$	$K_1$	$C_2$	4	2a	0
$[K_1, K_1, K_2]$	$L_1$	$C_2^2$	4	4f	2
$[K_1, K_1, K_3]$	$L_1$	$C_2^2$	4	4f	5
$[K_1, K_2, K_2]$	$L_1$	$C_2^2$	4	4f	2
$[K_1, K_2, K_3]$	$L_1$	$C_2^2$	4	4b	4
$[K_1, K_3, K_3]$	$L_1$	$C_2^2$	4	4f	12
$[K_2, K_2, K_2]$	$K_2$	$C_2$	4	2a	0
$[K_2, K_2, K_3]$	$L_1$	$C_2^2$	4	4f	2
$[K_2, K_3, K_3]$	$L_1$	$C_2^2$	4	4f	6
$[K_3, K_3, K_3]$	$K_3$	$C_2$	4	2a	2
$[K_1, L_1]$	$L_1$	$C_2^2$	2	4d	4



Table A.1 (continued).

Field System	$\mathbb{Q}(J[2])$	$\text{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$	$\#J(\mathbb{Q})[2]$	$\text{Im}(\bar{\rho}_{C,2})$	Num curves
$[K_1, L_2]$	$M_2$	$D_4$	2	8d	14
$[K_1, L_3]$	$M_2$	$D_4$	2	8d	10
$[K_1, L_4]$	$M_1$	$C_2 \times C_4$	2	8e	12
$[K_1, L_5]$	$M_1$	$C_2 \times C_4$	2	8e	10
$[K_1, L_6]$	$M_3$	$D_4$	2	8a	24
$[K_1, L_7]$	$M_3$	$D_4$	2	8b	10
$[K_2, L_1]$	$L_1$	$C_2^2$	2	4d	6
$[K_2, L_2]$	$M_2$	$D_4$	2	8a	16
$[K_2, L_3]$	$M_2$	$D_4$	2	8b	4
$[K_2, L_4]$	$M_1$	$C_2 \times C_4$	2	8e	8
$[K_2, L_5]$	$M_1$	$C_2 \times C_4$	2	8e	10
$[K_2, L_6]$	$M_3$	$D_4$	2	8d	20
$[K_2, L_7]$	$M_3$	$D_4$	2	8d	16
$[K_3, L_1]$	$L_1$	$C_2^2$	2	4d	5
$[K_3, L_2]$	$M_2$	$D_4$	2	8b	18
$[K_3, L_3]$	$M_2$	$D_4$	2	8a	12
$[K_3, L_4]$	$L_4$	$C_4$	2	4g	24
$[K_3, L_5]$	$L_5$	$C_4$	2	4g	8
$[K_3, L_6]$	$M_3$	$D_4$	2	8b	18
$[K_3, L_7]$	$M_3$	$D_4$	2	8a	16

# Appendix B

## Mod- $\ell$ Galois images

### B.1 Mod 2 Galois images

Table B.1: List of the 15 possible mod 2 Galois images  $\text{Im}(\bar{\rho}_{C,2})$  in  $\text{GSp}_4(\mathbb{F}_2)$  for our table of 512 genus 2 curves in Table 6.21. For each possible mod 2 image, we give our label, the corresponding LMFDB label, and a description of  $\text{Im}(\bar{\rho}_{C,2})$  as an abstract group. Here  $C_n$  denotes the cyclic group of order  $n$  and  $D_n$  denotes the dihedral group of order  $2n$ .

Label	LMFDB label	Order	Group	Matrix Generators	Num curves
2a	<a href="#">2.360.3</a>	2	$C_2$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	2
2b	<a href="#">2.360.2</a>	2	$C_2$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$	6
2c	<a href="#">2.360.1</a>	2	$C_2$	$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$	9

Table B.1 (continued).

Label	LMFDB label	Order	Group	Matrix Generators	Num curves
4a	<a href="#">2.180.5</a>	4	$C_2 \times C_2$	$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$	12
4b	<a href="#">2.180.6</a>	4	$C_2 \times C_2$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	4
4c	<a href="#">2.180.3</a>	4	$C_2 \times C_2$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$	19
4d	<a href="#">2.180.4</a>	4	$C_2 \times C_2$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	15
4e	<a href="#">2.180.2</a>	4	$C_4$	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$	64
4f	<a href="#">2.180.7</a>	4	$C_2 \times C_2$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	29
4g	<a href="#">2.180.1</a>	4	$C_4$	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$	32

Table B.1 (continued).

Label	LMFDB label	Order	Group	Matrix Generators	Num curves
8a	<a href="#">2.90.2</a>	8	$D_4$	$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	68
8b	<a href="#">2.90.1</a>	8	$D_4$	$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$	50
8c	<a href="#">2.90.3</a>	8	$D_4$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	102
8d	<a href="#">2.90.4</a>	8	$D_4$	$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$	60
8e	<a href="#">2.90.7</a>	8	$C_2 \times C_4$	$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	40

## B.2 Mod 3 Galois images

Table B.2: List of the 33 possible mod 3 Galois images  $\text{Im}(\bar{\rho}_{C,3})$  in  $\text{GSp}_4(\mathbb{F}_3)$  for our table of 512 genus 2 curves in Table 6.21. For each possible mod 3 image, we give the label (as provided by Chidambaram [101]), and the GAP ID and (possibly multiple) description(s) of  $\text{Im}(\bar{\rho}_{C,3})$  as an abstract group. As before,  $C_n$  denotes the cyclic group of order  $n$ ,  $D_n$  denotes the dihedral group of order  $2n$ , and  $Q_n$  denotes the (generalised) quaternion group of order  $n$ .

Label	GAP ID	Group	Matrix Generators	Num curves
3.12960.8	$\langle 8, 3 \rangle$	$D_4$	$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 1 & 2 & 1 & 2 \\ 2 & 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 \\ 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$	2
3.12960.18	$\langle 8, 3 \rangle$	$D_4$	$\begin{pmatrix} 1 & 2 & 1 & 2 \\ 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	2
3.6480.9	$\langle 16, 11 \rangle$	$C_2 \times D_4$	$\begin{pmatrix} 2 & 1 & 1 & 0 \\ 2 & 1 & 0 & 2 \\ 2 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	3
3.6480.17	$\langle 16, 13 \rangle$	$C_4 \circ D_4,$ $D_4 \rtimes C_2$	$\begin{pmatrix} 1 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \\ 2 & 2 & 0 & 1 \\ 1 & 2 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 2 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 2 & 2 \\ 0 & 2 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	1
3.6480.18	$\langle 16, 13 \rangle$	$C_4 \circ D_4,$ $D_4 \rtimes C_2$	$\begin{pmatrix} 2 & 1 & 2 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 2 & 2 \\ 0 & 2 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 2 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 2 & 0 \\ 0 & 2 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$	3
3.6480.22	$\langle 16, 8 \rangle$	$\text{SD}_{16},$ $2\text{-Sylow}(\text{GL}_2(\mathbb{F}_3))$	$\begin{pmatrix} 1 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \\ 2 & 0 & 1 & 1 \\ 1 & 2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	8
3.6480.28	$\langle 16, 11 \rangle$	$C_2 \times D_4$	$\begin{pmatrix} 2 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 \\ 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	6

Table B.2 (continued).

Label	GAP ID	Group	Matrix Generators	Num curves
3.6480.29	<a href="#">⟨16, 13⟩</a>	$C_4 \circ D_4$ , $D_4 \rtimes C_2$	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 2 \end{pmatrix}$	3
3.3240.4	<a href="#">⟨32, 44⟩</a>	$Q_{16} \rtimes C_2$ , $C_8.C_2^2$	$\begin{pmatrix} 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 \\ 2 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 2 & 1 \\ 0 & 2 & 2 & 2 \\ 1 & 1 & 0 & 2 \\ 2 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 2 & 0 \\ 1 & 2 & 0 & 1 \\ 1 & 0 & 2 & 2 \\ 0 & 2 & 1 & 1 \end{pmatrix}$	2
3.3240.5	<a href="#">⟨32, 42⟩</a>	$C_4 \circ D_8$ , $D_8 \rtimes C_2$	$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 2 \\ 2 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 1 & 2 \\ 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$	6
3.3240.7	<a href="#">⟨32, 43⟩</a>	$C_8 \rtimes C_2^2$ , $D_8 \rtimes C_2$ , $\text{Aut}(D_8)$	$\begin{pmatrix} 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 1 & 2 \\ 0 & 0 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 1 & 2 \\ 2 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$	4
3.3240.8	<a href="#">⟨32, 40⟩</a>	$C_2 \times \text{SD}_{16}$ , $2\text{-Sylow}(\text{GL}_3(\mathbb{F}_3))$	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 \\ 2 & 2 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 2 & 0 & 2 & 2 \\ 2 & 1 & 0 & 1 \\ 2 & 1 & 2 & 0 \end{pmatrix}$	14
3.3240.12	<a href="#">⟨32, 42⟩</a>	$C_4 \circ D_8$ , $D_8 \rtimes C_2$	$\begin{pmatrix} 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 2 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{pmatrix}$	4
3.3240.21	<a href="#">⟨32, 38⟩</a>	$C_8 \circ D_4$ , $\text{OD}_{16} \rtimes C_2$	$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 2 & 0 & 2 \\ 1 & 0 & 1 & 1 \\ 1 & 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 2 & 1 \\ 1 & 0 & 2 & 1 \\ 1 & 1 & 0 & 2 \\ 2 & 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{pmatrix}$	2
3.2160.36	<a href="#">⟨48, 29⟩</a>	$\text{GL}_2(\mathbb{F}_3)$	$\begin{pmatrix} 2 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 2 & 2 \\ 2 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 2 & 2 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 2 \end{pmatrix}$	4

Table B.2 (continued).

Label	GAP ID	Group	Matrix Generators	Num curves
3.1620.8	<a href="#">⟨64, 141⟩</a>	$Q_8 \rtimes D_4$ , $C_4 \rtimes \text{SD}_{16}$	$\begin{pmatrix} 2 & 1 & 1 & 2 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 2 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 0 \\ 2 & 0 & 0 & 2 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$	48
3.1620.12	<a href="#">⟨64, 152⟩</a>	$C_8.D_4$	$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 2 & 2 \\ 2 & 1 & 0 & 1 \\ 2 & 0 & 2 & 2 \\ 2 & 1 & 2 & 0 \end{pmatrix}$	8
3.1620.13	<a href="#">⟨64, 173⟩</a>	$C_8 \rtimes D_4$	$\begin{pmatrix} 0 & 1 & 1 & 2 \\ 2 & 2 & 0 & 1 \\ 2 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 2 & 0 \\ 1 & 1 & 0 & 2 \\ 2 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 \end{pmatrix}$	16
3.1296.1	<a href="#">⟨80, 29⟩</a>	$C_{20}.C_4$	$\begin{pmatrix} 0 & 1 & 2 & 0 \\ 2 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 2 \\ 1 & 0 & 1 & 1 \end{pmatrix}$	4
3.1080.7	<a href="#">⟨96, 192⟩</a>	$C_4 \circ \text{GL}_2(\mathbb{F}_3)$ , $\text{GL}_2(\mathbb{F}_3) \rtimes C_2$	$\begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 & 1 \\ 2 & 2 & 1 & 0 \\ 0 & 2 & 2 & 1 \\ 2 & 2 & 0 & 1 \end{pmatrix}$	6
3.1080.13	<a href="#">⟨96, 189⟩</a>	$C_2 \times \text{GL}_2(\mathbb{F}_3)$	$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 1 & 1 & 2 & 0 \\ 2 & 0 & 2 & 2 \\ 2 & 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 2 \\ 1 & 2 & 1 & 2 \end{pmatrix}$	20
3.1080.19	<a href="#">⟨96, 192⟩</a>	$C_4 \circ \text{GL}_2(\mathbb{F}_3)$ , $\text{GL}_2(\mathbb{F}_3) \rtimes C_2$	$\begin{pmatrix} 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 2 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$	4
3.540.4	<a href="#">⟨192, 1485⟩</a>	$\text{GL}_2(\mathbb{F}_3) \rtimes C_2^2$ , $D_4.S_4$	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 1 & 0 \\ 2 & 0 & 1 & 2 \\ 1 & 0 & 1 & 1 \end{pmatrix}$	10

Table B.2 (continued).

Label	GAP ID	Group	Matrix Generators	Num curves
3.540.10	<a href="#">⟨192, 963⟩</a>	$\text{CU}_2(\mathbb{F}_3),$ $\text{GL}_2(\mathbb{F}_3) \rtimes C_4$	$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 2 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 \\ 2 & 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 & 2 \\ 0 & 2 & 1 & 0 \\ 0 & 2 & 2 & 0 \\ 1 & 0 & 0 & 2 \end{pmatrix}$	16
3.540.12	<a href="#">⟨192, 952⟩</a>	$C_4 \rtimes \text{GL}_2(\mathbb{F}_3),$ $Q_8 \rtimes D_{12}$	$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 2 & 1 \\ 2 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 \end{pmatrix}$	32
3.405.1	<a href="#">⟨256, 6671⟩</a>	$Q_8^2 \rtimes C_2^2$	$\begin{pmatrix} 2 & 1 & 1 & 1 \\ 2 & 2 & 2 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 2 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 2 & 1 & 2 & 0 \\ 1 & 2 & 0 & 2 \end{pmatrix}$	8
3.360.1	<a href="#">⟨288, 875⟩</a>	$C_4.\text{SO}_4^+(\mathbb{F}_2)$	$\begin{pmatrix} 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 1 & 0 \\ 2 & 2 & 2 & 1 \\ 2 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 2 & 0 \\ 0 & 2 & 1 & 2 \\ 2 & 1 & 2 & 1 \\ 2 & 2 & 0 & 0 \end{pmatrix}$	8
3.270.1	<a href="#">⟨384, 18045⟩</a>	$\text{GL}_2(\mathbb{F}_3) \rtimes D_4$	$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 1 & 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}$	44
3.270.4	<a href="#">⟨384, 5676⟩</a>	$Q_8 \rtimes \text{GL}_2(\mathbb{F}_3)$	$\begin{pmatrix} 2 & 0 & 1 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 2 \\ 2 & 2 & 0 & 0 \\ 1 & 1 & 2 & 2 \\ 1 & 2 & 2 & 1 \end{pmatrix}$	64
3.135.1	<a href="#">⟨768, 1086054⟩</a>	$Q_8^2 \rtimes D_6$	$\begin{pmatrix} 2 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 \\ 2 & 0 & 2 & 2 \\ 1 & 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 2 & 2 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 2 & 2 & 0 & 0 \end{pmatrix}$	8
3.135.2	<a href="#">⟨768, 1086054⟩</a>	$Q_8^2 \rtimes D_6$	$\begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 2 & 0 & 1 \\ 1 & 0 & 0 & 2 \\ 1 & 1 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 1 & 2 & 2 \\ 2 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix}$	16



Table B.2 (continued).

Label	GAP ID	Group	Matrix Generators	Num curves
<b>3.45.1</b>	$\langle 2304, - \rangle$	$Q_8^2.S_3^2$	$\begin{pmatrix} 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 2 \\ 0 & 2 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 0 & 1 \\ 0 & 1 & 2 & 2 \\ 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 2 \end{pmatrix}$	32
<b>1.1.1</b>	$\langle 103680, - \rangle$	$\mathrm{GSp}_4(\mathbb{F}_3)$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 1 & 1 \\ 2 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	104

# Bibliography

- [1] ABRAMOVICH, D. Birational geometry for number theorists. In *Arithmetic geometry*, vol. 8 of *Clay Math. Proc.* Amer. Math. Soc., Providence, RI, 2009, pp. 335–373. [3](#)
- [2] ABRASHKIN, V. A. Galois modules of group schemes of period  $p$  over the ring of Witt vectors. *Izv. Akad. Nauk SSSR Ser. Mat.* 51, 4 (1987), 691–736, 910. [1.1.3](#)
- [3] ABRAŠKIN, V. A. Good reduction of two-dimensional Abelian varieties. *Izv. Akad. Nauk SSSR Ser. Mat.* 40, 2 (1976), 262–272, 460. [1.1.3](#)
- [4] ABRAŠKIN, V. A.  $p$ -divisible groups over  $\mathbb{Z}$ . *Izv. Akad. Nauk SSSR Ser. Mat.* 41, 5 (1977), 987–1007, 1199. [1.1.3](#)
- [5] ACHTER, J., AND WILLIAMS, C. Local heuristics and an exact formula for abelian surfaces over finite fields. *Canad. Math. Bull.* 58, 4 (2015), 673–691. [4.3.3](#)
- [6] ACHTER, J. D. Detecting complex multiplication. In *Computational aspects of algebraic curves*, vol. 13 of *Lecture Notes Ser. Comput.* World Sci. Publ., Hackensack, NJ, 2005, pp. 38–50. [4.2.1](#)
- [7] ACZEL, A. D. *Fermat’s Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem*. A Delta book. Dell Pub., 1997. [1.7.1](#)
- [8] AGRAWAL, M. K., COATES, J. H., HUNT, D. C., AND VAN DER POORTEN, A. J. Elliptic curves of conductor 11. *Math. Comp.* 35, 151 (1980), 991–1002. [1.1](#), [3](#)
- [9] ALLEN, P. B., CALEGARI, F., CARAIANI, A., GEE, T., HELM, D., LE HUNG, B. V., NEWTON, J., SCHOLZE, P., TAYLOR, R., AND THORNE, J. A. Potential automorphy over CM fields. *Ann. of Math. (2)* 197, 3 (2023), 897–1113. [1.7.1](#)

- [10] ALLEN, P. B., KHARE, C., AND THORNE, J. A. Modularity of  $\mathrm{GL}_2(\mathbb{F}_p)$ -representations over CM fields. *Camb. J. Math.* 11, 1 (2023), 1–158. [1.7.1](#)
- [11] ALPÖGE, L., AND LAWRENCE, B. Conditional algorithmic Mordell, 2024. arXiv:2408.11653 [math.NT]. [1.1.3](#), [4.3](#)
- [12] ALPÖGE, L. H. A. *Points on Curves*. ProQuest LLC, Ann Arbor, MI, 2020. Thesis (Ph.D.)–Princeton University. [1.1.3](#)
- [13] ALVARADO, A., KOUTSIANAS, A., MALMSKOG, B., RASMUSSEN, C., VINCENT, C., AND WEST, M. A robust implementation for solving the  $S$ -unit equation and several applications. In *Arithmetic geometry, number theory, and computation*, Simons Symp. Springer, Cham, [2021] ©2021, pp. 1–41. [5](#)
- [14] AMOROSO, F., AND VIADA, E. Small points on subvarieties of a torus. *Duke Math. J.* 150, 3 (2009), 407–442. [2.2](#)
- [15] ANDRÉ, Y. On the Shafarevich and Tate conjectures for hyper-Kähler varieties. *Math. Ann.* 305, 2 (1996), 205–248. [1](#)
- [16] ANNI, S., AND DOKCHITSER, V. Constructing hyperelliptic curves with surjective Galois representations. *Trans. Amer. Math. Soc.* 373, 2 (2020), 1477–1500. [1.4](#)
- [17] ARAKELOV, S. J. Families of algebraic curves with fixed degeneracies. *Izv. Akad. Nauk SSSR Ser. Mat.* 35 (1971), 1269–1293. [1](#)
- [18] AUBRY, Y., HALOUI, S., AND LACHAUD, G. On the number of points on abelian and Jacobian varieties over finite fields. *Acta Arith.* 160, 3 (2013), 201–241. [4.1](#), [5.1.3](#)
- [19] AVNI, N., ONN, U., PRASAD, A., AND VASERSTEIN, L. Similarity classes of  $3 \times 3$  matrices over a local principal ideal ring. *Comm. Algebra* 37, 8 (2009), 2601–2615. [4.3.3](#)
- [20] BAKER, A. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika* 13 (1966), 204–216; *ibid.* 14 (1967), 102–107; *ibid.* 14 (1967), 220–228. [5](#)
- [21] BAKER, A. Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms. *Philos. Trans. Roy. Soc. London Ser. A* 263 (1967/68), 173–191. [2](#)

- [22] BAKER, A. The Diophantine equation  $y^2 = ax^3 + bx^2 + cx + d$ . *J. London Math. Soc.* 43 (1968), 1–9. 2
- [23] BAKER, M. H., GONZÁLEZ-JIMÉNEZ, E., GONZÁLEZ, J., AND POONEN, B. Finiteness results for modular curves of genus at least 2. *Amer. J. Math.* 127, 6 (2005), 1325–1387. 3.8
- [24] BALAKRISHNAN, J., DOGRA, N., MÜLLER, J. S., TUITMAN, J., AND VONK, J. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)* 189, 3 (2019), 885–944. 1
- [25] BALAKRISHNAN, J. S., BEST, A. J., BIANCHI, F., LAWRENCE, B., MÜLLER, J. S., TRIANTAFILLOU, N., AND VONK, J. Two recent  $p$ -adic approaches towards the (effective) Mordell conjecture. In *Arithmetic L-functions and differential geometric methods*, vol. 338 of *Progr. Math.* Birkhäuser/Springer, Cham, [2021] ©2021, pp. 31–74. 1
- [26] BALAKRISHNAN, J. S., DOGRA, N., MÜLLER, J. S., TUITMAN, J., AND VONK, J. Quadratic Chabauty for modular curves: algorithms and examples. *Compos. Math.* 159, 6 (2023), 1111–1152. 1
- [27] BALAKRISHNAN, J. S., HO, W., KAPLAN, N., SPICER, S., STEIN, W., AND WEIGANDT, J. Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks. *LMS J. Comput. Math.* 19 (2016), 351–370. 1.1.1
- [28] BANWAIT, B. S., BRUMER, A., KIM, H. J., KLAGSBRUN, Z., MAYLE, J., SRINIVASAN, P., AND VOGT, I. Computing nonsurjective primes associated to Galois representations of genus 2 curves. In *LuCaNT: LMFDB, computation, and number theory*, vol. 796 of *Contemp. Math.* Amer. Math. Soc., [Providence], RI, [2024] ©2024, pp. 129–163. 6.1.12
- [29] BARSAGADE, M. W., AND MESHAM, S. A. Overview of History of Elliptic Curves and its use in cryptography. *Int. J. Sci. Engrg. Res.* 5, 4 (2014), 467–470. 1.1.1
- [30] BEASLEY, J. E., Ed. *Advances in linear and integer programming*, vol. 4 of *Oxford Lecture Series in Mathematics and its Applications*. The Clarendon Press, Oxford University Press, New York, 1996. Oxford Science Publications. 5.2.7
- [31] BEDRATYUK, L. On complete system of invariants for the binary form of degree 7. *J. Symbolic Comput.* 42, 10 (2007), 935–947. 1.5

- [32] BENNETT, M. A., GHERGA, A., AND RECHNITZER, A. Computing elliptic curves over  $\mathbb{Q}$ . *Math. Comp.* 88, 317 (2019), 1341–1390. **3, 3**
- [33] BENNETT, M. A., AND RECHNITZER, A. Computing elliptic curves over  $\mathbb{Q}$ : bad reduction at one prime. In *Recent progress and modern challenges in applied mathematics, modeling and computational science*, vol. 79 of *Fields Inst. Commun.* Springer, New York, 2017, pp. 387–415. **3**
- [34] BESCHE, H. U., EICK, B., AND O'BRIEN, E. A. A millennium project: constructing small groups. *Internat. J. Algebra Comput.* 12, 5 (2002), 623–644. **4.3.4**
- [35] BEST, A. J., BETTS, L. A., BISATT, M., VAN BOMMEL, R., DOKCHITSER, V., FARAGGI, O., KUNZWEILER, S., MAISTRET, C., MORGAN, A., MUSELLI, S., AND NOWELL, S. A user's guide to the local arithmetic of hyperelliptic curves. *Bull. Lond. Math. Soc.* 54, 3 (2022), 825–867. **1.4**
- [36] BEST, A. J., AND MATSCHKE, B. Elliptic curves with good reduction outside of the first six primes. In *Arithmetic geometry, number theory, and computation*, Simons Symp. Springer, Cham, [2021] ©2021, pp. 215–235. **1.1**
- [37] BEST, A. J., AND VAN BOMMEL, R. Cluster pictures in SageMath. [Online]. Available at <https://alexjbest.github.io/cluster-pictures/>, 2020. (Accessed: 21 August 2021). **1.4**
- [38] BETTS, L. A. Variation of Tamagawa numbers of Jacobians of hyperelliptic curves with semistable reduction. *J. Number Theory* 231 (2022), 158–213. **1.4**
- [39] BIAN, C. Computing  $GL(3)$  automorphic forms. *Bull. Lond. Math. Soc.* 42, 5 (2010), 827–842. **5.1.1**
- [40] BILU, Y., AND PARENT, P. Runge's method and modular curves. *Int. Math. Res. Not. IMRN*, 9 (2011), 1997–2027. **6**
- [41] BILU, Y., PARENT, P., AND REBOLLEDO, M. Rational points on  $X_0^+(p^r)$ . *Ann. Inst. Fourier (Grenoble)* 63, 3 (2013), 957–984. **6**
- [42] BILU, Y. F. The many faces of the subspace theorem [after Adamczewski, Bugeaud, Corvaja, Zannier...]. No. 317 in *Astérisque*. Société mathématique de France, 2008, pp. Exp. No. 967, vii, 1–38. Séminaire Bourbaki. Vol. 2006/2007. **3**

- [43] BIRCH, B. J. Elliptic curves over  $Q$ : A progress report. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, vol. Vol. XX of *Proc. Sympos. Pure Math.* Amer. Math. Soc., Providence, RI, 1971, pp. 396–400. [4](#)
- [44] BIRCH, B. J., AND KUYK, W., Eds. *Modular functions of one variable. IV* (1975), vol. Vol. 476 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin-New York. [4](#), [1.1.1](#)
- [45] BIRCH, B. J., AND MERRIMAN, J. R. Finiteness theorems for binary forms with given discriminant. *Proc. London Math. Soc. (3)* *24* (1972), 385–394. [5.2.4](#)
- [46] BIRCH, B. J., AND SWINNERTON-DYER, H. P. F. Notes on elliptic curves. II. *J. Reine Angew. Math.* *218* (1965), 79–108. [1.6](#)
- [47] BLOCH, S. The proof of the Mordell conjecture. *Math. Intelligencer* *6*, 2 (1984), 41–47. [1](#)
- [48] BOBER, J. W., BOOKER, A. R., COSTA, E., LEE, M., PLATT, D. J., AND SUTHERLAND, A. V. Computing motivic  $L$ -functions. (under preparation). [4](#)
- [49] BÖLLING, R. Elliptische Kurven mit Primzahlführer. *Math. Nachr.* *80* (1977), 253–278. [1.1.1](#)
- [50] BOMBIERI, E. The Mordell conjecture revisited. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* *17*, 4 (1990), 615–640. [1](#)
- [51] BOOKER, A. R. Numerical tests of modularity. *J. Ramanujan Math. Soc.* *20*, 4 (2005), 283–339. [5.1.1](#)
- [52] BOOKER, A. R. A converse theorem without root numbers. *Mathematika* *65*, 4 (2019), 862–873. [5.1](#)
- [53] BOOKER, A. R., SIJSLING, J., SUTHERLAND, A. V., VOIGHT, J., AND YASAKI, D. Sato-Tate groups and explicit modularity for atypical abelian surfaces. (under preparation). [1.7.2](#)
- [54] BOOKER, A. R., SIJSLING, J., SUTHERLAND, A. V., VOIGHT, J., AND YASAKI, D. A database of genus-2 curves over the rational numbers. *LMS J. Comput. Math.* *19* (2016), 235–254. [6](#), [1](#)

- [55] BOOKER, A. R., AND SUTHERLAND, A. V. Genus 2 curves over  $\mathbb{Q}$  of small conductor, 2024. Conference on Curves, Abelian Varieties and Related Topics, Barcelona. [1.7.2](#), [5.1](#), [1](#)
- [56] BÖRNER, M., BOUW, I. I., AND WEWERS, S. The functional equation for  $L$ -functions of hyperelliptic curves. *Exp. Math.* **26**, 4 (2017), 396–411. [1.15](#)
- [57] BOSCH, S., LÜTKEBOHMERT, W., AND RAYNAUD, M. *Néron models*, vol. 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990. [1.3](#)
- [58] BOSMA, W., CANNON, J., AND PLAYOUST, C. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24**, 3-4 (1997), 235–265. Computational algebra and number theory (London, 1993). [1.6.2](#), [4.3.5](#), [6](#)
- [59] BOST, J.-B. Périodes et isogenies des variétés abéliennes sur les corps de nombres (d’après D. Masser et G. Wüstholz). No. 237 in *Astérisque*. Société mathématique de France, 1996, pp. Exp. No. 795, 4, 115–161. Séminaire Bourbaki, Vol. 1994/95. [5.3.1](#)
- [60] BOSTON, N. A refinement of the Faltings-Serre method. In *Number theory (Paris, 1992–1993)*, vol. 215 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 1995, pp. 61–68. [4.2](#)
- [61] BOUW, I. I., DO, D. K., AND WEWERS, S. Computing the Weil representation of a superelliptic curve. *Indag. Math. (N.S.)* **35**, 4 (2024), 708–727. [6](#)
- [62] BOUW, I. I., KOUTSIANAS, A., SIJSLING, J., AND WEWERS, S. Conductor and discriminant of Picard curves. *J. Lond. Math. Soc. (2)* **102**, 1 (2020), 368–404. [1.1.2](#)
- [63] BOUW, I. I., AND WEWERS, S. Computing  $L$ -functions and semistable reduction of superelliptic curves. *Glasg. Math. J.* **59**, 1 (2017), 77–108. [1.20](#), [1.6.2](#)
- [64] BOX, J. Elliptic curves over totally real quartic fields not containing  $\sqrt{5}$  are modular. *Trans. Amer. Math. Soc.* **375**, 5 (2022), 3129–3172. [1.7.1](#)
- [65] BOX, J., AND FOURN, S. L. Bounding integral points on the Siegel modular variety  $A_2(2)$ . *Res. Number Theory* **9**, 2 (2023), Paper No. 25, 18. [2](#), [2.3](#), [2.20](#)

- [66] BOXER, G., CALEGARI, F., GEE, T., AND PILLONI, V. Abelian surfaces over totally real fields are potentially modular. *Publ. Math. Inst. Hautes Études Sci.* 134 (2021), 153–501. [1.7.1](#), [1.7.2](#), [5.1.1](#), [6.1.11](#)
- [67] BOXER, G., CALEGARI, F., GEE, T., AND PILLONI, V. Modularity theorems for abelian surfaces, 2025. [arXiv:2502.20645 \[math.NT\]](#). [1.7.2](#)
- [68] BREUIL, C., CONRAD, B., DIAMOND, F., AND TAYLOR, R. On the modularity of elliptic curves over  $\mathbf{Q}$ : wild 3-adic exercises. *J. Amer. Math. Soc.* 14, 4 (2001), 843–939. [4](#), [1.7.1](#), [1.16](#)
- [69] BRÖKER, R., HOWE, E. W., LAUTER, K. E., AND STEVENHAGEN, P. Genus-2 curves and Jacobians with a given number of points. *LMS J. Comput. Math.* 18, 1 (2015), 170–197. [5.3.1](#)
- [70] BROUWER, A. E., AND POPOVICIU, M. The invariants of the binary decimic. *J. Symbolic Comput.* 45, 8 (2010), 837–843. [1.5](#)
- [71] BROUWER, A. E., AND POPOVICIU, M. The invariants of the binary nonic. *J. Symbolic Comput.* 45, 6 (2010), 709–720. [1.5](#)
- [72] BROWN, J. Residually reducible representations of algebras over local Artinian rings. *Proc. Amer. Math. Soc.* 136, 10 (2008), 3409–3414. [4.2.2](#)
- [73] BRUIN, N., FLYNN, E. V., GONZÁLEZ, J., AND ROTGER, V. On finiteness conjectures for endomorphism algebras of abelian surfaces. *Math. Proc. Cambridge Philos. Soc.* 141, 3 (2006), 383–408. [6.1.6](#)
- [74] BRUIN, N., FLYNN, E. V., AND SHNIDMAN, A. Genus two curves with full  $\sqrt{3}$ -level structure and Tate-Shafarevich groups. *Selecta Math. (N.S.)* 29, 3 (2023), Paper No. 42, 33. [1.4](#)
- [75] BRUIN, N., AND STOLL, M. Two-cover descent on hyperelliptic curves. *Math. Comp.* 78, 268 (2009), 2347–2370. [6.1.10](#)
- [76] BRUMER, A. Personal communication, 2024. [1.3.1](#)
- [77] BRUMER, A., AND KRAMER, K. The conductor of an abelian variety. *Compositio Math.* 92, 2 (1994), 227–248. [1.3.1](#), [5.1](#)
- [78] BRUMER, A., AND KRAMER, K. Non-existence of certain semistable abelian varieties. *Manuscripta Math.* 106, 3 (2001), 291–304. [1.1.3](#)



- [79] BRUMER, A., AND KRAMER, K. Paramodular abelian varieties of odd conductor. *Trans. Amer. Math. Soc.* 366, 5 (2014), 2463–2516. 1.7.2
- [80] BRUMER, A., AND KRAMER, K. Certain abelian varieties bad at only one prime. *Algebra Number Theory* 12, 5 (2018), 1027–1071. 1.1.3
- [81] BRUMER, A., AND KRAMER, K. Corrigendum to “Paramodular abelian varieties of odd conductor”. *Trans. Amer. Math. Soc.* 372, 3 (2019), 2251–2254. 1.7.2
- [82] BRUMER, A., AND MCGUINNESS, O. The behavior of the Mordell-Weil group of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)* 23, 2 (1990), 375–382. 1.1.1
- [83] BRUMER, A., PACETTI, A., POOR, C., TORNARÍA, G., VOIGHT, J., AND YUEN, D. S. On the paramodularity of typical abelian surfaces. *Algebra Number Theory* 13, 5 (2019), 1145–1195. 4.2.2
- [84] BUGEAUD, Y., AND GYÖRY, K. Bounds for the solutions of Thue-Mahler equations and norm form equations. *Acta Arith.* 74, 3 (1996), 273–292. 3
- [85] BUHLER, J., POMERANCE, C., AND ROBERTSON, L. Heuristics for class numbers of prime-power real cyclotomic fields. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, vol. 41 of *Fields Inst. Commun.* Amer. Math. Soc., Providence, RI, 2004, pp. 149–157. 3.9
- [86] BUZZARD, K. Potential modularity—a survey. In *Non-abelian fundamental groups and Iwasawa theory*, vol. 393 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 2012, pp. 188–211. 1.7.1
- [87] BUZZARD, K., AND GEE, T. The conjectural connections between automorphic representations and Galois representations. In *Automorphic forms and Galois representations. Vol. 1*, vol. 414 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 2014, pp. 135–187. 5.1
- [88] CALEGARI, F. Semistable abelian varieties over  $\mathbb{Q}$ . *Manuscripta Math.* 113, 4 (2004), 507–529. 1.1.3
- [89] CALEGARI, F. The paramodular conjecture is false for trivial reasons. [Online]. Available at <https://www.galoisrepresentations.com/2018/01/15/the-paramodular-conjecture-is-false-for-trivial-reasons/>, 2018. (Accessed: 03 March 2024). 1.7.2

- [90] CANTOR, D. G. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.* 48, 177 (1987), 95–101. 1.7, 1.3.2
- [91] CARAIANI, A., AND NEWTON, J. On the modularity of elliptic curves over imaginary quadratic fields, 2023. arXiv:2301.10509 [math.NT]. 1.7.1
- [92] CARAYOL, H. Sur les représentations  $l$ -adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)* 19, 3 (1986), 409–468. 1.7.1
- [93] CARAYOL, H. Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet. In  *$p$ -adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, vol. 165 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1994, pp. 213–237. 4.2.2
- [94] CARDONA, G., NART, E., AND PUJOLÀS, J. Curves of genus two over fields of even characteristic. *Math. Z.* 250, 1 (2005), 177–201. 1.5.1
- [95] CARDONA, G., AND QUER, J. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, vol. 13 of *Lecture Notes Ser. Comput.* World Sci. Publ., Hackensack, NJ, 2005, pp. 71–83. 1.5.1
- [96] CARLETTI, E., MONTI BRAGADIN, G., AND PERELLI, A. On general  $L$ -functions. *Acta Arith.* 66, 2 (1994), 147–179. 5.1
- [97] CASSELS, J. W. S. *Lectures on elliptic curves*, vol. 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991. 1.1.1
- [98] CASSELS, J. W. S., AND FLYNN, E. V. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, vol. 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996. 1.3, 1.10, 1.3.3, 4
- [99] CHABAUTY, C. Sur les points rationnels des courbes algébriques de genre supérieur à l’unité. *C. R. Acad. Sci. Paris* 212 (1941), 882–885. 1, 1
- [100] CHÊNEVERT, G. *Exponential sums, hypersurfaces with many symmetries and Galois representations*. ProQuest LLC, Ann Arbor, MI, 2008. Thesis (Ph.D.)—McGill University (Canada). 4.2, 4.2.1, 4.3, 4.2.1, 4.7, 4.2.1, 4.2.2, 4.2.2, 4.10, 4.2.2, 4.2.3
- [101] CHIDAMBARAM, S. Mod3Image. [Online]. Available at <https://github.com/shiva-chid/threetorsimage>, 2023. (Accessed: 09 April 2024). 6.1.12, 6.1.12, B.2

- [102] CHIDAMBARAM, S. Mod2Image. [Online]. Available at <https://github.com/shiva-chid/mod4Galoisimage>, 2024. (Accessed: 09 April 2024). 6.1.12, 8
- [103] CLEBSCH, R. F. A. *Theorie der binären algebraischen Formen*. 1872. 1.5.1
- [104] CLOZEL, L. Motifs et formes automorphes: applications du principe de fonctorialité. In *Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988)*, vol. 10 of *Perspect. Math.* Academic Press, Boston, MA, 1990, pp. 77–159. 5.1
- [105] CLOZEL, L. Motives and automorphic representations. In *Autour des motifs—École d’été Franco-Asiatique de Géométrie Algébrique et de Théorie des Nombres/Asian-French Summer School on Algebraic Geometry and Number Theory. Vol. III*, vol. 49 of *Panor. Synthèses*. Soc. Math. France, Paris, 2016, pp. 29–60. 5.1
- [106] COATES, J. An effective  $p$ -adic analogue of a theorem of Thue. II. The greatest prime factor of a binary form. *Acta Arith.* 16 (1969/70), 399–412. 3
- [107] COATES, J. An effective  $p$ -adic analogue of a theorem of Thue. III. The diophantine equation  $y^2 = x^3 + k$ . *Acta Arith.* 16 (1969/70), 425–435. 1.1.1, 2
- [108] COGHLAN, F. B. *Elliptic Curves with Conductor  $N = 2^m 3^n$* . ProQuest LLC, Ann Arbor, MI, 1967. Thesis (Ph.D.)—The University of Manchester (United Kingdom). 1.1.1, 1.1
- [109] COHEN, H. *Advanced topics in computational number theory*, vol. 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. 5, 1b, 4.2.1, 1
- [110] COHEN, H., FREY, G., AVANZI, R., DOCHE, C., LANGE, T., NGUYEN, K., AND VERCAUTEREN, F., Eds. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006. 1.6.1
- [111] COLEMAN, R. F. Effective Chabauty. *Duke Math. J.* 52, 3 (1985), 765–770. 1, 1
- [112] COMALADA, S. Courbes elliptiques à bonne réduction d’invariant  $j$  fixé. *C. R. Acad. Sci. Paris Sér. I Math.* 311, 11 (1990), 667–670. 1.1.1
- [113] COMALADA, S. Elliptic curves with trivial conductor over quadratic fields. *Pacific J. Math.* 144, 2 (1990), 237–258. 1.1.1

- [114] COMALADA, S., AND NART, E. Courbes elliptiques avec bonne réduction partout. *C. R. Acad. Sci. Paris Sér. I Math.* 305, 6 (1987), 223–224. 1.1.1
- [115] COMMELIN, J. Algebraic cycles, chow motives, and  $l$ -functions. Master’s thesis, Mathematisch Instituut, Universiteit Leiden, 2013. 19
- [116] CONREY, J. B., AND FARMER, D. W. An extension of Hecke’s converse theorem. *Internat. Math. Res. Notices*, 9 (1995), 445–463. 5.1
- [117] CONREY, J. B., AND GHOSH, A. On the Selberg class of Dirichlet series: small degrees. *Duke Math. J.* 72, 3 (1993), 673–693. 5.1
- [118] CORNELL, G., AND SILVERMAN, J. H., Eds. *Arithmetic geometry*. Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. 1, 2.2
- [119] CORWIN, D. From Chabauty’s Method to Kim’s Non-abelian Chabauty’s Method. [Online]. Available at <https://math.berkeley.edu/~dcorwin/files/ChabautytoKim.pdf>, 2021. (Accessed 11 March 2024). 1
- [120] COSTA, E., MASCOT, N., SIJSLING, J., AND VOIGHT, J. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.* 88, 317 (2019), 1303–1339. 6.1.6, 6.1.7, 6.1.8
- [121] CREMONA, J. E. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Math.* 51, 3 (1984), 275–324. 1.7.1
- [122] CREMONA, J. E. Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields. *J. London Math. Soc. (2)* 45, 3 (1992), 404–416. 1.7.1
- [123] CREMONA, J. E. Modular symbols for  $\Gamma_1(N)$  and elliptic curves with everywhere good reduction. *Math. Proc. Cambridge Philos. Soc.* 111, 2 (1992), 199–218. 1.1.1
- [124] CREMONA, J. E. *Algorithms for modular elliptic curves*, second ed. Cambridge University Press, Cambridge, 1997. 4
- [125] CREMONA, J. E. Reduction of binary cubic and quartic forms. *LMS J. Comput. Math.* 2 (1999), 64–94. 3

- [126] CREMONA, J. E., AND FREITAS, N. Global methods for the symplectic type of congruences between elliptic curves. *Rev. Mat. Iberoam.* 38, 1 (2022), 1–32. 5.3.1, 9
- [127] CREMONA, J. E., AND LINGHAM, M. P. Finding all elliptic curves with good reduction outside a given set of primes. *Experiment. Math.* 16, 3 (2007), 303–312. 1.1, 1.1.1, 2
- [128] DAMIANOU, P. A. Monic polynomials in  $\mathbf{Z}[x]$  with roots in the unit disc. *Amer. Math. Monthly* 108, 3 (2001), 253–257. 3.2
- [129] DARMON, H., DIAMOND, F., AND TAYLOR, R. Fermat’s last theorem. In *Elliptic curves, modular forms & Fermat’s last theorem (Hong Kong, 1993)*. Int. Press, Cambridge, MA, 1997, pp. 2–140. 1.7.1
- [130] DAVIS, M., PUTNAM, H., AND ROBINSON, J. The decision problem for exponential diophantine equations. *Ann. of Math. (2)* 74 (1961), 425–436. 5
- [131] DE FRANCESCHI, G., LIEBECK, M. W., AND O’BRIEN, E. A. Code to solve conjugacy and centralizer problems for arbitrary elements of classical groups. [Online]. Available at <https://github.com/eamonnaobrien/ClassicalConjugacy>, 2024. (Accessed: 21 August 2024). 4.3.3
- [132] DE FRANCESCHI, G., LIEBECK, M. W., AND O’BRIEN, E. A. Conjugacy in finite classical groups, 2024. arXiv:2401.07557 [math.GR]. 4.3.3
- [133] DE JONG, J., AND OORT, F. The fundamental group of an algebraic curve, 2002. Seminar on Algebraic Geometry, MIT 2002. 1.3.1
- [134] DEMBÉLÉ, L. Abelian varieties with everywhere good reduction over certain real quadratic fields with small discriminant, 2019. (preprint). 1.1.3
- [135] DEMBÉLÉ, L., AND KUMAR, A. Examples of abelian surfaces with everywhere good reduction. *Math. Ann.* 364, 3-4 (2016), 1365–1392. 1.1.3
- [136] DERICKX, M., NAJMAN, F., AND SIKSEK, S. Elliptic curves over totally real cubic fields are modular. *Algebra Number Theory* 14, 7 (2020), 1791–1800. 4, 1.7.1
- [137] DIAMOND, F., AND SHURMAN, J. *A first course in modular forms*, vol. 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. 1.7.1

- [138] DICKSON, L. E. *Algebraic theories*. Dover Publications, Inc., New York, 1959. 4.3.3
- [139] DIEULEFAIT, L., GUERBEROFF, L., AND PACETTI, A. Proving modularity for a given elliptic curve over an imaginary quadratic field. *Math. Comp.* 79, 270 (2010), 1145–1170. 4.2
- [140] DIEULEFAIT, L. V. Explicit determination of the images of the Galois representations attached to abelian surfaces with  $\text{End}(A) = \mathbb{Z}$ . *Experiment. Math.* 11, 4 (2002), 503–512. 6.1.12
- [141] DIMITROV. An integral converse theorem for  $\text{GL}(2)$ , 2023. (under preparation). 5.1
- [142] DJUKANOVIĆ, M. Split Jacobians with isogenous components. Slides available at [https://www.cirm-math.fr/RepOrga/2889/Slides/Djukanovic\\_slides.pdf](https://www.cirm-math.fr/RepOrga/2889/Slides/Djukanovic_slides.pdf), 2023. Conference on Arithmetic, Geometry, Cryptography and Coding Theory, CIRM, Marseille. 10
- [143] DĄBROWSKI, A., AND SADEK, M. Genus two curves with everywhere good reduction over quadratic fields, 2023. arXiv:2109.00616 [math.NT]. 1.1.2
- [144] DĄBROWSKI, A., AND SADEK, M. Genus 2 curves with bad reduction at one odd prime. *Nagoya Math. J.* 254 (2024), 498–512. 1.1.2, 1.2.2, 2.3
- [145] DOKCHITSER, T. Computing special values of motivic  $L$ -functions. *Experiment. Math.* 13, 2 (2004), 137–149. 6.1.4, 6.1.5, 6.1.11
- [146] DOKCHITSER, T., AND DOKCHITSER, V. Local invariants of isogenous elliptic curves. *Trans. Amer. Math. Soc.* 367, 6 (2015), 4339–4358. 3.7
- [147] DOKCHITSER, T., DOKCHITSER, V., MAISTRET, C., AND MORGAN, A. Semistable types of hyperelliptic curves. In *Algebraic curves and their applications*, vol. 724 of *Contemp. Math.* Amer. Math. Soc., [Providence], RI, [2019] ©2019, pp. 73–135. 1.4
- [148] DOKCHITSER, T., DOKCHITSER, V., MAISTRET, C., AND MORGAN, A. Arithmetic of hyperelliptic curves over local fields. *Math. Ann.* 385, 3-4 (2023), 1213–1322. 1.3, 1.4, 1.15, 1.4, 1.11, 2.1.2
- [149] DOKCHITSER, T., AND DORIS, C. 3-torsion and conductor of genus 2 curves. *Math. Comp.* 88, 318 (2019), 1913–1927. 6.1.4

- [150] DOKCHITSER, V., AND MAISTRET, C. On the parity conjecture for abelian surfaces. *Proc. Lond. Math. Soc. (3)* 127, 2 (2023), 295–365. With appendix A by Adam Morgan and appendix B by T. Dokchitser and V. Dokchitser. 1.4
- [151] DOKCHITSER, V., AND MORGAN, A. A note on hyperelliptic curves with ordinary reduction over 2-adic fields. *J. Number Theory* 244 (2023), 264–278. 1.4
- [152] DUAN, L. Faltings-Serre method on three dimensional selfdual representations. *Math. Comp.* 90, 328 (2021), 931–951. 4.2, 4.2.4, 4.14
- [153] DUBOIS, E., AND RHIN, G. Sur la majoration de formes linéaires à coefficients algébriques réels et  $p$ -adiques. Démonstration d’une conjecture de K. Mahler. *C. R. Acad. Sci. Paris Sér. A-B* 282, 21 (1976), Ai, A1211–A1214. 2.2
- [154] EDWARDS, H. M. *Fermat’s last theorem*, vol. 50 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1977. A genetic introduction to algebraic number theory. 1.7.1
- [155] ELKIES, N. D.  $ABC$  implies Mordell. *Internat. Math. Res. Notices*, 7 (1991), 99–109. 1
- [156] ELKIES, N. D. Elliptic curves of unit discriminant over real quadratic number fields. [Online]. Available at <https://math.harvard.edu/~elkies/rqfu/>, 2010. (Accessed: 03 March 2024). 1.1.1
- [157] ELLIOTT, E. B. *An Introduction to the Algebra of Quantics*. Clarendon Press, 1895. 1.5
- [158] ESTES, D. R. On the parity of the class number of the field of  $q$ th roots of unity. *Rocky Mountain J. Math.* 19, 3 (1989), 675–682. Quadratic forms and real algebraic geometry (Corvallis, OR, 1986). 3.9
- [159] EVERTSE, J.-H. On sums of  $S$ -units and linear recurrences. *Compositio Math.* 53, 2 (1984), 225–244. 3, 2.2
- [160] EVERTSE, J.-H., AND GYÖRY, K. Effective finiteness results for binary forms with given discriminant. *Compositio Math.* 79, 2 (1991), 169–204. 1.1.2, 5.2.4
- [161] EVERTSE, J.-H., AND GYÖRY, K. *Unit equations in Diophantine number theory*, vol. 146 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2015. 2.1.1, 2.2, 2.17, 2.2



- [162] EVERTSE, J.-H., AND GYÖRY, K. *Discriminant equations in Diophantine number theory*, vol. 32 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2017. [2.1.1](#)
- [163] EVERTSE, J.-H., SCHLICKWEI, H. P., AND SCHMIDT, W. M. Linear equations in variables which lie in a multiplicative group. *Ann. of Math. (2)* **155**, 3 (2002), 807–836. [2.2](#)
- [164] FALTINGS, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73**, 3 (1983), 349–366. [1](#), [1.6](#), [3](#), [3](#), [3](#), [3](#), [4](#), [5.3.1](#), [6.1.9](#)
- [165] FALTINGS, G. Diophantine approximation on abelian varieties. *Ann. of Math. (2)* **133**, 3 (1991), 549–576. [1](#)
- [166] FARMER, D. W., KOUTSOLIOTAS, S., AND LEMURELL, S. Varieties via their L-functions. *J. Number Theory* **196** (2019), 364–380. [1.6.3](#), [5.1](#), [5.1.1](#), [5.1.1](#), [5.1.2](#)
- [167] FARMER, D. W., KOUTSOLIOTAS, S., LEMURELL, S., AND ROBERTS, D. P. The landscape of L-functions: degree 3 and conductor 1. In *LuCaNT: LMFDB, computation, and number theory*, vol. 796 of *Contemp. Math.* Amer. Math. Soc., [Providence], RI, [2024] ©2024, pp. 313–338. [5.1](#)
- [168] FARMER, D. W., PITALE, A., RYAN, N. C., AND SCHMIDT, R. Analytic L-functions: definitions, theorems, and connections. *Bull. Amer. Math. Soc. (N.S.)* **56**, 2 (2019), 261–280. [5.1](#), [5.1](#), [5.1](#), [5.2](#), [5.1](#)
- [169] FARMER, M. A converse theorem for degree 2 elements of the Selberg class with restricted gamma factor. *Acta Arith.* **205**, 1 (2022), 41–52. [5.1](#)
- [170] FINCKE, U., AND POHST, M. A procedure for determining algebraic integers of given norm. In *Computer algebra (London, 1983)*, vol. 162 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 1983, pp. 194–202. [5.2.6](#)
- [171] FINCKE, U., AND POHST, M. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.* **44**, 170 (1985), 463–471. [5.2.6](#)
- [172] FIORE, L., AND YELTON, J. Clusters and semistable models of hyperelliptic curves in the wild case, 2023. arXiv:2207.12490 [math.NT]. [1.4](#)
- [173] FISCHER, I. The moduli of hyperelliptic curves. *Trans. Amer. Math. Soc.* **82** (1956), 64–84. [1.2.3](#)



- [174] FITÉ, F., AND GUITART, X. Endomorphism algebras of geometrically split abelian surfaces over  $\mathbb{Q}$ . *Algebra Number Theory* 14, 6 (2020), 1399–1421. 6.1.6
- [175] FITÉ, F., KEDLAYA, K. S., ROTGER, V., AND SUTHERLAND, A. V. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.* 148, 5 (2012), 1390–1442. 6.1.7, 6.1.7, 9
- [176] FITÉ, F., KEDLAYA, K. S., AND SUTHERLAND, A. V. Sato-Tate groups of abelian threefolds: a preview of the classification. In *Arithmetic, geometry, cryptography and coding theory*, vol. 770 of *Contemp. Math.* Amer. Math. Soc., [Providence], RI, [2021] ©2021, pp. 103–129. 6.1.7
- [177] FITÉ, F., KEDLAYA, K. S., AND SUTHERLAND, A. V. Sato-tate groups of abelian threefolds, 2023. arXiv:2106.13759 [math.NT]. 6.1.7
- [178] FLYNN, E. V. Arbitrarily large 2-torsion in Tate-Shafarevich groups of abelian varieties. *Acta Arith.* 191, 2 (2019), 101–114. 7
- [179] FLYNN, E. V., AND WETHERELL, J. L. Finding rational points on bielliptic genus 2 curves. *Manuscripta Math.* 100, 4 (1999), 519–533. 6.1.10
- [180] FONTAINE, J.-M. Il n’y a pas de variété abélienne sur  $\mathbf{Z}$ . *Invent. Math.* 81, 3 (1985), 515–538. 1.1.3
- [181] FPLLL DEVELOPMENT TEAM, T. `fp111`, a lattice reduction library, Version: 5.4.5. Available at <https://github.com/fp111/fp111>, 2023. 5.2.6
- [182] FREITAS, N., KRAUS, A., AND SIKSEK, S. On asymptotic Fermat over  $\mathbb{Z}_p$ -extensions of  $\mathbb{Q}$ . *Algebra Number Theory* 14, 9 (2020), 2571–2574. 3, 3
- [183] FREITAS, N., KRAUS, A., AND SIKSEK, S. Local criteria for the unit equation and the asymptotic Fermat’s last theorem. *Proc. Natl. Acad. Sci. USA* 118, 12 (2021), Paper No. 2026449118, 5. 3
- [184] FREITAS, N., KRAUS, A., AND SIKSEK, S. The unit equation over cyclic number fields of prime degree. *Algebra Number Theory* 15, 10 (2021), 2647–2653. 3
- [185] FREITAS, N., LE HUNG, B. V., AND SIKSEK, S. Elliptic curves over real quadratic fields are modular. *Invent. Math.* 201, 1 (2015), 159–206. 4, 1.7.1
- [186] FREY, G., AND KANI, E. Curves of genus 2 covering elliptic curves and an arithmetical application. In *Arithmetic algebraic geometry (Texel, 1989)*,

- vol. 89 of *Progr. Math.* Birkhäuser Boston, Boston, MA, 1991, pp. 153–176. 5.3, 8
- [187] FU, L., LI, Z., TAKAMATSU, T., AND ZOU, H. Unpolarized Shafarevich conjectures for hyper-Kähler varieties, 2022. arXiv:2203.10391 [math.AG]. 1
- [188] GALBRAITH, S. D. *Mathematics of public key cryptography*. Cambridge University Press, Cambridge, 2012. 1.2
- [189] GAUDRON, E., AND RÉMOND, G. Polarisations et isogénies. *Duke Math. J.* 163, 11 (2014), 2057–2108. 5.3.1
- [190] GEHRUNGER, T., AND PINK, R. Reduction of Hyperelliptic Curves in Residue Characteristic 2, 2024. arXiv:2404.14214 [math.AG]. 1.4
- [191] GHERGA, A., AND SIKSEK, S. Efficient resolution of Thue–Mahler equations. *Algebra Number Theory* 19, 4 (2025), 667–714. 3
- [192] GNU PROJECT. GNU Linear Programming Kit (Version 5.0). [Online]. Available at <https://www.gnu.org/software/glpk/>, 2020. (Accessed: 10 March 2024). 5.2.7
- [193] GONZÁLEZ, J., GUÀRDIA, J., AND ROTGER, V. Abelian surfaces of  $GL_2$ -type as Jacobians of curves. *Acta Arith.* 116, 3 (2005), 263–287. 1.1.3, 4
- [194] GONZÁLEZ-JIMÉNEZ, E., GONZÁLEZ, J., AND GUÀRDIA, J. Computations on modular Jacobian surfaces. In *Algorithmic number theory (Sydney, 2002)*, vol. 2369 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2002, pp. 189–197. 1.1.3
- [195] GOODMAN, P. *On the interplay between Galois representations and endomorphism algebras of abelian varieties*. PhD thesis, University of Bristol, 2021. 3.10, 3.10
- [196] GOODMAN, P. Restrictions on endomorphism rings of Jacobians and their minimal fields of definition. *Trans. Amer. Math. Soc.* 374, 7 (2021), 4639–4654. 3.10, 3.10, 3.10
- [197] GORDAN, P. Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist. *J. Reine Angew. Math.* 69 (1868), 323–354. 1.5

- [198] GRAUERT, H. Mordells Vermutung über rationale Punkte auf algebraischen Kurven und Funktionenkörper. *Inst. Hautes Études Sci. Publ. Math.*, 25 (1965), 131–149. [1](#)
- [199] GREEN, H., AND MAISTRET, C. The 2-parity conjecture for elliptic curves with isomorphic 2-torsion. *Proc. A.* 478, 2265 (2022), Paper No. 20220112, 16. [1.4](#)
- [200] GREENBERG, R. Introduction to Iwasawa theory for elliptic curves. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, vol. 9 of *IAS/Park City Math. Ser.* Amer. Math. Soc., Providence, RI, 2001, pp. 407–464. [3](#)
- [201] GRENIÉ, L. Comparison of semi-simplifications of Galois representations. *J. Algebra* 316, 2 (2007), 608–618. [4.2](#), [4.2.4](#), [4.5](#), [4.13](#), [4.2.4](#), [4.15](#), [4.2.4](#), [4.16](#), [4.2.4](#), [4.17](#), [6.1.9](#)
- [202] GRIFFITHS, P. A. *Introduction to algebraic curves*, vol. 76 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1989. Translated from the Chinese by Kuniko Weltin. [1.3](#), [1.12](#), [1.3](#)
- [203] GRITSSENKO, V. Arithmetical lifting and its applications. In *Number theory (Paris, 1992–1993)*, vol. 215 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 1995, pp. 103–126. [1.7.2](#)
- [204] GRITSSENKO, V. Irrationality of the moduli spaces of polarized abelian surfaces. In *Abelian varieties (Egloffstein, 1993)*. de Gruyter, Berlin, 1995, pp. 63–84. With an appendix by the author and K. Hulek. [1.7.2](#)
- [205] GRITSSENKO, V., POOR, C., AND YUEN, D. S. Antisymmetric paramodular forms of weights 2 and 3. *Int. Math. Res. Not. IMRN*, 20 (2020), 6926–6946. [1.7.2](#)
- [206] GROSS, B. H. On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication. In *Number theory related to Fermat’s last theorem (Cambridge, Mass., 1981)*, vol. 26 of *Progr. Math.* Birkhäuser, Boston, MA, 1982, pp. 219–236. [1.6](#)
- [207] GYÖRY, K. On the number of solutions of linear equations in units of an algebraic number field. *Comment. Math. Helv.* 54, 4 (1979), 583–600. [5](#)
- [208] GYÖRY, K. On the solutions of linear Diophantine equations in algebraic integers of bounded norm. *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* 22/23 (1979/80), 225–233. [5](#)

- [209] GYÖRY, K., AND YU, K. Bounds for the solutions of  $S$ -unit equations and decomposable form equations. *Acta Arith.* 123, 1 (2006), 9–41. 5
- [210] HADANO, T. On the conductor of an elliptic curve with a rational point of order 2. *Nagoya Math. J.* 53 (1974), 199–210. 1.1.1
- [211] HADANO, T. Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor. *Proc. Japan Acad.* 51 (1975), 92–95. 1.1.1
- [212] HAMBURGER, H. Über die Riemannsche Funktionalgleichung der  $\xi$ -Funktion. *Math. Z.* 13, 1 (1922), 283–311. 5.1
- [213] HANROT, G., PUJOL, X., AND STEHLÉ, D. Algorithms for the shortest and closest lattice vector problems. In *Coding and cryptology*, vol. 6639 of *Lecture Notes in Comput. Sci.* Springer, Heidelberg, 2011, pp. 159–190. 5.2.6
- [214] HANSELMAN, J., SCHIAVONE, S., AND SIJSLING, J. **gluing**, a Magma package for gluing curves of low genus along their torsion. [Online]. Available at <https://github.com/JRSijsling/gluing>, 2022. (Accessed: 03 June 2024). 5.3.1
- [215] HARBATER, D. Galois groups with prescribed ramification. In *Arithmetic geometry (Tempe, AZ, 1993)*, vol. 174 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1994, pp. 35–60. 4.2.4, 6
- [216] HARDY, G. H., AND LITTLEWOOD, J. E. Some problems of ‘Partitio numerorum’; III: On the expression of a number as a sum of primes. *Acta Math.* 44, 1 (1923), 1–70. 2.4
- [217] HARRIS, J., AND MORRISON, I. *Moduli of curves*, vol. 187 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998. 2.3
- [218] HASSE, H. Zetafunktionen und  $L$ -Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus. *Abh. S. Akad. Wiss. Berlin Math. Kl.* (1954), 5–70. 1.7
- [219] HAYASHIDA, T., AND NISHI, M. Existence of curves of genus two on a product of two elliptic curves. *J. Math. Soc. Japan* 17 (1965), 1–16. 7
- [220] HECKE, E. Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung. *Math. Ann.* 112, 1 (1936), 664–699. 5.1
- [221] HILBERT, D. Über die Theorie der algebraischen Formen. *Math. Ann.* 36, 4 (1890), 473–534. 1.5, 1.5

- [222] HINDRY, M., AND SILVERMAN, J. H. *Diophantine geometry*, vol. 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction. [1.2.2](#)
- [223] HOFFMAN, K., AND KUNZE, R. *Linear algebra*, second ed. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1971. [4.3.3](#)
- [224] HOLT, D. F. Cohomology and group extensions in Magma. In *Discovering mathematics with Magma*, vol. 19 of *Algorithms Comput. Math.* Springer, Berlin, 2006, pp. 221–241. [4.3.4](#)
- [225] HOWE, E. W. Genus-2 Jacobians with torsion points of large order. *Bull. Lond. Math. Soc.* *47*, 1 (2015), 127–135. [5.3.1](#)
- [226] HOWE, E. W., LEPRÉVOST, F., AND POONEN, B. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.* *12*, 3 (2000), 315–364. [5.3](#), [5.3.1](#)
- [227] HURWITZ, A. Ueber algebraische Gebilde mit eindeutigen Transformationen in sich. *Math. Ann.* *41*, 3 (1892), 403–442. [6.1.2](#)
- [228] IBUKIYAMA, T., KATSURA, T., AND OORT, F. Supersingular curves of genus two and class numbers. *Compositio Math.* *57*, 2 (1986), 127–152. [7](#), [8](#)
- [229] ICHIMURA, H., AND NAKAJIMA, S. On the 2-part of the class numbers of cyclotomic fields of prime power conductors. *J. Math. Soc. Japan* *64*, 1 (2012), 317–342. [3.9](#)
- [230] IGUSA, J.-I. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)* *72* (1960), 612–649. [1.5](#), [1.5.1](#)
- [231] IKOMA, H., KAWAGUCHI, S., AND MORIWAKI, A. *The Mordell conjecture—a complete proof from Diophantine geometry*, vol. 226 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2022. [1](#)
- [232] ISHII, H. The nonexistence of elliptic curves with everywhere good reduction over certain imaginary quadratic fields. *J. Math. Soc. Japan* *31*, 2 (1979), 273–279. [1.1.1](#)
- [233] ISHII, H. The nonexistence of elliptic curves with everywhere good reduction over certain quadratic fields. *Japan. J. Math. (N.S.)* *12*, 1 (1986), 45–52. [1.1.1](#)

- [234] ISHITSUKA, Y., ITO, T., AND YOSHIKAWA, S. The modularity of elliptic curves over all but finitely many totally real fields of degree 5. *Res. Number Theory* 8, 4 (2022), Paper No. 82, 23. [1.7.1](#)
- [235] JARVIS, F., AND MANOHARMAYUM, J. On the modularity of supersingular elliptic curves over certain totally real number fields. *J. Number Theory* 128, 3 (2008), 589–618. [1.7.1](#)
- [236] JAVANPEYKAR, A. Néron models and the arithmetic Shafarevich conjecture for certain canonically polarized surfaces. *Bull. Lond. Math. Soc.* 47, 1 (2015), 55–64. [1](#)
- [237] JAVANPEYKAR, A., AND LOUGHRAN, D. Good reduction of algebraic groups and flag varieties. *Arch. Math. (Basel)* 104, 2 (2015), 133–143. [1](#)
- [238] JAVANPEYKAR, A., AND LOUGHRAN, D. Good reduction of Fano threefolds and sextic surfaces. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* 18, 2 (2018), 509–535. [1](#)
- [239] JONES, J. W. Number fields unramified away from 2. *J. Number Theory* 130, 6 (2010), 1282–1291. [4.2.4](#)
- [240] KACZOROWSKI, J., AND PERELLI, A. On the structure of the Selberg class. I.  $0 \leq d \leq 1$ . *Acta Math.* 182, 2 (1999), 207–241. [5.1](#)
- [241] KACZOROWSKI, J., AND PERELLI, A. Twists, Euler products and a converse theorem for  $L$ -functions of degree 2. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* 14, 2 (2015), 441–480. [5.1](#)
- [242] KACZOROWSKI, J., AND PERELLI, A. On a Hecke-type functional equation with conductor  $q = 5$ . *Ann. Mat. Pura Appl. (4)* 197, 6 (2018), 1707–1728. [5.1](#)
- [243] KACZOROWSKI, J., AND PERELLI, A. Classification of  $L$ -functions of degree 2 and conductor 1. *Adv. Math.* 408 (2022), Paper No. 108569, 46. [5.1](#)
- [244] KAGAWA, T. Determination of elliptic curves with everywhere good reduction over  $\mathbf{Q}(\sqrt{37})$ . *Acta Arith.* 83, 3 (1998), 253–269. [1.1.1](#)
- [245] KAGAWA, T. Elliptic curves over  $\mathbf{Q}(\sqrt{2})$  with good reduction outside  $\sqrt{2}$ . *Mem. Inst. Sci. Engrg. Ritsumeikan Univ.*, 59 (2000), 63–79. [4](#)

- [246] KAGAWA, T. Determination of elliptic curves with everywhere good reduction over real quadratic fields  $\mathbb{Q}(\sqrt{3p})$ . *Acta Arith.* 96, 3 (2001), 231–245. 1.1.1
- [247] KAHN, B. A motivic formula for the  $L$ -function of an abelian variety over a function field, 2016. arXiv:1401.6847 [math.NT]. 1.20
- [248] KANI, E. The existence of curves of genus two with elliptic differentials. *J. Number Theory* 64, 1 (1997), 130–161. 5.3
- [249] KANI, E. The number of curves of genus two with elliptic differentials. *J. Reine Angew. Math.* 485 (1997), 93–121. 5.3, 5.10, 5.3
- [250] KANI, E. Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. *J. Number Theory* 139 (2014), 138–174. 7
- [251] KANI, E. The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Collect. Math.* 67, 1 (2016), 21–54. 7
- [252] KANNAN, R. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 1983), STOC '83, Association for Computing Machinery, p. 193–206. 5.2.6
- [253] KANNAN, R. Minkowski's convex body theorem and integer programming. *Math. Oper. Res.* 12, 3 (1987), 415–440. 5.2.6
- [254] KATO, K.  $p$ -adic Hodge theory and values of zeta functions of modular forms. No. 295 in *Astérisque*. Société mathématique de France, 2004, pp. ix, 117–290. Cohomologies  $p$ -adiques et applications arithmétiques. III. 3.6
- [255] KATZ, N. M. Galois properties of torsion points on abelian varieties. *Invent. Math.* 62, 3 (1981), 481–502. 4.1, 5.1.3
- [256] KEDLAYA, K. S., AND SUTHERLAND, A. V. Computing  $L$ -series of hyperelliptic curves. In *Algorithmic number theory*, vol. 5011 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2008, pp. 312–326. 1.6.1
- [257] KHARE, C., AND WINTENBERGER, J.-P. Serre's modularity conjecture. I. *Invent. Math.* 178, 3 (2009), 485–504. 1.7.2
- [258] KHARE, C., AND WINTENBERGER, J.-P. Serre's modularity conjecture. II. *Invent. Math.* 178, 3 (2009), 505–586. 1.7.2



- [259] KIDA, M. Reduction of elliptic curves over certain real quadratic number fields. *Math. Comp.* 68, 228 (1999), 1679–1685. [1.1.1](#)
- [260] KIDA, M. Computing elliptic curves having good reduction everywhere over quadratic fields. II. In *Algebraic number theory and Diophantine analysis (Graz, 1998)*. de Gruyter, Berlin, 2000, pp. 239–247. [1.1.1](#)
- [261] KIDA, M. Computing elliptic curves having good reduction everywhere over quadratic fields. *Tokyo J. Math.* 24, 2 (2001), 545–558. [1.1.1](#)
- [262] KIDA, M. Good reduction of elliptic curves over imaginary quadratic fields. vol. 13. Université Bordeaux I, 2001, pp. 201–209. 21st Journées Arithmétiques (Rome, 2001). [1.1.1](#)
- [263] KIDA, M. Nonexistence of elliptic curves having good reduction everywhere over certain quadratic fields. *Arch. Math. (Basel)* 76, 6 (2001), 436–440. [1.1.1](#)
- [264] KIDA, M., AND KAGAWA, T. Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields. *J. Number Theory* 66, 2 (1997), 201–210. [1.1.1](#)
- [265] KIM, M. The motivic fundamental group of  $\mathbf{P}^1 \setminus \{0, 1, \infty\}$  and the theorem of Siegel. *Invent. Math.* 161, 3 (2005), 629–656. [1](#), [3](#)
- [266] KISIN, M. Modularity of 2-adic Barsotti-Tate representations. *Invent. Math.* 178, 3 (2009), 587–634. [1.7.2](#)
- [267] KLEINER, I. From Fermat to Wiles: Fermat’s last theorem becomes a theorem. *Elem. Math.* 55, 1 (2000), 19–37. [1.7.1](#)
- [268] KOHLS, R. *Conductors of Superelliptic Curves*. PhD thesis, Universität Ulm, 2019. [1.3.1](#)
- [269] KOLYVAGIN, V. A. Finiteness of  $E(\mathbf{Q})$  and  $\text{III}(E, \mathbf{Q})$  for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.* 52, 3 (1988), 522–540, 670–671. [1.6](#)
- [270] KOUTSIANAS, A. Computing all elliptic curves over an arbitrary number field with prescribed primes of bad reduction. *Exp. Math.* 28, 1 (2019), 1–15. [1.1](#)
- [271] KRONECKER, L. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.* 53 (1857), 173–175. [3.2](#)
- [272] KUNZWEILER, S. Differential forms on hyperelliptic curves with semistable reduction. *Res. Number Theory* 6, 2 (2020), Paper No. 25, 17. [1.4](#)



- [273] KUNZWEILER, S. *Models of Curves and Integral Differential Forms*. PhD thesis, Ulm University, 2020. [1.4](#)
- [274] LAGA, J., SCHEMBRI, C., SHNIDMAN, A., AND VOIGHT, J. Rational torsion points on abelian surfaces with quaternionic multiplication. *Forum Math. Sigma* 12 (2024), Paper No. e92, 33. [6.1.3](#)
- [275] LANG, S. Some history of the Shimura-Taniyama conjecture. *Notices Amer. Math. Soc.* 42, 11 (1995), 1301–1307. [22](#)
- [276] LANG, S. *Algebra*, third ed., vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. [4.2.1](#)
- [277] LANG, S., AND TATE, J. Principal homogeneous spaces over abelian varieties. *Amer. J. Math.* 80 (1958), 659–684. [6.1.11](#)
- [278] LASKA, M. *Elliptic curves over number fields with prescribed reduction type*, vol. E4 of *Aspects of Mathematics*. Friedr. Vieweg & Sohn, Braunschweig; distributed by Heyden & Son, Inc., Philadelphia, PA, 1983. [1.1.1](#)
- [279] LAUTER, K. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. *J. Algebraic Geom.* 10, 1 (2001), 19–36. With an appendix in French by J.-P. Serre. [1](#)
- [280] LAWRENCE, B., AND VENKATESH, A. Diophantine problems and  $p$ -adic period mappings. *Invent. Math.* 221, 3 (2020), 893–999. [1](#), [3](#)
- [281] LERCIER, R., AND RITZENTHALER, C. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra* 372 (2012), 595–636. [1.13](#)
- [282] LI, M., AND OTGONBAYAR, M. On constructing solutions to  $S$ -unit equations in  $\mathbb{Q}_{\infty, \ell}$ . [Online]. Available at [https://math.mit.edu/research/undergraduate/spur/documents/2023/Li\\_Otgonbayar.pdf](https://math.mit.edu/research/undergraduate/spur/documents/2023/Li_Otgonbayar.pdf), 2023. SPUR project (Accessed 05 May 2024). [3.5](#)
- [283] LIU, H. Lawrence-Venkatesh’s  $p$ -adic approach to Mordell’s conjecture. [Online]. Available at <https://webusers.imj-prg.fr/~haohao.liu/LV.pdf>, 2024. (Accessed: 02 June 2024). [1](#)
- [284] LIU, Q. Courbes stables de genre 2 et leur schéma de modules. *Math. Ann.* 295, 2 (1993), 201–222. [1.14](#)

- [285] LIU, Q. Conducteur et discriminant minimal de courbes de genre 2. *Compositio Math.* 94, 1 (1994), 51–79. 1.3.1
- [286] LIU, Q. Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète. *Trans. Amer. Math. Soc.* 348, 11 (1996), 4577–4610. 1.9, 1.2.2
- [287] LIU, Q. *Algebraic geometry and arithmetic curves*, vol. 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Ern , Oxford Science Publications. 1.2.2
- [288] LIU, Q. Computing minimal Weierstrass equations of hyperelliptic curves. *Res. Number Theory* 9, 4 (2023), Paper No. 76, 22. 1.2.2
- [289] LIVN , R. Cubic exponential sums and Galois representations. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, vol. 67 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1987, pp. 247–261. 4.2, 4.2.3, 4.11
- [290] LMFDB COLLABORATION, T. The L-functions and modular forms database. <https://www.lmfdb.org>, 2024. [Online] (Accessed: 10 October 2020). 1.12, 3, 6, 6.1.1, 2, 6.1.3, 1, 2
- [291] LOCKHART, P. On the discriminant of a hyperelliptic curve. *Trans. Amer. Math. Soc.* 342, 2 (1994), 729–752. 1.2.2
- [292] LOCKHART, P., ROSEN, M., AND SILVERMAN, J. H. An upper bound for the conductor of an abelian variety. *J. Algebraic Geom.* 2, 4 (1993), 569–601. 1.3.1
- [293] LOEFFLER, D., AND ZERBES, S. L. On the Birch-Swinnerton-Dyer conjecture for modular abelian surfaces, 2023. arXiv:2110.13102 [math.NT]. 1.6
- [294] LORENZINI, D. *An invitation to arithmetic geometry*, vol. 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996. 5.1.3
- [295] MAHLER, K. Zur Approximation algebraischer Zahlen. I. *Math. Ann.* 107, 1 (1933), 691–730. 3, 5, 3
- [296] MAHLER, K.  ber die rationalen Punkte auf Kurven vom Geschlecht Eins. *J. Reine Angew. Math.* 170 (1934), 168–178. 2

- [297] MAISTRET, C., AND SUTHERLAND, A. V. Computing Euler factors of genus 2 curves at odd primes of almost good reduction. *Res. Number Theory* 11, 1 (2025), Paper No. 37. 1.6.2
- [298] MALMENDIER, A., AND SHASKA, T. The Satake sextic in F-theory. *J. Geom. Phys.* 120 (2017), 290–305. 1.5.1
- [299] MALMSKOG, B., AND RASMUSSEN, C. Picard curves over  $\mathbb{Q}$  with good reduction away from 3. *LMS J. Comput. Math.* 19, 2 (2016), 382–408. 1.1.2
- [300] MANIN, J. I. Rational points on algebraic curves over function fields. *Izv. Akad. Nauk SSSR Ser. Mat.* 27 (1963), 1395–1440. 1
- [301] MARKŠAITIS, G. N. On  $p$ -extensions with one critical number. *Izv. Akad. Nauk SSSR Ser. Mat.* 27 (1963), 463–466. 4.3.2
- [302] MASSER, D., AND WÜSTHOLZ, G. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)* 137, 3 (1993), 459–472. 5.3.1
- [303] MASSER, D. W. Open problems. In *Proceedings of the symposium on Analytic Number Theory, London, 1985*. 1985. 1
- [304] MASSER, D. W., AND WÜSTHOLZ, G. Some effective estimates for elliptic curves. In *Arithmetic of complex manifolds (Erlangen, 1988)*, vol. 1399 of *Lecture Notes in Math.* Springer, Berlin, 1989, pp. 103–109. 5.3.1
- [305] MATIJASEVIČ, J. V. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR* 191 (1970), 279–282. 5
- [306] MATSCHKE, B. A general  $S$ -unit equation solver and tables of elliptic curves over number fields. *Modern Breakthroughs in Diophantine Problems*, BIRS, 2020. 1.1, 5
- [307] MATSCHKE, B. Personal communication, 2021. (document), 5.2.2, 5.7, 5.2.3, 5.9
- [308] MATSCHKE, B.  $S$ -unit equations. [Online]. Available at <https://github.com/bmatschke/s-unit-equations>, 2021. (Accessed: 03 March 2021). 1.1, 5
- [309] MAZUR, B. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* 18 (1972), 183–266. 3

- [310] MAZUR, B. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47 (1977), 33–186. With an appendix by Mazur and M. Rapoport. [6.1.3](#)
- [311] MAZUR, B. Arithmetic on curves. *Bull. Amer. Math. Soc. (N.S.)* 14, 2 (1986), 207–259. [1](#), [3](#)
- [312] MAZUR, B. On the passage from local to global in number theory. *Bull. Amer. Math. Soc. (N.S.)* 29, 1 (1993), 14–50. [6](#)
- [313] MCCALLUM, W., AND POONEN, B. The method of Chabauty and Coleman. In *Explicit methods in number theory*, vol. 36 of *Panor. Synthèses*. Soc. Math. France, Paris, 2012, pp. 99–117. [1](#)
- [314] MERRIMAN, J. R., AND SMART, N. P. Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point. *Math. Proc. Cambridge Philos. Soc.* 114, 2 (1993), 203–214. [1.1.2](#), [5.2.1](#), [5.8](#), [1](#)
- [315] MERRIMAN, J. R., AND SMART, N. P. Corrigenda: “Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point” [Math. Proc. Cambridge Philos. Soc. 114 (1993), no. 2, 203–214; MR1230127 (94h:14031)]. *Math. Proc. Cambridge Philos. Soc.* 118, 1 (1995), 189. [1.1.2](#)
- [316] MESTRE, J.-F. Formules explicites et minoration de conducteurs de variétés algébriques. *Compositio Math.* 58, 2 (1986), 209–232. [5.1](#)
- [317] MESTRE, J.-F. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglione, 1990)*, vol. 94 of *Progr. Math.* Birkhäuser Boston, Boston, MA, 1991, pp. 313–334. [1](#)
- [318] MILNE, J. S. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*. Springer, New York, 1986, pp. 103–150. [1.20](#)
- [319] MILNE, J. S. Abelian Varieties (v2.00). [Online]. Available at <https://www.jmilne.org/math/CourseNotes/AV.pdf>, 2008. (Accessed 01 February 2021). [1.4](#), [1.3](#), [1.3](#), [1.13](#), [1.3](#), [4.1](#)
- [320] MORDELL, L. J. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Philos. Soc.* 21 (1922/23), 179–192. [1](#), [1.1](#)
- [321] MORGAN, A. Local Arithmetic of Curves and Jacobians. [Online]. Available at <https://heilbronn.ac.uk/wp-content/uploads/2019/>

- 06/Morgan-bristol\_lecture\_1.pdf, 2019. CMI-HIMR Summer School in Computational Number Theory. [19](#)
- [322] MORGAN, A. Quadratic twists of abelian varieties and disparity in Selmer ranks. *Algebra Number Theory* 13, 4 (2019), 839–899. [5.1.3](#)
  - [323] MORGAN, A. 2-Selmer parity for hyperelliptic curves in quadratic extensions. *Proc. Lond. Math. Soc. (3)* 127, 5 (2023), 1507–1576. [1.4](#)
  - [324] MUMFORD, D. *Abelian varieties*, vol. 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay by Oxford University Press, London, 1970. [1.3](#), [1.3.3](#), [6.1.7](#), [6.1.8](#)
  - [325] MUMFORD, D. *Tata lectures on theta. II*, vol. 43 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. [1.3.2](#)
  - [326] MURABAYASHI, N., AND UMEGAKI, A. Determination of all  $\mathbf{Q}$ -rational CM-points in the moduli space of principally polarized abelian surfaces. *J. Algebra* 235, 1 (2001), 267–274. [6.1.6](#)
  - [327] MURTY, M. R., AND VATWANI, A. A higher rank Selberg sieve with an additive twist and applications. *Funct. Approx. Comment. Math.* 57, 2 (2017), 151–184. [2.4](#)
  - [328] NAGELL, T. Sur un type particulier d’unités algébriques. *Ark. Mat.* 8 (1969), 163–184. [3](#)
  - [329] NECHAEV, A. A. Similarity of matrices over a commutative local Artinian ring. *Trudy Sem. Petrovsk.*, 9 (1983), 81–101. [4.3.3](#)
  - [330] NEUKIRCH, J. *Algebraic number theory*, vol. 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. [1a](#)
  - [331] NEUMANN, O. Die elliptischen Kurven mit den Führern  $3.2^m$  und  $9.2^m$ . *Math. Nachr.* 48 (1971), 387–389. [1.1.1](#)
  - [332] NEUMANN, O. Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I. *Math. Nachr.* 49 (1971), 107–123. [1.1.1](#)

- [333] NEUMANN, O. Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. II. *Math. Nachr.* 56 (1973), 269–280. [1.1.1](#)
- [334] OBUS, A., AND SRINIVASAN, P. Conductor-discriminant inequality for hyperelliptic curves in odd residue characteristic. *Int. Math. Res. Not. IMRN*, 9 (2024), 7343–7359. [1.3.1](#)
- [335] ODA, T. A note on ramification of the Galois representation on the fundamental group of an algebraic curve. II. *J. Number Theory* 53, 2 (1995), 342–355. [1.3.1](#)
- [336] OESTERLÉ, J. Nouvelles approches du “théorème” de Fermat. No. 161-162 in *Astérisque*. Société mathématique de France, 1988, pp. Exp. No. 694, 4, 165–186. Séminaire Bourbaki, Vol. 1987/88. [1](#)
- [337] OGG, A. P. Abelian curves of 2-power conductor. *Proc. Cambridge Philos. Soc.* 62 (1966), 143–148. [1.1.1](#), [1.1](#), [1](#), [4](#), [4](#), [5.3.1](#), [5.11](#)
- [338] OGG, A. P. Abelian curves of small conductor. *J. Reine Angew. Math.* 226 (1967), 204–215. [1.1.1](#)
- [339] OORT, F. Hyperelliptic curves over number fields. In *Classification of algebraic varieties and compact complex manifolds*, vol. Vol. 412 of *Lecture Notes in Math.* Springer, Berlin-New York, 1974, pp. 211–218. [1](#)
- [340] PACETTI, A., AND VILLANUEVA, A. Galois representations of superelliptic curves. *Glasg. Math. J.* 65, 2 (2023), 356–382. [1.4](#)
- [341] PADBERG, M. *Linear optimization and extensions*, expanded ed., vol. 12 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, 1999. [5.2.7](#)
- [342] PARRY, C. J. The  $\mathfrak{p}$ -adic generalisation of the Thue-Siegel theorem. *Acta Math.* 83 (1950), 1–100. [5](#)
- [343] PARŠIN, A. N. Algebraic curves over function fields. I. *Izv. Akad. Nauk SSSR Ser. Mat.* 32 (1968), 1191–1219. [1](#)
- [344] PARŠIN, A. N. Minimal models of curves of genus 2, and homomorphisms of abelian varieties defined over a field of finite characteristic. *Izv. Akad. Nauk SSSR Ser. Mat.* 36 (1972), 67–109. [1](#)
- [345] PATRIKIS, S., VOLOCH, J. F., AND ZARHIN, Y. G. Anabelian geometry and descent obstructions on moduli spaces. *Algebra Number Theory* 10, 6 (2016), 1191–1219. [1.1.3](#)

- [346] PIATETSKI-SHAPIRO, I. Arithmetic Dirichlet series: Conjectures. In *Structure Theory of Set Addition* (1993), CIRM Marseille, pp. 271–281. 5.1
- [347] PINCH, R. G. E. Elliptic curves with good reduction away from 2. *Math. Proc. Cambridge Philos. Soc.* 96, 1 (1984), 25–38. 1.1.1, 4
- [348] PINCH, R. G. E. Elliptic curves with good reduction away from 2. II. *Math. Proc. Cambridge Philos. Soc.* 100, 3 (1986), 435–457. 1.1.1
- [349] PINCH, R. G. E. Elliptic curves with good reduction away from 3. *Math. Proc. Cambridge Philos. Soc.* 101, 3 (1987), 451–459. 1.1.1
- [350] POHST, M. On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields. *J. Number Theory* 14, 1 (1982), 99–117. 5.2.1
- [351] POONEN, B. Remarks and Errata. [Online]. Available at <https://math.mit.edu/~poonen/papers/errata.pdf>. (Accessed: 03 June 2024). 3
- [352] POONEN, B. Computational aspects of curves of genus at least 2. In *Algorithmic number theory (Talence, 1996)*, vol. 1122 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 1996, pp. 283–306. 4, 5
- [353] POONEN, B. The  $S$ -integral points on the projective line minus three points via finite covers and Skolem’s method. In *Arithmetic geometry, number theory, and computation*, Simons Symp. Springer, Cham, [2021] ©2021, pp. 583–587. 3
- [354] POONEN, B., AND STOLL, M. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)* 150, 3 (1999), 1109–1149. 6.1.11
- [355] POOR, C., SHURMAN, J., AND YUEN, D. S. Siegel paramodular forms of weight 2 and squarefree level. *Int. J. Number Theory* 13, 10 (2017), 2627–2652. 1.7.2
- [356] POOR, C., SHURMAN, J., AND YUEN, D. S. Nonlift weight two paramodular eigenform constructions. *J. Korean Math. Soc.* 57, 2 (2020), 507–522. 1.7.2
- [357] POOR, C., AND YUEN, D. S. Paramodular cusp forms. *Math. Comp.* 84, 293 (2015), 1401–1438. 1.7.2
- [358] POOR, C., AND YUEN, D. S. Heuristic tables of nonlift weight two paramodular cuspidal newforms to level 1000, 2022. 1.7.2



- [359] PRASAD, A., SINGLA, P., AND SPALLONE, S. Similarity of matrices over local rings of length two. *Indiana Univ. Math. J.* 64, 2 (2015), 471–514. 4.3.3
- [360] RASMUSSEN, C., AND TAMAGAWA, A. Abelian surfaces good away from 2. *Int. J. Number Theory* 13, 4 (2017), 991–1001. 4.1, 4.1
- [361] RÉMOND, G. Hauteurs thêta et construction de Kodaira. *J. Number Theory* 78, 2 (1999), 287–311. 1
- [362] RIBENBOIM, P. *13 lectures on Fermat’s last theorem*. Springer-Verlag, New York-Heidelberg, 1979. 1.7.1
- [363] RIBET, K. A. On modular representations of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  arising from modular forms. *Invent. Math.* 100, 2 (1990), 431–476. 1.7.1
- [364] RIBET, K. A. Abelian varieties over  $\mathbf{Q}$  and modular forms. In *Algebra and topology 1992 (Taejŏn)*. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79. 1.7.2
- [365] RIEMANN, B. Ueber die anzahl der primzahlen unter einer gegebenen grosse. *Ges. Math. Werke und Wissenschaftlicher Nachlaß* 2, 145–155 (1859), 2. 1.7
- [366] ROHRLICH, D. E. Elliptic curves with good reduction everywhere. *J. London Math. Soc. (2)* 25, 2 (1982), 216–222. 1.1.1
- [367] ROHRLICH, D. E. On  $L$ -functions of elliptic curves and cyclotomic towers. *Invent. Math.* 75, 3 (1984), 409–423. 3.6
- [368] ROSENHAIN, G. Abhandlung über die Functionen zweier Variablen mit vier Perioden welche die Inversion sind der ultra-elliptische Integrale erster klasse, 1851. Translation to German from Latin manuscript. 1.2.3
- [369] ROTH, K. F. Rational approximations to algebraic numbers. *Mathematika* 2 (1955), 1–20; corrigendum, 168. 3
- [370] ROWAN, J.  $S$ -unit equations and curves of genus 2 with good reduction away from 3. [Online]. Available at <https://math.mit.edu/research/undergraduate/spur/documents/2016Rowan.pdf>, 2016. SPUR project (Accessed 05 May 2024). 1.1.2
- [371] RUBINSTEIN, M. Computational methods and experiments in analytic number theory. In *Recent perspectives in random matrix theory and number theory*, vol. 322 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 2005, pp. 425–506. 5.5, 5.1.1, 5.1.1



- [372] RÜTH, J., AND WEWERS, S. MCLF (Models of Curves over Local Fields). [Online]. Available at <https://github.com/MCLF/mclf>. (Accessed: 09 September 2024). 2.3, 6.1.4
- [373] SAGE DEVELOPERS, T. *SageMath, the Sage Mathematics Software System (Version 10.3)*, 2024. <https://www.sagemath.org>. 2, 2.3, 4.3.5, 5.1.2, 5.2.7, 6
- [374] SAMUEL, P. Compléments à un article de Hans Grauert sur la conjecture de Mordell. *Inst. Hautes Études Sci. Publ. Math.*, 29 (1966), 55–62. 1
- [375] SÁNCHEZ RODRÍGUEZ, I. Comparing Galois representations and the Faltings-Serre-Livné method. Master’s thesis, Universitat de Barcelona, 2020. 4.2
- [376] SÁNCHEZ RODRÍGUEZ, I. Personal communication, 2024. 4.2.4
- [377] SCHAEFER, E. F. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory* 51, 2 (1995), 219–232. 3.9
- [378] SCHINZEL, A., AND SIERPIŃSKI, W. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.* 4 (1958), 185–208; erratum 5 (1958), 259. 2.4
- [379] SCHLICKWEI, H. P. Über die diophantische Gleichung  $x_1 + x_2 \cdots + x_n = 0$ . *Acta Arith.* 33, 2 (1977), 183–185. 2.2
- [380] SCHMIDT, W. M. Norm form equations. *Ann. of Math. (2)* 96 (1972), 526–551. 2.2
- [381] SCHOLL, A. J. A finiteness theorem for del Pezzo surfaces over algebraic number fields. *J. London Math. Soc. (2)* 32, 1 (1985), 31–40. 1
- [382] SCHOOF, R. Abelian varieties over  $\mathbf{Q}(\sqrt{6})$  with good reduction everywhere. In *Class field theory—its centenary and prospect (Tokyo, 1998)*, vol. 30 of *Adv. Stud. Pure Math.* Math. Soc. Japan, Tokyo, 2001, pp. 287–306. 1.1.3
- [383] SCHOOF, R. Abelian varieties over the field of the 20th roots of unity that have good reduction everywhere. In *Applications of algebraic geometry to coding theory, physics and computation (Eilat, 2001)*, vol. 36 of *NATO Sci. Ser. II Math. Phys. Chem.* Kluwer Acad. Publ., Dordrecht, 2001, pp. 291–296. 1.1.3
- [384] SCHOOF, R. Abelian varieties over  $\mathbf{Q}$  with bad reduction in one prime only. *Compos. Math.* 141, 4 (2005), 847–868. 1.1.3

- [385] SCHOOF, R. On the modular curve  $X_0(23)$ . In *Geometry and arithmetic*, EMS Ser. Congr. Rep. Eur. Math. Soc., Zürich, 2012, pp. 317–345. [1.1.3](#)
- [386] SCHOOF, R. Semistable abelian varieties with good reduction outside 15. *Manuscripta Math.* **139**, 1-2 (2012), 49–70. [1.1.3](#)
- [387] SCHOOF, R. Abelian varieties over real quadratic fields with good reduction everywhere, 2019. (in preparation). [1.1.3](#)
- [388] SCHOTTENLOHER, M. *A mathematical introduction to conformal field theory*, second ed., vol. 759 of *Lecture Notes in Physics*. Springer-Verlag, Berlin, 2008. [4.3.4](#)
- [389] SCHÜTT, M. On the modularity of three Calabi-Yau threefolds with bad reduction at 11. *Canad. Math. Bull.* **49**, 2 (2006), 296–312. [4.2](#)
- [390] SELBERG, A. Old and new conjectures and results about a class of Dirichlet series. In *Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989)* (1992), Univ. Salerno, Salerno, pp. 367–385. [5.1](#)
- [391] SERRA, M. Smooth models of curves. Master’s thesis, Universiteit Leiden, 2013. [1.2.2](#)
- [392] SERRE, J.-P. *Abelian  $l$ -adic representations and elliptic curves*. W. A. Benjamin, Inc., New York-Amsterdam, 1968. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. [3.6](#)
- [393] SERRE, J.-P. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.* **15**, 4 (1972), 259–331. [3.6](#)
- [394] SERRE, J.-P. Nombres de points des courbes algébriques sur  $\mathbf{F}_q$ . In *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*. Univ. Bordeaux I, Talence, 1983, pp. Exp. No. 22, 8. [8](#)
- [395] SERRE, J.-P. Sur les représentations modulaires de degré 2 de  $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ . *Duke Math. J.* **54**, 1 (1987), 179–230. [1.7.2](#)
- [396] SERRE, J.-P. *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000. 1985–1998. [4.2](#), [4.2.1](#), [6.1.12](#)
- [397] SERRE, J.-P., AND TATE, J. Good reduction of abelian varieties. *Ann. of Math. (2)* **88** (1968), 492–517. [1.3.1](#)

- [398] SETZER, B. Elliptic curves of prime conductor. *J. London Math. Soc. (2)* 10 (1975), 367–378. [1.1.1](#)
- [399] SETZER, B. Elliptic curves over complex quadratic fields. *Pacific J. Math.* 74, 1 (1978), 235–250. [1.1.1](#)
- [400] SETZER, B. Elliptic curves with good reduction everywhere over quadratic fields and having rational  $j$ -invariant. *Illinois J. Math.* 25, 2 (1981), 233–245. [1.1.1](#)
- [401] SHAPIRO, H. An arithmetic function arising from the  $\phi$  function. *Amer. Math. Monthly* 50 (1943), 18–30. [3.8](#)
- [402] SHASKA, R. Equations of curves with minimal discriminant, 2014. arXiv:1407.7064 [math.NT]. [2.1.1](#)
- [403] SHASKA, T., AND VÖLKLEIN, H. Elliptic subfields and automorphisms of genus 2 function fields. In *Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000)*. Springer, Berlin, 2004, pp. 703–723. [6.1.2](#)
- [404] SHE, Y. *The Shafarevich conjecture for K3 surfaces*. ProQuest LLC, Ann Arbor, MI, 2015. Thesis (Ph.D.)—The University of Chicago. [1](#)
- [405] SHIMURA, G. On analytic families of polarized abelian varieties and automorphic functions. *Ann. of Math. (2)* 78 (1963), 149–192. [6.1.7](#)
- [406] SHIMURA, G. *Introduction to the arithmetic theory of automorphic functions*. Kanô Memorial Lectures, No. 1. Iwanami Shoten Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. Publications of the Mathematical Society of Japan, No. 11. [3.7](#)
- [407] SHIMURA, G. On the field of rationality for an abelian variety. *Nagoya Math. J.* 45 (1972), 167–178. [1](#)
- [408] SHIODA, T. On the graded ring of invariants of binary octavics. *Amer. J. Math.* 89 (1967), 1022–1046. [1.5](#)
- [409] SIEGEL, C. L. Über einige anwendungen diophantischer approximationen. *Abh. Preuss. Akad. Wiss. Phys.-Math. Kl.* 1 (1929), 41–69. [2](#), [5](#), [3](#)
- [410] SIJSLING, J. Personal communication, 2024. [5.3.1](#)

- [411] SIKSEK, S. Chabauty and the Mordell-Weil sieve. In *Advances on superelliptic curves and their applications*, vol. 41 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.* IOS, Amsterdam, 2015, pp. 194–224. [1](#)
- [412] SIKSEK, S. Integral points on punctured abelian varieties. *Eur. J. Math.* 8 (2022), S687–S703. [3](#)
- [413] SIKSEK, S., AND VISSER, R. Curves with few bad primes over cyclotomic  $\mathbb{Z}_\ell$ -extensions. *Algebra Number Theory* 19, 1 (2025), 113–141. [\(document\)](#), [3](#)
- [414] SILVERMAN, J. H. *Advanced topics in the arithmetic of elliptic curves*, vol. 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. [1.1.1](#)
- [415] SILVERMAN, J. H. *The arithmetic of elliptic curves*, second ed., vol. 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2009. [1.1.1](#), [1](#), [1.2](#), [1.2.3](#), [3.7](#), [6.1.11](#)
- [416] SINGH, S. *Fermat’s Last Theorem*. Fourth Estate, 1997. [1.7.1](#)
- [417] SMART, N. P. The solution of triangularly connected decomposable form equations. *Math. Comp.* 64, 210 (1995), 819–840. [5.2.3](#)
- [418] SMART, N. P.  $S$ -unit equations, binary forms and curves of genus 2. *Proc. London Math. Soc. (3)* 75, 2 (1997), 271–307. [1.1.2](#), [1.5](#), [2.1.1](#), [4](#), [5.2](#), [5.2](#), [5.2.1](#), [5.8](#), [5.2.1](#), [5.2.2](#), [5.2.2](#), [5.2.3](#), [5.2.4](#), [1](#), [6.3](#)
- [419] SNOWDEN, A. Jacobians. [Online]. Available at <https://websites.umich.edu/~asnowden/teaching/2013/679/L10.html>, 2013. Course Notes for MA679, University of Michigan (Accessed: 03 May 2022). [15](#)
- [420] SRINIVASAN, P. Conductors and minimal discriminants of hyperelliptic curves with rational weierstrass points, 2015. arXiv:1508.05172 [math.AG]. [1.3.1](#)
- [421] SRINIVASAN, P. Conductors and minimal discriminants of hyperelliptic curves: A comparison in the tame case, 2021. arXiv:1910.08228 [math.AG]. [1.3.1](#)
- [422] STEIN, W. *Modular forms, a computational approach*, vol. 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells. [4](#)
- [423] STEIN, W. A., AND WATKINS, M. A database of elliptic curves—first report. In *Algorithmic number theory (Sydney, 2002)*, vol. 2369 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2002, pp. 267–275. [1.1.1](#)

- [424] STEPHENS, N. M. *The Birch Swinnerton-Dyer Conjecture for Selmer curves of positive rank*. PhD thesis, University of Manchester, 1965. 1.1.1, 1.1
- [425] STEVENHAGEN, P. Class number parity for the  $p$ th cyclotomic field. *Math. Comp.* 63, 208 (1994), 773–784. 3.9
- [426] STEWART, I., AND TALL, D. *Algebraic number theory and Fermat’s last theorem*, third ed. A K Peters, Ltd., Natick, MA, 2002. 1.7.1
- [427] STIX, J. *Rational points and arithmetic of fundamental groups*, vol. 2054 of *Lecture Notes in Mathematics*. Springer, Heidelberg, 2013. Evidence for the section conjecture. 1.3.1
- [428] STOLL, M. On the height constant for curves of genus two. *Acta Arith.* 90, 2 (1999), 183–201. 6.1.3
- [429] STOLL, M. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.* 98, 3 (2001), 245–277. 3.9, 3.9, 6.1.5
- [430] STOLL, M. Implementation of Chabauty and the Mordell-Weil Sieve. [Online]. Available at <https://www.mathe2.uni-bayreuth.de/stoll/magma/chabauty-MWS.m>, 2007. (Accessed: 03 March 2024). 6.1.10
- [431] STOLL, M. Arithmetic of Hyperelliptic Curves. [Online]. Available at <https://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2019/Skript-ArithHypCurves-pub-screen.pdf>, 2019. Summer Semester 2019, University of Bayreuth (Accessed: 15 March 2021). 1.2, 1.2, 1.3, 1.8, 1.3
- [432] STROEKER, R. J. Reduction of elliptic curves over imaginary quadratic number fields. *Pacific J. Math.* 108, 2 (1983), 451–463. 1.1.1
- [433] SUTHERLAND, A. V. A generic approach to searching for Jacobians. *Math. Comp.* 78, 265 (2009), 485–507. 1.6.1
- [434] SUTHERLAND, A. V. A database of nonhyperelliptic genus-3 curves over  $\mathbb{Q}$ . In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium* (2019), vol. 2 of *Open Book Ser.*, Math. Sci. Publ., Berkeley, CA, pp. 443–459. 1.7.2
- [435] SUTHERLAND, A. V. Personal communication, 2023. 1
- [436] SZPIRO, L. Sur le théorème de rigidité de Parsin et Arakelov. In *Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II*, vol. 64 of *Astérisque*. Soc. Math. France, Paris, 1979, pp. 169–202. 1

- [437] SZPIRO, L. Un peu d'effectivité. In *Séminaire sur les pinceaux arithmétiques : la conjecture de Mordell*, no. 127 in Astérisque. Société mathématique de France, 1985, pp. 275–287. Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84). [1](#)
- [438] SZPIRO, L. Présentation de la théorie d'Arakélov. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, vol. 67 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1987, pp. 279–293. [1](#)
- [439] TAKAMATSU, T. On the Shafarevich conjecture for Enriques surfaces. *Math. Z.* **298**, 1-2 (2021), 489–495. [1](#)
- [440] TANGE, O. *GNU Parallel 2018*. Ole Tange, Mar. 2018. [4.3.5](#)
- [441] TATE, J. The non-existence of certain Galois extensions of  $\mathbf{Q}$  unramified outside 2. In *Arithmetic geometry (Tempe, AZ, 1993)*, vol. 174 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1994, pp. 153–156. [4.2.4](#)
- [442] TATE, J. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*. Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440. [1.6](#)
- [443] TATE, J. T. The arithmetic of elliptic curves. *Invent. Math.* **23** (1974), 179–206. [20](#)
- [444] TAYLOR, R. Remarks on a conjecture of Fontaine and Mazur. *J. Inst. Math. Jussieu* **1**, 1 (2002), 125–143. [1.16](#), [1.7.1](#)
- [445] TAYLOR, R., AND WILES, A. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)* **141**, 3 (1995), 553–572. [1.7.1](#), [1.16](#)
- [446] THORNE, J. A. Elliptic curves over  $\mathbb{Q}_\infty$  are modular. *J. Eur. Math. Soc. (JEMS)* **21**, 7 (2019), 1943–1948. [1.7.1](#)
- [447] THORNE, J. A. Elliptic curves and modularity. In *European Congress of Mathematics*. EMS Press, Berlin, [2023] ©2023, pp. 643–662. [1.7.1](#)
- [448] THUE, A. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew. Math.* **135** (1909), 284–305. [3](#)
- [449] TINGLEY, D. J. *Elliptic curves uniformized by modular functions*. PhD thesis, University of Oxford, 1975. [4](#)

- [450] TORELLI, R. Sulle varietà di jacobí. *Rend. R. Accad. Lincei* 22, 5 (1913), 98–103. [1](#)
- [451] TOTARO, B. Recent progress on the Tate conjecture. *Bull. Amer. Math. Soc. (N.S.)* 54, 4 (2017), 575–590. [1](#)
- [452] TRIANTAFILLOU, N. There are no exceptional units in number fields of degree prime to 3 where 3 splits completely. *Proc. Amer. Math. Soc. Ser. B* 8 (2021), 371–376. [3](#)
- [453] TZANAKIS, N., AND DE WEGER, B. M. M. On the practical solution of the Thue equation. *J. Number Theory* 31, 2 (1989), 99–132. [3](#)
- [454] TZANAKIS, N., AND DE WEGER, B. M. M. How to explicitly solve a Thue-Mahler equation. *Compositio Math.* 84, 3 (1992), 223–288. [3](#)
- [455] URBAN, E. On residually reducible representations on local rings. *J. Algebra* 212, 2 (1999), 738–742. [4.2.2](#)
- [456] URBANIK, D. Abstract and Explicit Constructions of Jacobian Varieties. Master’s thesis, University Of Waterloo, 2018. [1.3](#)
- [457] VAN BOMMEL, R. Efficient computation of BSD invariants in genus 2. In *Arithmetic geometry, number theory, and computation*, Simons Symp. Springer, Cham, [2021] ©2021, pp. 237–258. [6.1.11](#)
- [458] VAN BOMMEL, R. Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over  $\mathbb{Q}$  up to squares. *Exp. Math.* 31, 1 (2022), 138–145. [6.1.11](#)
- [459] VAN BOMMEL, R., CHIDAMBARAM, S., COSTA, E., AND KIEFFER, J. Computing isogeny classes of typical principally polarized abelian surfaces over the rationals. In *LuCaNT: LMFDB, computation, and number theory*, vol. 796 of *Contemp. Math.* Amer. Math. Soc., [Providence], RI, [2024] ©2024, pp. 187–214. [5.3.1](#), [6.1.9](#)
- [460] VAN DER POORTEN, A. J., AND SCHLICKWEI, H. P. The growth condition for recurrence sequences, 1982. Macquarie University Math. Rep. 82–0041. [2.2](#)
- [461] VAN WAMELEN, P. Poonen’s question concerning isogenies between Smart’s genus 2 curves. *Math. Comp.* 69, 232 (2000), 1685–1697. [10](#), [6.1.9](#)

- [462] VAN WAMELEN, P. B. Computing with the analytic Jacobian of a genus 2 curve. In *Discovering mathematics with Magma*, vol. 19 of *Algorithms Comput. Math.* Springer, Berlin, 2006, pp. 117–135. 6.1.9
- [463] VAUGHN, V. Certain Set of Smooth Conics is Finite. Mathematics Stack Exchange. [Online]. Available at <https://math.stackexchange.com/q/4438802>, 2022. (Accessed: 03 June 2024). 3
- [464] VINOGRADOV, A. I., AND SPRINDŽUK, V. G. The representation of numbers by binary forms. *Mat. Zametki* 3 (1968), 369–376. 3
- [465] VISSER, R. Potential good reduction of hyperelliptic curves, 2022. arXiv:2201.07825 [math.NT]. (document), 2
- [466] VOJTA, P. *Diophantine approximations and value distribution theory*, vol. 1239 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1987. 1
- [467] VOJTA, P. Siegel’s theorem in the compact case. *Ann. of Math. (2)* 133, 3 (1991), 509–548. 1
- [468] VON KÄNEL, R. An effective proof of the hyperelliptic Shafarevich conjecture. *J. Théor. Nombres Bordeaux* 26, 2 (2014), 507–530. 1.1.2, 2.1.1
- [469] VON KÄNEL, R. On Szpiro’s discriminant conjecture. *Int. Math. Res. Not. IMRN*, 16 (2014), 4457–4491. 16
- [470] VON KÄNEL, R. The effective Shafarevich conjecture for abelian varieties of  $GL_2$ -type. *Forum Math. Sigma* 9 (2021), Paper No. e39, 29. 1, 1.1.3
- [471] VON KÄNEL, R., AND MATSCHKE, B. Solving  $S$ -unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via the Shimura-Taniyama conjecture. *Mem. Amer. Math. Soc.* 286, 1419 (2023), vi+142. 1.1, 5, 2.3, 2
- [472] ŠAFAREVIČ, I. R. The group of principal homogeneous algebraic manifolds. *Dokl. Akad. Nauk SSSR* 124 (1959), 42–43. 6.1.11
- [473] ŠAFAREVIČ, I. R. Algebraic number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*. Inst. Mittag-Leffler, Djursholm, 1963, pp. 163–176. 1.2, 1.3, 3
- [474] WASHINGTON, L. C. The non- $p$ -part of the class number in a cyclotomic  $\mathbb{Z}_p$ -extension. *Invent. Math.* 49, 1 (1978), 87–97. 3.9



- [475] WASHINGTON, L. C. *Introduction to cyclotomic fields*, second ed., vol. 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1997. [3.1.1](#), [3.1.1](#), [3.1.2](#), [3.9](#), [3.9](#)
- [476] WEIL, A. *Variétés abéliennes et courbes algébriques*, vol. 8 (1946) of *Publications de l'Institut de Mathématiques de l'Université de Strasbourg [Publications of the Mathematical Institute of the University of Strasbourg]*. Hermann & Cie, Paris, 1948. *Actualités Scientifiques et Industrielles*, No. 1064. [Current Scientific and Industrial Topics]. [1.13](#)
- [477] WEIL, A. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* 55 (1949), 497–508. [1.6.1](#)
- [478] WEIL, A. Number-theory and algebraic geometry. In *Proceedings of the International Congress of Mathematicians, Cambridge, Mass., 1950, vol. 2* (1952), Amer. Math. Soc., Providence, RI, pp. 90–100. [1.7](#)
- [479] WEIL, A. Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.* 168 (1967), 149–156. [1.7.1](#), [5.1](#)
- [480] WEIL, A. *Scientific works. Collected papers. Vol. III (1964–1978)*. Springer-Verlag, New York-Heidelberg, 1979. [1](#)
- [481] WHITMORE, D. The Taylor-Wiles method for reductive groups, 2023. arXiv:2205.05062 [math.NT]. [1.7.1](#)
- [482] WILES, A. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* (2) 141, 3 (1995), 443–551. [1.7.1](#)
- [483] WILLIAMS, C. L. *Conjugacy classes of matrix groups over local rings and an application to the enumeration of abelian varieties*. ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)—Colorado State University. [4.3.3](#)
- [484] WÜSTHOLZ, G. The finiteness theorems of Faltings. In *Rational points (Bonn, 1983/1984)*, vol. E6 of *Aspects Math.* Friedr. Vieweg, Braunschweig, 1984, pp. 154–202. [4.8](#)
- [485] YELTON, J. S. *Hyperelliptic Jacobians and their associated  $l$ -adic Galois representations*. ProQuest LLC, Ann Arbor, MI, 2015. Thesis (Ph.D.)—The Pennsylvania State University. [1.8](#), [1.3.3](#), [1.9](#), [3.9](#)
- [486] YOSHIDA, H. Siegel's modular forms and the arithmetic of quadratic forms. *Invent. Math.* 60, 3 (1980), 193–248. [1.7.2](#)

- [487] YU, J. An Explicit Uniform Mordell Conjecture over Function Fields of Characteristic Zero, 2023. arXiv:2307.02101 [math.NT]. 1
- [488] ZARHIN, Y. G. A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction. *Invent. Math.* 79, 2 (1985), 309–321. 1
- [489] ZARHIN, Y. G., AND PARSHIN, A. N. Finiteness Problems in Diophantine Geometry, 2009. arXiv:0912.4325 [math.NT]. 3
- [490] ZARKHIN, Y. G. Endomorphisms of abelian varieties, cyclotomic extensions, and Lie algebras. *Mat. Sb.* 201, 12 (2010), 93–102. 3
- [491] ZHANG, R. The Mordell conjecture 100 years later: Open Problems. [Online]. Available at <https://math.mit.edu/~robinz/files/Mordell%20100%20Problem%20List.pdf>, 2024. (Accessed 09 September 2024). 1
- [492] ZHAO, Y. Elliptic curves over real quadratic fields with everywhere good reduction and a non-trivial 3-division point. *J. Number Theory* 133, 9 (2013), 2901–2913. 1.1.1