Reduction of Hyperelliptic Curves

Robin Visser

Supervisor: **Prof Samir Siksek**

1st Year PhD Project 1, 2021

University of Warwick

Contents

Abstract

Let C/K be a hyperelliptic curve over some number field K. We study the general reduction behaviour of both C and its Jacobian $\mathrm{Jac}(C)$ using the method of cluster pictures, introduced by [31]. Using these ideas, we also attempt to characterise and give some results on when $\mathrm{Jac}(C)$ has good reduction outside 2 for genus 2 curves $C/\mathbb{Q}$. By computing L-functions and solving the required S-unit equations, we give a (non-exhaustive) list of 115 genus 2 curves $C/\mathbb{Q}$, separated into 53 isogeny classes, such that $\mathrm{Jac}(C)$ has good reduction outside 2, with C not having good reduction outside 2.

Introduction

For a given number field K, the problem of studying and classifying both elliptic and hyperelliptic curves C/K has been an important problem in number theory over the last few decades.

We first consider the simplest case: the theory of elliptic curves. The study of elliptic curves had their origins as far back as Diophantus [4] 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 elliptic curves in cryptography has truly cemented its importance both in pure number theory as well as applications in computer science. An excellent overview of the theory of elliptic curves is given by Silverman [85, 86].

Whilst there is an extensive swathe of literature covering the theory of elliptic curves, for our purposes, we shall be interested more generally in the theory of hyperelliptic curves. Whilst it originally didn't receive as much attention as elliptic curves, nowadays there has been a lot more further research done in this area. In addition to elliptic curves, hyperelliptic curves have also started to see their use in integer factorisation algorithms [58] and public-key cryptography [55], making its study just as important as the elliptic case.

For this project, we shall be interested in classifying hyperelliptic curves specifically by their reduction behaviour. Many authors have previously classified elliptic curves with good reduction outside some finite set S. For the genus 2 case, Merriman and Smart [66, 87] have classified all curves $C/\mathbb{Q}$ with good reduction outside 2. Indeed, these procedures have been generalised to give a practical algorithm for determining all hyperelliptic curves of a given genus g with good reduction outside a given finite set of primes S.

We shall aim to revisit the above ideas for general hyperelliptic curves, using the recent notion of cluster pictures introduced by Dokchitser, Dokchitser, Maistret, Morgan [31]. This will help us extend some results to analysing the Jacobian $\mathrm{Jac}(C)$ of hyperelliptic curves C. Our primary goal will be to extend Merriman and Smart's list whereby we shall attempt to classify all genus 2 curves C over $\mathbb{Q}$ such that $\mathrm{Jac}(C)$ has good reduction outside 2.

History

It's perhaps worth first giving a brief history of the classification of hyperelliptic curves with good reduction outside a finite set of primes S. Naturally, we first start with the genus 1 case, elliptic curves.

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.

Firstly, we note that the case $K = \mathbb{Q}$, and $S = \emptyset$ simply corresponds to showing that there is 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 [72, p. 144]. In the 1960s, Ogg [72] then classified all 24 elliptic curves over $\mathbb{Q}$ with good reduction outside $S = \{2\}$, followed independently by Coghlan [17] and Stephens [89] who handled the $S = \{2, 3\}$ case.

Various 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.

Table 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	$\lvert E(S)\rvert$	**Authors**	**Year**
$\emptyset$	0	Tate, proof published by Ogg [72]	1965
$\{2\}$	24	Ogg [72]	1965
$\{2, 3\}$	752	Coghlan[1][17], Stephens [89]	1967, 1965
$\{11\}$	12	Agrawal-Coates-Hunt-Van der Poorten [1]	1980
$\{2, p\}$, $p \in \{5, \ldots, 23\}$	$280, 288, \ldots$	Cremona, Lingham [25]	2007
$\{2, 3, 23\}$	5520	Koutsianas [56]	2015
$\{2, 3, 5, 7, 11\}$	592 192	von Känel, Matschke [96]	2016
$\{2, 3, \ldots, 23\}$	1 390 818 304	Matschke[2]	2021

The next step would be to classify elliptic curves over various quadratic fields K. Indeed, as with the rational case, this has similarly been extensively studied by many authors [57, 73, 74, 75, 91, 26], with the specific case of $S = \emptyset$ receiving much attention over the last few decades by Setzer [83, 84], Ishii [43, 44], Rohrlich [77], Comalada, Nart [20, 21, 22], and Kida, Kagawa [49, 50, 51, 52, 53, 54].

Whilst an exhaustive overview of results computed over quadratic fields K is certainly not possible within the scope of this project, we simply give a brief table summarising some of the results, given in Table 2.

Table 2: Summary of elliptic curves over quadratic fields K with good reduction outside S.

Field K	**Set** S		
	$\emptyset$	$\{2\}$	$\{2, 3\}$
$\mathbb{Q}(i)$	0	64	1280
$\mathbb{Q}(\sqrt{-2})$	0	40	2570
$\mathbb{Q}(\sqrt{-3})$	0	44	1776
$\mathbb{Q}(\sqrt{2})$	0	400	9536

Nowadays, effective algorithms to classify all elliptic curves over K with good reduction outside any finite set S have been well-studied [25], with many practical optimisations having being well-developed in the elliptic case.

It's also worth mentioning that historically many early classifications of elliptic curves were computed only for modular elliptic curves, before an unconditional computation was performed. For

[1] We note the Coghlan's original paper mentions 760 curves, however a few of these are actually $\mathbb{Q}$-isomorphic.
[2] This was computed assuming the generalised Riemann hypothesis.

example, we should also mention the list of modular elliptic curves $E/\mathbb{Q}$ with conductor $N \leq 200$ computed in 1975, given in [6].

The corresponding problem of determining all genus 2 curves with good reduction outside a given set S has similarly been well-studied, with Merriman, Smart [66, 87] having classified all genus 2 curves over $\mathbb{Q}$ with good reduction outside $\{2\}$, by using finiteness results from Evertse and Győry [34]. A recent project by Rowan [78] has also considered the case of genus 2 curves with good reduction outside $\{3\}$.

Very recently, Dabrowski-Sadek [27] have attempted to classify all genus 2 curves with good reduction outside one odd prime, under the assumption that C has at least two rational Weierstrass points.

Finally, we mention the works of Malmskog, Rasmussen [62] as well as Bouw-Koutsianas-Sijsling-Wewers [9] 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 $\{2\}$ and $\{2, 3\}$ respectively.

Preliminaries

We shall first state some preliminary definitions and results: Before we can define hyperelliptic curves, we first need to define a suitable ambient space.

Definition 1: [90, 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** $\mathbb{P}^2_{d_1,d_2,d_3}$ as the ambient space whose points over K are weighted equivalence classes of $K^3\backslash\{0,0,0\}$. In other words, we define

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

where $\sim$ denotes an equivalence on $K^3\backslash\{0,0,0\}$, where for $(X,Y,Z),(X',Y',Z') \in K^3\backslash\{0,0,0\}$, 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 $\lambda \in K^\times$.

We do note that there are various equivalent ways of defining hyperelliptic curves. 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 $x : C \to \mathbb{P}^1$ 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 2: [90, p. 5] Let K be a field, and let $g \geq 2$ be a fixed positive integer. If $\mathrm{char}(K) \neq 2$, then a **hyperelliptic curve of genus** g is a subvariety of $\mathbb{P}^2_{1,g+1,1}$ defined by an equation of the form

$$Y^2 = F(X,Z) \tag{1}$$

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

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

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

We note in the above definition that, if $\mathrm{char}(K) \neq 2$, then if some curve C is given in the form (2), then one can complete the square on the left hand side to obtain a curve in the form (1).

It's also worth noting that one can define hyperelliptic curves without needing weighted projective space, however it's not as simple as just 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 $C_0 : y^2 = f(x)$, and then define the hyperelliptic curve C as the closure of the image of the map $[1, x, x^2, \ldots, x^{g+1}, y] : C_0 \longrightarrow \mathbb{P}^{g+2}$ [85, p. 40].

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

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 ψ_1 and ψ_2:

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

and

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

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 ∞ if $\deg f(x)$ is odd, or as the two points ∞_1 and ∞_2 if $\deg f(x)$ is even.

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

$$y^2 + h(x)y = f(x) \tag{3}$$

where $\deg h(x) < g + 2$ and $\deg f(x) \in \{2g + 1, 2g + 2\}$ with $f(x)$ having distinct roots. We shall furthermore assume that K doesn't have characteristic 2, then as before we can complete the square on the left hand side of (3) which allows us to assume $h = 0$, and thus obtain a simplified affine model for C as

$$y^2 = f(x)$$

where $\deg f(x) \in \{2g + 1, 2g + 2\}$.

We denote the roots of $f(x)$ as the **Weierstrass points** of C, or equivalently, these are the ramification points of the degree-2 cover $C \to \mathbb{P}^1$.

Given a hyperelliptic curve C/K, for many of our arguments, it will be most convenient to assume some structure on the Weierstrass points of C, such as assuming that all Weierstrass points are integral, or alternatively that $0, 1$ are Weierstrass points. With this aim, we consider the following computations:

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 $\lambda \neq 0, 1$ [85, p. 49]. This allows us to study the $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves by simply specifying λ. We now consider the generalisation of this argument to hyperelliptic curves:

Let C/K be a hyperelliptic curve over some field K, with $\mathrm{char}(K) \neq 2$. 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

$$y^2 = c(x - a_1)(x - a_2) \cdots (x - a_{2g+2})$$

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

Now we consider the Mobius transformations sending the roots a_1, a_2, a_3 to $0, 1$ and ∞ respectively, given by

$$x = \frac{a_3(a_2 - a_1)x' + a_1(a_3 - a_2)}{(a_2 - a_1)x' + (a_3 - a_2)} \quad \text{and} \quad y = \frac{Ay'}{\big((a_2 - a_1)x' + (a_3 - a_2)\big)^{g+1}}$$

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

$$A = \sqrt{c} \cdot (a_3 - a_2)(a_3 - a_1)(a_2 - a_1)^g \cdot \sqrt{a_1 - a_2} \cdot \prod_{i=4}^{2g+2} \sqrt{a_3 - a_i}.$$

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

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2) \cdots (x-\lambda_{2g-1}) \tag{4}$$

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

$$\lambda_i = \frac{(a_3 - a_2)(a_{i+3} - a_1)}{(a_2 - a_1)(a_3 - a_{i+3})} \tag{5}$$

for all $i \in \{1, \ldots, 2g-1\}$. Similarly, in the case where $\deg f = 2g + 1$, then we obtain a similar result by considering the simpler transformations

$$x = (a_2 - a_1)x' + a_1 \quad \text{and} \quad y = \sqrt{c} \cdot (a_2 - a_1)^{(2g+1)/2} y'$$

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

$$\lambda_i = \frac{a_{i+2} - a_1}{a_2 - a_1}$$

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

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

Whilst the above isomorphism allows us to represent any hyperelliptic curve as one with Weierstrass points including 0, 1, and ∞, we note that this only yields an isomorphic curve over some quadratic extension of $K(a_1, \ldots, a_n)$. To instead consider isomorphisms only over $K(a_1, \ldots, a_n)$, we can instead adjust the constant A to be in $K(a_1, \ldots, a_n)$. This therefore yields an isomorphism of C over $K(a_1, \ldots, a_n)$ to an equation of the form:

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

where λ_i is given as before in (5), and $c' \in K(a_1, \ldots, a_n)$.

We also note that we are free to choose any three of the roots $a_1, \ldots, a_{2g+2}$ to send to 0, 1, ∞, and not necessarily just a_1, a_2, a_3. Thus, for a given hyperelliptic curve of genus g, there may be several possible representations given in the form (4), however there will always be only finitely many (specifically, at most $(2g+2)!$) possible representations in the form (4). We note that this agrees with the fact that the moduli space of genus g hyperelliptic curves $\mathcal{H}_g$ has dimension $2g-1$ [38, p. 75].

Jacobians

As with hyperelliptic curves, there are various ways one can define and work with the Jacobian. We shall not dive too deeply into the specifics of working with Jacobians, but will simply consider them for the most part in a naive black box sense. However, for completeness, we shall give the following general functorial definition for the Jacobian for arbitrary non-singular curves:

Definition 3: [68, p. 85] Let C be a smooth projective curve. Let $\mathbf{Var}_K$ denote the category of varieties[3] over K and let **Set** denote the category of sets. For any variety T in $\mathbf{Var}_K$, we denote $\mathrm{Pic}^0(T)$ as the *degree 0 Picard group* of T.

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

$$\begin{aligned} P_C^0 : \mathbf{Var}_K &\longrightarrow \mathbf{Set} \\ T &\longmapsto \frac{\mathrm{Pic}^0(C \times T)}{\mathrm{Pic}^0(T)}. \end{aligned}$$

Furthermore, for any variety J', we define the contravariant functor $h_{J'}$ given by

$$\begin{aligned} h_{J'} : \mathbf{Var}_K &\longrightarrow \mathbf{Set} \\ T &\longmapsto \mathrm{Hom}(T, J'). \end{aligned}$$

We thus define the **Jacobian** $J(C)$ of C as the variety J such that the functor P_C^0 is isomorphic to h_J.[4] We note that J is *unique* (up to isomorphism) by Yoneda's lemma.

We note that, in the general case, $J(C)$ may not exist if $C(K) = \emptyset$ [68, p. 86], however since hyperelliptic curves always contain at least one point at infinity, the Jacobian $J(C)$ of any hyperelliptic curve C always exists.

[3] Here, we consider varieties in the most general sense, as a topological space covered by finitely many open sets, each of which has the structure of an affine variety. See Milne's notes [68] for a full formal definition.

[4] We remark that this definition is also simply the statement that P_C^0 is *represented* by $J(C)$.

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 construction for $J(C)$.

In general, providing an explicit description of the Jacobian 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 [16] gave an explicit construction for the Jacobian of an arbitrary genus 2 curve over K as a smooth projective curve in $\mathbb{P}^{15}$ defined by 72 quadratic forms over K.

Giving a full overview of Jacobian varieties is far beyond the scope of this project, so we shall not go into much further detail regarding Jacobians, as most of our calculations will simply use results from [31] and not need to work directly with the Jacobian. For the most part, it suffices to know that the **Jacobian** of a hyperelliptic curve C/K of genus g is some finitely generated abelian variety (by the Mordell-Weil theorem [90, p. 20]) of dimension g which naturally represents the group $\mathrm{Pic}^0(C)$.

Finally, we shall give some results about torsion points over the Jacobian $\mathrm{Jac}(C)$. If the context of the hyperelliptic curve C is clear, we abbreviate $\mathrm{Jac}(C)$ simply by J. As with elliptic curves, we also denote the set of n-torsion points on J (over $\overline{K}$) by $J[n]$. It's well-known that $J[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ if $\mathrm{char}(K)$ does not divide n. Otherwise, if $\mathrm{char}(K) = p$, then there exists some integer $i \in \{0, \ldots, g\}$ such that for all $m \geq 1$. we have $J[p^m] \cong (\mathbb{Z}/p^m\mathbb{Z})^i$ [69, p. 64].

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

Theorem 4: [97, p. 5] Let C/K be a hyperelliptic curve with affine model $C : y^2 = c(x - a_1) \cdots (x - a_n)$. Then the field of 2-torsion $K(J[2])$ is $K(a_1, \ldots, a_n)$.

Proof: [97, 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 $e_U \in \mathrm{Div}^0(C)$ as

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

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 a_i, we have that the divisor of the function $x - a_i \in K(C)^\times$ is

$$\mathrm{div}(x - a_i) = \begin{cases} 2(a_i, 0) - 2(\infty) & \text{if } n \text{ odd} \\ 2(a_i, 0) - \big((\infty_1) + (\infty_2)\big) & \text{if } n \text{ even} \end{cases}$$

Therefore, by taking the appropriate product of functions $(x - a_i)$, 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 $\mathrm{Pic}^0(C)$. We first note that $e_{U_1} + e_{U_2}$ is equivalent to $e_{U_1 \ominus U_2}$ where $U_1 \ominus U_2 = (U_1 \cup U_2) \backslash (U_1 \cap U_2)$ is the symmetric difference of U_1 and U_2. Since $\mathrm{div}(y) = e_{\mathcal{W}}$, we have that $e_{\mathcal{W}}$ is principal, and furthermore that e_U is principal if and only if $e_{\mathcal{W} \backslash U}$ 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 $e_U = \text{div}(g)$ for some function $g \in K(C)^\times$. By definition of e_U, g cannot have any poles at any affine (i.e. non-infinite) point in C, thus g 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 g has degree $|U| \leq g = \lfloor \frac{n-1}{2} \rfloor$, this implies g must be a polynomial only in x. As U non-empty, we have for some $(a_i, 0) \in U$, that $g(a_i) = 0$ and so $(x - a_i)$ divides g. However, since $\text{ord}_{(a_i,0)}(x - a_i) = 2$, this implies that $g/(x - a_i)$ 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, $K(J[2]) \subseteq K(a_1, \ldots, a_n)$.

For the other inclusion, one can show that the only permutation in the Galois group $\text{Gal}(K(a_1, \ldots, a_n)/K)$ which fixes every partition of $\mathcal{W}$ into two even subsets is the identity [97, p. 6], assuming $n \neq 4$. This therefore proves the other inclusion, and thus the claim holds. □

We shall also state without proof an analogous result for the four-torsion $J[4]$. This will be useful when proving Theorem 22 in a later section.

Theorem 5: [97, p. 7] Let C/K be a hyperelliptic curve with affine model $C : y^2 = c(x - a_1) \cdots (x - a_n)$. Then the field of 4-torsion $K(J[4])$ is

$$K(J[4]) = \begin{cases} K(J[2])\Big(\zeta_4,\ \big\{\sqrt{a_i - a_j}\big\}_{1 \leq i,j \leq n}\Big) & \text{if } n \text{ odd} \\ K(J[2])\Big(\zeta_4,\ \big\{\sqrt{a_i - a_j} \prod_{\substack{1 \leq \ell \leq n-1 \\ \ell \neq i,j}} \sqrt{a_\ell - a_n}\big\}_{1 \leq i,j \leq n}\Big) & \text{if } n \text{ even} \end{cases}$$

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 6: 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 7: [16, p. 155] Let C/K be a genus 2 curve, and assume it has a model of the form

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

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

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

We further note that this also gives an alternative way to calculate the rank, since we have that $\mathrm{rank}(\mathrm{Jac}(C)) = \mathrm{rank}(E_1) + \mathrm{rank}(E_2)$. A proof of this theorem can be found in Cassels-Flynn [16, p. 155].

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*, introduced by Dokchitser, Dokchitser, Maistret, Morgan [31].

Definition 8: [30, p. 2] Let $g \geq 2$, and let C/K be a hyperelliptic curve of genus g given by

$$y^2 = f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

where $n \in \{2g+1, 2g+2\}$. Let $\mathcal{R} = \{a_1, \ldots, a_n\}$ denote the set of roots of f, with $\mathcal{P}(\mathcal{R})$ being 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:

$$\Sigma_\mathfrak{p} := \left\{ \mathfrak{s} \in \mathcal{P}(\mathcal{R}) \mid \forall x \in \mathfrak{s},\, v_\mathfrak{p}(x - z) \geq d \text{ for some } z \in \overline{K}, d \in \mathbb{Q} \right\}$$

i.e. these are simply the subsets of $\mathcal{R}$ which are cut out by bounded p-adic discs in K. [5]

We also define the **depth** $d_\mathfrak{s}$ of a cluster $\mathfrak{s}$ as

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

(i.e. the maximal valuation which cuts out $\mathfrak{s}$) and furthermore define ν_s as

$$\nu_s := v_p(c) + \sum_{r \in \mathcal{R}} d_{r \wedge s}$$

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). We call $\mathfrak{s}$ **principal** if $|\mathfrak{s}| \geq 3$ except if either $\mathfrak{s} = \mathcal{R}$ is even and has exactly two children, or if 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 $\mathrm{Jac}(C)$ at any odd prime $\mathfrak{p}$.

[5] Strictly speaking, the extension of the p-adic valuation from K to $K(J[2])$ is not uniquely determined if $\mathfrak{p}$ is not totally ramified in $K(J[2])/K$, however choosing a different valuation simply corresponds to constructing Σ_p over $\sigma(\mathcal{R})$ for some $\sigma \in \mathrm{Gal}(K(\mathcal{R})/K)$, and thus yields an isomorphic cluster picture.

We now partially restate the main theorem given in [30]:

Theorem 9: [30, p. 4] 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. Σ_p is either trivial, or consists of a single non-trivial cluster of size $2g+1$)

(ii) Assuming C has potentially good reduction at 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.

(iii) $\mathrm{Jac}(C)$ has *potentially good reduction* at $\mathfrak{p}$ if and only if all clusters $s \neq \mathcal{R}$ in $\Sigma_{\mathfrak{p}}$ is odd.

(iv) Furthermore, $\mathrm{Jac}(C)$ has *good reduction* at $\mathfrak{p}$ if and only if $K(\mathcal{R})/K$ is unramified and $v_{\mathfrak{s}} \in 2\mathbb{Z}$ for all principal clusters.

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

Example 10: Let $C/\mathbb{Q}$ be a genus 2 curve given by [6]

$$y^2 = 6x^6 - 13x^5 + 27x^4 - 28x^3 + 27x^2 - 13x + 6 \tag{6}$$

By factorising the right hand side of (6), 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

$$y^2 = 6(x - a_1)(x - a_2)\cdots(x - a_6)$$

where

$$a_1 = \tfrac{1+i\sqrt{3}}{2}, \quad a_2 = \tfrac{1-i\sqrt{3}}{2}, \quad a_3 = \tfrac{1+i\sqrt{15}}{4}, \quad a_4 = \tfrac{1-i\sqrt{15}}{4}, \quad a_5 = \tfrac{1+2i\sqrt{2}}{3}, \quad a_6 = \tfrac{1-2i\sqrt{2}}{3},$$

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 into two prime factors each:

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

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 a_i: Note that $(a_1 - a_2) = (i\sqrt{3}) = \mathfrak{p}_3\mathfrak{q}_3$, and thus $v_3(a_1 - a_2) = \frac{1}{2}$.

Similarly, we note $(a_3 - a_4) = (\frac{i\sqrt{15}}{2})$, which also has 3-adic valuation of $1/2$. Indeed, we can tabulate the the differences between each of the roots $a_1, \ldots, a_6$:

Table 3: Factorisation of the ideals $(a_i - a_j)$ (i.e. up to units)

	a_1	a_2	a_3	a_4	a_5	a_6
a_1	0	$\mathfrak{p}_3\mathfrak{q}_3$	$\mathfrak{p}_2^{-2}$	$\mathfrak{q}_2^{-2}$	$\mathfrak{p}_3^{-2}$	$\mathfrak{q}_3^{-2}$
a_2		0	$\mathfrak{p}_2^{-2}$	$\mathfrak{q}_2^{-2}$	$\mathfrak{p}_3^{-2}$	$\mathfrak{q}_3^{-2}$
a_3			0	$\mathfrak{p}_2^{-2}\mathfrak{q}_2^{-2}\mathfrak{p}_3\mathfrak{q}_3\mathfrak{p}_5\mathfrak{q}_5$	$\mathfrak{p}_2^{-2}\mathfrak{p}_3^{-2}$	$\mathfrak{p}_2^{-2}\mathfrak{q}_3^{-2}$
a_4				0	$\mathfrak{q}_2^{-2}\mathfrak{p}_3^{-2}$	$\mathfrak{q}_2^{-2}\mathfrak{q}_3^{-2}$
a_5					0	$\mathfrak{p}_2^5\mathfrak{q}_2^5\mathfrak{p}_3^{-2}\mathfrak{q}_3^{-2}$
a_6						0

[6] This is the genus 2 curve 2880.c.368640.1 given on the LMFDB: `https://www.lmfdb.org/Genus2Curve/Q/2880/c/368640/1`

From the above table, we note that 3-adic valuation, is at least -1 for any difference $a_i - a_j$, 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 a_6, and finally we'll have two twin clusters around $\{a_1, a_2\}$, and $\{a_3, a_4\}$ of depth $1/2$. This yields the following cluster picture Σ_3:

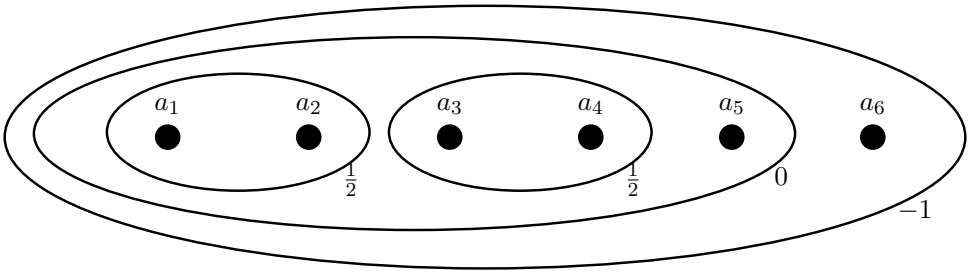

Figure 1: Cluster picture Σ_3 for the genus 2 curve C given in (6).

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 a_5 and a_6 swapped.

Using the above Theorem 9, we can show that determining whether a curve C or its Jacobian $\mathrm{Jac}(C)$ has (potentially) good reduction can be done purely by analysing the p-adic valuations of differences between the roots:

Proposition 11: Let C/K be a hyperelliptic curve, given in the form

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

Let $\mathfrak{p}$ be an odd prime of K. Then C has potentially good reduction at $\mathfrak{p}$ if and only if we have $v_p(\lambda_i) = v_p(\lambda_i - 1) = 0$ for all $i \in 1, \dots, 2g-1$, and $v_p(\lambda_i - \lambda_j) = 0$ 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 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 9, 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 $v_p(r_i - r_j)$ is constant over all distinct pairs $r_i, r_j \in \mathcal{R}$. However, since $v_p(1-0) = 0$, this implies that $v_p(\lambda_i) = v_p(\lambda_i - 1) = 0$ for all i, and that $v_p(\lambda_i - \lambda_j) = 0$ for all i, j, which yields the result. □

This immediately yields the following corollary:

Corollary 12: Let K be a number field, and let S be a finite set of primes of K, and assume that S consists of 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 λ_i and $\lambda_i - 1$ are in $\mathcal{O}_S^\times$, and if $\lambda_i - \lambda_j$ are in $\mathcal{O}_S^\times$.

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 prime 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. Initialise a list $\mathcal{A}$ of all such curves.

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

   (a) Use [71, p. 203] to show that any such field must have discriminant dividing the ideal $\prod_{\mathfrak{p} \in S} \mathfrak{p}^{d(d+1)}$. This yields a finite number of possible discriminants for L.
   (b) For each possible discriminant, do a Hunter search [18, p. 445] to compute all possible number fields with degree d and given discriminant.

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

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

   $$\lambda_1 + \mu_1 = 1, \quad \ldots, \quad \lambda_{2g-1} + \mu_{2g+1} = 1, \quad \lambda_i, \mu_i \in \mathcal{O}_S^\times$$

   such that $\lambda_i - \lambda_j \in \mathcal{O}_S^\times$ for all $i, j \in \{1, \ldots, 2g - 1\}$.

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

   (c) If $C \cong C^\sigma$ for all $\sigma \in \mathrm{Gal}(L/K)$, then C can be defined over K, and so we add C to $\mathcal{A}$.

This therefore gives an effective procedure to find all possible Rosenhain normal forms of hyperelliptic curves, and thus all possible $\overline{K}$-isomorphism classes. However, to translate this into a complete list of K-isomorphism classes requires some more technical details, which we defer (in the genus 2 case over $\mathbb{Q}$) to a later section.

It's easy to note that, as there are only finitely many solutions to any given S-unit equation, we have the following corollary:

Corollary 13: For a given number field K, finite set of primes S, and genus g, there are only finitely many 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.

We now present a theorem which yields a lower bound on the number of bad primes for a given genus g:

Theorem 14: Let C 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:

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

and let $\mathfrak{p}$ be a prime ideal of K such that the norm satisfies $N(\mathfrak{p}) \leq 2g$.

We have by Theorem 11 that $\lambda_1, \ldots, \lambda_{2g-1}$ must all be $\mathfrak{p}$-units. Furthermore, note that each of the roots $0, 1, \lambda_1, \ldots, \lambda_{2g-1}$ must yield distinct values under the reduction map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$. However, this is a contradiction if $2g + 1 > N(\mathfrak{p})$, noting that the size of the residue field $\mathcal{O}_K/\mathfrak{p}$ is $N(\mathfrak{p})$. □

It's furthermore clear that the above inequality is tight, since given any $\mathfrak{p}$ with $N(\mathfrak{p}) > 2g$, we can simply let $0, 1, \lambda_1, \ldots, \lambda_{2g-1}$ be some distinct representative elements in the residue ideal

to yield an example of a curve C with good reduction at $\mathfrak{p}$.

Unfortunately, it doesn't seem as easy to derive a similarly simple necessary and sufficient condition for the Jacobian $\mathrm{Jac}(C)$ to have potentially good reduction at $\mathfrak{p}$, other than restating Theorem 9. This is a matter which we shall investigate in more detail in a later section.

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 $\mathbb{Q}$.

Hyperelliptic curves with rational Weierstrass points

Firstly, it's worth stating the application of Theorem 14 to the rational case:

Corollary 15: Let C be a hyperelliptic curve with rational Weierstrass points. Then C cannot have potentially good reduction at any odd prime $p \leq 2g$.

Note that this clearly implies that no genus 2 hyperelliptic curve with rational Weierstrass points has potentially good reduction at 3. As no such curve has potentially good reduction at $p = 2$ either, we note that this therefore yields a quick proof of the following result from Box and Le Fourn [11]:

Corollary 16: [11, p. 3] 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.

Already, this illustrates the versatility of cluster pictures by easily proving not just the above corollary, but a generalisation for hyperelliptic curves of any genus g over arbitrary number fields K.

Of course, we remark that the above is not true for genus 2 curves over $\mathbb{Q}$ with non-rational Weierstrass points. For example $y^2 = x(x-1)(x+1)(x-i)(x+i)$ does have good reduction at $p = 3$.

Note that this immediately implies that there are only finitely many hyperelliptic curves of genus g with rational Weierstrass points having potentially good reduction outside at most $\pi(2g) - 1$ odd primes. However, we can go one step further:

Theorem 17: There are only finitely many hyperelliptic curves of genus g with rational Weierstrass points having potentially good reduction outside at most $\pi(2g)$ odd primes.

Proof: Let $C/\mathbb{Q}$ 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 rational Weierstrass points. By Corollary 15, C cannot have potentially good reduction at any odd primes less than $2g$. Now assume C has potentially good reduction outside exactly $\pi(2g)$ odd primes S.

Thus, S must consist of all primes below $2g$, plus one additional prime p. Now by Theorem 11, we must have that $\lambda_1, \lambda_2, \lambda_1 - 1, \lambda_2 - 1$ and $\lambda_1 - \lambda_2$ are all S-units. Therefore, by Lemma 28, there are only finitely many possible primes p, and thus by Corollary 13, there are only finitely many hyperelliptic curves with potentially good reduction outside S. □

It's worth mentioning that at this stage, we are still unsure if there are only finitely many hyperelliptic curves of genus g having potentially good reduction outside r odd primes, for any

$r > \pi(2g)$.

We can illustrate the effectiveness of the above theorem by applying Lemma 28 concretely to the genus 2 case:

Theorem 18: Let C be a genus 2 hyperelliptic curve with rational Weierstrass points, having potentially good reduction outside $S = \{2, 3, p\}$ for some prime $p \geq 5$. Then $p \in \{5, 7, 11, 13, 17, 73\}$.

Proof: This follows by effectively going through the computations in Lemma 28. □

We also mention that for hyperelliptic curves $C/\mathbb{Q}$ of genus 3 with rational Weierstrass points having potentially good reduction outside $\{2, 3, 5, p\}$, we've checked computationally that $p \in \{7, 11, 13, 17, 19, 23, 29, 41, 43, 53\}$ after an extensive search, although this hasn't been formally proven.

We now shift our attention to studying the Jacobian $\mathrm{Jac}(C)$ of hyperelliptic curves. We shall first 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.

Proposition 19: There are infinitely many (non-isomorphic over $\overline{\mathbb{Q}}$) genus 2 hyperelliptic curves C over $\mathbb{Q}$ with rational Weierstrass points with $\mathrm{Jac}(C)$ 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 $\lambda_1 = 2^r + 1, \lambda_2 = \frac{2^r+1}{2}, \lambda_3 = 2^r$., i.e.

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

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 $\{0, \lambda_1, \lambda_2\}$.

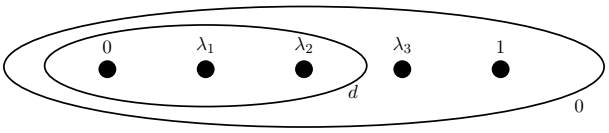

Figure 2: Cluster picture Σ_p for primes p dividing $2^r + 1$.

- **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 $\{1, \lambda_2, \lambda_3\}$.

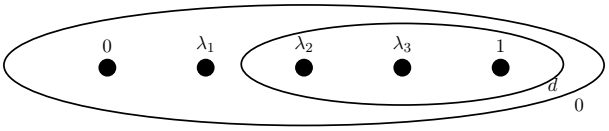

Figure 3: Cluster picture Σ_p for primes p dividing $2^r - 1$.

- **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 Σ_p is trivial.

Therefore, in all cases, the cluster picture Σ_p only contains odd clusters, which proves that $\mathrm{Jac}(C)$ has potentially good reduction at all primes outside $\{2\}$. □

We also remark that hyperelliptic curves of genus $3, 4$ and 5 with potentially good reduction outside $\{2\}$ can easily be found, however we are still unsure if any such curves exist with genus ≥ 6. In many cases, the numerical evidence suggests that constructions similar to those given in Theorem 19 seem to yield infinite families of curves, however it's certainly not trivial to prove these for higher genus.

For example, one can prove that there are infinitely many genus 3 curves C with rational Weierstrass points such that $\mathrm{Jac}(C)$ has potentially good reduction outside $\{2\}$, if one can prove that there are infinitely many triples of distinct primes (p, q, r) such that $\mathrm{rad}(p^2-q^2) = \mathrm{rad}(p^2-r^2) = \mathrm{rad}(q^2 - r^2)$.

We now look at conditions for when the Jacobian itself has good reduction:

Theorem 20: Let C/K be a hyperelliptic curve in the form

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

Then $\mathrm{Jac}(C)$ has good reduction at an odd prime p if and only if $\mathrm{Jac}(C)$ has potentially good reduction at p, and $K(\mathcal{R})/K$ is unramified, and if $v_p(\lambda_i)$, $v_p(\lambda_i - 1)$ and $v_p(\lambda_i - \lambda_j)$ all have the same parity as $v_p(c)$.

Proof: Let Σ_p be the cluster picture of C at p. By Theorem 9, to show that $\mathrm{Jac}(C)$ has good reduction at p, it suffices to show that $\nu_{\mathfrak{s}}$ is even, for all principal clusters $\mathfrak{s}$.

Firstly, we note that since $v_p(\lambda_i)$, $v_p(\lambda_i - 1)$ and $v_p(\lambda_i - \lambda_j)$ all have the same parity as $v_p(c)$, this implies the depths d_s of all principal clusters have the same parity as $v_p(c)$.

We can proceed by a standard inductive approach. Let $\mathfrak{s}$ be a principal cluster of Σ_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 4. 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

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

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

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

$$\nu_s \equiv v_p(c_f) + d_s \equiv 0 \pmod 2$$

which proves the claim. □

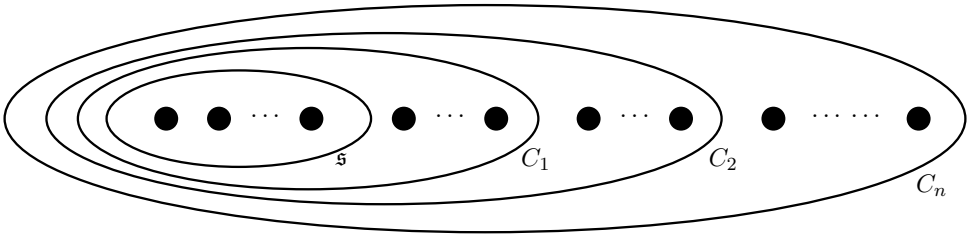

Figure 4: A chain of clusters $\mathfrak{s} \subsetneq C_1 \subsetneq C_2 \subsetneq \cdots \subsetneq C_n$.

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

Corollary 21: Let C/K be a hyperelliptic curve given as above. Then $\mathrm{Jac}(C)$ has good reduction outside S if and only if $\mathrm{Jac}(C)$ has potentially good reduction outside S, and $K(\mathcal{R})/K$ unramified outside S, and such that $\lambda_i, \lambda_i - 1$ and $\lambda_i - \lambda_j$ are in $c\,\mathcal{O}_S^\times \cdot (K^\times)^2$.

Finally, we show that there are no solutions in the case where $g = 2$, $K = \mathbb{Q}$ and $S = \{2\}$.

Theorem 22: Let $C/\mathbb{Q}$ be a hyperelliptic curve with rational Weierstrass points. Then $\mathrm{Jac}(C)$ cannot have good reduction outside $\{2\}$.

Proof: Let $a_1, a_2, \ldots, a_n$ be the rational Weierstrass points of C. By sending one of the roots to ∞, we may also assume that an affine model for C is $y^2 = f(x)$ where $f(x)$ is monic of degree 5. Now the main idea is to analyse the 4-torsion field $\mathbb{Q}(J[4])$ where $J = \mathrm{Jac}(C)$.

Firstly, since C has all rational Weierstrass points, this implies $\mathbb{Q}(J[2]) = \mathbb{Q}$. Furthermore, since $\mathrm{Jac}(C)$ has good reduction outside 2, then by Corollary 21, this implies that $\sqrt{a_i - a_j}$ all lie in $\mathbb{Q}(i, \sqrt{2})$.

Therefore, by Theorem 5, we have that $\mathbb{Q}(J[4])$ is either $\mathbb{Q}(i)$ or $\mathbb{Q}(i, \sqrt{2})$. Let $K = \mathbb{Q}(J[4])$. We now recall that the torsion subgroup $C(K)_{\mathrm{tors}}$ injects into $J(\mathcal{O}_K/\mathfrak{p})$ for all primes $\mathfrak{p}$ of good reduction for J, as noted in the Appendix of [47].

We shall assume for contradiction that J has good reduction specifically at $p = 3$. Considering the two cases for K, if $K = \mathbb{Q}(i)$, then the ideal (3) is prime (3 is inert), otherwise if $\mathbb{Q}(i, \sqrt{2})$ then (3) splits into two primes $\mathfrak{p}_1\mathfrak{p}_2$. In either case, we note that the prime(s) $\mathfrak{p}$ above 3 have norm $N(\mathfrak{p}) = 9$.

Thus by considering the 4-torsion over K, and noting that $\#J[4] = \#(\mathbb{Z}/4\mathbb{Z})^4 = 256$, this implies that 256 divides $J(\mathcal{O}_K/\mathfrak{p})$ for the prime $\mathfrak{p}$ lying above 3. However, by Weil's inequality, we have

$$\#J(\mathcal{O}_K/\mathfrak{p}) = N(\mathfrak{p})^2 + 1 + \sum_{i=1}^{4} \alpha_i \leq 82 + 4 \cdot 9 = 118,$$

and thus, since $256 > 118$, this contradicts the fact that $C(K)_{\mathrm{tors}}$ injects into $J(\mathcal{O}_K/\mathfrak{p})$. □

Invariants

When characterising hyperelliptic curves C, it is often useful to work with a set of invariants corresponding to the $\overline{\mathbb{Q}}$-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 [33].

Let C be a hyperelliptic curve of the form $y^2 = c(x - a_1) \cdots (x - a_n)$. For some positive even integer m, we define the invariant $I_m(C)$ by

$$I_m(C) = (4c)^m \sum (\alpha_i - \alpha_j) \cdots (\alpha_k - \alpha_\ell)$$

where the expression under the sum contains each a_i m times, and where the sum runs over all permutations of the index set $\{1, \ldots, n\}$ which yield distinct expressions (i.e. over all S_n-Galois orbits of the given expression).

We can then characterise $\overline{\mathbb{Q}}$-isomorphism classes of hyperelliptic curves by noting the following proposition:

Proposition 23: Let C, D be two hyperelliptic curves of genus g over K. 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.

In practice, one need only compute finitely many of the Igusa invariants I_m, by a famous result of Hilbert which states that the dimension of the space of invariants is finite.

Invariants for genus 2

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 $\mathrm{char}(K) \neq 2$, and let C/K be a genus 2 hyperelliptic curve. We can therefore explicitly define the following set of **Igusa-Clebsch invariants** [42, p. 620]:

$$\begin{aligned}
I_2 &:= (4c)^2 \sum (a_1 - a_2)^2 (a_3 - a_4)^2 (a_5 - a_6)^2 \\
I_4 &:= (4c)^4 \sum (a_1 - a_2)^2 (a_2 - a_3)^2 (a_3 - a_1)^2 (a_4 - a_5)^2 (a_5 - a_6)^2 (a_6 - a_4)^2 \\
I_6 &:= (4c)^6 \sum (a_1 - a_2)^2 (a_2 - a_3)^2 (a_3 - a_1)^2 (a_4 - a_5)^2 (a_5 - a_6)^2 (a_6 - a_4)^2 \\
&\qquad\qquad (a_1 - a_4)^2 (a_2 - a_5)^2 (a_3 - a_6)^2 \\
I_{10} &:= (4c)^{10} \prod (a_i - a_j)^2
\end{aligned}$$

where, as before, each sum/product runs over the permutations of $\{1, \ldots, 6\}$ which yield different expressions.

To work in addition to the case where $\mathrm{char}(K) = 2$, we can furthermore define the **Igusa invariants** [42, p. 621-622], as follows:

$$\begin{aligned}
J_2 &:= I_2/8, \\
J_4 &:= (4J_2^2 - I_4)/96,
\end{aligned}$$

$$J_6 := (8J_2^3 - 160J_2J_4 - I_6)/576,$$
$$J_8 := (J_2J_6 - J_4^2)/4,$$
$$J_{10} := I_{10}/4096.$$

whereby we also that, for any two genus 2 curves C, D, then C is isomorphic to D over $\overline{K}$ if and only if $J_m(C) = \lambda^m J_m(D)$ for some $\lambda \in \overline{K}^\times$.

To give a simpler description of the $\overline{\mathbb{Q}}$-isomorphism classes of genus 2 curves, we also consider the **G2 invariants**, defined by Cardona-Quer-Nart-Pujolás [14, 15], defined in terms of the Igusa invarints, as follows:

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

This time, we have that two genus 2 curves C, D are $\overline{K}$-isomorphic if and only if their G2-invarints are the same. We also remark 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 invariants I_2, I_4, I_6 and I_{10} in terms of $\lambda_1, \lambda_2, \lambda_3$ for a curve C in Rosenhain norm form $C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ is given in the appendix of Malmendier-Shaska [61, p. 20].

L-functions

One of the most important isogeny invariants of hyperelliptic curves C/K is its L-function $L(C/K, s)$. Since the L-function of a curve C is the same as its Jacobian $\mathrm{Jac}(C)$, studying $L(C/K, s)$ is instrumental into understanding and classifying curves according to its Jacobian.

We first define the L-function of a hyperelliptic curve:

Definition 24: Let C be a hyperelliptic curve over some number field K. We recall the L-function of C/K is given by the Euler product:

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

where $N(\mathfrak{p})$ denotes the norm 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 $\mathrm{Jac}(C)$ at $\mathfrak{p}$. It can be defined generally in terms of the geometric Frobenius in a decomposition group at $\mathfrak{p}$, as follows: [10] Let $D_{\mathfrak{p}} \subset \mathrm{Gal}(\overline{K}/K)$ be a decomposition group at $\mathfrak{p}$, and let $I_{\mathfrak{p}} \subset D_p$ denote the inertia group at $\mathfrak{p}$. We pick an arithmetic Frovenius element $\sigma_{\mathfrak{p}} \in D_{\mathfrak{p}}$ (i.e. $\sigma_{\mathfrak{p}}(\alpha) \equiv \alpha^{N(\mathfrak{p})} (\mathrm{mod}\ \mathfrak{p})$).

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

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

where V denotes

$$V := H^1_{et}(C \otimes_K \overline{K},\ \mathbb{Q}_\ell)$$

being the first étale cohomology group of C, for some prime ℓ different from the residue characteristic of $\mathfrak{p}$.

Whilst this gives a full general definition of the local Euler factors for any prime $\mathfrak{p}$, we can be more specific in the case where $\mathfrak{p}$ is a prime of good reduction for C:

Good reduction

Indeed, if $\mathfrak{p}$ is a prime of good reduction, then the local Euler factor $L_{\mathfrak{p}}(T)$ is simply given by the zeta function:

$$L_{\mathfrak{p}}(T) = Z_{\mathfrak{p}}(T)(1-T)(1-N(\mathfrak{p})T) \tag{7}$$

In order to define $Z_{\mathfrak{p}}(T)$, we let $\#\widetilde{C}_{\mathfrak{p}^k}$ denote the number of points in the reduction of C modulo $\mathfrak{p}^k$. We can then give $Z_{\mathfrak{p}}(T)$ as

$$Z_{\mathfrak{p}}(T) = \exp\Big(\sum_{k=1}^{\infty} \frac{\#\widetilde{C}_{\mathfrak{p}^k}}{k} T^k\Big)$$

where the above is interpreted as a formal power series with coefficients in $\mathbb{Q}$. Whilst it might seem that we need to evaluate $\#\widetilde{C}_{\mathfrak{p}^k}$ for infinitely many k to evaluate $L_{\mathfrak{p}}(T)$, we can use the fact that $L_{\mathfrak{p}}(T)$ is a degree $2g$ polynomial. If we let $L_p(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$ for some $\alpha_i \in \mathbb{C}$, then we can evaluate $L_p(T)$ by taking logarithms of (7) and subsequently using the power series for log, to obtain

$$\#\widetilde{C}_{\mathfrak{p}^k} = N(\mathfrak{p})^k + 1 - \sum_{i=1}^{2g} \alpha_i^k \tag{8}$$

for all positive k [19, p. 135]. Therefore, by utilising Newton relations between the roots and coefficients of $L_{\mathfrak{p}}(T)$, we can calculate any good Euler factor by simply counting points on C modulo p^k for $k = 1, \ldots, g$.

It's worth also mentioning that an alternative method to computing $L_p(T)$ directly from $\mathrm{Jac}(C)$ if $g \leq 3$ involves first calculating $J(C/F_p) = L_p(1)$, and $J(\widetilde{C}/F_p) = L_p(-1)$, where $\widetilde{C}$ denotes the quadratic twist of C mod p. We can then use Lemma 4 from [92] to compute $L_p(T)$ for sufficienfly large p. Kedlaya and Sutherland [48] gives a nice overview of computing L-functions of hyperelliptic curves in the genus $g \leq 3$ case.

Bad reduction

If $\mathfrak{p}$ is a prime of bad reduction, then it's usually not as simple to calculate the Euler factor $L_{\mathfrak{p}}(T)$. Whilst there are ways to do this calculation by computing regular models of C at $\mathfrak{p}$, a simpler (albeit conjectural) way is to simply 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 functional equation.

Since, 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 calculate both the conductor N and all the Euler factors $L_{\mathfrak{p}}(T)$ at all primes.

We now state the conjectural functional equation for C/K:

Conjecture 25: [36, p. 368] (*L-modularity*) Let C be a hyperelliptic curve over K of genus g. We define the completed L-function $\Lambda(C/K, s)$ of C as [8]

$$\Lambda(C/K, s) := N^{s/2}(2\pi)^{-gs}\Gamma(s)^g L(C/K, s)$$

Then $\Lambda(C/K, s)$ has analytic continuation to the complex plane and satisfies the conjectured functional equation:

$$\Lambda(C/K, s) = \epsilon\Lambda(C/K, 2 - s) \tag{9}$$

for some $\epsilon \in \{-1, +1\}$.
We note that the above conjecture is known in some special cases (such as for elliptic curves over $\mathbb{Q}$), but is otherwise still conjectural in almost all cases.

It's also worth noting that the above conjecture is weaker than the Paramodular conjecture, sated by Brumer-Kramer [13]. At a very naive level, this essentially asserts moreover that isogenies classes of paramodular abelian surfaces of conductor N are in 1-1 correspondence with paramodular newforms of level N.

Genus 2 case

Let's now restrict to the genus 2 case: Let C/K be a genus 2 curve. For a prime p of good reduction at C, we let $\#\widetilde{C}_{\mathfrak{p}}$ and $\#\widetilde{C}_{\mathfrak{p}^2}$denote the number of points in the reduction of E modulo $\mathfrak{p}$ and modulo $\mathfrak{p}^2$ respecitvely. We define the trace at $\mathfrak{p}$ as $a_{\mathfrak{p}} := N(\mathfrak{p}) + 1 - \#\widetilde{C}_{\mathfrak{p}}$, and similarly define $a_{\mathfrak{p}^2} := N(\mathfrak{p}) + 1 - \#\widetilde{C}_{\mathfrak{p}^2}$.

Now, by using (8) and Newton relations between the roots and coefficients of $L_{\mathfrak{p}}(T)$, we obtain the following formula for all good Euler factors

$$L_{\mathfrak{p}}(T) = 1 - a_{\mathfrak{p}}T + (a_{\mathfrak{p}}^2 - a_{\mathfrak{p}^2})T^2 - a_{\mathfrak{p}}N(\mathfrak{p})T^3 + N(\mathfrak{p})^2T^4 \tag{10}$$

For primes $\mathfrak{p}$ of bad reduction, we simply make a guess of the Euler factor, 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 size no greater than $\sqrt{N(\mathfrak{p})}$, this yields a bound on the coefficients A_i, which therefore implies there are only finitely many possible bad Euler factors to check. For example, if $C/\mathbb{Q}$ is a genus 2 curve with bad reduction at $p = 2$, then there are only 26 possible bad Euler factors for $L_2(T)$.

Classifying genus 2 curves $C/\mathbb{Q}$ where $\mathbf{Jac}(C)$ is good outside 2

We shall now attempt to classify all hyperelliptic curves C of genus 2 over $\mathbb{Q}$, such that $\mathrm{Jac}(C)$ has good reduction outside 2.

We first note from [70, p. 1] that, given some abelian variety J, there are only finitely many curves C such that $\mathrm{Jac}(C) = J$. Furthermore, by Falting's theorem [23, p. 22], there are only finitely many abelian varieties with good reduction outside a given set S. Therefore, we expect there to only be finitely many such curves (up to $\mathbb{Q}$ isomorphism) where $J(C)$ has good reduction outside $\{2\}$.

Unfortunately, this theorem of Falting's is ineffective and so doesn't provide us with any algorithm to practically compute such a list of curve.

It's perhaps also worth noting that Schoof [81] has shown that no curve C exists such that $\mathrm{Jac}(C)$ has good reduction outside 2 with semi-stable reduction at 2. However these results do make essential use of the fact that the abelian variety $\mathrm{Jac}(C)$ is semi-stable, and thus cannot be applied to our case in general.

First of all, we note that such a list must contain all 428 equivalence classes of curves with good reduction outside 2, given by Smart [87]. Thus, it suffices for us to simply present a list of curves C such that $\mathrm{Jac}(C)$ has good reduction outside 2, but C does not have good reduction outside 2.

Now let $C/\mathbb{Q}$ be a genus 2 curve with $\mathrm{Jac}(C)$ having good reduction outside 2. Then if $\mathcal{R}$ denotes the Weierstrass points of C, then by Theorem 9, we have that $\mathbb{Q}(\mathcal{R})/\mathbb{Q}$ is unramified outside 2. Thus, our first task is to classify all such number fields $K(\mathcal{R})$. Fortunately, this has already been well-studied for small degrees:

Theorem 26: [66, p. 206] 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 conjugation) are:[7]

$$\begin{aligned} \mathbb{Q} \quad & \text{if } [K:\mathbb{Q}]=1 \\ \mathbb{Q}\big(\sqrt{-1}\big),\ \mathbb{Q}\big(\sqrt{2}\big),\ \mathbb{Q}\big(\sqrt{-2}\big), \quad & \text{if } [K:\mathbb{Q}]=2 \\ \mathbb{Q}\big(\sqrt[4]{-1}\big),\ \mathbb{Q}\big(\sqrt{1+\sqrt{-1}}\big),\ \mathbb{Q}\big(\sqrt{1+\sqrt{2}}\big), & \\ \mathbb{Q}\big(\sqrt[4]{2}\big),\ \mathbb{Q}\big(\sqrt[4]{-2}\big),\ \mathbb{Q}\big(\sqrt{-2-\sqrt{2}}\big),\ \mathbb{Q}\big(\sqrt{2+\sqrt{2}}\big), \quad & \text{if } [K:\mathbb{Q}]=4 \end{aligned}$$

Therefore, if α 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.[8]

For brevity, we shall adopt the same as Smart's [87, p. 290] notation for field systems, That is, we let K_1, K_2, K_3 denote the quadratic fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{2})$ respectively, and $L_1, L_2, \ldots, L_7$ denote the 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.

From a technical standpoint, it's perhaps also worth noting that all possible extensions $K(\mathcal{R})$ will have class number 1 in the genus 2 case, however this need not be true in the general case.

We first introduce the notion of field system for a curve C. Indeed, let $C : y^2 = f(x)$ be a hyperelliptic curve. Let $f(x)$ factor over K as

$$f(x) = cf_1(x)f_2(x)\ldots f_m(x)$$

where $f_i(x)$ are irreducible polynomials over K. Let M_i be the field $K(\alpha_i)$ where $f_i(\alpha_i) = 0$. Then we call the typle $(M_1, M_2, \ldots, M_m)$ a **field system** for C. Indeed, one can show that field systems are invariant (up to ordering) under K-isomorphism [88].

From Theorem 26, it's not hard to observe that there are only a finite number of possible field systems for curves C where $\mathrm{Jac}(C)$ has good reduction outside 2. These are given in Table 4.

[7] We remark that the quartic field $\mathbb{Q}(i,\sqrt{2})$ is the same as $\mathbb{Q}\big(\sqrt[4]{-1}\big)$.

[8] At this stage, one might 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 [39, p. 57].

Table 4: List of possible field systems for genus 2 curves $C : y^2 = f(x)$ with $\mathbb{Q}(\mathcal{R})$ unramified outside 2. The number of rational 2-torsion points on $\mathrm{Jac}(C)$ is also tabulated.

Field system	$\mathbf{Jac}(C)[2](\mathbb{Q})$
$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}]$	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

At this stage, we unfortunately don't yet have an unconditional effective algorithm to yield all possible curves with $\mathrm{Jac}(C)$ good outside 2. We therefore focus our efforts on rather giving as complete a list of possible, by considering two possible approaches: directly computing L-functions, and computing curves C with good reduction outside a small finite list of primes. These are described in the following two sections:

Computing L-functions of 2-power conductor

One of the first approaches one can take is to 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 [36], where they generate L-functions purely from the assumption of its functional equation, without any prior knowledge of the coefficients.

In summary, the procedure is as follows: We fix some conductor N and sign ϵ 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 $a_n = \mathcal{O}(n^{1/2+\varepsilon})$. We also assume L-modularity, that is that the completed L-function

$$\Lambda(s) := N^{s/2}\Gamma_{\mathbb{C}}(s)^2 L(s)$$

satisfies the functional equation

$$\Lambda(s) = \epsilon\Lambda(2-s).$$

At this stage, we form a system of equations, from which we hope to at least solve for the first few Dirichlet coefficients a_n. To do this, we shall use the approximate functional equation:

Theorem 27: [79, p. 444] Let $L(s)$ be an L-function as described above, with completed L-function $\Lambda(s)$. Let $g : \mathbb{C} \to \mathbb{C}$ be an entire function such that, for a fixed s, we have

$$|\Lambda(z+s)g(z+s)z^{-1}| \to 0$$

as $|\mathrm{Im}(z)| \to \infty$ in vertical strips where $-x_0 \leq \mathrm{Re}(z) \leq x_0$ for some $x_0 \in \mathbb{R}_+$. Also define $Q := \sqrt{N}/\pi^2$. Then for any s for which $\Lambda(s)$ well-defined, we have

$$\Lambda(s)g(s) = \sum_{k=1}^{\ell} \frac{r_k g(s_k)}{s - s_k} + \sum_{n=1}^{\infty} a_n \left(\left(\frac{Q}{n}\right)^s f_1(s,n) + \epsilon \left(\frac{Q}{n}\right)^{2-s} f_2(s,n) \right)$$

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 $\nu > \max(0, -\mathrm{Re}(s))$.

Proof sketch: [79, p. 445] The result follows by doing a standard contour integral argument, where we evaluate a contour integral of $\Lambda(s)g(s)$ over the rectangle with vertices $(-\alpha, -iT), (\alpha, -iT)$, $(\alpha, iT), (-\alpha, iT)$ and apply Cauchy's theorem. By letting $T \to \infty$, this yields the desired result. The full calculations (for an analytic normalisation of $\Lambda(s)$) are given in Rubinstein [79, p. 445]. □

By thus using the approximate functional equation for various points s and functions g, we can divide through by $g(s)$ to yield several equations of the form

$$\Lambda(s) = c_{g,s,1}a_1 + c_{g,s,2}a_2 + \cdots + c_{g,s,i}a_i + \ldots$$

where $c_{g,s,i}$ are explicitly calculated coefficients, depending on the weight function g and the point s. We can therefore generate an arbitrary number of these equations by simply choosing different points s and functions g.

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, which will ideally allow us to efficiently solve for the first few Dirichlet coefficients a_n.

Thus is done by performing a breadth first search, going through 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 search of genus 2 curve $C/\mathbb{Q}$ having the L-function $L(s)$.

For our purposes, we do this for all possible Euler factors $L_p(T)$ for all primes $p < 250$. We can thus describe 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 $p < 250$.
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 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 $(L_{2,j_1}, L_{3,j_2}, \ldots)$).
4. For each prime p from 2 to 241, 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 genus 2 curve that gives the desired L-function.

Results

We performed the above procedure for conductors $N = 2^a$ for powers $a = 1, \ldots, 10$, and $\epsilon \in \{-1, +1\}$, implemented with Sage [80] using complex ball arithmetic. We verified that no L-functions of conductor $N \leq 2^7$ exist, and that there exists exactly one L-function of conductor $N = 2^8$, corresponding to the square of the elliptic curve isogeny class 4.4.2048.1-1.1-a. These agreed with Farmer-Koutsoliotas-Lemurell's calculations [36].

We furthermore obtained that no L-function exists with conductor 2^9, and that there is only one L-function of conductor 2^{10}, corresponding to the split 32a $\times$ 32a isogeny class.

Whilst the above algorithm is in principle effective for any conductor N, in practice we were unfortunately unable to extend our calculations beyond $N = 2^{10}$. As an example, for $N = 2^{12}$ and $\epsilon = +1$, after searching through the first four primes, no pruning occurs and all branches are still possible, which makes the search unbearably slow. In order to overcome this hurdle, we will need to investigate a better way of choosing weight functions $g(s)$, a matter of which could be the focus of future work.

Table 5: List of all L-functions computed so far corresponding to genus 2 curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ is good outside 2. The set of L-functions for $N \leq 2^{10}$ is conjecturally complete (assuming L-modularity). For $N \geq 2^{11}$, the values quoted below are only lower bounds.

Conductor	**Rank**			**Split**	**Simple**	**Totals**
N	**0**	**1**	**2**	(over $\overline{\mathbb{Q}}$)		
$\leq 2^7$	0	0	0	0	0	**0**
2^8	1	0	0	1	0	**1**
2^9	0	0	0	0	0	**0**
2^{10}	1	0	0	1	0	**1**
2^{11}	1	0	0	1	0	**1**
2^{12}	6	1	0	7	0	**7**
2^{13}	7	3	0	10	0	**10**
2^{14}	13	5	1	19	0	**19**
2^{15}	10	10	2	22	0	**22**
2^{16}	10	6	2	18	0	**18**
2^{17}	11	12	1	16	8	**24**
2^{18}	6	7	6	15	4	**19**
2^{19}	8	8	4	0	20	**20**
2^{20}	11	14	7	20	12	**32**
Total:	**85**	**66**	**23**	**130**	**44**	**174**

In total, we obtained 174 isogeny classes which have good reduction outside 2, including 9

classes not obtained from Smart's original list (8 of which were split over $\mathbb{Q}$, and one which was split over $\mathbb{Q}(\sqrt{2})$).

Remark: By a result of [12], one can check that the highest exponent of 2 in the conductor of a genus 2 curve over $\mathbb{Q}$ is 20.

We also note that the Euler factor at $p = 2$, for every L-function found was $L_2(T) = 1$, with the only exception being the unique conductor 2^8 L-function, where the Euler factor was $L_2(T) = 2T^2 + 2T + 1$.

It's worth mentioning that, on the rare occasion, we can read off primes p from the L-function which are good for $\mathrm{Jac}(C)$, but must be bad for C. For example, some of the L-functions yield an Euler factor at 3 as $L_3(T) = 1 - 6T^2 + 9T^4$. Now assuming C has good reduction at 3, then using (10), we obtain that $\#\widetilde{C}_{3^2} = -2$, which is clearly impossible.

Solving the S-unit equations

We now focus on solving the required S-unit equations, following the procedure laid out by Smart [88]. Whilst we cannot use this to provably provide a complete list of genus 2 curves with $\mathrm{Jac}(C)$ good outside 2, we can at least give a partial list with completeness guaranteed for C having good reduction outside some finite set of primes S.

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 $\mathbb{Q}(\alpha)$, given by

$$\begin{aligned}
&\mathbb{Q}(\alpha), \text{ where } \alpha^8 + 1 = 0, && \text{(LMFDB label: 8.0.16777216.1)}\\
&\mathbb{Q}(\alpha), \text{ where } \alpha^8 - 4\alpha^6 + 8\alpha^4 - 4\alpha^2 + 1 = 0, && \text{(LMFDB label: 8.0.16777216.2)}\\
&\mathbb{Q}(\alpha), \text{ where } \alpha^8 + 6\alpha^4 + 1 = 0. && \text{(LMFDB label: 8.0.4194304.1)}
\end{aligned}$$

We therefore 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 [65] very kindly provided these solutions, described below:

- We first consider the octic field $\mathbb{Q}(\alpha)$ where $\alpha^8 + 1 = 0$. Solving the S-unit equation

  $$\tau_1 + \tau_2 = 1$$

  for τ_1, τ_2 S-units where S denotes all primes above $\{2, 3\}$, $\{2, 5\}$ and $\{2, 7\}$, yields a total of 2019, 1155, and 7881 solutions respectively.

- For the octic field $\mathbb{Q}(\alpha)$ where $\alpha^8 - 4\alpha^6 + 8\alpha^4 - 4\alpha^2 + 1 = 0$, the number of solutions to the S-unit equation $\tau_1 + \tau_2 = 1$ where S denotes all primes above $\{2, 3\}$, $\{2, 5\}$ and $\{2, 7\}$, yields a total of 59595, 807, 7197 respectively.

- Finally, for the octic field $\mathbb{Q}(\alpha)$ where $\alpha^8 + 6\alpha^4 + 1 = 0$, the number of solutions obtained was 3723, 33387, and 18501 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 [88].

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 the S-unit solutions is given in Table 6.

Table 6: Number of S-unit solutions to $\tau_1 + \tau_2 = 1$ where $\tau_i \in \mathcal{O}_S^\times$ over the field $\mathbb{Q}(\alpha)$. All computations were run by Matschke [65]. 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:**						
$\mathbb{Q}(\alpha)$	$\{2\}$	$\{2,3\}$	$\{2,5\}$	$\{2,7\}$	$\{2,3,5\}$	$\{2,3,7\}$	$\{2,5,7\}$
α^8+1	795 (81s)	2019 (453s)	1155 (355s)	7881 (8822s)	4653 (4925s)	21 927 (769 586s)	13 401 (388 501s)
$\alpha^8-4\alpha^6+8\alpha^4-4\alpha^2+1$	459 (62s)	59 595 (54 061s)	807 (304s)	7197 (8528s)	?	?	11 877 (380 463s)
$\alpha^8+6\alpha^4+1$	1335 (88s)	3723 (766s)	33 387 (37 920s)	18 501 (18 853s)	?	52 563 (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 $|S| > 3$, it is thus essential that we make use of Galois symmetries, to constrain the possible solutions.

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 τ_1, τ_2 arise from roots from polynomials, which are in one of the fields listed in Theorem 26.

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 $f(x) = c(x-a_1)(x-a_2)\cdots(x-a_6)$. As shown on page 5, we can write $f(x)$ in Rosenhain normal form as $x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ where

$$\lambda_1 = \frac{(a_3-a_2)(a_4-a_1)}{(a_2-a_1)(a_3-a_4)}, \qquad \lambda_2 = \frac{(a_3-a_2)(a_5-a_1)}{(a_2-a_1)(a_3-a_5)}, \qquad \lambda_3 = \frac{(a_3-a_2)(a_6-a_1)}{(a_2-a_1)(a_3-a_6)}$$

Now, assume that four of the roots a_1, a_2, a_3, a_4 of $f(x)$ arise from one of the fields L_i given in Theorem 26. Let $\sigma \in \mathrm{Gal}(L_i/\mathbb{Q})$ be an automorphism of order 4 which permutes the roots in the order $a_1 \mapsto a_3 \mapsto a_2 \mapsto a_4 \mapsto a_1$. Then we have

$$\sigma(\lambda_1) = \frac{(\sigma(a_3)-\sigma(a_2))(\sigma(a_4)-\sigma(a_1))}{(\sigma(a_2)-\sigma(a_1))(\sigma(a_3)-\sigma(a_4))} = \frac{(a_2-a_4)(a_3-a_1)}{(a_2-a_1)(a_3-a_4)} = 1-\lambda_1$$

This therefore yields the constraint that $\sigma(\lambda_1) = 1-\lambda_1$, which heavily constrains the number of S-unit solutions. In general, if the roots a_1, a_2, a_3, a_4 arise from an irreducible quartic, then one can verify that $\sigma(\lambda_1)$ will be one of

$$\lambda_1, \quad 1-\lambda_1, \quad \frac{1}{\lambda_1}, \quad \frac{1}{1-\lambda_1}, \quad \frac{\lambda_1-1}{\lambda_1}, \quad \frac{\lambda_1}{\lambda_1-1}$$

Therefore, in order to make effective use of these Galois constraints, we first need to consider all possible Galois groups arising from the possible field systems.

In our case, we note that the Galois group $\mathrm{Gal}(M/\mathbb{Q})$ 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 quartic fields are $\mathrm{Gal}(L_1/\mathbb{Q}) = C_2^2$, $\mathrm{Gal}(L_i/\mathbb{Q}) = C_4$ for $i = 4, 5$, and $\mathrm{Gal}(L_i/\mathbb{Q}) = D_4$ for $i = 2, 3, 6, 7$ (where C_n denotes the cyclic group of order n, and D_n denotes the dihedral group of order $2n$).

Therefore, in all but one of the Galois groups, we have the existence of a unique order 2 automorphism $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$, with the exception of $\sigma \in \mathrm{Gal}(L_1/\mathbb{Q})$ which contains three 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 σ.

Table 7: 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 $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$, and where S denotes all primes in M above the first N rational primes. All computations were run by Matschke [65]. Note that σ is uniquely determined in almost all cases, except for $M = L_1$ for which the number of solutions are given for the automorphisms $\sigma_1 : \sqrt[4]{-1} \mapsto -\sqrt[4]{-1}$, $\sigma_2 : \sqrt[4]{-1} \mapsto -\sqrt[4]{-1}^3$, and $\sigma_3 : \sqrt[4]{-1} \mapsto \sqrt[4]{-1}^3$ 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
	75	225	351	825	1479	.	.	.
L_1	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	.	.	.

With the above mentioned Galois constraints in place, all of the computations done in Table 7 took merely a few minutes at most, hence there is certainly scope to extend these computations further.

Finally, to compute a full list of genus 2 curves C corresponding to the above S-unit solutions, we follow Section 5 of Smart [88, p. 279] which describes an explicit algorithm to calculate all possible curves up to $\mathbb{Q}$-isomorphism, given the values of λ_1, λ_2 and λ_3.

Our current implementation of this final step is done rather naively, and optimisations can certainly be made to improve this.

With all these computations done, we finally present a list of curves which we've obtained so far:

List of curves

We note that a full list of curves C with good reduction outside 2 has already been tabulated in [88, pp. 296-305], so we do not include these curves as this would be superfluous.

In total, there are 12 $\overline{\mathbb{Q}}$-isomorphism classes containing curves where $\mathrm{Jac}(C)$ is good outside 2, but C isn't. For each $\overline{\mathbb{Q}}$-isomorphism class, we present a table consisting of all curves separated by isogeny class.

It's worth mentioning that most of the curves presented in our list have split Jacobian. If this is the case, we therefore give its isogeny class by the split elliptic curve isogeny class labels. Specifically, if $\mathrm{Jac}(C)$ splits over $\mathbb{Q}$, we give its isogeny classes over $\mathbb{Q}$, otherwise we give its labels over one of the quadratic or quartic fields given in Theorem 26.

As there own only 10 isogeny classes of elliptic curves $E/\mathbb{Q}$ with good reduction outside 2, we tabulate a list of these classes. We also note that the Cremona labels agree with the LMFDB labels in these cases.

Table 8: List of isogeny classes of elliptic curves $E/\mathbb{Q}$ with good reduction outside 2.

Cremona label	**Rank**	**CM**	**Sato-Tate group**
32a	0	yes (in $\mathbb{Q}(\sqrt{-1})$)	$N(\mathrm{U}(1))$
64a	0	yes (in $\mathbb{Q}(\sqrt{-1})$)	$N(\mathrm{U}(1))$
128a	1	.	$\mathrm{SU}(2)$
128b	0	.	$\mathrm{SU}(2)$
128c	0	.	$\mathrm{SU}(2)$
128d	0	.	$\mathrm{SU}(2)$
256a	1	yes (in $\mathbb{Q}(\sqrt{-2})$)	$N(\mathrm{U}(1))$
256b	1	yes (in $\mathbb{Q}(\sqrt{-1})$)	$N(\mathrm{U}(1))$
256c	0	yes (in $\mathbb{Q}(\sqrt{-1})$)	$N(\mathrm{U}(1))$
256d	0	yes (in $\mathbb{Q}(\sqrt{-2})$)	$N(\mathrm{U}(1))$

Interestingly, we observed that any two curves in the same isogeny class appearing in our list also had the same G2-invariants. We do recall that, in general, an isogeny class can consist of curves with several different G2-invariants (for example the split isogeny class 32a $\times$ 128c consists of both the curve 4096.c.65536.1 (with bad reduction at $\{2\}$) as well as two of the curves given in Table 17 (with bad reduction at $\{2, 5\}$)).

For each curve C in our list, we computed the following various arithmetic invariants:

- For each curve $C/\mathbb{Q}$, we calculated a minimal Weierstrass model for C using the Magma function `ReducedMinimalWeierstrassModel`. This returns a minimal integral model of C which is reduced with respect to the action of $\mathrm{SL}_2(\mathbb{Z})$ using Stoll's algorithm. In most cases, this model was already in simplified form $y^2 = f(x)$, in which case we simply tabulate the polynomial $f(x)$. Otherwise, we tabulate a simplified model for C, with a globally

minimal model given as an additional footnote.

- The conductor N for each curve C was computed using the Dokchitser-Doris [32] Magma package. We present the conductor in the format $2^{n_t+n_w}$ where n_t and n_w denote the tame and wild part of the conductor at 2 respectively. Indeed, one notes that $n_t = 4$ for all curves in our tables.

  We furthermore verified for all curves found, that the functional equation for $L(C/\mathbb{Q}, s)$ as given in (9), holds for the value of N obtained. This was verified using the Sage implementation of Dokchitser's L-function calculator [29].

- For each curve C, the Mordell-Weil rank of $\mathrm{Jac}(C)$ and torsion subgroup over $\mathbb{Q}$ are also given. These were again computed using the built-in Magma functions. There were a few cases where the rank could not be unconditionally verified, and we therefore simply give lower and upper bounds in these cases.

- The Sato-Tate identity component ST^0 for the Jacobian $J = \mathrm{Jac}(C)$ was calculated by computing the geometric endomorphism ring $\mathrm{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$. This was done using a Magma package developed by Costa-Mascot-Sijsling-Voight [24].

- Each of the 115 curves were grouped into their isogeny class by computing the number of points in the reduction $\#\widetilde{C}_p$ of C, for all primes $p < 1000$ of good reduction. In many cases, we were able to use Theorem 7 to unconditionally classify curves into their split isogeny class.

  We do mention that, in principle, one could apply the Faltings-Serre method [63] (or alternatively explicitly construct isogenies, as done in [95]) to prove that all of our isogeny classes are correct, however these computations were not done for this project.

- For each curve C, we also calculated all rational points lying on C with height less than 10^7 using Magma's default `RationalPoints` function (however, these values are not included in the tables below). We were able to prove that all the rational points found were a complete list for all the rank 0 curves and some of the rank 1 curves using Chabauty's method.

  The point with largest height found was $P = (-\frac{4}{17}, \frac{\pm 13392}{17})$ lying on the rank 2 curve[9] $C : y^2 = x^6 + 4x^5 - 40x^4 + 32x^3 + 8x^2 - 32x$. It's worth remarking that all rational points found, except for this one, had height less than 500, and so it appears rather likely that our list of rational points is complete.

Without further ado, we present our (partial) list of 115 genus 2 curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ has good reduction outside 2, but C has bad reduction at some odd prime.

[9] This curve also had the most number of rational points (10 points) out of all curves in our list.

Table 9: A list of all 12 G2-invariants found for curves C where $\mathrm{Jac}(C)$, but not C, is good away from 2.

Bad Primes	**G2 Invariants** (g_1, g_2, g_3)	**Num Isog Classes**	**Num Curves**
$\{2,3\}$	$\left(\frac{2^9\cdot 23^5}{3^7}, \frac{2^4\cdot 5\cdot 11\cdot 23^3\cdot 37}{3^8}, \frac{-2^8\cdot 23^2\cdot 89}{3^{10}}\right)$	5	19
.	$\left(\frac{-2^{18}\cdot 5^5}{3^7}, \frac{2^{10}\cdot 5^3\cdot 1549}{3^8}, \frac{-2^{11}\cdot 5^2\cdot 3673}{3^{10}}\right)$	4	16
.	$\left(\frac{2^{10}\cdot 13^5}{3^7}, \frac{2^5\cdot 13^3\cdot 883}{3^8}, \frac{-2^8\cdot 13^2\cdot 281}{3^{10}}\right)$	4	4
.	$\left(-\frac{2^4\cdot 23^5}{3^7}, \frac{-2^6\cdot 23^3\cdot 239}{3^8}, \frac{-2^2\cdot 5\cdot 23^2\cdot 29\cdot 1451}{3^{10}}\right)$	2	4
.	$\left(-\frac{2^{19}}{3^7}, \frac{2^{11}\cdot 13}{3^8}, \frac{-2^{11}\cdot 11\cdot 107}{3^{10}}\right)$	8	16
.	$\left(-\frac{5^5\cdot 13^5}{2^2\cdot 3^7}, \frac{-5^3\cdot 13^4\cdot 829}{2^5\cdot 3^8}, \frac{-5^3\cdot 13^2\cdot 29\cdot 163\cdot 179}{2^6\cdot 3^{10}}\right)$	2	4
.	$\left(-\frac{2^4\cdot 41^5}{3^7}, \frac{-2\cdot 41^3\cdot 1789}{3^8}, \frac{-5\cdot 17\cdot 41^2\cdot 281}{3^{10}}\right)$	4	4
$\{2,5\}$	$\left(\frac{-2^9\cdot 3^5\cdot 67^5}{5^{12}}, \frac{-2^5\cdot 3^3\cdot 23\cdot 67^3\cdot 383}{5^{12}}, \frac{-2^7\cdot 3^2\cdot 13^2\cdot 67^2\cdot 113}{5^{12}}\right)$	8	16
.	$\left(\frac{2^5\cdot 13^5\cdot 137^5}{5^{12}}, \frac{2^2\cdot 13^4\cdot 137^3\cdot 193\cdot 443}{5^{12}}, \frac{2\cdot 7\cdot 13^2\cdot 89\cdot 137^2\cdot 390821}{5^{12}}\right)$	4	4
.	$\left(\frac{-2^9\cdot 29^5}{5^{12}}, \frac{2^4\cdot 29^3\cdot 61\cdot 67}{5^{12}}, \frac{-2^8\cdot 29^2\cdot 27529}{5^{12}}\right)$	3	6
$\{2,7\}$	$\left(\frac{2^{13}\cdot 3^{10}\cdot 19^5}{7^{12}}, \frac{2^7\cdot 3^6\cdot 19^3\cdot 59\cdot 2339}{7^{12}}, \frac{-2^9\cdot 3^4\cdot 17\cdot 19^2\cdot 6337}{7^{12}}\right)$	4	16
.	$\left(\frac{-2^8\cdot 151^5}{7^{12}}, \frac{2^3\cdot 5\cdot 41\cdot 43\cdot 151^3}{7^{12}}, \frac{-2^8\cdot 71\cdot 151^2\cdot 2663}{7^{12}}\right)$	5	6
Total:	**12**	**53**	**115**

For each of the 12 G2-invariants, we tabulate a full list of such curves C. In each table, the curves are ordered first by conductor, then grouped by isogeny class which are ordered lexicography by isogeny label, if available. Within each isogeny class, the curves are not given in any particular order. For each curve C, a simplified minimal model $y^2 = f(x)$ is given wherever possible. If not, a simplified model is tabulated, with a global minimal model given thereafter as a remark.

Table 10: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(\frac{2^9 \cdot 23^5}{3^7},\ \frac{2^4 \cdot 5 \cdot 11 \cdot 23^3 \cdot 37}{3^8},\ \frac{-2^8 \cdot 23^2 \cdot 89}{3^{10}}\right)$. A total of 19 curves separated into 5 isogeny classes are given.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	$\mathbf{GL_2}$**−type**	$\mathbf{ST^0}$
32a × 32a	$(2x+1)(x^2+2)(x^2+2x+3)$	$[\mathbb{Q}, \mathbb{Q}, K_2, K_2]$	$2^{16}3^{12}$	2^{4+6}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$		U(1)
	$2x(x^4 - 14x^2 + 81)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{36}3^{12}$	2^{4+6}	0	$\mathbb{Z}/4\mathbb{Z}$		U(1)
	$3(x^2-2)(x^2+1)(2x^2-1)$	$[K_1, K_3, K_3]$	$2^{16}3^{22}$	2^{4+6}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$		U(1)
	$-3(x^2-2)(x^2+1)(2x^2-1)$	$[K_1, K_3, K_3]$	$2^{16}3^{22}$	2^{4+6}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$		U(1)
32a × 64a	$3(x^2-2)(x^4+68x^2+4)$	$[K_3, L_1]$	$2^{51}3^{22}$	2^{4+7}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
	$-3(x^2-2)(x^4+68x^2+4)$	$[K_3, L_1]$	$2^{51}3^{22}$	2^{4+7}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
	$3(x^2-2)(x^2+1)(x^2+4)$	$[K_1, K_1, K_3]$	$2^{21}3^{22}$	2^{4+7}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$-3(x^2-2)(x^2+1)(x^2+4)$	$[K_1, K_1, K_3]$	$2^{21}3^{22}$	2^{4+7}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	✓	U(1)
	$-(x^2-2)(x^2+2)(7x^2+16x-14)$	$[K_2, K_3, K_3]$	$2^{51}3^{12}$	2^{4+7}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$(x^2-2)(x^2+2)(7x^2+16x-14)$	$[K_2, K_3, K_3]$	$2^{51}3^{12}$	2^{4+7}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	✓	U(1)
	$x(2x+1)(x-4)(x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_2]$	$2^{21}3^{12}$	2^{4+7}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$-x(2x+1)(x-4)(x^2+2)$	$[\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_2]$	$2^{21}3^{12}$	2^{4+7}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	✓	U(1)
64a × 64a	$2(2x+1)(x^2+2)(x^2+2x+3)$	$[\mathbb{Q}, \mathbb{Q}, K_2, K_2]$	$2^{26}3^{12}$	2^{4+8}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$		U(1)
	$x(x^4 - 14x^2 + 81)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{26}3^{12}$	2^{4+8}	0	$\mathbb{Z}/4\mathbb{Z}$		U(1)
	$6(x^2-2)(x^2+1)(2x^2-1)$	$[K_1, K_3, K_3]$	$2^{26}3^{22}$	2^{4+8}	0	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$		U(1)
	$-6(x^2-2)(x^2+1)(2x^2-1)$	$[K_1, K_3, K_3]$	$2^{26}3^{22}$	2^{4+8}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$		U(1)
(2.2.8.1-256.1-a)^2	$-3(x^2-4x+5)(x^2+2x-1)(5x^2+4x+1)$	$[K_1, K_1, K_3]$	$2^{41}3^{22}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	✓	U(1)
256b × 256c	$x(x^2-8x+18)(x^2+8x+18)$	$[\mathbb{Q}, \mathbb{Q}, K_2, K_2]$	$2^{36}3^{12}$	2^{4+12}	1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$x(x^4 + 28x^2 + 324)$	$[\mathbb{Q}, \mathbb{Q}, L_1]$	$2^{36}3^{12}$	2^{4+12}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)

Table 11: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(\frac{-2^{18}\cdot 5^5}{3^7}, \frac{2^{10}\cdot 5^3\cdot 1549}{3^8}, \frac{-2^{11}\cdot 5^2\cdot 3673}{3^{10}}\right)$. A total of 16 curves seperated into 4 isogeny classes are given

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	**GL$_2$−type**	**ST^0**
32a × 256b	$(x^2+2)(x^4+4x^3+2x^2+4x+7)$	$[K_2, L_2]$	$2^{22}3^{12}$	2^{4+9}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
	$-(x^2+2)(x^4+4x^3+2x^2+4x+7)$	$[K_2, L_2]$	$2^{22}3^{12}$	2^{4+9}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$3(x^2-2)(2x^4-8x^2-1)$	$[K_3, L_2]$	$2^{22}3^{22}$	2^{4+9}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
	$-3(x^2-2)(2x^4-8x^2-1)$	$[K_3, L_2]$	$2^{22}3^{22}$	2^{4+9}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
32a × 256c	$3(x^2+1)(x^4-16x^2-8)$	$[K_1, L_2]$	$2^{27}3^{22}$	2^{4+9}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$-3(x^2+1)(x^4-16x^2-8)$	$[K_1, L_2]$	$2^{27}3^{22}$	2^{4+9}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
	$-(2x+1)(x^4+8x^3-8x^2+8)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{27}3^{12}$	2^{4+9}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$(2x+1)(x^4+8x^3-8x^2+8)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{27}3^{12}$	2^{4+9}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
64a × 256b	$-3(x^2+4)(x^4+8x^2-2)$	$[K_1, L_2]$	$2^{27}3^{22}$	2^{4+10}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$3(x^2+4)(x^4+8x^2-2)$	$[K_1, L_2]$	$2^{27}3^{22}$	2^{4+10}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
	$-x(x-4)(x^4-4x^2-8x+2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{27}3^{12}$	2^{4+10}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$x(x-4)(x^4-4x^2-8x+2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{27}3^{12}$	2^{4+10}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
64a × 256c	$2(x^2+2)(x^4+4x^3+2x^2+4x+7)$	$[K_2, L_2]$	$2^{32}3^{12}$	2^{4+10}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
	$-(3x^2+4x+4)(x^4-8x^3-8x^2+8)$[a]	$[K_2, L_2]$	$2^{22}3^{12}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$6(x^2-2)(2x^4-8x^2-1)$	$[K_3, L_2]$	$2^{32}3^{12}$	2^{4+10}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
.	$-3(x^2-8)(x^4-16x^2-8)$[b]	$[K_3, L_2]$	$2^{22}3^{12}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)

[a] A global minimal model for this curve is $y^2+x^3y = -x^6+5x^5+13x^4+16x^3+2x^2-8x-8$.
[b] A global minimal model for this curve is $y^2+x^3y = -x^6+18x^4-90x^2-48$.

Table 12: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(\frac{2^{10}\cdot 13^5}{3^7},\ \frac{2^5\cdot 13^3\cdot 883}{3^8},\ \frac{-2^8\cdot 13^2\cdot 281}{3^{10}}\right)$. A total of 4 curves separated into 4 isogeny classes are given.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	**GL_2−type**	**ST^0**
2.2.8.1-512.1-e × 2.2.8.1-512.1-g	$(2x^2+1)(4x^4-4x^2-32x-31)$	$[K_2, L_2]$	$2^{50}3^{12}$	2^{4+11}	0..1	$\mathbb{Z}/2\mathbb{Z}$	no	$\mathrm{SU}(2)\times\mathrm{SU}(2)$
2.2.8.1-512.1-a × 2.2.8.1-512.1-c	$-(2x^2+1)(4x^4-4x^2-32x-31)$	$[K_2, L_2]$	$2^{50}3^{12}$	2^{4+11}	0	$\mathbb{Z}/2\mathbb{Z}$	no	$\mathrm{SU}(2)\times\mathrm{SU}(2)$
2.2.8.1-1024.1-a × 2.2.8.1-1024.1-o	$(x-1)(4x^4+16x^3+20x^2+40x+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{35}3^{12}$	2^{4+12}	0	$\mathbb{Z}/2\mathbb{Z}$	no	$\mathrm{SU}(2)\times\mathrm{SU}(2)$
2.2.8.1-1024.1-e × 2.2.8.1-1024.1-n	$-(x-1)(4x^4+16x^3+20x^2+40x+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{35}3^{12}$	2^{4+12}	1	$\mathbb{Z}/2\mathbb{Z}$	no	$\mathrm{SU}(2)\times\mathrm{SU}(2)$

Table 13: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(-\frac{2^4\cdot 23^5}{3^7},\ \frac{-2^6\cdot 23^3\cdot 239}{3^8},\ \frac{-2^2\cdot 5\cdot 23^2\cdot 29\cdot 1451}{3^{10}}\right)$. A total of 4 curves separated into 2 isogeny classes are given.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	**GL_2−type**	**ST^0**
128c × 128d	$(x-1)(x^4+40x^3+20x^2+16x+4)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{31}3^{12}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{SU}(2)$
	$-2(x-1)(x^4+40x^3+20x^2+16x+4)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{41}3^{12}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{SU}(2)$
128a × 128b	$-(x-1)(x^4+40x^3+20x^2+16x+4)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{31}3^{12}$	2^{4+10}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{SU}(2)$
	$2(x-1)(x^4+40x^3+20x^2+16x+4)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{41}3^{12}$	2^{4+10}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{SU}(2)$

Table 14: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(-\frac{2^{19}}{3^7},\ \frac{2^{11}\cdot 13}{3^8},\ \frac{-2^{11}\cdot 11\cdot 107}{3^{10}}\right)$. A total of 16 curves separated into 8 isogeny classes are given

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	**GL$_2$−type**	**ST^0**
128a × 256a	$(x^2+2)(x^4-4x^2+8x+2)$	$[K_2, L_2]$	$2^{26}3^{12}$	2^{4+11}	2	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
.	$x(x-4)(x^4+8x^3-8x^2+8)$[a]	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{21}3^{12}$	2^{4+11}	2	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
128a × 256d	$-3(x^2-2)(x^4+8x^2-2)$	$[K_3, L_2]$	$2^{26}3^{22}$	2^{4+11}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$-3(x^2+4)(x^4-16x^2-8)$[b]	$[K_1, L_2]$	$2^{21}3^{22}$	2^{4+11}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
128b × 256a	$-2(x^2+2)(x^4-4x^2+8x+2)$	$[K_2, L_2]$	$2^{36}3^{12}$	2^{4+11}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
.	$-(2x+1)(x^4-4x^2-8x+2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{21}3^{12}$	2^{4+11}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
128b × 256d	$6(x^2-2)(x^4+8x^2-2)$	$[K_3, L_2]$	$2^{36}3^{22}$	2^{4+11}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$-3(x^2+1)(x^4+8x^2-2)$	$[K_1, L_2]$	$2^{21}3^{22}$	2^{4+11}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
128c × 256a	$3(x^2-2)(x^4+8x^2-2)$	$[K_3, L_2]$	$2^{26}3^{22}$	2^{4+11}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
.	$-6(x^2+1)(x^4+8x^2-2)$	$[K_1, L_2]$	$2^{31}3^{22}$	2^{4+11}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
128c × 256d	$-(x^2+2)(x^4-4x^2+8x+2)$	$[K_2, L_2]$	$2^{26}3^{12}$	2^{4+11}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
.	$-2(2x+1)(x^4-4x^2-8x+2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{31}3^{12}$	2^{4+11}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
128d × 256a	$3(x^2+1)(x^4+8x^2-2)$	$[K_1, L_2]$	$2^{21}3^{22}$	2^{4+11}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$-6(x^2-2)(x^4+8x^2-2)$	$[K_3, L_2]$	$2^{36}3^{22}$	2^{4+11}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
128d × 256d	$2(x^2+2)(x^4-4x^2+8x+2)$	$[K_2, L_2]$	$2^{36}3^{12}$	2^{4+11}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
.	$(2x+1)(x^4-4x^2-8x+2)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{21}3^{12}$	2^{4+11}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$

[a] A global minimal model for this curve is $y^2 + x^3y = x^5 - 10x^4 + 8x^3 + 2x^2 - 8x$.
[b] A global minimal model for this curve is $y^2 + x^3y = -x^6 + 9x^4 + 54x^2 + 24$.

Table 15: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(\frac{-5^5\cdot 13^5}{2^2\cdot 3^7},\ \frac{-5^3\cdot 13^4\cdot 829}{2^5\cdot 3^8},\ \frac{-5^3\cdot 13^2\cdot 29\cdot 163\cdot 179}{2^6\cdot 3^{10}}\right)$. A total of 4 curves separated into 2 isogeny classes are given. Both of the isogeny classes split over the number field L_2.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Torsion subgroup**	**GL_2−type**	**ST^0**
8192a	$3(x^2-2x-1)(x^2-2x+2)(x^2+4x+2)$	$[K_1, K_3, K_3]$	$2^{22}3^{22}$	2^{4+9}	0	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	no	SU(2)
	$-3(x^2-2x-1)(x^2-2x+2)(x^2+4x+2)$	$[K_1, K_3, K_3]$	$2^{22}3^{22}$	2^{4+9}	0	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$	no	SU(2)
16384a	$6(x^2-2x-1)(x^2-2x+2)(x^2+4x+2)$	$[K_1, K_3, K_3]$	$2^{32}3^{22}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	no	SU(2)
	$-6(x^2-2x-1)(x^2-2x+2)(x^2+4x+2)$	$[K_1, K_3, K_3]$	$2^{32}3^{22}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	no	SU(2)

Table 16: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(-\frac{2^4\cdot 41^5}{3^7},\ \frac{-2\cdot 41^3\cdot 1789}{3^8},\ \frac{-5\cdot 17\cdot 41^2\cdot 281}{3^{10}}\right)$. A total of 4 curves separated into 4 isogeny classes are given. None of the isogeny classes below have been allocated an LMFDB label currently.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Torsion subgroup**	**GL_2−type**	**ST^0**
*	$(x+2)(2x^4-8x^3-4x^2+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{21}3^{12}$	2^{4+16}	0	$\mathbb{Z}/2\mathbb{Z}$	no	USp(4)
*	$-(x+2)(2x^4-8x^3-4x^2+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{21}3^{12}$	2^{4+16}	1	$\mathbb{Z}/2\mathbb{Z}$	no	USp(4)
*	$-2(x+2)(2x^4-8x^3-4x^2+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{31}3^{12}$	2^{4+16}	1	$\mathbb{Z}/2\mathbb{Z}$	no	USp(4)
*	$2(x+2)(2x^4-8x^3-4x^2+1)$	$[\mathbb{Q}, \mathbb{Q}, L_2]$	$2^{31}3^{12}$	2^{4+16}	2	$\mathbb{Z}/2\mathbb{Z}$	no	USp(4)

Table 17: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(\frac{-2^9\cdot 3^5\cdot 67^5}{5^{12}}, \frac{-2^5\cdot 3^3\cdot 23\cdot 67^3\cdot 383}{5^{12}}, \frac{-2^7\cdot 3^2\cdot 13^2\cdot 67^2\cdot 113}{5^{12}}\right)$. A total of 16 curves separated into 8 isogeny classes are given.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	**GL$_2$−type**	**ST^0**
32a × 128a	$(2x-1)(x^4-4x^3-14x^2+4x+41)$	$[\mathbb{Q},\mathbb{Q},L_6]$	$2^{26}5^{12}$	2^{4+8}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$(x^2+4)(x^4+8x^3+4x^2-16x+28)$[a]	$[K_1,L_6]$	$2^{16}5^{12}$	2^{4+8}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
32a × 128b	$5(x^2-2)(x^4-14x^2-1)$	$[K_3,L_6]$	$2^{21}5^{22}$	2^{4+8}	0	$\mathbb{Z}/8\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$-5(x^2+2)(x^4+14x^2-1)$	$[K_2,L_6]$	$2^{21}5^{22}$	2^{4+8}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
32a × 128c	$-(4x+1)(4x^4-20x^2-16x+7)$[b]	$[\mathbb{Q},\mathbb{Q},L_6]$	$2^{16}5^{12}$	2^{4+8}	0	$\mathbb{Z}/8\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$-(x^2+1)(4x^4+16x^3+4x^2-8x+7)$	$[K_1,L_6]$	$2^{26}5^{12}$	2^{4+8}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
32a × 128d	$-5(x^2-2)(x^4-14x^2-1)$	$[K_3,L_6]$	$2^{21}5^{22}$	2^{4+8}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$5(x^2+2)(x^4+14x^2-1)$	$[K_2,L_6]$	$2^{21}5^{22}$	2^{4+8}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
64a × 128a	$-5(x^2-6x+1)(7x^4-4x^3-14x^2-4x+7)$[c]	$[K_3,L_6]$	$2^{21}5^{22}$	2^{4+9}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$5(3x^2+2x+3)(7x^4-4x^3-14x^2-4x+7)$[d]	$[K_2,L_6]$	$2^{21}5^{22}$	2^{4+9}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
64a × 128b	$-2(2x-1)(x^4-4x^3-14x^2+4x+41)$	$[\mathbb{Q},\mathbb{Q},L_6]$	$2^{36}5^{12}$	2^{4+9}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$-2(x^2+1)(4x^4+16x^3+4x^2-8x+7)$	$[K_1,L_6]$	$2^{36}5^{12}$	2^{4+9}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
64a × 128c	$10(x^2-2)(x^4-14x^2-1)$	$[K_3,L_6]$	$2^{31}5^{22}$	2^{4+9}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$-10(x^2+2)(x^4+14x^2-1)$	$[K_2,L_6]$	$2^{31}5^{22}$	2^{4+9}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
64a × 128d	$2(2x-1)(x^4-4x^3-14x^2+4x+41)$	$[\mathbb{Q},\mathbb{Q},L_6]$	$2^{36}5^{12}$	2^{4+9}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$
	$2(x^2+1)(4x^4+16x^3+4x^2-8x+7)$	$[K_1,L_6]$	$2^{36}5^{12}$	2^{4+9}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{SU}(2)$

[a] A global minimal model for this curve is $y^2+x^3y = 2x^5+2x^4+4x^3+11x^2-16x+28$.
[b] A global minimal model for this curve is $y^2+y = -4x^5-x^4+20x^3+21x^2-3x-2$.

[c] A global minimal model for this curve is $y^2 + (x^3 + x^2 + x + 1)y = -9x^6 + 57x^5 - 22x^4 - 96x^3 - 22x^2 + 57x - 9$.
[d] A global minimal model for this curve is $y^2 + (x^3 + x^2 + x + 1)y = 26x^6 + 2x^5 - 37x^4 - 66x^3 - 37x^2 + 2x + 26$.

Table 18: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(\frac{2^5 \cdot 13^5 \cdot 137^5}{5^{12}}, \frac{2^2 \cdot 13^4 \cdot 137^3 \cdot 193 \cdot 443}{5^{12}}, \frac{2 \cdot 7 \cdot 13^2 \cdot 89 \cdot 137^2 \cdot 390821}{5^{12}}\right)$. A total of 4 curves separated into 4 isogeny classes are given. None of the isogeny classes below have been allocated an LMFDB label currently.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	**GL$_2$−type**	**ST^0**
*	$-(x^2 - 4x + 5)(7x^4 + 12x^3 - 26x^2 - 60x - 25)$	$[K_1, L_6]$	$2^{40}5^{12}$	2^{4+15}	0	$\mathbb{Z}/2\mathbb{Z}$	no	USp(4)
*	$(x^2 - 4x + 5)(7x^4 + 12x^3 - 26x^2 - 60x - 25)$	$[K_1, L_6]$	$2^{40}5^{12}$	2^{4+15}	0..1	$\mathbb{Z}/2\mathbb{Z}$	no	USp(4)
*	$(x^2 + 2x + 2)(23x^4 - 24x^3 - 52x^2 + 80x - 28)$	$[K_1, L_6]$	$2^{40}5^{12}$	2^{4+15}	0	$\mathbb{Z}/2\mathbb{Z}$	no	USp(4)
*	$-(x^2 + 2x + 2)(23x^4 - 24x^3 - 52x^2 + 80x - 28)$	$[K_1, L_6]$	$2^{40}5^{12}$	2^{4+15}	0..1	$\mathbb{Z}/2\mathbb{Z}$	no	USp(4)

Table 19: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(\frac{-2^9 \cdot 29^5}{5^{12}}, \frac{2^4 \cdot 29^3 \cdot 61 \cdot 67}{5^{12}}, \frac{-2^8 \cdot 29^2 \cdot 27529}{5^{12}}\right)$. A total of 6 curves separated into 3 isogeny classes are given.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	**GL$_2$−type**	**ST^0**
(2.2.8.1-256.1-c)^2	$5(x^2 - 4x + 2)(x^4 + 32x^3 + 60x^2 + 64x + 4)$	$[K_3, L_6]$	$2^{51}5^{22}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$-5(x^2 - 4x + 2)(x^4 + 32x^3 + 60x^2 + 64x + 4)$	$[K_3, L_6]$	$2^{51}5^{22}$	2^{4+10}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	U(1)
(2.0.4.1-4096.1-b)^2	$(x + 3)(4x^4 - 16x^3 - 12x^2 - 8x - 47)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$2^{36}5^{12}$	2^{4+12}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$-(x + 3)(4x^4 - 16x^3 - 12x^2 - 8x - 47)$	$[\mathbb{Q}, \mathbb{Q}, L_6]$	$2^{36}5^{12}$	2^{4+12}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
256a × 256d	$(x^2 + 1)(x^4 + 4x^3 - 30x^2 + 60x - 223)$	$[K_1, L_6]$	$2^{46}5^{12}$	2^{4+12}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)
	$-(x^2 + 1)(x^4 + 4x^3 - 30x^2 + 60x - 223)$	$[K_1, L_6]$	$2^{46}5^{12}$	2^{4+12}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	U(1)

Table 20: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(\frac{2^{13}\cdot 3^{10}\cdot 19^5}{7^{12}}, \frac{2^7\cdot 3^6\cdot 19^3\cdot 59\cdot 2339}{7^{12}}, \frac{-2^9\cdot 3^4\cdot 17\cdot 19^2\cdot 6337}{7^{12}}\right)$. A total of 16 curves separated into 4 isogeny classes are given.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	**GL$_2$−type**	**ST^0**
32a × 256a	$(2x+1)(x^4-8x^2-32x+136)$	$[\mathbb{Q},\mathbb{Q},L_5]$	$2^{27}7^{12}$	2^{4+9}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$-(x^2+2x-1)(2x^4-8x^3+8x^2+8x+7)$	$[K_3,L_5]$	$2^{22}7^{12}$	2^{4+9}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$7(x^2+1)(x^4-40x^2+8)$	$[K_1,L_4]$	$2^{27}7^{22}$	2^{4+9}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$-7(x^2+2)(2x^4-20x^2+1)$	$[K_2,L_4]$	$2^{22}7^{22}$	2^{4+9}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
32a × 256d	$-(2x+1)(x^4-8x^2-32x+136)$	$[\mathbb{Q},\mathbb{Q},L_5]$	$2^{27}7^{12}$	2^{4+9}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$(x^2+2x-1)(2x^4-8x^3+8x^2+8x+7)$	$[K_3,L_5]$	$2^{22}7^{12}$	2^{4+9}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$-7(x^2+1)(x^4-40x^2+8)$	$[K_1,L_4]$	$2^{27}7^{22}$	2^{4+9}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$7(x^2+2)(2x^4-20x^2+1)$	$[K_2,L_4]$	$2^{22}7^{22}$	2^{4+9}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
64a × 256a	$-(4x+1)(2x^4-4x^2-8x+17)$	$[\mathbb{Q},\mathbb{Q},L_5]$	$2^{27}7^{12}$	2^{4+10}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$(x^2+4x-4)(x^4-8x^3+16x^2+32x+56)$[a]	$[K_3,L_5]$	$2^{22}7^{12}$	2^{4+10}	1	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$-7(x^2+4)(x^4-20x^2+2)$	$[K_1,L_4]$	$2^{27}7^{22}$	2^{4+10}	1	$\mathbb{Z}/8\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$14(x^2+2)(2x^4-20x^2+1)$	$[K_2,L_4]$	$2^{32}7^{22}$	2^{4+10}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
64a × 256d	$(4x+1)(2x^4-4x^2-8x+17)$	$[\mathbb{Q},\mathbb{Q},L_5]$	$2^{27}7^{12}$	2^{4+10}	0	$\mathbb{Z}/4\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$-2(x^2+2x-1)(2x^4-8x^3+8x^2+8x+7)$	$[K_3,L_5]$	$2^{32}7^{12}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$7(x^2+4)(x^4-20x^2+2)$	$[K_1,L_4]$	$2^{27}7^{22}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$
	$-7(x^2+8)(x^4-40x^2+8)$[b]	$[K_2,L_4]$	$2^{22}7^{22}$	2^{4+10}	0	$\mathbb{Z}/8\mathbb{Z}$	✓	$\mathrm{U}(1)\times\mathrm{U}(1)$

[a] A global minimal model for this curve is $y^2+x^3y=-x^5-5x^4+32x^3+30x^2+24x-56$.
[b] A global minimal model for this curve is $y^2+x^3y=-2x^6+56x^4+546x^2-112$.

Table 21: List of genus 2 curves C where $\mathrm{Jac}(C)$ has good reduction outside 2, with G2 invariants $(g_1, g_2, g_3) = \left(\frac{-2^8 \cdot 151^5}{7^{12}}, \frac{2^3 \cdot 5 \cdot 41 \cdot 43 \cdot 151^3}{7^{12}}, \frac{-2^8 \cdot 71 \cdot 151^2 \cdot 2663}{7^{12}}\right)$. A total of 6 curves separated into 5 isogeny classes are given.

Isogeny Class	**Minimal Weierstrass equation**	**Field system**	$\Delta_{\mathbf{min}}$	**Conductor**	**Rank**	**Tors. subgroup**	**GL$_2$−type**	**ST^0**
128a × 128d	$(x^2+2x-1)(x^4-4x^3+66x^2+4x+577)$	$[K_3, L_5]$	$2^{52}7^{12}$	2^{4+10}	1	$\mathbb{Z}/2\mathbb{Z}$	✓	SU(2)
128b × 128c	$-(x^2+2x-1)(x^4-4x^3+66x^2+4x+577)$	$[K_3, L_5]$	$2^{52}7^{12}$	2^{4+10}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	SU(2)
(2.2.8.1-1024.1-j)^2	$(x+7)(x^4-4x^3+66x^2-252x+833)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{37}7^{12}$	2^{4+12}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	SU(2)
(2.2.8.1-1024.1-h)^2	$-(x+7)(x^4-4x^3+66x^2-252x+833)$	$[\mathbb{Q}, \mathbb{Q}, L_5]$	$2^{37}7^{12}$	2^{4+12}	0	$\mathbb{Z}/2\mathbb{Z}$	✓	SU(2)
2.0.8.1-1024.1-a ×	$7(x^2+2x+2)(x^4+32x^3-132x^2+64x+4)$	$[K_1, L_4]$	$2^{47}7^{22}$	2^{4+12}	0	$\mathbb{Z}/2\mathbb{Z}$	no	SU(2)
2.0.8.1-1024.1-c	$-7(x^2+2x+2)(x^4+32x^3-132x^2+64x+4)$	$[K_1, L_4]$	$2^{47}7^{22}$	2^{4+12}	0	$\mathbb{Z}/4\mathbb{Z}$	no	SU(2)

Conclusion

In conclusion, we've shown that the method of cluster pictures introduced by Dokchitser, Dokchitser, Maistret, Morgan [31] can be effectively applied to yield many quick proofs of various results regarding the reduction behaviour of hyperelliptic curves. Not only have these generalised existing theorems, such as those from Box and Le Fourn [11], but can also give simple criterion for determining whether a given curve C or its Jacobian $\mathrm{Jac}(C)$ has (potentially) good reduction outside a given set of primes, as illustrated in Corollaries 12 and 21.

On the computational side, we have also been able to extend Smart's [88] original list by presenting 115 new genus 2 curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ has good reduction outside 2, with C having bad reduction at some odd prime. Interestingly, none of our curves are currently listed on the LMFDB, and so extending the LMFDB database would hopefully be on our radar for future work.

There are certainly many further avenues one could still investigate. One such possibility is to effectively extend the computations done by Farmer-Koutsoliotas-Lemurell [36] where we use L-modularity to give a conjecturally complete list of L-functions for conductors $N > 2^{10}$. As higher precision is required for larger conductors, a practical algorithm would thus require further investigation into choosing a more optimal choice of weight functions $g(s)$.

Another possibility would be to extend the computation of solutions to S-unit equations by either considering further Galois constraints or symmetries. Of course, our ideal goal would be to construct an effective algorithm to calculate all curves C/K with $\mathrm{Jac}(C)$ having good reduction outside some finite set of primes. Even with the method of cluster pictures under our belt, this still seems out of reach at the moment, although we will certainly keep working towards this goal in future work.

Acknowledgements

First and foremost, I would like to thank my supervisor, Professor Samir Siksek, for his incredible support over the last year and his many insightful comments and suggestions regarding the project. I would also like to thank Benjamin Matschke for computing all the solutions to the numerous S-unit equations mentioned above, as well as David Farmer for his insights regarding the computation of L-functions. Finally, I would like to thank the University of Warwick Mathematics Institute for providing this valuable opportunity to do a summer project during our first year of PhD studies.

References

[1] Agrawal, M., Coates, J., Hunt, D., Van der Poorten, A. (1980). Elliptic Curves of Conductor 11. Mathematics of Computation, 35(151), 991-1002. doi:10.2307/2006209

[2] Alvarado, A., Koutsianas, A., Malmskog, B., Rasmussen, C., Vincent, C., West, M. (2020) *A robust implementation for solving the S-unit equation and several applications*, arXiv:1903.00977v5 [math.NT].

[3] Aubry, Y., Haloui, S., Lachaud, G. (2013) *On the number of points on abelian and Jacobian varieties over finite fields*. Acta Arithmetica, Instytut Matematyczny PAN, Vol. 160, No. 3, pp.201–241.

[4] Barsagade, M.W., Meshram, S. (2014) *Overview of History of Elliptic Curves and its use in cryptography*, International Journal of Scientific & Engineering Research, Vol.5, No. 4, pp.467-470.

[5] Best, A.J., Matschke, B. (2020). *Elliptic curves with good reduction outside of the first six primes*, arXiv:2007.10535 [math.NT].

[6] Birch, B.J., Kuyk, W (1975) *Modular Functions of One Variable, IV*, Lecture Notes in Mathematics, Vol. 476. Berlin: Springer-Verlag.

[7] Booker, A. R., Sijsling, J., Sutherland, A. V., Voight, J. and Yasaki, D. (2016) *A database of genus-2 curves over the rational numbers,* LMS J. Comput. Math. London Mathematical Society, Vol. 19 (A), pp. 235–254.

[8] Börner, M., Bouw, I.I., Wewers, S. (2017) *The Functional Equation for L-Functions of Hyperelliptic Curves*, Experimental Mathematics, Vol. 26, No. 4, pp.396-411.

[9] Bouw, I.I, Koutsianas, A., Sijsling, J., Wewers, S. (2019) *Conductor and discriminant of Picard curves*, arXiv:1902.09624 [math.NT].

[10] Bouw, I.I., Wewers, S. (2012) *Computing L-functions and semistable reduction of superelliptic curves*, arXiv:1211.4459 [math.NT].

[11] Box, J., le Fourn, S. (2020) *Bounding integral points on the Siegel modular variety* $A_2(2)$, arXiv:2007.14422v2 [math.NT].

[12] Brumer, A., Kramer, K. (1994) *The conductor of an abelian variety*, Compositio Mathematica, Vol. 92, No. 2, pp.227-248.

[13] Brumer, A., Kramer, K. (2014) *Paramodular abelian varieties of odd conductor*, Trans. Amer. Math. Soc. Vol. 366, pp.2463-2516.

[14] Cardona, G., Nart, E., Pujolás, J. (2005) *Curves of genus two over fields of even characteristic*. Math. Z. Vol. 250, No. 1, pp.177–201.

[15] Cardona, G., Quer, J. *Field of moduli and field of definition for curves of genus 2*. Computational aspects of algebraic curves, Lecture Notes Ser. Comput., Vol. 13, World Sci. Publ., Hackensack, NJ, pp.71–83.

[16] Cassels, J., Flynn, E. (1996). *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2* (London Mathematical Society Lecture Note Series). Cambridge: Cambridge University Press.

[17] Coghlan, F.B. (1967), *Elliptic Curves with Conductor* $N = 2^m 3^n$, Thesis (Ph.D.), The University of Manchester (United Kingdom).

[18] Cohen, H., (2000) *Advanced Topics in Computational Number Theory*, Springer-Verlag New York.

[19] Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F. (2005) *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Mathematics and Its Applications, No. 34.

[20] Comalada, S. (1990) *Courbes elliptiques á bonne réduction d'invariant j fixé.* C. R. Acad. Sci. Paris S´er. I Math. Vol. 311, No. 11, pp.667–670.

[21] Comalada, S. (1990) *Elliptic Curves with Trivial Conductor over Quadratic Fields.* Pacific J. Math. Vol. 144, No. 2, pp.237–258.

[22] Comalada, S., Nart, E. (1987) *Courbes elliptiques avec bonne réduction partout.* C. R. Acad. Sci. Paris Sér. I Math. Vol. 305, No. 6, pp.223–224.

[23] Cornell G., Silverman J.H. (1986) *Arithmetic Geometry*, Springer, New York, NY.

[24] Costa, E. Mascot, N. Sijsling, J., Voight J. (2017) *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. Vol. 88, pp.1303-1339.

[25] Cremona, J. E. and Lingham, M. P. (2007) *Finding All Elliptic Curves with Good Reduction Outside a Given Set of Primes,* Experiment. Math. Vol. 16, No. 3, pp.303-312.

[26] Cremona, J. (1992) *Modular symbols for* $\Gamma_1(N)$ *and elliptic curves with everywhere good reduction.* Math. Proc. Cambridge Philos. Soc. Vol. 111, pp.199-218.

[27] Dabrowski, A., Sadek, M. (2020) *Genus 2 curves with bad reduction at one odd prime*, arXiv:2003.09010 [math.NT]

[28] Deconinck, H. (2016) *On the generalized Fermat equation over totally real fields,* Acta Arith. Vol. 173, No. 3, pp. 225–237.

[29] Dokchitser, T. (2004) *Computing Special Values of Motivic L-Functions,* Experimental Mathematics, Experiment. Math. Vol. 13, No. 2, pp.137-150.

[30] Dokchitser, T., Dokchitser, V., Maistret, C., Morgan, A. (2018), *Arithmetic of hyperelliptic curves over local fields*, arXiv:1808.02936v2 [math.NT].

[31] Dokchitser, T., Dokchitser, V., Maistret, C., Morgan, A. (2019). *Semistable types of hyperelliptic curves,* In: Algebraic curves and their applications, Contemp. Math., Vol. 724, pp. 73-135.

[32] Dokchitser, T., Doris, C. (2019) *3-torsion and conductor of genus 2 curves*, Math. Comp. Vol. 88, pp.1913-1927.

[33] Elliott, E.B. (1895) *An introduction to the algebra of quantics*, Oxford University Press.

[34] Evertse, J.H., Győry, K. (1991) *Effective finiteness results for binary forms with given discriminant*, Compositio Math, Vol. 79, pp.169-204.

[35] Evertse, J.H., Győry, K. (2015) *Unit Equations in Diophantine Number Theory.* Cambridge: Cambridge University Press (Cambridge Studies in Advanced Mathematics).

[36] Farmer, D., Koutsoliotas, S., Lemurell, S. (2019) *Varieties via their L-functions*,

[37] Farmer, D., Ryan, N. (2014) *Evaluating L-functions with few known coefficients*, LMS J. Comput. Math. Vol. 17 pp.245-258.

[38] Fischer, I. (1956) *The moduli of hyperelliptic curves.* Trans. Amer. Math. Soc. Vol. 82, pp.64-84.

[39] Harbater, D. (1993) *Galois groups with prescribed ramification* (English summary) Arithmetic geometry (Tempe, AZ, 1993), 35–60, Contemp. Math., 174, Amer. Math. Soc., Providence, RI, 1994.

[40] Hayashida, T. (1968) *A class number associated with the product of an elliptic curve with itself*, J. Math. Soc. Japan, Vol. 20, pp.26-43.

[41] Hayashida, T., Nishi, M. (1965) *Existence of curves of genus two on a product of two elliptic curves*, J. Math. Soc. Japan, Vol. 17, pp.1-16.

[42] Igusa, J. (1960). *Arithmetic Variety of Moduli for Genus Two,* Annals of Mathematics, Second Series, Vol. 72, No. 3, pp. 612-649.

[43] Ishii, H. (1979) *The nonexistence of elliptic curves with everywhere good reduction over certain imaginary quadratic fields*, J. Math. Soc. Japan, Vol. 31, No. 2, pp.273-279.

[44] Ishii, H. (1986) *The Nonexistence of Elliptic Curves with Everywhere Good Reduction over Certain Quadratic Fields.* Japan. J. Math. (N.S.) Vol.12, No. 1, pp.45–52.

[45] Kani, E. (2011) *Products of CM elliptic curves.* Collect. Math. Vol. 62, pp.297-339.

[46] Kani, E. (2014) *Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms.* J. Number Theory Vol. 139, pp.138-174.

[47] Katz, N.M. (1980) *Galois Properties of Torsion Points on Abelian Varieties*, Invent Math, Vol. 62, pp.481–502.

[48] Kedlaya, K. S., Sutherland, A. V., (2008) *Computing L-series of hyperelliptic curves*, Algorithmic Number Theory 8th International Symposium (ANTS VIII) , Lecture Notes in Computational Science Vol. 5011 (Springer, Berlin, 2008) pp.312–326

[49] Kida, M. (1999) *Reduction of Elliptic Curves over Certain Real Quadratic Number Fields.* Math. Comp. Vol. 68, No. 228, pp.1679–1685.

[50] Kida, M. (2000) *Computing elliptic curves having good reduction everywhere over quadratic fields. II.* In Algebraic number theory and Diophantine analysis (Graz, 1998), pp.239–247.

[51] Kida, M. (2001) *Computing elliptic curves having good reduction everywhere over quadratic fields.* Tokyo J. Math., Vol. 24, No. 2, pp.545–558.

[52] Kida, M. (2001) *Good Reduction of Elliptic Curves over Imaginary Quadratic Fields.* J. Théor. Nombres Bordeaux, Vol. 13, No. 1, pp.201–209.

[53] Kida, M. (2001) *Nonexistence of Elliptic Curves Having Good Reduction Everywhere over Certain Quadratic Fields.* Arch. Math. (Basel) Vol. 76, No. 6, pp.436–440.

[54] Kida, M., Kagawa, T. (1997) *Nonexistence of Elliptic Curves with Good Reduction Everywhere over Real Quadratic Fields.* J. Number Theory Vol. 66, No. 2, pp.201–210.

[55] Koblitz, N. (1989) *Hyperelliptic cryptosystems*, Journal of Cryptology, Vol. 1, pp.139-150.

[56] Koutsianas, A. (2019) *Computing All Elliptic Curves Over an Arbitrary Number Field with Prescribed Primes of Bad Reduction*, Experimental Mathematics, Vol. 28, No.1, pp.1-15,

[57] Laska, M. (1983) *Elliptic Curves Over Number Fields with Prescribed Reduction Type.* Aspects of Mathematics, Vol. E4. Friedr. Vieweg & Sohn, Braunschweig; distributed by Philadelphia, PA: Heyden & Son, Inc.

[58] Lenstra, H.W., Pila, J., Pomerance, C. (1993) *A hyperelliptic smoothness test. I*, Philosophical Transactions of the Royal Society of London A, Vol. 345 pp.397-408.

[59] The LMFDB Collaboration, (2021) *The L-functions and modular forms database*, [online] Available at: `http://www.lmfdb.org`.

[60] Lombardo, D. (2018) *Abelian varieties*, Luxembourg Summer School on Galois representations. [online] Available at: `https://people.dm.unipi.it/lombardo/Teaching/VarietaAbeliane1718/Notes.pdf` [Accessed on 19 May 2021]

[61] Malmendier, A., Shaska, T. (2016). *The Satake sextic in elliptic fibrations on K3.* Journal of Geometry and Physics, Vol. 120, pp.290-305.

[62] Malmskog, B., Rasmussen, C. *Picard curves over* $\mathbb{Q}$ *with good reduction away from* 3, LMS J. Comput. Math. Vol. 19, pp.382-408.

[63] Matei, V. (2013) *Faltings Serre method*, [online] Available at: `https://people.math.wisc.edu/ boston/FLTMatei.pdf`.

[64] Matschke, B. (2020) *A general S-unit equation solver and tables of elliptic curves over number fields*, Modern Breakthroughs in Diophantine Problems BIRS, 2020.

[65] Matschke, B. (2021) Personal communication.

[66] Merriman, J. R. and Smart, N. P. (1993) *Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point,* Math. Proc. Cambridge Philos. Soc. Cambridge University Press, Vol. 114, pp.203-214. Corrigenda: Math. Proc. Camb. Phil. Soc. Vol. 118 (1995), pp. 189.

[67] Mestre, J. (1986) *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Mathematica Vol. 58. No. 2, pp.209-232.

[68] Milne, J. (2008). *Abelian varieties.* [online] Available at: `https://www.jmilne.org/math/CourseNotes/AV.pdf` [Accessed 19 Dec. 2020].

[69] Mumford, D. (1974) *Abelian varieties* (2nd edition), Oxford Univ Press.

[70] Narasimhan, M.S., Nori, N.V. (1981) *Polarisations on an abelian variety*, Proc. Indian Acad., Sci. (Math. Sci.), Vol. 90, No. 20, pp.125-128.

[71] Neukirch, J. (1999) *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg.

[72] Ogg, A. P. (1966) *Abelian curves of 2-power conductor,* Math. Proc. Cambridge Philos. Soc. Cambridge University Press, Vol. 62, No.2, pp. 143–148.

[73] Pinch, R. G. E. (1984) *Elliptic curves with good reduction away from 2,* Math. Proc. Cambridge Philos. Soc. Cambridge University Press, Vol. 96, No. 1, pp. 25–38.

[74] Pinch, R. G. E. (1986) *Elliptic curves with good reduction away from 2: II,* Math. Proc. Cambridge Philos. Soc. Cambridge University Press, Vol. 100, No. 3, pp. 435–457.

[75] Pinch, R. G. E. (1987) *Elliptic curves with good reduction away from 3,* Math. Proc. Cambridge Philos. Soc. Cambridge University Press, Vol. 101, No.3, pp. 451–459.

[76] Poonen, B. (1996) *Computational Aspects of Curves of Genus at Least 2,* In Proceedings of the Second International Symposium on Algorithmic Number Theory (ANTS-II). Springer-Verlag, Berlin, Heidelberg, pp.283–306.

[77] Rohrlich, D.E. (1982) *Elliptic curves with good reduction everywhere*, J. London Math. Soc. Vol. 25, No. 2, pp.216-222.

[78] Rowan, J. (2016) *S-unit equations and curves of genus 2 with good reduction away from 3*, SPUR Project, Massachusetts Institute of Technology.

[79] Rubinstein, M. (2005) *Computational methods and experiments in analytic number theory*, in: Mezzadri, F., Snaith, N.C. (Eds.), Recent Perspectives in Random Matrix Theory and Number Theory, in: London Math. Soc. Lecture Note Ser.

[80] The Sage Developers (2021) *SageMath, the Sage Mathematics Software System (Version 9.3)*, Available at `https://www.sagemath.org`.

[81] Schoof, R. (2005) *Abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only*, Compositio Math. Vol. 141, pp.847–868.

[82] Serre, J., and Tate, J. (1968). *Good Reduction of Abelian Varieties,* Annals of Mathematics, Second Series, Vol. 88, No. 3, pp.492-517.

[83] Setzer, B. (1978) *Elliptic curves over complex quadratic fields.* Pacific J. Math., Vol. 74, No. 1, pp.235–250.

[84] Setzer, B. (1981) *Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant*, Illinois J. Math., Vol. 25, No. 2, pp.233–245.

[85] Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves* 2nd edition, Springer-Verlag New York.

[86] Silverman, J. H. (1994). *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag New York.

[87] Smart, N. P. (1997) *S-unit equations, binary forms and curves of genus* 2, Proc. London Math. Soc. (3). Vol. 75, No. 2, pp.271-307.

[88] Smart, N. P. (1998). *The Algorithmic Resolution of Diophantine Equations.* London Mathematical Society Student Texts. 41. Cambridge University Press.

[89] Stephens, N.M. (1965) *The Birch Swinnerton-Dyer Conjecture for Selmer curves of positive rank*, Ph.D. Thesis, Manchester.

[90] Stoll, M. (2014) *Arithmetic of Hyperelliptic Curves*, Summer Semester 2014, University of Bayreuth [online] Available at: `http://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2014/Skript-ArithHypCurves-pub-screen.pdf`.

[91] Stroeker, R. J. (1983) *Reduction of elliptic curves over imaginary quadratic number fields,* Pacific J. Math. Vol. 108, No. 2, pp.451-463.

[92] Sutherland, A. (2009). *A Generic Approach to Searching for Jacobians*, Mathematics of Computation, Vol. 78, No. 265, pp.485-507.

[93] van Bommel, R. (2018) *Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over $\mathbb{Q}$ up to squares*, arXiv:1711.10409v3 [math.NT].

[94] van Luijk, R. (2000) *On Perfect Cuboids*, Doctoral Thesis, Mathematisch Instituut Universiteit Utrecht.

[95] van Wamelen, P. (2000) *Poonen's question concerning isogenies between Smart's genus 2 curves*, Math. Comp. Vol. 69, No. 232, pp.1685-1697.

[96] von Känel, R., Matschke, B. (2016) *Solving S-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture*, arXiv:1605.06079 [math.NT].

[97] Yelton, J. (2015) *Hyperelliptic Jacobians and their associated ℓ-adic Galois representations*, PhD Thesis, Pennsylvania State University.

Appendix

The following lemma is used to prove Theorem 17 (i.e. there exist only finitely many hyperelliptic curves of genus g with rational Weierstrass points and with potentially good reduction at all but at most $\pi(2g)$ odd primes).

Lemma 28: Let K be a number field, and S a fixed finite set of primes of K, Then there are only finitely many odd primes p, such that there exist distinct T-units $x, y, z \in \mathcal{O}_T^\times$, where $T = S \cup \{p\}$ such that $x - y, x - z$ and $y - z$ are all T-units (and where p appears at least once in at least one of $x, y, z, x - y, x - z, y - z$).

Proof: We first fix some odd prime p, and shall aim to derive a system of equations which can only be satisfied for finitely many p. With this in mind, we can first assume without loss of generality that $v_p(x) \geq v_p(y) \geq v_p(z)$. Therefore, we have $\frac{x}{z} = sp^a$ and $\frac{y}{z} = tp^b$ for some S-units $s, t \in \mathcal{O}_S^\times$ and non-negative integers $a, b \in \mathbb{Z}_{\geq 0}$ where $a \geq b$. By assumption, since $\frac{x}{z} - 1, \frac{y}{z} - 1$ and $\frac{x}{z} - \frac{y}{z}$ are in $\mathcal{O}_T^\times$, we have $u, v, w \in \mathcal{O}_S^\times$ and $c, d, e \in \mathbb{Z}$ such that

$$\begin{aligned} sp^a - 1 &= up^c \\ tp^b - 1 &= vp^d \\ sp^a - tp^b &= wp^e \end{aligned} \tag{11}$$

Now, by considering the valuation at p, we have that $c = 0$ if $a \neq 0$, and similarly $d = 0$ if $b \neq 0$, and $e = b$ if $a \neq b$. Thus, informally speaking, we have 6 equations restricting the 5 variables a, b, c, d, e, and therefore we can aim to eliminate the prime p and obtain a three term S-unit equation which yields finitely many solutions.

With this in mind, we can proceed formally by considering the various cases:

- **Case 1:** $a, b > 0$ and $a > b$. We therefore have $c = d = 0$ and $e = b$. This yields the equations

$$\begin{aligned} sp^a - 1 &= u, \\ tp^b - 1 &= v, \\ sp^a - tp^b &= wp^b \end{aligned}$$

  By solving for p^a and p^b in the 1st and 2nd equation, and substituting into the third, we obtain the three term S-unit equation:

$$s(u+1)/s - t(v+1)/t = w(v+1)/t \quad \Longrightarrow \quad tuw^{-1} - tvw^{-1} - v = 1$$

  At this stage, we would like to apply Theorem 6.1.1 from [35, p. 130] in order to conclude that there are only finitely many solutions to the above equation. This however requires showing that we do not obtain (or only obtain finitely many) *degenerate* solutions where some subset of the above three terms equals 0. This is equivalent to checking the three cases where each term above is 1:

  (i) If $tu = w$, then $t = -w$, which from the third equation implies $x = 0$, contradiction.

  (ii) If $tv = -w$, then $sp^a - tp^b = -tvp^b$ and thus $sp^a = t(1 - v)p^b$, which implies $1 - v$ has positive p-adic valuation. But $v - 1 = tp^b - 2$ which yields a contradiction, since p is odd.

  (iii) If $v = -1$, then $y = tp^b = 0$, contradiction.

Therefore, we have a 3-term S-unit equation with no subset being 0. Therefore, by the result from [35, p. 130], there are only finitely many solutions to the above, and thus only finitely many v, and thus clearly only finitely many p, noting that b is positive.

- **Case 2:** $a, b > 0$ and $a = b$. We therefore have $c = d = 0$. This yields the equations

$$\begin{aligned} sp^a - 1 &= u, \\ tp^a - 1 &= v, \\ sp^a - tp^a &= wp^e \end{aligned}$$

By equating p^a from the first two equations, we get

$$(u+1)/s = p^a = (v+1)/t \quad \implies \quad tus^{-1} + ts^{-1} - v = 1$$

Once again, we check no subset can be zero:

(i) If $tu = s$, then $t = vs$. This implies $uv = 1$. Now by multiply the first two equations we get

$$stp^{2a} - (s+t)p^a + 1 = (sp^a - 1)(tp^a - 1) = uv = 1$$

This yields $stp^a = s + t$, and thus $s + t$ has valuation $a > 0$. Therefore $s - t$ has p-adic valuation 0. By eq 3, this implies $e = a$, and thus $s - t = w$. By finiteness of two-term S-unit equations, this implies finitely many values for s/t and thus for u. Therefore by eq 1, only finitely many values for p.

(ii) If $t = s$, then $x = y$, contradiction.

(iii) If $v = -1$, then $u = 1$, and so $sp^a = 2$, contradiction.

Thus, as before, only finitely many solutions.

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

$$\begin{aligned} sp^a - 1 &= u, \\ t - 1 &= vp^d, \\ sp^a - t &= w \end{aligned}$$

By equating p^a from the first and third equations, we have

$$(u+1)/s = (w+t)/s \quad \implies \quad w + t - u = 1$$

(i) If $w = 1$, then $t = u$. This implies $sp^a - 2 = t - 1 = vp^d$, and thus $d = 0$ (as p odd). This yields a 2-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 $c > d$. We therefore have

$$\begin{aligned} s - 1 &= up^c, \\ t - 1 &= vp^d, \\ s - t &= wp^d \end{aligned}$$

By solving for p^d in the last two equations, we get

$$(t-1)/v = p^d = (s-t)/w \quad \implies \quad vtw^{-1} - vsw^{-1} + t = 1$$

(i) If $vt = w$, then we have $s - t = vtp^d$, which implies $s = t(vp^d + 1) = t^2$. This yields

$$up^c = s - 1 = t^2 - 1 = (t-1)(t+1) = vp^d(t+1)$$

which implies $t + 1$ has positive p-adic valuation. But $t + 1 = vp^d + 2$, which yields a contradiction as p odd.

(ii) If $vs = -w$, then $v = -w$. This implies $t - 1 = -wp^d = t - s$, and thus $s = 1$, contradiction.

(iii) If $t = 1$, then $y = z$, contradiction.

- **Case 5:** $a = b = 0$ and $c = d$. We therefore have

$$\begin{aligned} s - 1 &= up^c, \\ t - 1 &= vp^c, \\ s - t &= wp^e \end{aligned}$$

Firstly, we note that if $c = d = 0$, then s and t satisfy two-term S-unit equations, of which there are only finitely many solutions. In the third equation, this thus implies only finitely many p, since we'd then have $e \neq 0$ by assumption.

Now assume $c, d \neq 0$, and note that c, e must necessarily be positive. By equating the first two equations, we get

$$(s-1)/u = p^c = (t-1)/v \quad \implies \quad uv^{-1} - utv^{-1} + s = 1$$

(i) If $u = v$, then $s = t$. This implies $x = y$ which is a contradiction.

(ii) If $ut = -v$, then $u = -sv$ and $st = 1$. Note that we have

$$\frac{-vp^c(vp^c + 2)}{t} = \frac{(1-t)(1+t)}{t} = \frac{1 - t^2}{t} = s - t = wp^e$$

Since $vp^c + 2$ has zero p-adic valuation, this implies $e = c$. Therefore, substituting the first two equations into the third yields

$$up^c - vp^c = wp^c \quad \implies \quad uv^{-1} - wv^{-1} = 1$$

which gives a two-term S-unit equation, and thus finitely many solutions for uv^{-1}. Therefore, this gives finitely many t, and thus finitely many p.

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

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

Therefore, in all cases, only finitely many primes p satisfy the given equations in (11), which concludes the proof. □

We note that effectively obtaining a list of all possible p depends entirely on the effectiveness of solving the above three term S-unit equations. From the results of [35], no finite algorithm has been found to determine all possible solutions, however one can obtain an explicit bound on the number of possible p, which for a fixed number of terms, is exponential in $|S|$ [35, p. 132].

Aside: To potentially generalise the above argument, let's fix some set of primes S, and consider adjoining an extra k primes $p_1, \ldots, p_k$ and let $T := S \cup \{p_1, \ldots, p_k\}$. Now given a hyperelliptic curve of genus g having potentially good reduction outside T, this yields $\binom{2g}{2}$ T-unit

equations. Note that each variable λ_i introduces k new variables for the exponents of $p_1, \ldots, p_k$.

Thus, in a very informal sense, if we have the number of equations more than variables in the exponents, i.e.

$$k(2g-1) < \binom{2g}{2} \qquad (\implies k < g \quad)$$

then we expect that a similar (albeit tedious) case-by-case argument could yield only finitely many choices for the primes $p_1, \ldots, p_k$.

With this in mind, we can formulate the following conjecture:

Conjecture 29: There are only finitely many hyperelliptic curves $C/\mathbb{Q}$ of genus g (with rational Weierstrass points) having potentially good reduction at all but at most $\pi(2g) + g - 2$ odd primes.

Jacobians of genus 2 curves split over $\mathbb{Q}$

We've noted that the problem of classifying all genus 2 curves $C/\mathbb{Q}$ with $\mathrm{Jac}(C)$ having good reduction outside 2 is certainly a non-trivial task, whereby proving completeness for a given list seems to be currently out of reach.

The aim of this section is to therefore try to understand the (hopefully simpler) sub-problem of finding all genus 2 curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ is good outside 2 in the case where $\mathrm{Jac}(C)$ is split over $\mathbb{Q}$.

We note from Table 8 that there are 10 isogeny classes of elliptic curves $E/\mathbb{Q}$ having good reduction outside 2. By therefore considering each pair $E_1 \times E_2$, this therefore yields a total of 55 isogeny classes of abelian surfaces (split over $\mathbb{Q}$) which have good reduction outside 2. The next natural question is to ask whether we can classify all genus 2 curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ is isogenous to one of these abelian surfaces.

Whilst this is not proven here, we do give a summary of the possible primes of bad reduction for C which we've found, as shown in Table 22.

Firstly, we note that examples of genus 2 curves $C/\mathbb{Q}$ have been found such that $\mathrm{Jac}(C)$ is isogenous to each of the above isogeny classes in almost all cases, the only exception being the 256b $\times$ 256b, and 256c $\times$ 256c isogeny classes.

Of particular interest is that the isogeny classes A for which there does not exist a genus 2 curve $C/\mathbb{Q}$ with good reduction outside 2, such that $\mathrm{Jac}(C) \cong A$, are precisely the classes $A = E_1 \times E_2$ where E_1, E_2 are elliptic curves with CM by an order in $\mathbb{Q}(i)$, i.e. the classes 32a, 64a, 256b, and 256c (noting that all other possibilities arise from one of the genus 2 curves $C/\mathbb{Q}$ in Smart's [88] list).

Indeed, the question of whether an abelian surface of the form $E_1 \times E_2$ can be the Jacobian of a genus 2 curve has been extensively studied since the 1960s, with Hayashida and Nishi [41, 40] obtaining some of the first partial results. More recently, Kani [45, 46] has obtained further results which essentially settles the existence problem (in least in our case of interest).

Despite proving the existence of genus 2 curves $C/\mathbb{Q}$ with given Jacobian A, the more general question still remains of how whether one can provide a full classification of all such curves, up to $\mathbb{Q}$-isomorphism, and in particular, what the possible bad primes for C could be given its Jacobian $\mathrm{Jac}(C)$. This could certainly be an interesting topic of further research.

Table 22: Table of all 55 isogeny classes of genus 2 curves $C/\mathbb{Q}$ with split Jacobian over $\mathbb{Q}$, i.e. where $\mathrm{Jac}(C) \cong E_1 \times E_2$ for some two elliptic curves E_1, E_2 good outside 2. Each cell in the table denotes a list of subsets of primes S for which there exists a genus 2 curve C with $\mathrm{Jac}(C) \cong E_1 \times E_2$ where C is bad at S (with the rows (resp. columns) denoting the isogeny class of E_1 (resp. E_2)).

	32a	**64a**	**128a**	**128b**	**128c**	**128d**	**256a**	**256b**	**256c**	**256d**
32a	$\{2,3\}$	$\{2,3\}$	$\{2\}$, $\{2,5\}$	$\{2\}$, $\{2,5\}$	$\{2\}$, $\{2,5\}$	$\{2\}$, $\{2,5\}$	$\{2\}$, $\{2,7\}$	$\{2,3\}$	$\{2,3\}$	$\{2\}$, $\{2,7\}$
64a		$\{2,3\}$	$\{2\}$, $\{2,5\}$	$\{2\}$, $\{2,5\}$	$\{2\}$, $\{2,5\}$	$\{2\}$, $\{2,5\}$	$\{2\}$, $\{2,7\}$	$\{2,3\}$	$\{2,3\}$	$\{2\}$, $\{2,7\}$
128a			$\{2\}$	$\{2\}$, $\{2,3\}$	$\{2\}$	$\{2\}$, $\{2,7\}$	$\{2\}$, $\{2,3\}$	$\{2\}$	$\{2\}$	$\{2\}$, $\{2,3\}$
128b				$\{2\}$	$\{2\}$, $\{2,7\}$	$\{2\}$	$\{2\}$, $\{2,3\}$	$\{2\}$	$\{2\}$	$\{2\}$, $\{2,3\}$
128c					$\{2\}$	$\{2\}$, $\{2,3\}$	$\{2\}$, $\{2,3\}$	$\{2\}$	$\{2\}$	$\{2\}$, $\{2,3\}$
128d						$\{2\}$	$\{2\}$, $\{2,3\}$	$\{2\}$	$\{2\}$	$\{2\}$, $\{2,3\}$
256a							$\{2\}$	$\{2\}$	$\{2\}$	$\{2\}$, $\{2,5\}$
256b								?	$\{2,3\}$	$\{2\}$
256c									?	$\{2\}$
256d										$\{2\}$