First Year Report

Elvira Lupoian

August 2021

1 Introduction

The main objective of this report is to present a method of finding the two torsion subgroup of the Mordell-Weil group of non-hyperelliptic curves of genus 3 and 4.
Example. Let C be the plane quartic

$$C : x^3z - x^2y^2 + xyz^2 - y^3z - 5z^4 \subset \mathbb{P}^2$$

and let $J = J(\mathbb{Q})$ be it's Mordell-Weil group. Additionally, assume that we know

$$J \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$$

If we can calculate the two torsion subgroup of J and if $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^3$, then this is sufficient to conclude that $J \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

Sections 2 and 3 will give the background necessary for our calculations. In section 3, we establish a a bijection between divisors formed from theta hyperplanes to the curves and the two-torsion points, and give a strategy for computing the two torsion subgroup. Sections 4 and 5 describe a method for finding the theta hyperplanes to a non-hyperelliptic genus 3 or 4 curve. Section 6 describes how the two torsion subgroup is calculated using these theta hyperplanes. Finally, Sections 7 and 8 give examples of how the strategy described works in practice.

2 Curves and Jacobians

This is a brief summary of the algebraic geometry background used throughout our calculations. The main purpose of this section is to establish notation and terminology for the rest of the report. Results will be stated without proof, for details [10, Chapter 8] or [13, Chapters 1 and 2]

2.1 Curves

Fix a field k. An affine variety $V \subset \mathbb{A}_k^n$ defined over k is a set

$$V = \{x\ = (x_1 \dots x_n) \in k^n \mid f_i(x) = 0 \text{ for all i}\}$$

for some polynomials $f_1 \dots f_m \in k[x_1 \dots x_n]$.Given any field $K \supset k$, the set of K-points of V is

$$V(K) = \{x\ = (x_1 \dots x_n) \in K^n \mid f_i(x) = 0 \text{ for all i}\}$$

A projective variety $V \subset \mathbb{P}_k^n$ over k is a set

$$V = \{x \ = (x_0 \dots x_n) \ \in k^{n+1} \mid x \neq 0 \text{ and } f_i(x) = 0 \text{ for all i}\}/\sim$$

for some homogeneous polynomials $f_1 \dots f_m \in k[x_0 \dots x_n]$ and $\sim$ is the usual projective equivalence relation, identifying points which are non zero scalar multiples of one another. Given any field $K \supset k$, the set of K-points of the projective variety V is

$$V(K) = \{x \ = (x_0 \dots x_n) \in K^{n+1} \mid x \neq 0 \text{ and } f_i(x) = 0 \text{ for all i}\}/\sim$$

where $\sim$ is the same identification as above.
Note. A projective variety $V \subset \mathbb{P}_k^n$ can be expressed as the union of its affine patches

$$V = \bigcap_{k=0}^{n} (V \cap \{x_k = 1\})$$

On any variety V, affine or projective, there is a topology, whose closed sets are the subvarieties of V. This is known as the Zariski topology.

If $V \subset \mathbb{A}_k^n$ and $W \subset \mathbb{A}_k^m$ are any two affine varieties, a map $V \longrightarrow W$ is called a morphism if it is given by $x = (x_1 \dots x_n) \longmapsto (f_1(x) \dots f_m(x))$ for some $f_1 \dots f_m \in k[x_1 \dots x_n]$. If V and W are projective varieties, a morphism $V \longrightarrow W$ is a continuous map, given locally by morphism on affine charts.
Definition. An abelian variety over k is a variety, affine or projective, equipped with a group structure, where the group operations are given by morphisms.

Definition. The dimension d of an affine variety $V \subset \mathbb{A}_k^n$ is the length of the longest chain $\emptyset \subsetneqq V_0 \subsetneqq \dots \subsetneqq V_d \subset V$, where each V_i is a variety.
The dimension of a union of affine varieties is the maximum dimension of the components, thus allowing us to define the dimension of a projective variety.

Fact. Over $\mathbb{C}$, any abelian variety of dimension d is isomorphic to $\mathbb{C}^d/\Lambda$, for some lattice $\Lambda \cong \mathbb{Z}^{2d} \subset \mathbb{C}^d$.

Let $V \subset \mathbb{A}_k^n$ be a d dimensional variety given by m polynomials $f_1 \dots f_m \in k[x_1 \dots x_n]$.
Definition. A point $P \in V(\bar{k})$ is smooth if matrix $M = \left(\frac{\partial f_j}{\partial x_i}\right)$ has rank at most $n - d$. Otherwise, the point is called singular. The variety V is smooth if all points $P \in V(\bar{k})$ are smooth. A projective variety is smooth if all of its affine patches are smooth.

Definition. An affine variety $V \subset \mathbb{A}_k^n$ is absolutely irreducible if $V \neq \emptyset$ and when viewed as a variety over $\bar{k}$, it cannot be written as $V_1 \cup V_2$ for any $\bar{k}$-varieties $V_i \subsetneq V$. A projective variety is absolutely irreducible if all its affine patches are irreducible.

Definition. A curve over k is a 1-dimensional, projective, smooth and absolutely irreducible k-variety.

An important family of curves are the hyperelliptic curves. A hyperelliptic curve C is given by a single equation in the weighted projective plane $\mathbb{P}(1, 1, g+1)$

$$f_{2g+2}(t_0, t_1) - t_2^2 = 0 \subset \mathbb{P}_{t_0,t_1,t_2}(1, 1, g+1)$$

where $f_{2g+2} \in \mathbb{Q}[t_0, t_1]$ is a homogeneous polynomial of degree $2g+2$, for some $g \geq 1$, and it is square free.

Let $V \subset \mathbb{A}_k^n$ be an absolutely irreducible affine k variety defined by $f_1 \dots f_m \in k[x_1 \dots x_n]$. The affine coordinate ring of V is

$$k[V] \ = k[x_1 \dots x_n] / (f_1 \dots f_m)$$

adn the function field of V, $k(V)$, is the field of fractions of $k[V]$.

For a projective variety V, the coordinate ring $k[V]$ is the coordinate ring of an affine patch of V, and it's function field if the field of fractions of $k[V]$.

For non-singular curves, the map $C \mapsto k(C)$ defines an equivalence between the category of non-singular cuves over k and the category of finitely generated field extensions K/k of transcendence degree 1. That is, $k(C)$ is a finite, separable extension of $k(t)$, for some t, which is transcendental over k.

Let C be a curve over k. Rational differentials on C are formal finite sums

$$\omega = \sum_i f_i dg_i \text{ where } f_i, g_i \in k(C)$$

modulo the following relations

- $d(f+g) = df + dg$
- $d(fg) = fdg + dgf$
- $dc = 0$ for all $c \in k$

For a curve C, $k(C)$ is a finite and separable extension of $k(t)$, for some t, so any differential can be expressed as $\omega = g\ dt$ for some $g \in k(C)$.

Let $P \in C\left(\overline{k}\right)$, $f \in k(C)$ is regular at P if the order of vanishing of f at P is non-negative.

A differential ω on C is called regular at $P \in C\left(\overline{k}\right)$ if it has a representation $\omega = g\ dt$ with $t, g \in k(C)$ and regular at P. A differential ω is regular if it's regular at all $P \in C\left(\overline{k}\right)$. Let Ω_C be the space of all regular differentials on C. This is a finite dimensional k-vector space.
Definition. The genus of C is $\dim_k \Omega_C$.

2.2 Divisors and the Riemann-Roch Theorem

Let C be a curve over a field k . A divisor D on C is a formal finite linear combination of points in $C\left(\bar{k}\right)$,

$$D = \sum_{P \in C\left(\bar{k}\right)} a_P P$$

for some $a_P \in \mathbb{Z}$, all but finitely many a_P are zero. The degree of D is $\mathrm{D} = \sum_{P \in C\left(\bar{k}\right)} a_P$.

A divisor is called effective if $a_P \geq 0$ for all i, and we write $D \geq 0$.

A rational divisor is one that is invariant $\mathrm{Gal}\left(\bar{k}/k\right)$, where the Galois group acts on a divisor, by acting on its points.

The divisor group of C, denoted by $\mathrm{Div}(C)$, is the set of rational divisors of C/k. This is an abelian group, with addition of two divisors being defined in the following way,

$$\sum_{P \in C\left(\bar{k}\right)} a_P P + \sum_{P \in C\left(\bar{k}\right)} b_P P = \sum_{P \in C\left(\bar{k}\right)} (a_P + b_P) P$$

The degree 0 divisors form a subgroup of $\mathrm{Div}(C)$

$$\mathrm{Div}^0(C) = \{D\ \in \mathrm{Div}(C)\ \mid \deg(D) = 0\}$$

For any non zero $f \in k(C)$, define a divisor

$$\operatorname{div}(f) = \sum_{P \in C(\bar{k})} v_P(f)\, P$$

where $v_P(f) \in \mathbb{Z}$ measures the multiplicity with which f vanished at P. A divisor of this form is called a principal divisor.
Definition. Two divisors $A, B \in \operatorname{Div}(C)$ are said to be linearly equivalent, and write $A \sim B$, if they differ by a principal divisor.

Linear equivalence of divisors forms an equivalence relation $\operatorname{Div}(C)$
Fact. For all non zero $f \in k(C)$, $\operatorname{div}(f)$ has degree 0.

The principal divisors form a subgroup of $\operatorname{Div}^0(C)$,

$$\operatorname{Princ}(C) = \{\operatorname{div}(f) \mid f \in k(C),\ f \neq 0\}$$

since elementary calculations show that for any $f, g \in k(C)$:

- $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$
- $\operatorname{div}\left(f^{-1}\right) = -\operatorname{div}(f)$

To summarise there are the following inclusion of groups

$$\operatorname{Princ}(C) \subset \operatorname{Div}^0(C) \subset \operatorname{Div}(C)$$

Thus we can form the Picard group and the zero Picard group

$$\operatorname{Pic}(C) = \operatorname{Div}(C) / \operatorname{Princ}(C)$$
$$\operatorname{Pic}^0(C) = \operatorname{Div}^0(C) / \operatorname{Princ}(C)$$

Recall that a differential on C, regular at P can be written as $\omega = f\ dt$ where $f, t \in k(C)$. In fact, since C is assumed to be non singular, we can assume that t is a uniformizer at P, that is, $t(P) \neq 0$. Define $v_P(\omega) = v_p(f)$, and this is well defined for any choice of uniformizer t at P. Define a principal divisor corresponding to $\omega \in \Omega_C$,

$$\operatorname{div}(\omega) = \sum_{P \in C(\bar{k})} v_P(\omega)\, P$$

Observe that all principal divisors defined by regular differentials on C are linearly equivalent, and so they form a single element in the Picard group, $K_C = [\operatorname{div}(\omega)] \in \operatorname{Pic}(C)$. This K_C is called the canonical class of C.
Fact. $\deg(K) = 2g - 2$ for any representative K of K_C.

Let D be any divisor on C. The Riemann-Roch Space of D is

$$L(D) = \{f \in k(C) \,|\operatorname{div}(f) + D \geq 0\} \bigcup \{0\}$$

This is a finite dimensional k-vector space, and let $l(D)$ denote its dimension.Observe that

1 If $D \sim D'$, then $l(D) = l(D')$

2 $L(0) = k$

3 $L(D) = 0$ for all D with $\deg(D) < 0$.

Theorem 1. *(Riemann-Roch) Let C be a curve of genus g. Then for any divisor D on C*

$$l(L(D)) - l(L(K - D)) = deg(D) - g + 1$$

where K is any divisor representative of the canonical class K_C.
Corollary 2. *If $deg(D) \geq 2g - 1$, then $l(D) = deg(D) + 1 - g$.*
Corollary 3. *$l(K) = g$ where K is any representative of K_C.*

2.3 Classification of Curves

Let C be a curve over k of genus g. Using the Riemann-Roch theorem, it's possible to classify all curve of genus $g \leq 5$ with a market point $P \in C(k)$. The case $g = 3, 4$ are of special interest to us, as the models of these are used in Sections 4 and 5.

As in the previous subsection, results will be stated here without proof. For more details refer to [13, Pages 316 -355].

g=0

Let $P \in C(k)$. By the Riemann-Roch theorem, $l(P) = 2$, with P viewed as a degree 1 divisor. Thus, $L(D)$ is a 2 dimensional k-vector space. Take $\{1, f\}$ to be its basis. Then, one can check that

$$f : C \longrightarrow \mathbb{P}^1$$

is a degree 1 map, and therefore it defines an isomorphism $C \cong \mathbb{P}^1$.

g=1

Definition. A genus 1 curves C over k with a point $P \in C\left(\overline{k}\right)$ is called an elliptic curve.

An affine model of every elliptic curve is isomorphic to an affine curve with Weierstrass model

$$C : Y^2 + a_1XY + a_3 = X^3 + a_2X^2 + a_4X + a_6$$

for some $a_i \in k$. Furthermore, when the characteristic of k is different form 2 or 3, completing the square shows that C is isomorphic a curve with model

$$C' : Y^2 = X^3 + aX + b$$

where $a, b \in k$ and $4a^3 + 27b^2 \neq 0$.

g=2

A similar argument to the genus 1 case shows that every genus 2 affine curve has a model

$$C : y^2 + f_3(x)\, y = f_6(x) \text{ for some polynomials with } \deg(f_3) \leq 3, \deg(f_6) \leq 6$$

Moreover, when the characteristic of k is different from 2, with a suitable coordinate change, we can rewrite the above as

$$y^2 = F(x) \text{ where } F \text{ has degree 5 or 6.}$$

Canonical Embedding

Let C be a curve over k of genus $g \geq 3$. Recall $L(K)$ has dimension g, as a k vector space, for any representative K of the canonical class K_C. Let $\{f_1 \dots f_g\}$ be a basis of the Riemann Roch space. Define a map

$$\begin{gathered} \phi : C \longrightarrow \mathbb{P}^{g-1} \\ P \longmapsto [f_1(P) : \cdots : f_g(P)] \end{gathered}$$

This is a rational map which is independent of the choice of representative of K_C, and this map can be extended to a morphism. This is known as the canonical map.

The image of C in $\mathbb{P}^{g-1}$ is a degree $2g-2$ curve. For a non-hyperelliptic curve the canonical map is an embedding and for a hyperelliptic curve the map is 2 to 1.

Using the canonical embedding and basis facts about degree, including Bezout's theorem, we can conclude the following

- a genus 3 curve is either hyperelliptic or it's a plane quartic in $\mathbb{P}^2$, realised as the image of the canonical embedding
- a genus 4 curve is hyperelliptic or it's a sextic, the intersection of a quadric and a cubic surface in $\mathbb{P}^3$
- a genus 5 curve is either hyperelliptic or it's the intersection of 3 quadric surfaces in $\mathbb{P}^4$

2.4 Jacobians of Curves

Let C be a curve of genus g defined over a field k. The Jacobian of C, J_C, is an abelian variety over k and it is functionally associated to C.

There is also an analytic model of the Jacobian given in [6, Chapter 6].

If C is a genus g hyperelliptic curve, Casses and Flynn gave J_C the structure of a g dimensional, smooth and projective variety.
Theorem 4. *Let C be a hyperelliptic genus g curve over $\mathbb{Q}$., with Jacobian J_C. There is an embedding of J_C in $\mathbb{P}^{4^g-1}$ as smooth projective variety of dimension g, with defining equations given by quadratic forms and the group law given by a biquadratic map.*

Proof. See [2, Chapter 2]. □

For our purposes, an algebraic description of the Jacobian, is sufficient, and we use the following theorem as a definition.
Theorem 5. *For a curve C over k with $C(k) \neq \emptyset$, $J_C(k) \cong Pic^0(C)$.*

Proof. See [6, Chapter 6]. □

Therefore the elements of $J_C(k)$ can be represented by equivalence classes of degree 0 divisors on the curve.

The Jacobian can be used to define a group structure on $C(k)$. Suppose $P \in C(k)$. The Abel-Jacobi map associated to P is the embedding

$$\begin{aligned} C(k) &\hookrightarrow J_C(k) \\ Q &\longmapsto [Q-P] \end{aligned}$$

This suggest that we can view $C(k)$ as subset of $J_C(k)$, hence inheriting its group structure. Moreover if $J_C(k)$ is computable, then we can also compute $C(k)$.

There are various results concerning the computation of $J_C(k)$. Firstly, J_C is a g dimensional abelian variety over k, so $J_C\left(\overline{k}\right) \cong \mathbb{C}^g/\Lambda$ for some lattice $\Lambda \cong \mathbb{Z}^{2g} \subset \mathbb{C}^g$.
Notation. For any field extension $k \subset K$ and $n \geq 1$, let $J_C(K)[n]$ be the set of points of $J_C(K)$ of order n (where term order is used in the context of J_C being a group).

If n and $\mathrm{char}(k)$ are coprime, $J_C\left(\overline{k}\right) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.
Theorem 6. *(Mordell-Weil) If K is a number field, then $J_C(K)$ is finitely generated,*

$$J_C(K) \cong J_C(K)_{tors} \bigoplus \mathbb{Z}^r$$

where $J_C(K)_{tors}$ is a finite abelian group and $r \geq 0$ is an integer.

This integer r is called the rank of J_C over K.

From now on, our curves will be defined over $\mathbb{Q}$, so the Mordell-Weil theorem holds. The group $J_C(\mathbb{Q})$ will be referred to as the Mordell-Weil group of J_C.

3 Two Torsion Subgroup

Let C be a curve of genus g over $\mathbb{Q}$, J_C its Jacobian. We aim to determine the Mordell-Weil Group $J_C(\mathbb{Q})$. As previously stated

$$J_C(\mathbb{C}) \cong \mathbb{C}^g/\mathbb{Z}^{2g} \text{ and so } J_C(\mathbb{C})_{\text{tors}} \cong (\mathbb{Q}/\mathbb{Z})^{2g}$$

For a general curve, more than this cannot be said about the Mordell-Weil group. When C is a modular curve, there are various useful results, which in some cases can help to determine the Mordell-Weil group.
Note. Modular curves will not be defined in this report since the methods described in the sections which follow are applicable to any non-hyperelliptic curve of genus 3 or 4. We simply note that modular curves are curves with models over $\mathbb{Q}$ and some extra structure., see [6] for details.

Ozman and Siksek [17] computed the rational cuspidal subgroup $H = H_C(\mathbb{Q})$ of $J = J_C(\mathbb{Q})$, and gave a bound on the index $[J : H]$, for all non-hyperelliptic modular curves $C = X_0(N)$ of genus g where $3 \leq g \leq 5$ and for which $J_C(\mathbb{Q})$ is finite. The calculations relied on the fact that these are modular curves, for instance the existence of the subgroup H of J is consequence of the curves being modular. Also when computing the bound on the index, a theorem of Snowden can be used to compute the number of real components of $X_0(N)$, for any positive integers N, and this in turn can be used to give the precise presentation of $J(\mathbb{R})$ as finitely generated group, which can then be used with the embedding $J(\mathbb{Q})_{tors} = J(\mathbb{Q}) \subset J(\mathbb{R})$.

The subgroup H and the bound I on $[J : H]$ is often enough to determine the Mordell-Weil group. However, there are instances where this information eliminates all, but finitely many possibilities for J/H and hence for J. Additional information on the torsion is needed to compute the Mordell-Weil group in such cases. The following example is presented in the same paper.
Example. $X_0(45)$ is a genus 3 curve with $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and

$$J \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$$

To show $J = H$, it's sufficient to show that $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^3$. In this example, the authors computed the mod 2 representation of J and used this to show that $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^3$.

In fact, for all undetermined Mordell-Weil groups in [17], computing the rational two-torsion subgroup is sufficient to find the entire Mordell-Weil group.

Curve	Genus	Rational Cuspidal Subgroup H	J/H
$X_0(42)$	5	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$	0 or $\mathbb{Z}/2\mathbb{Z}$
$X_0(55)$	5	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$	0 or $\mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$
$X_0(63)$	5	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	0 or $\mathbb{Z}/2\mathbb{Z}$
$X_0(72)$	5	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	0 or $\mathbb{Z}/2\mathbb{Z}$
$X_0(75)$	5	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}$	0 or $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$

Observe that all of the above are genus 5 curves. Although we'll focus on the genus 3 and 4 cases, it's extremely likely that this methods presented in this report will generalise to higher genera.

3.1 Hyperelliptic Case

There is a direct method for computing the two torsion subgroup of a hyperelliptic curve. We'll follow the ideas of [7, Section 5.3]. Dolgachev uses the canonical embedding of a hyperelliptic curve and its ramification points, but the same ideas can be applied directly to the roots of the defining associated affine curve by carefully defining the sets B and $\widetilde{B}$ below.

Let C be a hyperelliptic curve of genus $g \geq 2$ over $\mathbb{Q}$. Recall that C is given by a single equation in the weighted projective plane $\mathbb{P}(1, 1, g+1)$

$$f_{2g+2}(t_0, t_1) - t_2^2 = 0 \subset \mathbb{P}_{t_0,t_1,t_2}(1, 1, g+1)$$

where $f_{2g+2} \in \mathbb{Q}[t_0, t_1]$ is a homogeneous polynomial of degree $2g+2$, and it is square free.

This can be dehomogenised to obtain the standard affine hyperelliptic curve C', which is given by

$$F(x) - y^2 = 0 \subset \mathbb{A}^2_{x,y}$$

where $F \in \mathbb{Q}[x, y]$ is a square free polynomial of degree $2g+1$ or $2g+2$., $F(x) = f_{2g+2}(x, 1)$ and $x = t_0/t_1$, $y = t_2/t_1^{g+1}$.

Definition. The points where $t_1 = 0$ are called the points at infinity of C.

When $\deg(F) = 2g+1$, F can be written as $F(x) = c\prod_{i=1}^{2g+1}(x - r_i)$, for some non-zero $c \in \mathbb{Q}$ and some distinct rational numbers $r_1, \ldots, r_{2g+1}$. Substituting $x = t_0/t_1$ and $y = t_2/t_1^{g+1}$ in this expression above

$$\frac{t_2^2}{t_1^{2g+2}} = c\prod_{i=1}^{2g+1}\left(\frac{t_0}{t_1} - r_i\right)$$
$$t_2^2 = t_1 c\prod_{i=1}^{2g+1}(t_0 - r_i y_1)$$

so when $t_1 = 0$, then $t_2 = 0$ so $t_0 = 1$. We conclude that there is a unique point at infinity on C, $P_\infty = (1 : 0 : 0)$.

When $\deg(F) = 2g+2$, F can be written as $F(x) = c\prod_{i=1}^{2g+2}(x - r_i)$, for some non-zero $c \in \mathbb{Q}$ and some distinct rational numbers $r_1, \ldots, r_{2g+2}$. Substituting $x = t_0/t_1$ and $y = t_2/t_1^{g+1}$ in this expression above

$$\frac{t_2^2}{t_1^{2g+2}} = c\prod_{i=1}^{2g+2}\left(\frac{t_0}{t_1} - r_i\right)$$
$$t_2^2 = c\prod_{i=1}^{2g+2}(t_0 - r_i y_1)$$

so when $t_1 = 0$, then taking $t_1 = 1$ gives $t_2^2 = c$. We conclude that there are two points are infinity on C, $P_{\infty_+} = (1 : 0 : \sqrt{c})$ and $P_{\infty_-} = (1 : 0 : -\sqrt{c})$.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of F, where $n = \deg(F)$. Define

$$B = \begin{cases} \{\alpha_1, \ldots, \alpha_{2g+2}\} & \text{if } n = 2g+2 \\ \{\alpha_1, \ldots, \alpha_{2g+1}\} \cup \{P_\infty\} & \text{if } n = 2g+1 \end{cases}$$

For any subset of even cardinality $U \in B$, define

$$B = \begin{cases} D_U = \sum_{\alpha \in U} (\alpha : 1 : 0) \ - \ \frac{|U|}{2}\left(P_{\infty_+} + P_{\infty_-}\right) & \text{if } n = 2g+2 \\ D_U = \sum_{\alpha \in U*} (\alpha : 1 : 0) \ - \ |U| P_\infty & \text{if } n = 2g+1 \end{cases}$$

Notation. By $\sum_{\alpha \in U*} (\alpha : 1 : 0)$ we mean that if $\alpha = \alpha_i$ for some i, then let $(\alpha : 1 : 0) = (\alpha_i : 1 : 0)$ and if $\alpha = P_\infty$ then let $(\alpha : 1 : 0) = P_\infty$.

Let $\widetilde{B} = \{[D_U] \in \mathrm{Pic}^0(C) : U \subset B \text{ of even cardinality}\}$. Observe that for any root α of F, $t_0 - t_1\alpha \in \mathbb{Q}(C)^*$ and

$$\mathrm{div}(t_0 - t_1\alpha) = \begin{cases} 2(\alpha : 1 : 0) - P_{\infty_+} - P_{\infty_-} & \text{if } n = 2g+2 \\ 2(\alpha : 1 : 0) - 2P_\infty & \text{if } n = 2g+1 \end{cases}$$

Therefore $[D_U] \in J_C[2]$ fro all subsets $U \subset B$ of even cardinality.
Theorem 7. $J_C[2] = \widetilde{B}$

Proof. Suppose $[D_X] = [D_Y]$ for some $X, Y \subset B$ of even cardinality. Then $D_X - D_Y$ is a principal divisor. By definition of D_Us,

$$D_X - D_Y = D_{X \diamond Y}$$

where $X \diamond Y = (X \cup Y) \ (X \cap Y)$.

Claim. *D_U is principal if and only if $U \in \{B, \emptyset\}$*

As $D_\emptyset = 0$, the zero divisor, this is clearly principal. Also $D_B = \mathrm{div}\left(\frac{t_2}{(bt_0 - at_1)^{g+1}}\right)$, so D_B is principal.

Observe that $D_U = D_B + D_U = D_{B \setminus U}$ for any $U \subset B$ of even cardinality, so $[D_U] = \left[D_{B \setminus U}\right] \in \widetilde{B}$

Suppose $D_U = \mathrm{div}(\phi)$ for some $\phi \in \mathbb{Q}(C)$. Replacing U by $B \setminus U$, we can assume that U doesn't contain the points at infinity and $|U| \leq g$. Thus ϕ has no poles at the points at infinity and is a polynomial in $x = t_0/t_1$ and $y = t_2/t_1^{g+1}$. The function y has $2g+1$ or $2g+2$ poles, but the divisor of ϕ has degree $\leq g$, hence ϕ must be a polynomial in x only.

If $U \neq \emptyset$, then $(x - \alpha)$ divides ϕ for some $\alpha \in U$. The divisor of $x - \alpha$ has a pole at a point at infinity, so ϕ has a pole, contradicting the previous statement. Thus $U = \emptyset$.

Hence $D_X \sim D_Y$ only if $Y \in \{X, B \setminus X\}$, and so

$$\widetilde{B} = \{[D_U] \in \mathrm{Pic}^0(C) : U \subset B \text{ of even cardinality and } \ |U| \leq g\}.$$

As B has cardinality $2g+2$, by a well known theorem it has 2^{2g+1} subsets of even cardinality, only half of which define distinct divisor classes $[D_U,]$, so $|\widetilde{B}| = 2^{2g} (= |J_C[2]|)$ and therefore $\widetilde{B} = J_C[2]$. $\square$

The above theorem shows that two torsion subgroup of the Jacobian of a hyperelliptic curve can be fully determined by computing the roots of the affine equation F and forming the divisors D_U.

The non-hyperelliptic case is not as direct and we require some background on symplectic spaces and theta characteristics.

3.2 Theta Characteristics

We'll provide a summary of [7, Chapter 5], and give the background required by our strategy for computing the two torsion subgroup of the Jacobian of a non-hyperelliptic curve.

3.2.1 Symplectic Spaces and Quadratic Forms

Definition. A symplectic space over a field k is a pair (V, b_V), where V is a finite dimensional k vector space and b_V is a nondegenerate alternating bilinear form on V.
Definition. A quadratic form q on (V, b_v) is a quadratic form on V, such that the corresponding alternating form $b_q(v, w) := q(v + w) - q(v) - q(w)$ coincides with b_V on V.
Remark. When the characteristic of k is not 2, given b_q we can recover the quadratic form q in a unique way, $2q(v) = b_q(v, v)$. However when k has characteristic 2, many quadratic forms correspond to the same bilinear form b_q.
Lemma 8. *Any symplectic space (V, b_V) is even dimensional and it admits a basis*

$$B = (e_1, \ldots, e_n, f_1, \ldots f_n)$$

with the following properties:

- $b_V(e_i, e_j) = b_V(f_i, f_j) = 0$ *for all* i, j
- $b_V(e_i, f_j) = \delta_{i,j}$ *for all* i, j

Note. A basis as above is called a symplectic basis.

Proof. See [14, Lemma1.2] □

Fix a symplectic space (V, b_V) over $\mathbb{F}_2$, with a symplectic basis $(e_1, \ldots, e_n, f_1, \ldots f_n)$. Let $Q(V)$ be the set of quadratic forms on (V, b_V). For any $q \in Q(V)$ and $v \in V$, a new quadratic form $q + v \in Q(V)$ can be defined by

$$(q + v)(x) = q(x) + b_V(v, x) \text{ for all } x \in V$$

The addition of two quadratic forms $q, q' \in Q(V)$ is also well defined by setting $q + q' = v \in V$ where v is a unique element of V with $q' = q + v$. In this way, $\widetilde{V} = Q(V) \sqcup V$ is a $2g + 1$ dimensional vector space over $\mathbb{F}_2$.
Definition. Let $q \in Q(V)$. The Arf invariant of q is

$$\operatorname{Arf}(q) = \sum_{i=1}^{n} q(e_i)\, q(f_i) \mod 2$$

Proposition 9. *The Arf invariant of any $q \in Q(V)$ is well defined and it's independent of the choice of symplectic basis.*

Proof. See [8, Page 36]. □

Definition. A quadratic form on (V, b_V) is called odd, resp. even, if $\operatorname{Arf}(q) = 1$, resp. 0.

Let $Q(V)_+$ be the set of even quadratic forms and $Q(V)_-$ the set of odd quadratic forms.

There is a natural action of the symplectic group $\mathrm{Sp}(V)$ on $Q(V)$. For any $T \in \mathrm{Sp}(V), q \in Q(V)$ define $T \cdot q \in Q(V)$ by

$$(T \cdot q)(x) = q\left(T^{-1}(x)\right) \text{ for all } x \in V$$

The two orbits of this action are $Q(V)_+$ and $Q(V)_-$.

3.2.2 Two Torsion Subgroup as a Symplectic Space

Let C be a genus g curve over a field $\mathbb{Q}$ and $J_C[2] = J_C\left(\overline{\mathbb{Q}}\right)[2]$ the two torsion subgroup. of its Jacobian. Recall that $J_C[2] \cong \mathbb{F}_2^{2g}$, and so $J_C[2]$ can be regarded as a $2g$-dimensional vector space over $\mathbb{F}_2$. Moreover, it is a symplectic space with the Weil pairing which can be defined as follows.

For any $f \in k(C) \setminus \{0\}$ and any divisor $D = \sum_{P \in C} n_P P$ on C with support disjoint form the support of $\mathrm{div}(f)$, define $f(D) = \prod_{P \in C} f(P)^{n_P}$.

Remark. Observe that $f(D_1 + D_2) = f(D_1) f(D_2)$ for any two divisors D_1, D_2 with support disjoint from $\mathrm{div}(f)$.

Theorem 10. *(Weil Reciprocity Law) For any $f, g \in k(C) \setminus \{0\}$ with disjoint support*

$$f(div(g)) = g(div(f))$$

Proof. See [11, Page 242]. □

Let $E_1, E_2 \in J_C[2]$, and take any representatives of these classes D_1, D_2 such that $2D_i = \mathrm{div}(f_i)$ for some $f_i \in k(C) \setminus \{0\}$ whose divisors have disjoint support.

Observe that

$$\left(\frac{f_1(D_2)}{f_2(D_1)}\right)^2 = \frac{f_1(2D_2)}{f_2(2D_1)} = \frac{f_1(\mathrm{div}(f_2))}{f_2(\mathrm{div}(f_1))} = 1$$

Thus $\frac{f_1(D_2)}{f_2(D_1)} = \pm 1$, and define

$$e_2(E_1, E_2) = \begin{cases} 1 \text{ if } f_1(D_2)/f_2(D_1) = -1 \\ 0 \text{ otherwise} \end{cases}$$

This is known as the Weil pairing on $J_C[2]$.

Suppose $D_1' = D_1 + \mathrm{div}(h_1)$ and $D_2' = D_2 + \mathrm{div}(h_2)$ for two rational function h_1, h_2 on C. Applying the Weil Reciprocity Law twice shows that

$$\frac{f_1\left(D_2'\right)}{f_2\left(D_1'\right)} = \frac{f_1(D_2) f_1(\mathrm{div}(h_2))}{f_2(D_1) f_2(\mathrm{div}(h_1))} = \frac{f_1(D_2) h_2(\mathrm{div}(f_1))}{f_2(D_1) f_1(\mathrm{div}(f_2))} = \frac{f_1(D_2)}{f_2(D_1)} \left(\frac{h_2(D_1)}{h_1(D_2)}\right)^2 = \frac{f_1(D_2)}{f_2(D_1)}$$

hence the Weil pairing is independent of the choice of representatives of E_1 and E_2, and thus it is well defined.

Elementary calculations show that

- e_2 is bilinear
- e_2 is symplectic : $e_2(E, E) = 0$ for all $E \in J_C[2]$

- e_2 is alternating : $e_2(E_1, E_2) = -e_2(E_2, E_1)$ for all $E_i \in J_C[2]$

and therefore the Weil pairing defines a nondegenerate alternating bilinear form on $J_C[2]$ with values in $\mathbb{F}_2$, giving $J_C[2]$ the structure of a $2g$-dimensional symplectic space over $\mathbb{F}_2$.

3.2.3 Theta Characteristics

Fix a curve C of genus g over a field $\mathbb{Q}$. Let J_C be its Jacobian with $J_C[2] := J_C\left(\overline{\mathbb{Q}}\right)[2]$ the two torsion subgroup.
Definition. A theta characteristic on C is a divisor class $\theta \in \mathrm{Pic}^{g-1}(C)$ with $2\theta = K_C$, where K_C is the canonical class of the curve C.

Let $\mathrm{TChar}(C)$ be the set of theta characteristics on C. For any $\theta_1, \theta_2 \in \mathrm{TChar}(C)$, $2\theta_1 - 2\theta_2 = K_C - K_C = 0$ and so $\theta_1 - \theta_2 \in J_C[2]$. so there are 2^{2g} theta characteristics.
Definition. The parity of a theta characteristic θ is the parity of $l(\theta)$, the dimension of the Riemann Roch space $L(\theta)$.
Fact. A curve of genus g has $2^{g-1}(2^g + 1)$ even theta characteristics and $2^{g-1}(2^g - 1)$ odd theta characteristics.

For any $\theta \in \mathrm{TChar}(C)$ and define

$$q_\theta : J_C[2] \longrightarrow \mathbb{F}_2$$

$$E \longmapsto l(\theta + E) + l(\theta) \mod 2$$

Theorem 11. *(Riemann-Mumford Relation) The function q_θ defined by any theta characteristic θ is a quadratic form on $J_C[2]$. The associated bilinear form $b_\theta(E_1, E_2) = q_\theta(E_1 + E_2) - q_\theta(E_1) - q_\theta(E_2)$ coincides with the Weil pairing e_2 on $J_C[2]$. Moreover, the function*

$$\begin{aligned} TChar(C) &\longrightarrow Q(J_C[2], e_2) \\ \theta &\longmapsto q_\theta \end{aligned}$$

is a bijection.

Proof. See [12, Theorem 1.13] □

Recall that $q \in Q((J_C[2], e_2))$ were defined to be even or odd depending on the value of the Arf invariant. This is consistent with the parity the theta characteristic θ defining $q = q_\theta$.
Theorem 12. *For any $\theta \in TChar(C)$, q_θ is an odd quadratic form if and only if θ is an odd theta characteristic.*

Proof. See [16, Page 186] □

From now on we'll identify the set odd quadratic forms on $(J_C[2], e_2)$ with the odd theta characteristics of C.

Let (V, b_V) be any symplectic space over $\mathbb{F}_2$ of dimension $2n$ and let $\mathbb{S}$ be the set of unordered pairs of elements in $Q(V)\_$. In 3.2.1 we defined addition on $Q(V)$, which can restricted to odd quadratic forms to give a map

$$s : \mathbb{S} \longmapsto V \setminus \{0\}$$

Definition. For any $v \in V \setminus \{0\}$ let $\sum(v) = \bigcup_{\alpha \in s^{-1}(v)} \alpha$, this is called a Steiner complex of V.

Theorem 13. *For an arbitrary symplectic space over $\mathbb{F}_2$ of dimension $2n$ there are $2^{2n} - 1$ Steiner complexes. Each Steiner complex consists of $2^{n-1}\left(2^{n-1} - 1\right)$ elements paired by translation $q \mapsto q + v$. An odd quadratic form q belongs to a Steiner complex $\sum(v)$ if and only if $q(v) = 0$.*

Proof. See [7, Page 227-228] □

Applying this theorem to $(J_C[2], e_2)$, since $|J_C[2] \setminus \{0\}| = 2^{2g} - 1$, Theorem 13 shows that the map defined by addition :

$$Q(J_C[2], e_2)_- \times Q(J_C[2], e_2)_- \longrightarrow J_C[2]$$

is a surjection. By Theorem 12 we can identify $Q(J_C[2], e_2)_-$ and the odd theta characteristics, and so by this identification, the surjectivity of addition and the definition of this addition, we conclude that all element of $J_C[2]$ can be expressed as $\theta_1 - \theta_2$, where θ_1, θ_2 are two odd theta characteristics.

The fact that the set differences of 2 odd theta characteristics generate the two torsion subgroup will be a key fact in our computation of $J_C[2]$ for non-hyperelliptic curves of genus 3 and 4. This can also be used in computing $J_C[2]$, for hyperelliptic curves of any genus, for details see [7, Section 5.3]. However this algebraic machinery is not necessary in that case since the direct method presented in (3.1) is computationally very effective.

3.2.4 Odd Theta Characteristics and Theta Hyperplanes

When C is non-hyperelliptic of genus 3 or 4, odd theta characteristics of C can be interpreted geometrically.
Definition. Let $C \subset \mathbb{P}^{g-1}$ be a canonical curve of genus g, over a field $\mathbb{Q}$. A theta hyperplane to C is a hyperplane which is everywhere tangent to C.

For non-hyperelliptic curves, the theta hyperplanes are bitangent lines in the genus 3 case and tritangent planes in the genus 4 case. We'll prove that in both cases, there is a bijection between the set of theta hyperplanes and the set of odd theta characteristics of the curve.

Recall that a genus 3 or 4 non-hyperelliptic curve can be viewed as the image of the embedding defined by a canonical divisor, which makes the canonical divisor very ample. We'll require some background on the canonical embedding, for more details see [13].

Suppose C is curve over an algebraically closed field k. Given any divisor D on C, any k basis of $L(D)$, $f_1, \ldots, f_n$ defines a map $\varphi_D : C \to \mathbb{P}^{n-1}$, $P \longmapsto (f_1(P) : \ldots : f_n(P))$.
Definition. A divsor D is called very ample if φ_D is an isomorphism onto its image
Theorem 14. *A divisor D is very ample if and only if the following conditions hold*

1. $l(D - P) = l(D) - 1$ *for all* $P \in C$
2. $l(D - P - Q) = l(D) - 2$ *for all* $P, Q \in C$

Proof. See [13, IV.3, Proposition 3.1]. □

Proposition 15. *Suppose C is curve of genus $g \geq 2$ over an algebraically closed field. A canonical divisor is very ample if and only if C is not hyperelliptic*

Proof. See [13, IV.5 Proposition 5.2] □

Proposition 16. *Suppose C is non-hyperelliptic. Any effective canonical divisor on C is of the form $C \cdot H$, where H is a hyperplane.*

Proof. See [13, IV.5, Proposition 5.3] □

Theorem 17. *(Clifford) Suppose C is non-hyperelliptic and D is a divisor with $l(K - D) > 0$. Then*

$$l(D) - 1 \leq \tfrac{1}{2} deg(D)$$

Proof. See [13, IV.5 Theorem 5.4] □

Let C be a genus 3 plane quartic over $\mathbb{Q}$. This may be viewed as a curve over $\overline{\mathbb{Q}}$, and any canonical divisor K_C is very ample. Let L be any bitangent to the curve. Then $C \cdot L = 2D_L$, where D_L is a degree 2, effective divisor $P+Q$ for some $P, Q \in C$. By Proposition 16, $C \cdot L = 2D_L$ is canonical, so D_L is a theta characteristic.

Also K_C is very ample, so $l(D_L) = l(K_C - P - Q) = l(K_C) - 2 = 1$, and so D_L is an odd theta characteristic. Therefore, this defines a map ϕ, from the bitangents to C, to the odd theta characteristics of C, $\phi(L) = D_L$.

Theorem 18. *The map ϕ, as described above, is a bijection from the set of bitangents to C, to the set of odd theta characteristics of C.*

Proof. For any odd theta characteristic θ, $l(\theta) > 0$ and $\deg(\theta) = 2$, so there exists a degree 2, effective divisor E equivalent to θ, $E = P + Q$, for some $P, Q \in C$. Let L be a line through P and Q. Then $C \cdot L = P + Q + R + S$ for some $R, S \in C$ and $C \cdot L \sim K_C$ by (16). Thus $P + Q + R + S \sim 2(P + Q)$ so $P + Q \sim R + S$. By the above argument $l(P + Q) = 1$ and so $P + Q = R + S$, that is $C \cdot L = 2(P + Q)$, and L is a bitangent, with $\phi(L) = 2\theta$, so ϕ is surjective.

Suppose $\phi(L_1) = \phi(L_2)$ for two bitangents L_1, L_2. Then there exists points $P, Q, R, S \in C$ with $2(P + Q) = 2(R + S)$. Then $P+Q \sim R+S$, so $P+Q-R-S = \operatorname{div}(f)$ for some $f \in L(P + Q)$. By the above arguments $l(P + Q) = 1$, so f must be a constant and $P + Q = R + S$, hence ϕ is injective. □

Note. A similar argument to the one above can be found in [1].

Corollary 19. *A plane quartic curve has 28 bitangent lines.*

There is an analogues argument for the genus 4 case .Let C be a non-hyperelliptic genus 4 curve over $\mathbb{Q}$, that is, a smooth sextic in $\mathbb{P}^3$, the intersection of a smooth quadric and a smooth cubic surface. If T is any tritangent plane to C, then $C \cdot T = 2D_T$, where D_T is an effective degree 3 divisor $D_T = P + Q + R$ for some $P, Q, R \in C$.

Define a map $\pi(T) = D_T$ from the set of tritangent planes to C to the theta characteristics of C.

Theorem 20. *The map ϕ, as described above, is a bijection from the set of tritangent planes to C to the set of odd theta characteristics of C.*

Proof. A very clear proof of this is presented in [12, Theorem 2.2]. The argument is very similar to the genus 3 case. □

Corollary 21. *A smooth sextic has 120 tritangent planes.*

To find the two-torsion subgroup of the Mordell Weil group of non-hyperelliptic curves of genus 3 and 4 we have the following strategy.

1. Find all the theta hyperplanes to the curve. These can be considered as non-zero rational functions on the curve.
2. All two torsion points on the Jacobian are of the form D where $2D = \operatorname{div}(l_1) - \operatorname{div}(l_2)$, and l_1,l_2 are theta hyperplanes.
3. Among the above divisors D we select the ones which are fixed by the action of the absolute Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. These form the two torsion subgroup of the Mordell-Weil group.

4 Scheme of Theta Hyperplanes

To find the two-torsion subgroup of the Jacobian of a non-hyperelliptic canonical curves of genus 3 and 4, we begin by finding the bitangents lines and the tritangent planes to these curves. From now on, all curves will be non-hyperelliptic, so a genus 3 curve will exclusively be a plane quartic and a genus 4 curve will be interpreted as a sextic in $\mathbb{P}^3$, the intersection of a quadric surface and a cubic surface.

The coefficients of the theta hyperplanes to these curves will be points on zero dimensional schemes of degree 28 in the genus 3 case and 120 in the genus 4 case. In this section we'll show how to solve these schemes over a finite field and subsequently describe the theta hyperplanes to a reduction of the curve. We'll also describe a method of 'lifting' these reductions in order to obtain better approximation for the corresponding theta hyperplane to the rational curve. In the next section we'll describe a method for finding the theta hyperplanes to the rational curve using these lifts.
Note. Schemes are not precisely defined in this report. They are simply considered to be generalisations of varieties, which keep track of the defining equations. For more details on schemes, see [13, Chapter 2].

4.1 Bitangents over Finite Fields

Let C be a genus 3 curve over $\mathbb{Q}$, so it has a model,

$$C \ : \ f(x,y,z) = 0 \ \subset \mathbb{P}^2$$

where $f \in \ \mathbb{Q}[x,y,z]$ is a homogeneous polynomial of degree 4. Clearing denominators, we can always assume that f has integer coefficients.

We work on an affine chart and dehomogenise with respect the appropriate coordinates. For notation purposes we'll work on the affine chart $\{z=1\}$.

A bitangent to the corresponding affine curve on this chart is given by a line

$$b_1 x + b_2 y + b_3 = 0$$

for some $b_i \in \overline{\mathbb{Q}}$ with $(b_1, b_2) \neq (0,0)$.
Suppose that $b_1 \neq 0$, so the bitangent is given by

$$x = a_1 y + a_2$$

for some $a_i \in \overline{\mathbb{Q}}$. The intersection of the affine curve with this bitangent is described by

$$F(y) = f(a_1 y + a_2, y, 1)$$

a degree 4 polynomial in y. As the line intersects the curve at 2 points, each with multiplicity 2 , F must be square, and hence there exist $a_3, a_4 \in \overline{\mathbb{Q}}$ such that

$$F(y) = l\left(y^2 + a_3 y + a_4\right)^2$$

where l is the coefficient of y^4 in F. Equating coefficients in the above expression gives 4 equations $f_1, f_2, f_3, f_4 \in \mathbb{Z}[a_1, a_2, a_3, a_4]$. Let S be the scheme over the rational numbers defined by these equations. This is has dimension 0 and degree at most 28.
Remark. In the simplest case S will have degree 28 and so the points of S will represent the complete set of bitangents to C. This is not always the case, as the bitangents don't necessarily all lie in the same affine chart and even when they do, the bitagents in an affine chart may not all be of the same form, for example the case $b_1 = 0$ should also be considered in the above argument.

However the above calculations and what follows can be repeated,on all affine charts and for all possible forms of bitanngents, to obtain a complete description of the bitangents to the curve.

For simplicity suppose that S, as previously defined, has degree 28.

Let p be an odd prime of good reduction for C and S. Denote by S_p the scheme S viewed as a scheme over $\mathbb{F}_p$, where the coefficients defining equation of S are reduced modulo p to describe S_p. The reductions of the four equations f_1, f_2, f_3, f_4 can be efficiently solved over the finite field $\mathbb{F}_p$ to give all points on the scheme $S_p(\mathbb{F}_p)$.

Ideally we would like to choose a rational prime p such that $S_p(\mathbb{F}_p)$ contains exactly 28 points. In practice this is often not possible as most bitangents are defined over $\overline{\mathbb{Q}}$ and not $\mathbb{Q}$. If the K_b is the number field over which the bitangents are defined, it is possible that the prime p ramifies in the ring of integers of K_b, and so residue field over which we search for the reduced bitangents, will have p^n elements for some $n > 1$.

Let S_{p^n} be the scheme obtained by changing the base field of S to $\mathbb{F}_{p^n}$, for some $n \geqslant 1$ and p a prime of good reduction for C and S, and as before compute the points of this $S_{p^n}(\mathbb{F}_{p^n})$. Assuming that S has degree 28, for a good choice of p and n, $S_{p^n}(\mathbb{F}_{p^n})$ should have 28 points.
Remark. Changing the base field of S and finding the points over an arbitrary field of p^n elements can be done efficiently in Magma.

Given such p and n, we choose a number field K such that its ring of integers O_K has a prime ideal $\mathfrak{p}$ of norm p^n. Then $\mathbb{F}_{p^n} \cong O_K/\mathfrak{p}$ and denote by $S_{\mathfrak{p}}$ the scheme S viewed over the field $O_K/\mathfrak{p}$. Observe that the defining equations of S have integer coefficient which can be embedded in O_K and reduced modulo $\mathfrak{p}$ to give the defining equations of $S_{\mathfrak{p}}$.
Remark. Although this sounds troublesome, it's often the case that K is a quadratic or cubic number field, and p is a small prime. In the examples of Sections 7 and 8, a short search gave a good pair (p, n) and a number field K. As previously noted, this search is easy to implement using Magma.

It is now a finite computation to find 28 all common solutions $(a_1, a_2, a_3, a_4) \in (O_K/\mathfrak{p})^4$ to the reductions of f_1, f_2, f_3, f_4. These completely describe the bitangents to the reduction of the affine curve modulo $\mathfrak{p}$,

$$x = a_1 y + a_2$$

In general this method will produce the set of coefficient of bitangents $(\alpha_1, \alpha_2, \alpha_3)$ where $\alpha_i \in O_K/\mathfrak{p}$, for some number field K and prime ideals $\mathfrak{p}$, and the bitangents of the reduced curve are of the form

$$\alpha_1 x + \alpha_2 y + \alpha_3 z = 0$$

See Section 7 for an example of this.

4.2 Tritangents over Finite Fields

In this section we'll describe a method for obtaining that 120 tritangent planes, defined over a finite field, to a reduction of a genus 4 curve. This is similar to the bitangents case, with small differences in how the scheme is defined.

Let C be a genus 4 curve over $\mathbb{Q}$. The curve C is given by the intersection of a quadric and a cubic surface, with a model

$$C : f(x, y, z, k) = g(x, y, z, k) = 0 \subset \mathbb{P}^3$$

where $f, g \in \mathbb{Q}[x, y, z, k]$ are homogeneous of degree 2 and 3 respectively. As before, clearing denominators we may assume that f, g have integer coefficients.

We work on an affine chart and dehomogenise the equations with respect to the appropriate coordinates. To simplify notation we work on the affine chart $\{k = 1\}$.

On this chart, a tritangent plane may be given by an equation

$$x = a_1 y + a_2 z + a_3$$

for some $a_i \in \overline{\mathbb{Q}}$.
Remark. As in the bitangents case, assuming that all tritangents are described by equations with non-zero x coefficient is a generalisation. This can be assumed for now as the method presented here can be repeated to cover all possible cases.

The intersection of the affine curve with the plane is given by

$$F(y, z) = f(a_1 y + a_2 z + a_3, y, z, 1)$$
$$G(y, z) = g(a_1 y + a_2 z + a_3, y, z, 1)$$

Taking the resultant of these with respect to z gives

$$R = \mathrm{Res}(F, G, z)$$

a degree 6 polynomial in y. As the plane intersects the curve in 3 points, each with multiplicity 2, R is square and hence there exist $a_4, a_5, a_6 \in \overline{\mathbb{Q}}$ with

$$R(y) = l\left(y^3 + a_4 y^2 + a_5 y + a_6\right)^2$$

where l is the coefficient of y^6 in $R(y)$.
Equating coefficients in the above expression give 6 equation $c_1 \dots c_6$ in the unknowns $a_1 \dots a_6$. As before, we use these to define a zero dimensional scheme. The same method as in the bitangents case can be used to solve this over a finite field consisting of p^n elements and give the 120 tritangents to a reduction of the curve C.

See Section 8 for an example of this.

4.3 Hensel Lifting

In this subsection, we work with the genus 3 case. The exact same method can be applied to the genus 4 case.

Let C be a genus 3 curve over $\mathbb{Q}$. Given a bitangent to the reduction of C at a prime ideal $\mathfrak{p}$ of some number field K,

$$\alpha_1 x + \alpha_2 y + \alpha_3 z = 0$$

We'll describe a method for finding the "lifts" of the coefficients of this bitangent modulo $\mathfrak{p}^k$ for each $k \geq 1$.
Definition. Let S be a finite rational scheme with good reduction at a prime $\mathfrak{p}$ of a number field K. Given a point on the reduced scheme $(\alpha_1, \dots, \alpha_n) \in (O_K/\mathfrak{p})^n$, a lift of this point modulo $\mathfrak{p}^k$ for any $k \geq 1$ is a point $(\alpha_{1,k}, \dots, \alpha_{n,k}) \in \left(O_K/\mathfrak{p}^k\right)^n$, where $(\alpha_{1,1}, \dots, \alpha_{n,1}) = (\alpha_1, \dots, \alpha_n)$ and

1. $\alpha_{i,k} \equiv \alpha_{i,k-1} \bmod \mathfrak{p}^{k-1}$ for all $k \geq 1$ and $i = 1, \dots n$
2. $(\alpha_{1,k}, \dots, \alpha_{n,k})$ solves the equations defining the rational scheme modulo $\mathfrak{p}^k$ for each $k \geq 1$
3. $\widetilde{\alpha_i} \equiv \alpha_{i,k} \bmod \mathfrak{p}^k$ for all $k \geq 1$, where $(\tilde{\alpha}_1, \dots, \tilde{\alpha}_n)$ is the point on to the rational scheme S which reduced to $(\alpha_1, \dots, \alpha_n)$ modulo $\mathfrak{p}$.

Note. The coefficient of the reduce bitangent $(\alpha_1, \alpha_2, \alpha_3)$ are part of tuples of points on the reduced scheme of bitangent coefficients. We'll find the lifts of the points of the reduces schemes of bitangents.

To find these lifts, we'll use a multivariate generalisation of Hensel's lemma.
Theorem 22. *(Hensel's Lemma) Let k be a number field and k_ν a non-Archimedean completion of k. Let O_ν denoted the ring of integers of k_ν. If $f \in O_\nu[x]$ and $x_0 \in O_\nu$ is such that*

$$| f(x_0) |_\nu < \left(| f'(x_0) |_\nu \right)^2$$

Then there exists a unique $x \in O_\nu$ satisfying:

$$| x - x_0 |_\nu < | f'(x_0) |_\nu \text{ and } f(x) = 0$$

Proof. See a complete argument [4, Theorem 4.1]. The ideas of the proof are summarised below. □

The proof of the above is based on the following identify, which is in fact a simple Taylor expansion of f about x,

$$f(x+y) = f(x) + f'(x)\, y + g(x)\, y^2$$

for all $f \in O_\nu[x]$, $y \in O_\nu$,with a unique $g \in O_\nu[x]$.

For any $n \geq 1$, define $a_{n+1} = a_n - f(a_n)/f'(a_n)$ where $a_1 = x_0$. Using the above identify, it's possible to show that the required point x is the limit of the sequence $(a_n)_{n\geq 1}$.

There is an analogue of Hensel's Lemma and of the above identify.
Lemma 23. *With k, ν and o_ν as above, let $F = (f_1 \dots f_n)$ for some $f_i \in O_\nu[x_1, \dots, x_n]$. Then for any $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$*

$$F(\mathbf{x}+\mathbf{y}) = F(\mathbf{x}) + ((DF)(\mathbf{x}))\,\mathbf{y} + R(\mathbf{x}, \mathbf{y})$$

where

- $DF(\mathbf{x})$ *is the Jacobian matrix*
- $R(\mathbf{x}, \mathbf{y}) = (R_1(\mathbf{x}, \mathbf{y}), \dots, R_n(\mathbf{x}, \mathbf{y}))$
- $R_k(\mathbf{x}, \mathbf{y}) = \sum_{1 \leq i,j \leq d} c_{ijk}(\mathbf{x}, \mathbf{y})\, y_i y_j$ *for some* $c_{ijk}(\mathbf{x}, \mathbf{y}) \in O_\nu[\mathbf{x}, \mathbf{y}]$.

Proof. See [5, Pages 5-6] □

This is used to prove the following generalisation of Hensel's lemma.
Theorem 24. *(Multivariate Hensel's Lemma) Let k be a number field and k_ν a non-Archimedean completion. Let O_ν denoted the ring of integers of k_ν. If $F \in O_\nu[x_1, \dots, x_n]$ and $\mathbf{x_0} \in O_\nu^n$ is such that*

$$\| F(\mathbf{x_0}) \| < \left(| J_F(x_0) |_\nu \right)^2$$

Then there exists a unique $\mathbf{x} \in O_\nu^n$ satisfying:

$$\| \mathbf{x} - \mathbf{x_0} \| < | J_F(x_0) |_\nu \text{ and } F(x) = 0$$

where J_F is the determinant of the Jacobian

Here $\| \cdot \|$ is the norm on k^n, defined as $\| \mathbf{x} \| = \max_{1 \leq i \leq n} | x_i |_\nu$.

Proof. See [5, Theorem 2.1] □

As before, define a sequence $\mathbf{a_{n+1}} = \mathbf{a_n} - (DF(\mathbf{a_n}))^{-1} F(\mathbf{a_n})$ where $\mathbf{a_1} = \mathbf{x_0}$. Using Lemma 23, it's possible to show that the required point $\mathbf{x}$ is the limit of the sequence $(\mathbf{a_n})_{n\geq 1}$.

Return to the setting of Section 4.1 and fix a reduced bitangent

$$x = a_1 y + a_2$$

where $a_i \in O_K/\mathfrak{p}$ for some number field K and prime ideal $\mathfrak{p}$, where $\mathfrak{p}$ lies above a rational prime p, which is a prime of good reduction for both C and S, the scheme of (some) bitangent coefficients.

Recall that (a_1, a_2) is part of the tuple (a_1, a_2, a_3, a_4) , which solves the four equations f_1, f_2, f_3, f_4 modulo $\mathfrak{p}$, where the f_i are the equations defining the scheme S. We will find lifts modulo $\mathfrak{p}^k$ for all $f \geq 1$ of the tuple (a_1, a_2, a_3, a_4).

Applying 24 to K, $\mathfrak{p}$ and the point (a_1, a_2, a_3, a_4) gives the existence of a tuple of algebraic numbers (A_1, A_2, A_3, A_4) which reduced to (a_1, a_2, a_3, a_4) modulo $\mathfrak{p}$ and with A_1, A_2 corresponding to the coefficients of a bitangent to the rational curve C.

The lifts modulo $\mathfrak{p}^k$ are defined by the sequence defined in the proof of 5.2.
Notation.

- $\left(\mathfrak{p}^k\right)^n$ will denote n tuples of elements of $\mathfrak{p}^k$
- $\mathfrak{p}^k$ denotes product of k copies of the ideal $\mathfrak{p}$, in the usual sense of ideal multiplication
- for $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{C}^n$ the congruence $\mathbf{u}_1 \equiv \mathbf{u}_2 \bmod \mathfrak{p}$ is taken coordinate wise
- $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{C}^n$ we'll denote by $\mathbf{u}_1 \cdot \mathbf{u}_2 = (u_{1,i} u_{2,i})_{1\leq i\leq n}$, the product taken component wise.

Let $\mathbf{a}_1 = (a_{1,1}, a_{2,1}, a_{3,1}, a_{4,1}) = (a_1, a_2, a_3, a_4)$. As $\mathbf{a}_1$ solves F modulo $\mathfrak{p}$, $F(\mathbf{a}_1) = \mathbf{u} \cdot \mathbf{u}_\mathfrak{p}$ for some $\mathbf{u}_\mathfrak{p} \in (\mathfrak{p})^4$. Choose $\mathbf{y} \in (\mathfrak{p})^4$ such that $DF(\mathbf{a}_1)\mathbf{y} \equiv -\mathbf{u} \bmod \mathfrak{p}$. Observe that S has smooth reduction at $\mathfrak{p}$, so $DF(\mathbf{a}_1)$ is invertible modulo $\mathfrak{p}$, so $\mathbf{y}$ is unique and satisfies

$$\mathbf{y} \equiv -DF(\mathbf{a}_1)^{-1} \cdot \mathbf{u} \bmod \mathfrak{p}$$

Let $\mathbf{a}_2 = \mathbf{a}_1 + \mathbf{y} \in \left(O_K/\mathfrak{p}^2\right)^4$. This is a lift of $\mathbf{a}_1$ modulo $\mathfrak{p}^2$. Conditions (1) and (3) (in the definition of a lift) are satisfied by definition and Hensel's Lemma (24). It remains to check that this is a solution of F modulo $\mathfrak{p}^2$. Applying Lemma 23 gives

$$\begin{aligned} F(\mathbf{a}_2) &= F(\mathbf{a}_1 + \mathbf{y}) \\ &= F(\mathbf{a}_1) + DF(\mathbf{a}_1)\mathbf{y} + R(\mathbf{a}_1, \mathbf{y}) \\ &= F(\mathbf{a}_1) + DF(\mathbf{a}_1)\mathbf{y} \bmod \mathfrak{p}^2 \end{aligned}$$

since $R(\mathbf{a}_1, \mathbf{y}) = (R_1(\mathbf{a}_1, \mathbf{y}), \ldots, R_4(\mathbf{a}_1, \mathbf{y}))$ and $R_k(\mathbf{a}_1, \mathbf{y}) = \sum_{1\leq i,j\leq d} c_{ijk}(\mathbf{a}_1, \mathbf{y})\, y_i y_j \in \mathfrak{p}^2$ for any k as $\mathbf{y} \in \mathfrak{p}$. As $F(\mathbf{a}_1) = \mathbf{u} \cdot \mathbf{u}_\mathfrak{p}$ for some $\mathbf{u}_\mathfrak{p} \in (\mathfrak{p})^4$

$$\begin{aligned} F(\mathbf{a}_2) &= F(\mathbf{a}_1) + DF(\mathbf{a}_1)\mathbf{y} \bmod \mathfrak{p}^2 \\ &= \mathbf{u} + DF(\mathbf{a}_1)\left(-DF(\mathbf{a}_1)^{-1} \cdot \mathbf{u}\right) \bmod \mathfrak{p}^2 \\ &= 0 \bmod \mathfrak{p}^2 \end{aligned}$$

Therefore $\mathbf{a}_2$ is the lift of $\mathbf{a}_1$ modulo $\mathfrak{p}^2$.

The rest of the lifts are defined inductively. Given the modulo $\mathfrak{p}^n$ lift $\mathbf{a}_n$, define $\mathbf{a}_{n+1} := \mathbf{a}_n + \mathbf{y} \in \left(O_K/\mathfrak{p}^{n+1}\right)^4$, where $\mathbf{y} \in (\mathfrak{p}^n)^4$ is the unique solution modulo $\mathfrak{p}$ to the equation $\mathbf{y} \equiv -\left(DF\left(\mathbf{a}_n\right)\right)^{-1} \cdot \mathbf{u} \bmod \mathfrak{p}$ where $F\left(\mathbf{a}_n\right) = \mathbf{u} \cdot \mathbf{u}_{\mathfrak{p}^n}$ for some $\mathbf{u}_{\mathfrak{p}^n} \in (\mathfrak{p}^n)^4$.
Note. This is well defined since $\mathbf{a}_n \equiv \mathbf{a}_1 \bmod \mathfrak{p}$ and so $\left(DF\left(\mathbf{a}_n\right)\right) = \left(DF\left(\mathbf{a}_1\right)\right) \bmod \mathfrak{p}$, hence $\left(DF\left(\mathbf{a}_n\right)\right)$ is invertible modulo $\mathfrak{p}$.

This is the lift of $\mathbf{a}_1$ modulo $\mathfrak{p}^{n+1}$. As before, (1) and (3) are satisfied by the the definition of $\mathbf{a}_n$ and Hensel's Lemma (24). To check (2), apply Lemma 23

$$\begin{aligned} F\left(\mathbf{a}_{n+1}\right) &= F\left(\mathbf{a}_n + \mathbf{y}\right) \\ &= F\left(\mathbf{a}_n\right) + DF\left(\mathbf{a}_n\right)\left(-\left(DF\left(\mathbf{a}_n\right)\right)^{-1} F\left(\mathbf{a}_n\right)\right) + R\left(\mathbf{x}_n, \mathbf{y}\right) \\ &= R\left(\mathbf{a}_n, \mathbf{y}\right) \bmod \mathfrak{p}^{n+1} \end{aligned}$$

where $R\left(\mathbf{a}_n, \mathbf{y}\right) = \left(R_1\left(\mathbf{a}_n, \mathbf{y}\right), , \ldots R_2\left(\mathbf{a}_n, \mathbf{y}\right)\right)$, with $R_k\left(\mathbf{a}_n, \mathbf{y}\right) = \sum_{1 \le i,j \le d} c_{ijk}\left(\mathbf{a}_n, \mathbf{y}\right) y_i y_j \in \mathfrak{p}^{n+1}$ for any k since $\mathbf{y} \in \mathfrak{p}^k$. Therefore $\mathbf{x}_{n+1}$ is a solution of F modulo $\mathfrak{p}^{n+1}$, and it lifts the points $\mathbf{x}_i$ for all $1 \le i \le n$.
Remark. This is easy to implement in magma - see Appendix 2.2.

5 Algebraic Theta Hyperplanes

In this section we'll focus on genus 3 curves. The same methods can be applied in the genus 4 case. Let C be a genus 3 curve over $\mathbb{Q}$ and S the scheme of the coefficients of the bitangents to C described in Section 4.1.

Fix $a_1x + a_2y + a_3z = 0$, a reduction of a bitangent modulo some prime ideal $\mathfrak{p}$ of a number field K, which lies over a rational prime p, which is a prime of good reduction for both C and S.

In the previous Section, we gave a method for computing lifts of the coefficients of this reduction $\{(a_{1,k}, a_{2,k}, a_{3,k})\}_{k \ge 1}$. We know that if $\tilde{a}_i$ are the coefficient of the bitangent to the rational curve C which reduces to above, then

$$\tilde{a_i} \equiv a_{i,k} \bmod \mathfrak{p}^k \text{ for all } k \ge 1$$

and we can use these lifts to determine the $\tilde{a}_i$.
Remark. In the notation of Section 4.3 we assumed that $\tilde{a_1} = 1$ and subsequently $a_{1,k} = 1$ for all $k \ge 1$. We take the more general approach in this section, accounting for any rescaling of the bitangents.

5.1 Lattices and Reduced Bases

This subsection is the background required for our calculations, to determine the minimal polynomials of the $\tilde{a_i}$s and the roots of these which determine the associated bitangent. Details can be found in [18, Chapter 5 and 6] and [3, Chapter 2].
Definition. A lattice L if a free $\mathbb{Z}$-module of finite rank, together with a positive definite quadratic form on $L \otimes \mathbb{R}$.

Fix a lattice (L, q) with $(b_i)_{1 \le i \le n}$ be a $\mathbb{Z}$-basis of a lattice L. For any element of L, $x = \sum_{1 \le i \le n} x_i b_i$ with $x_i \in \mathbb{Z}$, $q\left(x\right)$ can be expressed as

$$q(x) = \sum_{1 \leq i,j \leq n} q_{i,j} x_i x_j \text{ with } q_{i,j} = b(x_i, x_j)$$

where $b(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$ is the symmetric bilinear form associated to q.

Let $Q = (q_{i,j})_{1 \leq i,j \leq n}$, the $n \times n$ symmetric matrix with entries $q_{i,j}$. Then for any $x \in L$, $q(x) = X^T Q X$, where X is the column vector with entries are the coordinates of x in the given basis (b_i). A change of $\mathbb{Z}$-basis of the lattice corresponds to replacing X by PX for some $P \in GL_n(\mathbb{Z})$, and so $q(x) = (PX)^T Q(PX) = X^T Q' X$.
Note. $P \in \mathrm{GL}_n(\mathbb{Z}) \Leftrightarrow \det(P) = \pm 1$

This makes the following a well-defined invariant of the lattice L.
Definition. The determinant of the lattice is $d(L) = |\det(Q)|^{1/2}$

We can also represent a lattice (L, q) as follows. The free $\mathbb{Z}$ module L can be viewed as a discrete subgroup of rank n of the Euclidean vector space $E = L \otimes \mathbb{R}$. Observe that a $\mathbb{Z}$-basis of L is an $\mathbb{R}$ basis of E by definition of the tensor product.

By choosing an orthonormal basis of E, E can be identified with $\mathbb{R}^n$, with the usual Euclidean structure

$$q(x) = \left(x_1^2 + \ldots + x_n^2\right)$$

and $Q = B^T B$ where B is the matrix whose columns are the basis elements of the orthonormal basis. Then $d(L) = |\det(Q)|$, which is also well defined as a different choice orthonormal basis gives $B' = KB$ with $K^T K = KK^T = I_n$, an orthogonal matrix.

The existence of an orthonormal basis of a Euclidean space is given by the Gram-Schmidt theorem. We'll use the following version, with an orthogonal basis, which is sufficient for us.
Proposition 25. *Let b_i be a basis of a Euclidean vector space E. Define by induction*

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \text{ for all } 1 \leq i \leq n$$

$$\mu_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*} \text{ for all } 1 \leq j < i \leq n$$

then the b_i^* form an orthogonal basis of E.

Proof. See [3, Page 81] □

In the subsections that follow, we'll define lattices and look for the shortest vectors in these lattices. In order to do this, we need a basis whose vectors are short. The length of a lattice vector is simply $\| v \| = \sqrt{q(v)}$, the norm associated to q.
Definition. A basis B of a lattice L is called LLL-reduced if the associated Gram-Schmidt basis B^* and the constants μ_{ij} satisfy:

- $|\mu_{i,j}| \leq 1/2$ for all $1 \leq j < i \leq n$
- $\| b_i^* + \mu_{i,i-1} b_{i-1}^* \|^2 \geq 3/4 \| b_{i-1}^* \|^2$ for all $1 < i \leq n$.

Theorem 26. *Any lattice L has an LLL-reduced basis and it can be efficiently computed using the LLL algorithm.*

Proof. See [18, Chapter 5] or [3, Pages 85 -88] □

The following proposition allows us to compute the shortest vector in a lattice.

Theorem 27. *Let $b_1, \ldots, b_n$ be a reduced basis of a lattice L. Then for all non zero $x \in L$,*

$$\|b_1\| \leq c\|x\|$$

where $c = \max\{\|b_1\|^2/\|b_i^*\|^2\}$.

Proof. See [18, p69] or [3, Page 84] □

If B is an LLL-reduced basis, then the constant c is very close to 1, so b_1 the first element in the LLL-reduced basis, is a good candidate for the shortest vector in the lattice.

5.2 Minimal Polynomials

Let $\theta = \tilde{a_1}$. This is an algebraic number and we'd like to find its minimal polynomial. As it's algebraic, it must satisfy an expression of the form

$$d_n\theta^n + d_{n-1}\theta^{n-1} + \ldots + d_1\theta + d_0 = 0$$

for some $n \geq 1$, $d_i \in \mathbb{Z}$ and $d_n \neq 0$.

For any $k \geq 1$, $\theta \equiv a_{1,k} \bmod \mathfrak{p}^k$ and these satisfy the same expression modulo $\mathfrak{p}^k$

$$d_n a_{1,k}^n + d_{n-1}a_{1,k}^{n-1} + \ldots + d_1 a_{1,k} + d_0 \equiv 0 \bmod \mathfrak{p}^k$$

Define a homomorphism

$$\phi_k : \mathbb{Z}^{n+1} \longrightarrow O_K/\mathfrak{p}^k$$

$$(u_0, \ldots u_n) \longmapsto u_n a_{1,k}^n + u_{n-1}a_{1,k}^{n-1} + \ldots + u_1 a_{1,k} + u_0 \bmod \mathfrak{p}^k$$

Define $L_k = \ker(\phi_k) \leqslant \mathbb{Z}^{n+1}$, a discrete subgroup of $\mathbb{Z}^{n+1}$. This contains all elements of the form $P\mathbf{e}_i$, where P is any integer in $\mathfrak{p}^k$ and $\mathbf{e}_i$ is the ith element in the standard orthonormal basis of $\mathbb{Z}^{n+1}$, so L_k has full rank.

With the standard quadratic form on $\mathbb{Z}^{n+1}$, $q(\mathbf{x}) = x_1^2 + \ldots + x_n^2$, the discrete subgroup L_k is a full rank lattice, for any $k \geq 1$.

Observe that $(d_0, \ldots, d_n) \in L_k$ for all $k \geq 1$. Given all lattices L_k we want to find this common vector. As k increases, general the length of vectors in L_k increases and so eventually $(d_0, \ldots, d_n) \in L_k$ should be the shortest vector in L_k, or close to the shortest vector, when k is large enough.
Remark. We measure the length of $v \in L_k$with respect to the norm defined by the quadratic form q, which in this case is the Euclidean norm

$$\| v \| = \sqrt{q(v)} = \sqrt{v_1^2 + \ldots + v_n^2}$$

It remains to decide when k is large enough for $(d_0, \ldots, d_n)$ to be the shortest vector in L_k. This can be decided using Hermites's theorem.
Theorem 28. *(Hermite) Let L be an n dimensional lattice and M the length of the shortest non-zero vector in L. There exist constant $\mu_n \in \mathbb{R}_{\geq 0}$ depending on only on n such that*

$$M^n \leq \mu_n d(L)^2$$

There are bounds on these μ_n given in [18, Page 66]. For a general lattice of full rank, we expect this bound to be close to the actual size of the shortest non-zero vector in the lattice.

Proof. See [18, Page 66] □

Heuristic. For a full rank lattice $L \subset \mathbb{R}^n$, the length of the shortest vector in L is approximately $d(L)^{1/n}$

When k is large enough the length of the vector $(d_0, \ldots, d_n)$ should be smaller than the predicted bound, and this should help us identify it.

Regarding the choice of degree n, this is a guess, but there are a few things we should consider when making this choice. Given an n, and we can start with fairly small values, if this the degree or slightly bigger than the degree the following conditions should hold

- the minimum vector in the lattice, $v_{\min,k} \in L_k$ should be stable as k increases
- the length of $v_{\min,k}$ should decrease, and be significantly smaller than $d(L_k)^{\frac{1}{n+1}}$, as k increases.
- the polynomial $f_{\min}$ whose coefficient are $v_{\min,k}$ should be irreducible or its factorization should contain an irreducible polynomial of degree close to the degree of $f_{\min}$
- the minimal polynomials should respect the Galois action on the bitangents, so multiple points should have the same minimal polynomial

To summarise, the strategy for finding the coefficients of the minimal polynomial of θ is as follows

1. Guess the degree n.
2. Define the homomorphisms ϕ_k and the lattices L_k
3. In L_k look for vectors which are shorter than $1/1000d(L_k)$. For a large enough k' we expect to see a common such short vector in all lattices L_k for all $k \geq k^{'}$. If such a vector doesn't exists, guess a different degree and start again.
4. If such a vector exists, verify the conditions stated above, and if they are all satisfied, it's extremely likely that this vector represents the coefficients of the minimal polynomial. Otherwise, guess another degree and start again.

5.3 Algebraic Bitangents

Given the minimal polynomials of the coefficients of a bitangent $(\theta_1, \theta_2, \theta_3) = (\tilde{a_1}, \tilde{a_2}, \tilde{a_3})$, we would like to determine the exact roots of these minimal polynomials which determine the bitangent.

There are a few ways of doing this which will be describe here. In most examples, a blend of the methods which follow is used to determine all the bitangents.

Linear Relations

Firstly, we attempt to find any possible linear relations between the coefficients.

Suppose there exist $z_1, z_2, z_3, z_4 \in \mathbb{Z}$ such that

$$z_1\theta_1 + z_2\theta_2 + z_3\theta_3 + \theta_4 = 0$$

Using the lifts described in 4.3, for any $k \geq 1$ we have $\theta_i \equiv a_{i,k} \bmod \mathfrak{p}^k$, so the linear expressions are satisfied modulo $\mathfrak{p}^k$

$$z_1 a_{1,k} + z_2 a_{k,2} + z_3 a_{k,3} + z_4 \equiv 0 \bmod \mathfrak{p}^k$$

if such $z_i \in \mathbb{Z}$ exits.

For $k \geq 1$, define a homomorphism

$$l_k : \mathbb{Z}^4 \longrightarrow O_K/\mathfrak{p}^k$$
$$(n_1, n_2, n_3, n_4) \longmapsto n_1 a_{1,k} + n_2 a_{k,2} + n_3 a_{k,3} + n_4 \bmod \mathfrak{p}^k$$

Let $IL_k = \text{Kernel}\,(l_k) < \mathbb{Z}^4$. As in the previous section, this is a full rank discrete subgroup of $\mathbb{Z}^4$ and it forms a lattice with the standard Euclidean quadratic form on $\mathbb{R}^4$. If a linear relation $z_1\theta_1 + z_2\theta_2 + z_3\theta_3 + z_4 = 0$ exists, then $(z_1, z_2, z_3, z_4) \in L_k$ for all $k \geq 1$.

If such linear relation exists, we expect (z_1, z_2, z_3, z_4) to be the shortest vector in IL_k when k is large enough. By the same justification as in the previous subsection, we look for vectors in IL_k shorter than $1/1000d\,(IL_k)^{1/4}$ and we also expect these to be the shortest vector in every IL_k for all $k \geq N$ for some large N.

If such a vector exist, then it's extremely likely that these vectors give the coefficients of linear relations between the coefficients of the bitangent.

Higher Order Relations

If the coefficients are defined over the same number field, we may express one coefficient as a rational combination of powers of the other.

Let f_i be the minimal polynomial of θ_i and S_i the splitting field of f_i for $i = 1, 2, 3$.
Note. When the degree of f_i is large or S_i cannot be computed, similar computations can be carried out with the number fields defined by the f_i.

Suppose $S_2 \subseteq S_1$ so $\theta_1, \theta_2 \in S_1$, and we can express θ_2 as a rational combination of powers of θ_1, that is, we can find $q_0, \ldots, q_{n-1} \in \mathbb{Q}$ such that

$$\theta_2 = q_{n-1}\theta_1^{n-1} + \ldots + q_1\theta_1 + q_0$$

where n is the degree of f_1. Equivalently, there exist $z_{n-1}, \ldots, z_0, z \in \mathbb{Z}$ such that

$$z_{n-1}\theta_1^{n-1} + \ldots + z_1\theta_1 + z_0 + z\theta_2 = 0$$

As $\theta_i \equiv a_{i,k} \bmod \mathfrak{p}^k$ for all $k \geq 1$, substituting $a_{1,k}$ and $a_{2,k}$ in the above expression gives

$$z_{n-1}a_{1,k}^{n-1} + \ldots + z_1 a_{1,k} + z_0 + z a_{k,2} \equiv 0 \bmod \mathfrak{p}^k$$

For any $k \geq 1$, define a homomorphism,

$$r_k : \mathbb{Z}^{n+1} \longrightarrow O_K/\mathfrak{p}^k$$
$$(b, b_0, \ldots, b_{n-1}) \longmapsto b a_{2,k} + b_0 + b_1 a_{1,k} + \ldots b_{n-1} a_{1,k}^{n-1} \bmod \mathfrak{p}^k$$

Let $R_k = \text{Kernel}\,(r_k) < \mathbb{Z}^{n+1}$. As before, this is a full rank lattice in $\mathbb{Z}^{n+1}$ with the Euclidean quadratic form . For any $k \geq 1$ the vector of coefficients $(z, z_0, \ldots, z_{n-1})$ is an element of R_k for all $k \geq 1$, and when k is large enough, this will be the shortest vector R_k.

Following the same strategy as before, we search for vectors shorter than $1/1000d\,(R_k)^{1/n+1}$ and which are the shortest vectors in every R_k for $k \geq N$ for some large N.

Factorizing the Minimal Polynomial

When the minimal polynomials have large degree, looking for relations between the coefficients of the bitangents can be difficult. In this case, the mod $\mathfrak{p}^k$ approximations $\theta_i \equiv a_{i,k} \bmod \mathfrak{p}^k$ can

help us identify the roots of f_i corresponding to the coefficient of the bitangent $\theta_1 x+\theta_2 y+\theta_3 z = 0$.

let K be the number field defined by f_1. Suppose f_2 can be factorised over K as

$$f_2 = g_1 \dots g_m \text{ for some polynomials } g_i \in K[u], \text{ irreducible over } K$$

For any g_i, we can compute $n_{i,k} = g_i(a_{2,k}) \mod \mathfrak{p}^k$ for large k. For some $i \in \{1,\dots,k\}$, $|n_{1,k}|$ will be almost to 0 as k increases, indicating that θ_2 is a roots of g_i. This factor g_i will give a relation betwen θ_1 and θ_2, which can help in determining θ_2.
Remark. In the best possible scenario, the g_i's are linear and so they clearly identify θ_2. Even if these factors are not linear, they have degree slightly smaller than the degree of f_2, simplifying the problem of finding the root of f_2 corresponding to θ_2.
Remark. All methods described above are easily implemented in magma -see appendix 2.3.

6 Rational Two-Torsion Subgroup

As in the previous two sections, we work with the genus 3 case, but the same methods also apply in the genus 4 case.

Given the complete list of bitangents to a plane quartic, the two torsion subgroup of the Jacobian is completly determined. We'll describe a method to identifying the rational two torsion subgroup.

Let C be a genus 3 curve over $\mathbb{Q}$ and J_C it's Jacobian. As usual, C has a model

$$C : f(x,y,z) = 0$$

for some degree 4, homogeneous polynomial $f \in \mathbb{Q}[x,y,z]$.

Let $\{l_1,\dots,l_{28}\}$ be the 28 bitangents to the curve C. Let K be the field of definition of these bitangents. This is also the field of definition of the two-torsion subgroup.

By definition, the bitangents are non-zero elements of the function field of C over K, $K(C)$. Also, the quotients l_i/l_j are elements of $K(C)^*$ for all $i,j = 1\dots 28$.

For $i,j \geq 1$, consider the principal divisor

$$\operatorname{div}\left(\frac{l_i}{l_j}\right) = 2P_i + 2Q_i - 2P_j - 2Q_j$$

for some points $P_i, P_j, Q_i, Q_j \in C\left(\overline{K}\right)$.

Define $\frac{1}{2}\operatorname{div}\left(\frac{l_i}{l_j}\right) = P_i + Q_i - P_j - Q_j$ for $i,j \geq 1$. Observe that for any fixed bitangent l,

$$\operatorname{div}\left(\frac{l_i}{l_j}\right) = \operatorname{div}\left(\frac{l_i}{l}\right) + \operatorname{div}\left(\frac{l}{l_j}\right)$$

That is, any $\operatorname{div}\left(\frac{l_i}{l_j}\right)$ is linearly equivalent to $\operatorname{div}\left(\frac{l_i}{l}\right)$.

Let $D_i = \left[\frac{1}{2}\operatorname{div}\left(\frac{l_i}{l_1}\right)\right]$ be the divisor class in $\operatorname{Pic}^0(C)$ of $\frac{1}{2}\operatorname{div}\left(\frac{l_i}{l_1}\right)$ for all $i \geq 1$. Clearly $2D_i = 0$ and so $D_i \in J_C[2]$. By the above linear equivalences and the results of Section 3, the D_i generate the 2-torsion subgroup $J_C\left(\overline{\mathbb{Q}}\right)$, so

$$H = < D_i \mid i = 1,\dots,28 > = J_C\left(\overline{\mathbb{Q}}\right)[2] = J_C(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^6$$

We use H to find the rational two torsion subgroup $J_C(\mathbb{Q})[2]$. As in [9, Pages 19-21], we'll take Galois invariants in H and embed this subgroup into a finite Jacobian to find a presentation of the rational two torsion subgroup.

Let p be a prime of good reduction for C and $\mathfrak{p} \triangleleft O_K$ a prime ideal of norm p^n, for some $n \geq 1$. The reduction map induced by $\mathfrak{p}$

$$\text{red}_{\mathfrak{p}} : J_C(K) \longrightarrow J_C(\mathbb{F}_{p^n})$$

is injective on the torsion (see the appendix of [15]). In particular, it's injective on the two torsion.

Remark. The finite Jacobian $J_C(\mathbb{F}_{p^n})$ can be computed as the kernel of the degree map

$$d : \text{Pic}(C_{\mathfrak{p}}) \longrightarrow \mathbb{Z}$$

where $\text{Pic}(C_{\mathfrak{p}})$ is the divisor class group of the reduction of the curve C modulo $\mathfrak{p}$. This can all be done efficiently using Magma - see appendix 2.4.

Let $G = \text{Gal}(K/\mathbb{Q})$ and pick a set of generators of this group $\{\sigma_1, \ldots, \sigma_s\}$.
Note. $D \in J_C(\mathbb{Q})[2] \Leftrightarrow D^{\sigma} = D$ for all $\sigma \in G \Leftrightarrow D^{\sigma_i} = D$ for all $i = 1 \ldots s$

Therefore, the set $S = \{D \mid D = D_i \text{ for some } i \text{ and } D^{\sigma_j} = D \text{ for all } j = 1 \ldots s\}$ generates the rational two torsion subgroup. Using the injective reduction map $r_{\mathfrak{p}}$, we can embed the subgroup of $J_C(K)[2]$ generated by elements of S into the finite Jacobian $J_C(\mathbb{F}_{p^n})$ to obtain a presentation of $J_C(\mathbb{Q})[2]$,

$$J_C(\mathbb{Q})[2] = \langle S \rangle \cong (\mathbb{Z}/2\mathbb{Z})^t \text{ for some } t \leq 6$$

Given t, we can look for t linearly independent elements of S, $P_1 \ldots, P_t$. These will form a $\mathbb{Z}/2\mathbb{Z}$ basis for the rational two torsion subgroup of the Jacobian.

$$J_C(\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z} \cdot P_1 + \ldots + \mathbb{Z}/2\mathbb{Z} \cdot P_t$$

Remark. Magma is heavily used for these computations see appendix 2.4.

7 Example 1

Consider the non-hyperelliptic genus 3 curve X over $\mathbb{Q}$, defined by

$$X : f(x,y,z) = 3x^3z - 3x^2y^2 + 5x^2z^2 - 3xy^3 - 19xy^2z - xyz^2 + 3xz^3 + 2y^4 + 7y^3z - 7y^2z^2 - 3yz^3 \subseteq \mathbb{P}^2$$

This is isomorphic to the modular curve $X_0(75)$ modulo the action of the Atkin-Lehner operator w_{25} on the cusps $S_2(\Gamma_0(75))$, but this is not significant in calculations which follow.

Let J be the Jacobian of X. In [9, Pages 19-21] the authors showed that $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}$, and gave generators for this group. Using the methods described In Sections 4 and 5, we'll show $J(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ and also give generators for this group.

Working on the affine chart $\{z = 1\}$ suppose that there is a bitangent of the form $x = a_1y + a_2$ for some $a_1, a_2 \in \overline{\mathbb{Q}}$. Let $F(y) := f(a_1y + a_2, y, 1)$ and let l be the coefficient of y^4 in F. Equating coefficients in

$$F(y) = l\left(y^2 + u_3y + u_4\right)^2$$

gives 4 equations in u_1, u_2, u_3, u_4,

$$f_1(u_1,u_2,u_3,u_4) = 3u_1^2u_4^2 + 3u_1u_4^2 + 3u[2]^3 + 5u_2^2 + 3u_2 - 2u_4^2$$

$$f_2(u_1,u_2,u_3,u_4) = 6u_1^2u_3u_4 + 9u_1u_2^2 + 10u_1u_2 + 6u_1u_3u_4 + 3u_1 - u_2 - 4u_3u_4 - 3$$

$$f_3(u_1,u_2,u_3,u_4) = 9u_1^2u_2 + 3u_1^2u_3^2 + 6u_1^2u_4 + 5u_1^2 + 3u_1u_3^2 + 6u_1u_4 - u_1 - 3u_2^2 - 19u_2 - 2u_3^2 - 4u_4 - 7$$

$$f_4(u_1,u_2,u_3,u_4) = 3u_1^3 + 6u_1^2u_3 - 6u_1u_2 + 6u_1u_3 - 19u_1 - 3u_2 - 4u_3 + 7$$

Let S be the scheme over $\mathbb{Q}$ defined by f_1, f_2, f_3, f_4. Notably, 17 is a prime of good reduction for X and $S\mathbb{F}_{289}$ has degree 28. Thus we can find all bitangents on this affine chart and they are all of the form $x = a_1y + a_2$ for some $a_1, a_2 \in \overline{\mathbb{Q}}$.

Let $K = \mathbb{Q}(\sqrt{7})$ and $O_K = \mathbb{Z}[\sqrt{7}]$ its ring of integers. The prime ideal $\mathfrak{p} = \langle 17 \rangle$ of O_K has norm $17^2 = 289$, so we can use the isomorphism $\mathbb{F}_{289} \cong O_K/\mathfrak{p}$ to calculate the points in $S(\mathbb{F}_{289})$.

Each point in $S(\mathbb{F}_{289})$ has unique lift modulo $\mathfrak{p}^k$ for each $k \geq 1$ and using the method of 5.2 we find the minimal polynomials of the coefficients of each bitangent, see Table 1.

From the calculations of the minimal polynomials, we can see that the Galois orbits of the bitangents, and therefore of the two torsion points, are as follows

- 3 orbits with 6 bitangents each
- 3 orbits with 2 bitangents each
- 4 bitangents defined over $\mathbb{Q}$ and thus stable under Galois action

Table 1: Bitangents

Galois orbits of reductions of coefficients (a_1, a_2)	Minimal Polynomial of a_1	Minimal Polynomial of a_2
$(\theta+12, 3\theta+13)$ $(3\theta+2, 16\theta+12)$ $(5\theta+13, 12\theta+16)$ $(12\theta+13, 5\theta+16)$ $(14\theta+2, \theta+12)$ $(16\theta+12, 14\theta+13)$	$-u^6 - 14u^5 + 5u^4 + 20u^3 - 95u^2 - 134u + 139$	$u^6 + 54u^5 + 15u^4 + 180u^3 + 15u^2 + 54u + 1$
$(2\theta+8, 10\theta+2)$ $(7\theta+6, 14\theta+2)$ $(7\theta+10, 11\theta+4)$ $(10\theta+6, 3\theta+2)$ $(10\theta+10, 6\theta+4)$ $(15\theta+8, 7\theta+2)$	$-u^6-3u^5+5u^3-60u^2-63u+41$	$u^6+u^5-10u^4+25u^3-10u^2+u+1$
$(3\theta+11, 8\theta+5)$ $(3\theta+11, 14\theta+8)$ $(7\theta+9, 13\theta+11)$ $(10\theta+9, 4\theta+11)$ $(14\theta+11, 3\theta+8)$ $(14\theta+11, 9\theta+5)$	$11u^6 + 49u^5 + 20u^4 - 55u^3 + 40u^2 - 11u + 1$	$121u^6 + 669u^5 + 1590u^4 + 2085u^3 + 1590u^2 + 669u + 121$
$(6\theta+8, \theta+5)$ $(11\theta+8, 16\theta+5)$	$-u^2 - u + 1$	$u^2 + 7u + 1$
$(6\theta+12, 11\theta+7)$ $(11\theta+12, 6\theta+7)$	$u^2 - 7u + 11$	$u^2 + 3u + 1$
$(7\theta+13, 14\theta+8)$ $(10\theta+13, 3\theta+8)$	$-u^2 - 8u + 4$	$u^2 + 18u + 1$
$(1, 16)$	$-u + 1$	$u + 1$
$(2, 16)$	$-u + 2$	$u + 1$
$(14, 16)$	$u + 3$	$2u + 2$
$(15, 16)$	$u + 2$	$u + 1$

Let R be the splitting field of $u^6 - 14u^5 + 5u^4 + 20u^3 - 95u^2 - 134u + 139$, the first minimal polynomial in table 1. This is a degree 12 number field. A few straightforward calculations show that all minimal polynomials split over this number field, and thus this is the field of definition of our bitangents, and hence of the two-torsion points of the Jacobian.

Using the methods of Section (5.3) we can find relations between the bitangent coefficients. For the Galois orbits consisting of 6 bitangents the second coefficient u_2 can be expressed as an linear combination of $1, u_1, \ldots, u_1^{11}$. In the two-orbits case, the situation was easier as a linear relation between the two coordinates could be found in all case. These relations are shown in Table 2.

Table 2: Relations between u_1 and u_2

Galois orbits of reductions of coefficients (a_1, a_2)	Relations between u_1 and u_2
$(\theta + 12, 3\theta + 13)$ $(3\theta + 2, 16\theta + 12)$ $(5\theta + 13, 12\theta + 16)$ $(12\theta + 13, 5\theta + 16)$ $(14\theta + 2, \theta + 12)$ $(16\theta + 12, 14\theta + 13)$	$41u_1^5 + 467u_1^4 - 1312u_1^3 + 2604u_1^2 + 2687u_1 - 9164u_2 - 3083$
$(2\theta + 8, 10\theta + 2)$ $(7\theta + 6, 14\theta + 2)$ $(7\theta + 10, 11\theta + 4)$ $(10\theta + 6, 3\theta + 2)$ $(10\theta + 10, 6\theta + 4)$ $(15\theta + 8, 7\theta + 2)$	$u_1^5 + u_1^4 - 2u_1^3 - u_1^2 + 62u_1 - 27u_2 - 34$
$(3\theta + 11, 8\theta + 5)$ $(3\theta + 11, 14\theta + 8)$ $(7\theta + 9, 13\theta + 11)$ $(10\theta + 9, 4\theta + 11)$ $(14\theta + 11, 3\theta + 8)$ $(14\theta + 11, 9\theta + 5)$	$407u_1^5 + 1901u_1^4 + 1154u_1^3 - 1773u_1^2 + 1106u_1 - 17u_2 - 188,$
$(6\theta + 8, \theta + 5)$ $(11\theta + 8, 16\theta + 5)$	$3u_1 - u_2 - 2$
$(6\theta + 12, 11\theta + 7)$ $(11\theta + 12, 6\theta + 7)$	$u_1 + u_2 - 2$
$(7\theta + 13, 14\theta + 8)$ $(10\theta + 13, 3\theta + 8)$	$2u_1 - u_2 - 1$

The two tables give us the complete list of bitangents to C, $x = u_1 y + u_2$. Homogenizing these equations and clearing denominators gives all bitangents to the projective curve, $z_1 x + z_2 y + z_3 z = 0$, where z_i are element of the ring of integers O_R. Let BC be the set of bitangents. Note that we view this are a subset of non-zero elements of the function field $R(C)$, where the rational curve C is viewed as a curve over the number field R.

Fix the rational bitangent $b : x + 3y + z$. The set $H := \{\frac{1}{2}\text{div}\left(\frac{l}{b}\right) : l \in BC\}$ generates the two torsion subgroup .

Let O_R be the ring of integers of R. Factorizing $\langle 289 \rangle$ in O_R, we can find a prime ideal $\mathfrak{p}$ of norm $17^2 = 289$. Since 17 is a prime of good reduction for the curve, reduction mod $\mathfrak{p}$ gives an injection

$$\pi_{\mathfrak{p}} : J_C\left(\overline{\mathbb{Q}}\right)_{\text{tors}} \longrightarrow J\left(\mathbb{F}_{289}\right)_{\text{tors}}$$

Now $J\left(\mathbb{F}_{289}\right)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z} \times \mathbb{Z}/160\mathbb{Z}$ and we can verify that $\pi_{\mathfrak{p}}\left(\langle H \rangle\right) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^6$, further showing that H is indeed a generating group of the two torsion subgroup.

To determine $J\left[2\right]\left(\mathbb{Q}\right)_{\text{tors}}$ we take Galois invariants. The Galois group $G = \text{Gal}\left(R/\mathbb{Q}\right)$ can be viewed as a subgroup of S_{12}, and it's generated by two elements σ_1, σ_2. Let H_i be the subset of H fixed by σ_i, and let $H^* = H_1 \cap H_2$, that is H^* consists of all elements of H fixed by the entire Galois group G, so H^* generates the rational two torsion subgroup.

The image of the subgroup under the reduction map is $\pi_{\mathfrak{p}}\left(\langle H^* \rangle\right) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^2$ and so $J\left(\mathbb{Q}\right)\left[2\right] \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^2$, which confirms the result in [9] and it further suggests that the bitangents defined over $\mathbb{Q}$ are the only ones defining rational two torsion points.

The four rational bitangents are :

$$b : x + 3y + z$$

$$b_1 : x - y + z$$

$$b_2 : x - 2y + z$$

$$b_3 : x + 2y + z$$

and the corresponding divisors are:

$$D_1 = \tfrac{1}{2}\text{div}\left(\tfrac{b_1}{b}\right) = \left(\sqrt{2} - 2 : \sqrt{2} : 2\right) + \left(-\sqrt{2} - 2 : -\sqrt{2} : 2\right) - 2\left(1 : -1 : 2\right)$$

$$D_2 = \tfrac{1}{2}\text{div}\left(\tfrac{b_2}{b}\right) = \left(2\sqrt{-15} - 6 : 1 + \sqrt{-15} : 8\right) + \left(-2\sqrt{-15} - 6 : -\sqrt{-15} + 1 : 8\right) - 2\left(1 : -1 : 2\right)$$

$$D_3 = \tfrac{1}{2}\text{div}\left(\tfrac{b_3}{b}\right) = \left(-10 - 2\sqrt{17} : 3 + \sqrt{17} : 4\right) + \left(-10 + 2\sqrt{17} : 3 - \sqrt{17} : 4\right) - 2\left(1 : -1 : 2\right)$$

It is a straightforward calculation to check that $D_1 + D_2 + D_3$ has order 1, so $D_3 = -D_1 - D_2 = D_1 + D_2$, and thus

$$J\left(\mathbb{Q}\right)\left[2\right] = \left(\mathbb{Z}/2\mathbb{Z}\right) \cdot D_1 + \left(\mathbb{Z}/2\mathbb{Z}\right) \cdot D_2$$

which completes our example.

8 Example 2

In this section we'll compute the 2 torsion subgroup of the Jacobian of the non-hyperelliptic genus 4 modular curve $C = X_0\left(54\right)$. This has rational model

$$f_1 = x^2z - xz^2 - y^3 + y^2w - 3yw^2 + z^3 + 3w^3$$
$$f_2 = xw - yz + zw$$

Let J be the Jacobian of this curve. In [17], it's given that $J\left(\mathbb{Q}\right) \cong \left(\mathbb{Z}/3\mathbb{Z}\right) \times \left(\mathbb{Z}/3\mathbb{Z}\right) \times \left(\mathbb{Z}/9\mathbb{Z}\right)$, and so there is no rational two torsion. We'll verify this using our method.

Working on the affine chart $\{w = 1\}$, assume that there exists a tritangent plane of the form $x = u_1y + u_2z + u_3$ for some $u_i \in \overline{\mathbb{Q}}$.

The intersection of the affine curve with this plane is described by

$$F_1\left(y, z\right) = f_1\left(u_1y + u_2z + u_3, y, z, 1\right)$$
$$F_2\left(y, z\right) = f_2\left(u_1y + u_2z + u_3, y, z, 1\right)$$

Let H be the resultant of F_1 and F_2 with respect to z. This H is a degree 6 polynomial in y. Let l be the coefficient of y^6 in H. The plane intersects the affine curve at 3 points, each with multiplicity 2, so H is a square, and so there exist $u_4, u_5, u_6 \in \overline{\mathbb{Q}}$, such that

$$H(y) = l\left(y^3 + u_4 y^2 + u_5 y + u_6\right)^2$$

Equating coefficients in the above expression gives 6 equations in $u_1, \ldots, u_6$. These equations define a zero dimensional rational scheme S . It can be checked that 17 is a prime of good reduction for both C and S. A short search shows that over $\mathbb{F}_{289}$, S has 120 points, so the rational scheme describes the coefficients of all tritangent planes to the curve.

Take K to be the number field defined by x^2+x+1 and the prime ideal of O_K, $\mathfrak{p} = \langle 17 \rangle$, the we can find the 120 points of the reduced scheme defined over the finite field $O_K/\mathfrak{p} \cong \mathbb{F}_{289}$.

Each point in $S(\mathbb{F}_{289})$ has unique lift modulo $\mathfrak{p}^k$ for each $k \geq 1$ and using the method of 5.2 we find the minimal polynomials of the coefficients of each bitangent. See appendix 1 for these polynomials.

From the calculations of the minimal polynomials, we can see that the Galois orbits of the tritangent planes, and therefore of the 2 torsion, are as follows

- there are 2 orbits with 3 tritangents each
- there is one orbit with 6 tritangents
- there are 2 orbits with 9 tritangents each
- there are 3 orbits with 18 tritangents each
- there is 1 orbits with 36 tritangents

These orbits can be seen in Tables 3 to 11 in Appendix 1.

Let N be the number field defined by the degree 36 polynomial

$$f = u^{36} - 24u^{35} + 408u^{34} - 3372u^{33} + 22056u^{32} - 127776u^{31} + 630786u^{30} - 2714424u^{29} + 11261496u^{28} - 41046764u^{27} + 131733144u^{26} - 408414384u^{25} + 1150083423u^{24} - 2814636528u^{23} + 6374836368u^{22} - 13214216088u^{21} + 23592829968u^{20} - 36895248864u^{19} + 51352475964u^{18} - 58328930160u^{17} + 42803579664u^{16} + 3616822728u^{15} - 69219558864u^{14} + 126403035264u^{13} - 153084561489u^{12} + 151586318088u^{11} - 131113127592u^{10} + 78540995524u^9 + 18513274440u^8 - 121585972992u^7 + 155356552290u^6 - 110860906584u^5 + 57084024120u^4 - 38472387036u^3 + 36135508152u^2 - 21483956688u + 5029788241$$

All minimal polynomials split over this field, so N is the field of definition of the two torsion subgroup. Given N, Magma can be used to find all 120 points of $S(N)$, and so we have a complete list of tritangent planes to C.

Let O_N be the ring of integers of N. Clearing denominators and homogenising the above equations, we can assume that we have the complete list of tritangent planes $t_1, \ldots, t_{120}$ to the projective curve, whose defining equations have coefficients in O_N. Let TT be the set of these tritangent planes to C. Note that we view these as a subset of non-zero elements of the function field $N(C)$, where the rational curve C is viewed as a curve over the number field N.

Fix a tritangent plane t. The set $T = \{\frac{1}{2}\mathrm{div}\left(\frac{a}{t}\right) : a \in TT\}$ generates the two torsion subgroup.

By factorising $\langle 289 \rangle$ in O_N, we find a prime ideal $\mathfrak{p}$ of norm $17^2 = 289$. As 17 is a prime of good reduction of the curve, the reduction modulo $\mathfrak{p}$ map gives an injection

$$\pi_{\mathfrak{p}} : J_C\left(\overline{\mathbb{Q}}\right)_{\mathrm{tors}} \longrightarrow J\left(\mathbb{F}_{289}\right)_{\mathrm{tors}}$$

and by looking at the kernel of the degree map, whose domain is the divisor class group of the reduced curve $C_{\mathfrak{p}}$, we deduce that

$$J_C\left(\mathbb{F}_{289}\right)_{\text{tors}} \cong \left(\mathbb{Z}/18\mathbb{Z}\right)^8$$

Also the image of the subgroup generate by H in $J_C\left(\mathbb{F}_{289}\right)_{\text{tors}}$ is

$$\pi_{\mathfrak{p}}\left(\langle H\rangle\right) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^8$$

which is consistent with the fact that the divisors defined by the tritangents to C form the entire 2 torsion subgroup of $J_C\left(\overline{\mathbb{Q}}\right)_{\text{tors}}$. Taking Galois invariants of the above gives the rational two torsion subgroup.
Remark. It's sometimes necessary to divide the equations of the tritangents by a uniformizer of $\mathfrak{p}$ to ensure that they do not reduce to 0 modulo $\mathfrak{p}$.

Using Magma, we can find the 36 automorphisms of the number field N. Taking the second function in this list σ , we determine its action of the tritangents and the resulting action on the divisors defined by these planes. Then looking by at corresponding action on the elements of $\langle H\rangle$, we find that σ doesn't fix any element of $\langle H\rangle$.

Therefore, no element of $\langle H\rangle$ is fixed by the Galois group of N, and we can conclude that $J_C\left(\mathbb{Q}\right)[2] = \{0\}$, which completes this example.

References

[1] Matthew Baker, Yoav Len, Ralph Morrison, Nathan Pflueger, and Qingchun Ren. Bitangents of tropical plane quartic curves. *Mathematische Zeitschrift*, 282(3-4):1017–1031, 2016.

[2] John William Scott Cassels and E Victor Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230. Cambridge University Press, 1996.

[3] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.

[4] Keith Conrad. Hensels lemma. *Unpublished note, available at http://www. math. uconn. edu/˜ kconrad/blurbs/gradnumthy/hensel. pdf*, 2015.

[5] Keith Conrad. A multivariable hensels lemma. *Lecture note available at http://kconrad. math. uconn. edu/blurbs*, 2020.

[6] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermats Last Theorem, Providence, RI*, pages 39–133, 1995.

[7] Igor V Dolgachev. *Classical algebraic geometry: a modern view*. Cambridge University Press, 2012.

[8] Roger H Dye. On the arf invariant. *Journal of Algebra*, 53(1):36–39, 1978.

[9] Nuno Freitas, Bao V Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular. *Inventiones mathematicae*, 201(1):159–206, 2015.

[10] William Fulton. Algebraic curves. *An Introduction to Algebraic Geom*, page 54, 2008.

[11] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry*. John Wiley & Sons, 2014.

[12] Joe Harris. Theta-characteristics on algebraic curves. *Transactions of the American Mathematical Society*, 271(2):611–638, 1982.

[13] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[14] Gert Heckman. Symplectic geometry, 2013.

[15] Nicholas M Katz. Galois properties of torsion points on abelian varieties. *Inventiones mathematicae*, 62(3):481–502, 1980.

[16] David Mumford. Theta characteristics of an algebraic curve. In *Annales Scientifiques de l'École Normale Supérieure*, volume 4, pages 181–192, 1971.

[17] Ekin Ozman and Samir Siksek. Quadratic points on modular curves. *Mathematics of Computation*, 88(319):2461–2484, 2019.

[18] Nigel P Smart. *The algorithmic resolution of Diophantine equations: a computational cookbook*, volume 41. Cambridge University Press, 1998.

Appendix 1

Table 3:

Coefficient	Minimal Polynomial
u_1	$u^3 + 16$
u_2	$u - 2$
u_3	u

Table 4:

Coefficient	Minimal Polynomial
u_1	$u^3 + 4$
u_2	$-u + 2$
u_3	u

Table 5:

Coefficient	Minimal Polynomial
u_1	$u^6 - 34u^3 + 1$
u_2	$u + 1$
u_3	$u^6 + 918u^3 + 729$

Table 6:

Coefficient	Minimal Polynomial
u_1	$u^9 - 6u^8 - 33u^7 + 12u^6 + 159u^5 + 42u^4 - 303u^3 - 96u^2 + 336u - 368$
u_2	$u^9 + 96u^8 - 393u^7 + 2394u^6 - 5829u^5 + 13092u^4 - 16815u^3 + 14730u^2 - 7332u + 1528$
u_3	$u^9 + 114u^8 + 1287u^7 + 8316u^6 + 34911u^5 + 99954u^4 + 195129u^3 + 248832u^2 + 186624u + 62208$

Table 7:

Coefficient	Minimal Polynomial
u_1	$u^9 - 6u^8 + 39u^7 - 96u^6 + 231u^5 - 498u^4 + 705u^3 - 1068u^2 + 768u - 764$
u_2	$u^9 - 24u^8 + 231u^7 - 30u^6 + 195u^5 - 348u^4 + 1449u^3 - 1158u^2 + 636u + 184$
u_3	$u^9 - 6u^8 - 9u^7 + 1188u^6 + 10503u^5 + 41634u^4 + 93393u^3 + 124416u^2 + 93312u + 31104$

Table 8:

Coefficient	Minimal Polynomial
u_1	$u^{18}+24u^{17}+168u^{16}+330u^{15}-1752u^{14}-11760u^{13}-27345u^{12}-2496u^{11}+162960u^{10}+548084u^9+1080240u^8+1579776u^7+1920471u^6+2041608u^5+1873704u^4+1403970u^3+784392u^2+302928u+70921$
u_2	$u^{18}-342u^{17}-2727u^{16}-31080u^{15}-231588u^{14}-722304u^{13}-127524u^{12}-3918312u^{11}+4557654u^{10}-17955772u^9+26129286u^8-43900920u^7+45275388u^6-44664624u^5+29531196u^4-17402808u^3+6147153u^2-1918782u+70921$
u_3	$-u^{18}-648u^{17}+7560u^{16}-90450u^{15}-256392u^{14}-4087584u^{13}-8847063u^{12}-37250928u^{11}-91177488u^{10}-238928292u^9-594910656u^8-1440410688u^7-771829479u^6+7353516312u^5+14589826920u^4-7615864458u^3-31829300568u^2+21134286639$

Table 9:

Coefficient	Minimal Polynomial
u_1	$u^{18}+6u^{17}+69u^{16}-174u^{15}+1002u^{14}-1554u^{13}+5037u^{12}-6402u^{11}+15594u^{10}-15838u^9+26709u^8-33978u^7+33585u^6+57648u^5+126480u^4+255264u^3+77568u^2+123648u+135424$
u_2	$u^9+96u^8-393u^7+2394u^6-5829u^5+13092u^4-16815u^3+14730u^2-7332u+1528$
u_3	$u^{18}-114u^{17}+11709u^{16}-130086u^{15}+673434u^{14}-2842938u^{13}+13220901u^{12}-55531818u^{11}+192976506u^{10}-585506070u^9+1582645149u^8-3762003042u^7+7722985905u^6-13418452224u^5+19283671296u^4-22160853504u^3+19349176320u^2-11609505792u+3869835264$

Table 10:

Coefficient	Minimal Polynomial
u_1	$u^{18}+6u^{17}-3u^{16}+42u^{15}+714u^{14}+1470u^{13}-1371u^{12}-11370u^{11}-9894u^{10}+24410u^9+37941u^8-38802u^7-65559u^6+164496u^5+218712u^4-257016u^3-226128u^2+586752u+583696$
u_2	$u^9-24u^8+231u^7-30u^6+195u^5-348u^4+1449u^3-1158u^2+636u+184$
u_3	$u^{18}+6u^{17}+45u^{16}+2322u^{15}-3294u^{14}-156978u^{13}+1942461u^{12}-12791034u^{11}+60106050u^{10}-213638310u^9+603184077u^8-1385416386u^7+2636163873u^6-4176365184u^5+5469669504u^4-5799714048u^3+4837294080u^2-2902376448u+967458816$

Table 11:

Coefficient	Minimal Polynomial
u_1	$u^{36} - 24u^{35} + 408u^{34} - 3372u^{33} + 22056u^{32} - 127776u^{31} + 630786u^{30} - 2714424u^{29} + 11261496u^{28} - 41046764u^{27} + 131733144u^{26} - 408414384u^{25} + 1150083423u^{24} - 2814636528u^{23} + 6374836368u^{22} - 13214216088u^{21} + 23592829968u^{20} - 36895248864u^{19} + 51352475964u^{18} - 58328930160u^{17} + 42803579664u^{16} + 3616822728u^{15} - 69219558864u^{14} + 126403035264u^{13} - 153084561489u^{12} + 151586318088u^{11} - 131113127592u^{10} + 78540995524u^{9} + 18513274440u^{8} - 121585972992u^{7} + 155356552290u^{6} - 110860906584u^{5} + 57084024120u^{4} - 38472387036u^{3} + 36135508152u^{2} - 21483956688u + 5029788241$
u_2	$u^{18} - 342u^{17} - 2727u^{16} - 31080u^{15} - 231588u^{14} - 722304u^{13} - 127524u^{12} - 3918312u^{11} + 4557654u^{10} - 17955772u^{9} + 26129286u^{8} - 43900920u^{7} + 45275388u^{6} - 44664624u^{5} + 29531196u^{4} - 17402808u^{3} + 6147153u^{2} - 1918782u + 70921$
u_3	$u^{36} - 648u^{35} + 427464u^{34} + 5079780u^{33} - 1714392u^{32} + 1011998448u^{31} + 7488465714u^{30} - 90765074232u^{29} - 188915293656u^{28} + 775421719812u^{27} + 9536656280328u^{26} - 22732575404832u^{25} - 50585141939985u^{24} + 278489202327216u^{23} - 224565824538576u^{22} - 1876374984103416u^{21} + 6608286946129104u^{20} + 4286455663008960u^{19} - 1738389609137124u^{18} + 3273852914231745 6u^{17} - 4943518501987614 24u^{16} + 726695801515345320u^{15} + 1521737392783479 84u^{14} - 461186468126516937 6u^{13} + 202306703115533093 91u^{12} - 477034321504292637 84u^{11} + 941632394258274169 68u^{10} - 151476655600272256236u^{9} + 256872652931606406408u^{8} - 326558365206206923440u^{7} + 489761246823173262162u^{6} - 397818960461200567512u^{5} + 704758790507406600744u^{4} - 321911724918288753324u^{3} + 672689561722997510952u^{2} + 446658071739413916321$

Appendix 2

This is the Magma code used for the example in Section 7.

Appendix 2.1

The scheme of coefficients of bitangents describes in Section 4.1 is defined as follows.

```
Z<x,y,z> := PolynomialRing(Integers(),3);
f := 3*x^3*z - 3*x^2*y^2 + 5*x^2*z^2 -3*x*y^3 -19*x*y^2*z -x*y*z^2 +
        3*x*z^3 +2*y^4 + 7*y^3*z -7*y^2*z^2 -3*y*z^3;
Zz<X,Y> := PolynomialRing(Integers(),2);
F := Evaluate(f,[X,Y,1]);
Zu<[u]> := PolynomialRing(Integers(),4);
ZY<Y> := PolynomialRing(Zu);
h := Evaluate(F,[u[1]*Y + u[2],Y]);
l := MonomialCoefficient(h,Y^4);
H := h - l*(Y^2 + u[3]*Y + u[4])^2 ;
eqns := Coefficients(H);
S := Scheme(AffineSpace(Zu),eqns);
```

After a short search we find that over $\mathbb{F}_{289}$, S has 28 points. Taking $K = \mathbb{Q}\left(\sqrt{7}\right)$ and the prime ideal $\mathfrak{p} = \langle 17 \rangle$ of O_K, we can reduce the scheme S modulo $\mathfrak{p}$, and find all the points over the finite field $O_K/\mathfrak{p} \cong \mathbb{F}_{289}$.

```
K := QuadraticField(7) ;
OK := Integers(K) ;
P := 17*OK ;
F289,phi := ResidueClassField(P);
S2 := BaseChange(S,F289);
PTS := Points(S2) ;
```

Appendix 2.2

Any point of PTS can be lifted modulo $\mathfrak{p}^k$ for all $k \geq 1$. We begin by embedding the defining equations of the scheme in $O_K[u_1, u_2, u_3, u_4]$ and setting up the multivariate function $F = [f_1, f_2, f_3, f_4]$.

```
Zz<[u]> := PolynomialRing(OK,4);
f1 := Zz ! eqns[1];
f2 := Zz ! eqns[2];
f3 := Zz ! eqns[3];
f4 := Zz ! eqns[4];

H := [f1,f2,f3,f4];
J := JacobianMatrix(H) ;
```

Lifts are defined inductively as described in Section 4.3. In the 'lift' function below, the input (n, A) is a solution A of F modulo $\mathfrak{p}^n$, and its output is the lift of A modulo $\mathfrak{p}^{n+1}$.

```
lift := function(n,A) ;
a := Eltseq(A) ;
Fn,tn := quo<OK | P^(n) > ;
b := [ s@@tn : s in a ];
c := Evaluate(H,b);
d := [ (1/17^n)*s : s in c] ;
e := [ phi(s) : s in d ] ;
Y := Matrix(F289, 4,1, e ) ;
Jc := Evaluate(J,b) ;
s1 := Eltseq(Jc[1]) ;
s2 := Eltseq(Jc[2]) ;
s3 := Eltseq(Jc[3]) ;
s4 := Eltseq(Jc[4]) ;
d1 := [phi(s) : s in s1 ];
d2 := [phi(s) : s in s2 ];
d3 := [phi(s) : s in s3 ];
d4 := [phi(s) : s in s4 ];
s := d1 cat d2 cat d3 cat d4 ;
Jcc := Matrix(F289, 4,4, s);
Zu<[y]> := PolynomialRing(F289, 4) ;
B := Matrix(Zu, 4,1, [y[1],y[2],y[3],y[4]]) ;
JCc := RMatrixSpace(Zu, 4,4) ! Jcc ;
eqns := Eltseq( (JCc * B ) + Y ) ;
Zzz<[y]> := PolynomialRing(F289,4);
g1 := Zzz ! eqns[1] ;
g2 := Zzz ! eqns[2] ;
g3 := Zzz ! eqns[3] ;
g4 := Zzz ! eqns[4] ;
EQN := [g1,g2,g3,g4 ] ;
S1 := Scheme(AffineSpace(Zzz) , EQN) ;
PT := Points(S1) ;
PPT := [ Eltseq(a) : a in PT ] ;
PTT := [ s@@phi : s in PPT ] ;
NPT := [ [b[1] + (17^n)*s[1], b[2] + (17^n)*s[2], b[3] + (17^n)*s[3],
                b[4] + (17^n)*s[4] ] : s in PTT ] ;
return NPT ;
end function ;
```

Appendix 2.3

Inductively, we can define the lifts modulo $\mathfrak{p}^k$, for all $k \geq 1$ and for any point of PTS. Below we defined all lifts modulo $\mathfrak{p}^k$ for all $1 \leq k \leq 300$.

```
LIFTS := [ [PTS[j]] : j in [1..28] ];

for i in [1..28] do ;
for j in [2..300] do ;
LIFTS[i][j] := lift(j-1,LIFTS[i][j-1]);
end for ;
end for ;
```

Using these lifts, the function *apr* finds the minimal polynomial of each coefficient. The input (x, k, p, d) is a point x, the lift of a coefficient modulo $\mathfrak{p}^n$, the rational prime p below $\mathfrak{p}$, 17 in this case and a guess for the degree of the minimal polynomial d. The output is the polynomial which best fits our input, as well as the length of the vector of the coefficients of this polynomial and the bound specified in Section 5 . The last 2 outputs help in determining whether this really is the minimal polynomial.

```
apr := function(x,k,p,d) ;
ZZ := FreeAbelianGroup(d+1) ;
Z2 := FreeAbelianGroup(2) ;
Z2s := sub< Z2 | [(p^k)*Z2.1,(p^k)*Z2.2] > ;
Q,pi := quo< Z2 | Z2s > ;
R,r := quo<OK | P^k> ;
a := [ Z2 ! Eltseq((x^i)@@r) : i in [0..d] ] ;
c := [ pi(s) : s in a ] ;
phi := hom< ZZ -> Q | c > ; // the homomorphism defined in (5.2)
K := Kernel(phi) ; // the kernel containing the vector with the required coefficients
G := { Eltseq(ZZ ! g) : g in Generators(K) } ;
W := StandardLattice(d+1) ;
L := sub<W | [ W ! g : g in G ] > ;
v := ShortestVector(L) ; // the shortest vector in the lattice
II := Index(W,L) ;
Bound := (II)^(1/(d+1));
Bound2 := (1/1000)*Bound ; // the bound from (5.2)
Zx<u> := PolynomialRing(Integers());
O := [ v[s+1]*u^s : s in [0..d] ] ;
T := &+[ a : a in O] ;
return T, Length(v),Bound2;
end function ;
```

Given the minimal polynomials, we find that for all bitangnets $x = u_1 y + u_2$, the minimal polynomial of u_2 splits over the splitting field of the minimal polynomila of u_1, so we look for relations between u_2 and $1, u_1, \ldots, u_1^m$ where $m+1$ is the degree of the minimal polynomial of u_1. The input of the function below is $x = (u_1, u_2)$, coefficients of a bitangent modulo $\mathfrak{p}^a$ and n is the degree of the relation. If a is large enough, the output is the required relation.

```
rel := function(x,a,n) ;
ZZ := FreeAbelianGroup(n+2);
Z1 := FreeAbelianGroup(2);
Z1s := sub<Z1 |[(17^a)*Z1.1,(17^a)*Z1.2]>;
Q,pi := quo<Z1 | Z1s>;
R,r := quo<OK | P^a> ;
xx := [ s@@r : s in x ];
y := [ xx[1]^(n-t) : t in [0..n-1]] cat [xx[2]] ;
j := [ Z1 ! Eltseq(s) : s in y ];
c := [ pi(s) : s in j ] ;
d := c cat [ Q ! [1,0] ];
phi := hom< ZZ -> Q | d > ; \\ the homomorphism defined in (5.3)
K := Kernel(phi) ;
G := { Eltseq(ZZ ! g) : g in Generators(K) };
W := StandardLattice(n+2);
L := sub<W | [ W ! g : g in G ] > ;
i := Index(W, L );
```

```
B := (1/1000)*((i)^(1/(n+2))) ;
b := BestApproximation(B,10^10);
v := ShortVectors(L,b) ; \\ vectors shorter than the required bound
V := [ Eltseq(a[1]) : a in v ];
Z<[z]> := PolynomialRing(Integers(),2);
Vu := [ [t[s+1]*(z[1]^(n-s)) : s in [0..n-1] ] cat [t[n+1]*z[2],t[n+2] ] : t in V ];
Rel := [ &+[a : a in b] : b in Vu ];
return Rel;
end function ;
```

Appendix 2.4

Givent he bitangents we'll find the 2 torsion subgroup.

Given the minimal polynomials, we find that they all split over the splitting field K of $g := -u^6 - 14u^5 + 5u^4 + 20u^3 - 95u^2 - 134u + 139$. Using this we can define the bitangents to the projective curve as follows :

```
T<u> := PolynomialRing(Rationals());
g := -u^6 - 14*u^5 + 5*u^4 + 20*u^3 - 95*u^2 - 134*u + 139 ;
K := SplittingField(g);

g1 := g ;
g12 := 1/9164*(41*u^5 + 467*u^4 - 1312*u^3 + 2604*u^2 + 2687*u -3083);

g2 := -u^6 - 3*u^5 + 5*u^3 - 60*u^2 - 63*u + 41 ;
g22 := 1/27*( u^5 + u^4 - 2*u^3 - u^2 + 62*u - 34) ;

g3 := 11*u^6 + 49*u^5 + 20*u^4 - 55*u^3 + 40*u^2 - 11*u + 1 ;
g32 := 1/17*( 407*u^5 + 1901*u^4 + 1154*u^3 - 1773*u^2 + 1106*u -188) ;

R1 := Roots(g1,K);
PT1 := [ [R1[i,1],Evaluate(g12,R1[i,1])] : i in [1..6] ];
R2 := Roots(g2,K);
PT2 := [ [R2[i,1],Evaluate(g22,R2[i,1])] : i in [1..6] ];
R3 := Roots(g3,K);
PT3 := [ [R3[i,1],Evaluate(g32,R3[i,1])] : i in [1..6] ];

g4 := -u^2 - u + 1 ;
g42 := 3*u - 2 ;
g5 := u^2 - 7*u + 11 ;
g52 := -u + 2 ;
g6 := -u^2 - 8*u + 4 ;
g62 := 2*u - 1 ;
R4 := Roots(g4,K);
PT4 := [ [R4[i,1],Evaluate(g42,R4[i,1])] : i in [1..2] ];
R5 := Roots(g5,K);
PT5 := [ [R5[i,1],Evaluate(g52,R5[i,1])] : i in [1..2] ];
R6 := Roots(g6,K);
PT6 := [ [R6[i,1],Evaluate(g62,R6[i,1])] : i in [1..2] ];
```

```
PT7 := [ [1,-1], [2,-1], [-3,-1], [-2,-1] ];
BPT := PT1 cat PT2 cat PT3 cat PT4 cat PT5 cat PT6 cat PT7 ;
BF<[x]> := PolynomialRing(K,3);
Bbtan := [ x[1] - a[1]*x[2] -a[2]*x[3] : a in BPT ];
```

We clear the denominators, in order to define the bitangents over O_K.

```
CBtan := [ Coefficients(a) : a in Bbtan ];
DenomCBtan := [ [Denominator(s) : s in a ] : a in CBtan ];
LCmBtan := [ Lcm(s[2],s[3]) : s in DenomCBtan ];
Btan := [ LCmBtan[i]*Bbtan[i] : i in [1..28] ];
```

Define the projective curve and consider its coefficients in O_K, and these can be reduce the curve modulo $\mathfrak{p}$, to give a reduction of the curve. The bitangents are also defined over O_K and the coefficients reduced modulo $\mathfrak{p}$.

```
OK := Integers(K) ;
P := 289*OK ;
p1 := Factorization(P)[1,1] ;
R<[x]> := PolynomialRing(K,3);
eqn:=3*x[1]^3*x[3] - 3*x[1]^2*x[2]^2 + 5*x[1]^2*x[3]^2 - 3*x[1]*x[2]^3 -
 19*x[1]*x[2]^2*x[3] - x[1]*x[2]*x[3]^2 + 3*x[1]*x[3]^3 + 2*x[2]^4 +
 7*x[2]^3*x[3] - 7*x[2]^2*x[3]^2 - 3*x[2]*x[3]^3;

P2:=ProjectiveSpace(R);
X:=Curve(P2,eqn);
F289,pi := ResidueClassField(p1) ;
X289 := ChangeRing(X,F289);

CBtan := [ Coefficients(a) : a in Btan];
ACBta := [ [ OK ! s : s in a ] : a in CBtan ];
F289CBtan := [ [pi(s) : s in a ] : a in ACBta];
BB<[v]> := PolynomialRing(F289,3);
F289Btan := [ a[1]*v[1] + a[2]*v[2] + a[3]*v[3] : a in F289CBtan ];
```

There are magma commands which allow us the find the divisor class group of the reduced curve and it's function field.

```
Cl289, phi,psi := ClassGroup(X289) ;
FX289 := FunctionField(X289);
```

Define the bitangents as functions of the function field and form the divisors which generate the two torsion.

```
FX289 := FunctionField(X289);
FXBtan := [ Evaluate(a, [FX289.1, FX289.2, 1 ]) : a in F289Btan];
Db := [ Divisor(FXBtan[27]/FXBtan[i]) : i in [1..28] ];
DDb := [Decomposition(s) : s in Db];
DDb1 := [ [1/2*a[i,2] : i in [1..#a]] : a in DDb ];
DDb1 := [ [Integers()!s : s in a ] : a in DDb1] ;
DDb2 := [ [a[i,1] : i in [1..#a] ] : a in DDb];
divs := [ [DDb1[i][j]*DDb2[i][j] : j in [1..#DDb1[i]]] : i in [1..#DDb1] ];
divs := [ &+a : a in divs ];
```

Find $J(\mathbb{F}_{289})$ as the kernel of the degree map, and embed the generators of the 2 torsion subgroup H in this. The ih below is the subgroup generated by elements of H.

```
Z := FreeAbelianGroup(1);
degr := hom<Cl289 -> Z | [ Degree(phi(g)) : g in OrderedGenerators(Cl)] > ;
JF := Kernel(degr) ;
H := [ psi(a) : a in divs];
H := [JF!s : s in H ];

ZN := FreeAbelianGroup(#H);
h := hom<ZN -> JF | [ a : a in H ]>;
ih := Image(h) ;
```

To find the rational 2 torsion subgroup, we need to find the points of ih fixed by the Galois action. The Galois action can be determined as follows.

```
A,b,piK := AutomorphismGroup(K) ; \\ the automorphism group of K is
                                                    generated by 2 elements
s1 := piK(A.1);
s2 := piK(A.2); \\ these are the generators of the Galois Group

\\ The bitangents fixed by these two generators can be found by:

CCBtan := [Coefficients(a) : a in Btan ];
CBtanseq := [ [OK!s : s in Eltseq(a) ] : a in CCBtan];

CBtan := [ Coefficients(a) : a in Btan ];

for i in [1..28] do ;
a := CBtan[i] ;
b := [ s1(s) : s in a ];
d := [ Denominator(s) : s in b ];
l := LCM(d) ;
c := [ l*s : s in b ] ;
c := [ OK ! s : s in c ];
c := [ Eltseq(s) : s in c ];
cc := [ [Integers() ! s : s in Eltseq(a)] : a in c];
gcd1 := GCD(cc[1]);
gcd2 := GCD(cc[2]);
gcd3 := GCD(cc[3]);
gg := GCD([gcd1,gcd2,gcd3]);
dcc := [ [ s div gg : s in a ] : a in cc];
di := [ i : i in [1..28] | dcc eq GCDCBtan[i] ];
print <i,di> ;
end for ;

\\ this above finds the action of s1 on the bitangents.
This can be used to define the map


cpt := [ZN.4,ZN.6,ZN.5,ZN.1,ZN.3,ZN.2,ZN.8,ZN.7,ZN.10,ZN.9,ZN.12,

ZN.11,ZN.14,ZN.13,ZN.17,ZN.18,ZN.15,ZN.16,ZN.20,ZN.19,ZN.22,
```

```
ZN.21,ZN.24,ZN.23,ZN.25,ZN.26,ZN.27];

conj := hom< ZN -> ZN | cpt>;
mu := hom< ZN -> J289 | [ h(ZN.i) - h(conj(ZN.i)) : i in [1..27]]>;
ker := Kernel(mu);
imKer := sub<J289 | [h(k) : k in Generators(ker)]>;

\\ this is the image of the group fixed by s1

\\repeating with s2
cpt2 := [ ZN.3, ZN.1, ZN.5, ZN.6, ZN.4, ZN.2, ZN.11, ZN.10, ZN.7,
ZN.9, ZN.12, ZN.8, ZN.17, ZN.18, ZN.14, ZN.13, ZN.15, ZN.16, ZN.20,
ZN.19, ZN.22, ZN.21, ZN.24, ZN.23, ZN.25, ZN.26, ZN.27];
conj2 := hom< ZN -> ZN | cpt2>;
mu2 := hom< ZN -> J289 | [ h(ZN.i) - h(conj2(ZN.i)) : i in [1..27]]>;
ker2 := Kernel(mu2);
imKer2 := sub<J289 | [h(k) : k in Generators(ker2)]>;
\\ this is the image of the group fixed by s2

Intersecting these two groups give the rational 2 torsion subgroup.
```