The Arithmetic of Elliptic Curves and Jacobians of Genus 2 Curves

Tristan Pang

New College
The University of Oxford

Supervisor: Prof. Victor Flynn

A dissertation submitted for the degree
MSc in Mathematics and Foundations of Computer Science (MFoCS)
2020/21

Abstract

The Mordell-Weil theorem on elliptic curves states that the group structure on the rational points of an elliptic curve is finitely generated. This gives rise to descent techniques to find the rank of the elliptic curve. These results can be extended to Jacobians of higher genera curves, in particular genus 2 curves. In this dissertation, we will compare and summarise the fundamentals of genus 2 curves to elliptic curves, and investigate complete 2-descent and descent by Richelot isogeny with reference to examples. We shall also touch on using complete 2-descent on the Jacobian of genus 3 curves.

Acknowledgements

I would like to express my deepest gratitude to my dissertation supervisor Prof Victor Flynn for his invaluable advice and excellent supervision; not just during this research project or throughout my MFoCS programme, but from when I was still an undergrad student, he patiently walked me through p-adic numbers and the big picture of arithmetic geometry and its connections to other disciplines. Our fortnightly intellectually stimulating meetings have been a highlight of my Oxford journey.

I am genuinely grateful to Prof Steven Galbraith and Dr Jeroen Schillewaert. Not only did they provide me with an excellent foundation in number theory, but they also continued to support me all the way through to the present. Their above and beyond guardianship is something I will always value.

I am extremely thankful to Dr Jan Vonk, Prof Peter Stevenhagen and Prof Ronald van Luijk. Their faith in me and constant encouragement motivated me and gave me the confidence to complete this dissertation. The breadth and depth of their various research topics excite me, and thus my passion for number theory has grown stronger.

Last but not least, my immense appreciation to my dedicated and supportive parents and mentor Andrew Patterson. They are always there for me, wherever, whatever and whenever.

Contents

Chapter 1

Introduction

Elliptic curves (non-singular projective curves of the form $Y^2 = \text{cubic in } X$) is a topic of core study in arithmetic geometry. Given an elliptic curve E with at least one rational point, we can define a group law on the rational points $E(\mathbb{Q})$. The identity is the point at infinity and negation of a point is given by mirroring the point along the x axis. Addition of two points is defined to be the negation of the third point of intersection of the line between the two points and E.

When there is a group law, the structure will always be a point of investigation. Firstly, it is clear that the group is abelian. A theorem by Mordell and Weil states that $E(\mathbb{Q})$ is finitely generated, thus $E(\mathbb{Q})$ is a product of a finite abelian group called the torsion of E and a free part which is a power of $\mathbb{Z}$. This power of $\mathbb{Z}$ is called the rank of the curve, so a rank 0 curve has a finite number of points in $E(\mathbb{Q})$.

For any elliptic curve, there exists a method using the Nagell-Lutz theorem to find all torsion points. We can also bound the torsion by considering reductions modulo a prime. In fact, a theorem by Mazur limits the structure of $E(\mathbb{Q})$ to one of 15 finite abelian groups which all have order less than or equal to 12.

While the torsion seems to be easy to study, investigating the rank of the free component is usually harder. To date, there is no known algorithm that can find the rank for every elliptic curve, but there are a few methods that might work. The first method that one might come across is a descent by 2-isogeny. This method comes from a constructive proof of the Mordell-Weil theorem through a weaker theorem that states that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. This requires investigating maps between two isogenous curves, say $\varphi\colon E \mapsto E'$ and $\varphi\colon E' \mapsto E$, and finding $E(\mathbb{Q})/\varphi'(E'(\mathbb{Q}))$ and $E'(\mathbb{Q})/\varphi(E(\mathbb{Q}))$ by mapping these to $\mathbb{Q}^2/(\mathbb{Q}^*)^2$, the rational modulo squares.

Finding the image of this map (which happens to be a homomorphism and so the image is related to it's pre-image $E(\mathbb{Q})/\varphi'(E'(\mathbb{Q}))$ and its dual) requires either working with homogeneous spaces (sets of equations in $\mathbb{Z}$) or a commutative diagram (a method by Cassels and Flynn which we shall describe later). The first method generally requires more computational power, so will become unreasonable to do by hand as E becomes more complicated, but gives us more information about generators of $E(\mathbb{Q})/2E(\mathbb{Q})$ (and thus more information about $E(\mathbb{Q})$). The latter method is easier to do by hand.

If we have found the groups $E(\mathbb{Q})/\varphi'(E'(\mathbb{Q}))$ and its dual, we can put these together to form $E(\mathbb{Q})/2E(\mathbb{Q})$ which is related to $E(\mathbb{Q})$ as follows. Since $E(\mathbb{Q})$ is finite, write $E(\mathbb{Q}) \simeq E_{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^{\times r}$ (where the first component is the torsion and the second is the free part of rank r). We can then quotient out by the double of all points, $2E(\mathbb{Q})$ to get

$$E(\mathbb{Q})/2E(\mathbb{Q}) \simeq E(\mathbb{Q})[2] \times (\mathbb{Z}/2\mathbb{Z})^{\times r},$$

where the first component is the 2-torsion subgroup and the second component is r copies of the group of order 2. The rank is easily solvable if we already know $E(\mathbb{Q})/2E(\mathbb{Q})$ since finding $E(\mathbb{Q})[2]$ is an easy task of finding points of order 2.

A more effective method of finding the rank is called complete 2-descent. Again, we investigate a map to $\mathbb{Q}^2/(\mathbb{Q}^*)^2$, but this time, we take this map directly from $E/2E(\mathbb{Q})$. This reduces two separate calculations into one big calculation. It is also a method that scales well with higher genera of curves.

If descent by 2-isogeny yields a rank bound, then complete 2-descent always at least gives a better bound. Sometimes the bounds might be the same, but if complete 2-descent on a curve works, and descent by 2-isogeny doesn't, we have a member of the Tate-Shafarevich group, where the homogeneous spaces violate the Hasse principle (local solutions in $\mathbb{Q}_p$ and $\mathbb{R}$ implies a global solution in $\mathbb{Q}$).

A hyperelliptic curve is a non-singular curve $C\colon Y^2 = F(X)$ where $F(X) \in k[X]$ is a non-singular polynomial in X. A curve of genus g can be thought of as a hyperelliptic curve where F is of degree $2g+1$ or $2g+2$. Hence a curve $Y^2 =$ cubic (i.e. an elliptic curve when there is a k root) is of genus 1 and $Y^2 =$ quintic is of genus 2. Later, we shall show that this definition is more-or-less the same as the standard way of defining genus.

As with elliptic curves, it is possible to have a group structure. In this dissertation, we shall look at the Jacobian $\mathfrak{G}$ of genus 2 curves after describing arithmetic on genus 1 curves. The group structure on the Jacobian of a genus 2 curve C involves pairs of points (instead of single points on an elliptic curve), and these points can be rational or in a quadratic extension of $\mathbb{Q}$. Addition is given by the 5th and 6th intersection of C and the unique cubic that goes through the four points of two elements. We wish to show analogues of the elliptic curves results on Jacobians of genus 2 curves.

As with elliptic curves, we can consider a reduction of C modulo p to show that the torsion of $\mathfrak{G}$ is finite. Mordell-Weil also holds for genus 2 curves - that $\mathfrak{G}/2\mathfrak{G}$ is finite and $\mathfrak{G}$ is finitely generated.

Complete 2-descent works on $\mathfrak{G}$ with minor modifications. One line homogeneous spaces become several lines, so it is best to use the alternative method involving a commutative diagram. The analogue to descent by 2-isogeny is a descent by Richelot isogeny, which gives is used in the constructive proof of the Mordell-Weil theorem. As with the genus 1 case, complete 2-descent is always at least better than a descent by Richelot isogeny, and when it is strictly better, we have a member of the Tate-Shafarevich group.

These descent methods serve as a method to confirm the rank, provided we already know all generators of the group, though as with elliptic curves, is still an open question whether there exists a method that always works to find the rank and all generators of a group.

The rank gives us an idea of the structure of $\mathfrak{G}$, but what does $C(\mathbb{Q})$ look like? If C is an elliptic curve, then $C(\mathbb{Q}) = \mathfrak{G}$. But in genus 2, it is more complicated. If the rank of C is 0, then $\mathfrak{G}$ is all torsion, and $C(\mathbb{Q})$ can be found by looking at the pairs of points of elements of the torsion. If the rank is 1, we can apply Chabauty's Theorem which says that $C(\mathbb{Q})$ is finite. The proof is constructive and we shall explain how we can determine $C(\mathbb{Q})$ entirely given the rank and a free generator. In fact, a theorem by Falting says that $C(\mathbb{Q})$ is always finite for any rank, though the proof is not constructive.

Most results mentioned, especially the Mordell-Weil Theorem and Falting's Theorem hold for curves of higher genus. We shall see a genus 3 example of complete 2 descent at the end of this dissertation. Chabauty also holds with the condition that the genus $g \geq 1$ and the rank r is less than g. These results can also extend to arbitrary fields, especially number fields (finite field extensions of $\mathbb{Q}$).

On the other hand, there is no known general form of Mazur's theorem (which gives a complete list of torsion structures of the Jacobian of a genus 1 curve) that holds in any genera. At the end of this dissertation, we will give an example of how to construct a curve whose Jacobian has large torsion.

The arithmetic of curves of any genus is interesting on itself, but it is also used in other fields of study. Notable applications are the uses of elliptic curves and isogenies in cryptography. The latter of these is quantum resistant and so arithmetic on the Jacobian of curves has had increasing engagement in the wider community.

In this dissertation, we start with the aforementioned methods of descent to find the rank of an elliptic curve then move on to investigating genus 2 curves. The dissertation will mostly be based off [1] with points from other sources and a few examples. At the end, there is an appendix with code snippets that assist with the computational aspects of this dissertation.

1.1 Notation

Here are explanations of some notation that may cause confusion.

Let G be a group and $n \in \mathbb{N}$ then write $G^{\times n}$ for the n-fold direct product $\prod_{i=1}^{n} G = G \times \cdots \times G$. Write G^n to denote the subgroup $\{g^n : g \in G\}$ (where G is written with multiplicative notation).

If R is a ring then let R^* be the group of units (i.e. the group of multiplicatively invertible elements).

For any prime p, we use $\mathbb{Q}_p$ to denote the p-adic numbers and $\mathbb{Z}_p$ the ring of integers of $\mathbb{Q}_p$. Write $p = \infty$ for $\mathbb{R}$. Thus we write $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ for the abelian group of order p.

Let for $a \in \mathbb{Z}_p$, the p-adic integers, write $v_p(a)$ as usual the p-adic valuation, that is the largest p power of a (and $v_p(0) = \infty$). Furthermore, if $a/b \in \mathbb{Q}_p$, write $v_p(a/b) = v_p(a) - v_p(b)$. Let the p-adic absolute value be given by $| \cdot |_p = p^{-v_p}$.

In the context of curves, let ∞ denote the point at infinity (eg. on $\mathbb{P}^1$, the projective line).

Chapter 2

Elliptic Curves

We first give, without detailed proofs, a brief review on the basics of elliptic curves. Most proofs can be found in [3] and [5].

2.1 Definitions

Recall that an elliptic curve over a field is a non-singular projective cubic curve with at least one rational point. In a field of characteristic not 2 nor 3 (eg $\mathbb{Q}$), every elliptic curve can be birationally transformed into a curve $Y^2 = X^3 + AX + B$. Throughout this chapter, we shall assume that an elliptic curve has this form, unless otherwise stated. Let Δ denote the discriminant, so here $\Delta = 4A^3 + 27B^2 \neq 0$.

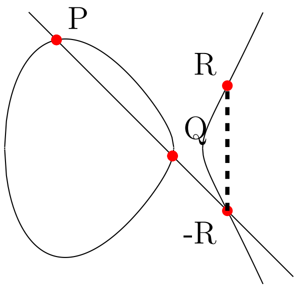
Let $E\colon Y^2 = X^3 + AX + B$ be an elliptic curve over k (char $\neq 2, 3$) with Jacobian J. The identity of J is the point at infinity, $\mathfrak{O} = \infty$ (i.e. $(0, 1, 0)$ on the projective form $Y^2Z = X^3 + AXZ^2 + BZ^3$). The points in the Jacobian are exactly the points on $E(k)$. These points form a group $\mathfrak{G} = J(k)$ with the following operations.

- $\mathfrak{O}$ is the identity.

- If $P = (x, y) \in \mathfrak{G}$, then $-P = (x, -y)$.

- If $P, Q, R \in \mathfrak{G}$ such that R is the third point of intersection of the line through P and Q with E, then $P + Q = -R$. We take multiplicities into account, so if for example, $P = Q$, then we use the line tangent to E at P.

This addition law is illustrated below.



$P + Q = R$

There are, of course, equations that define addition (eg. [5] 1.4) which are derived from substituting the equation of the line into the cubic, but in practice, it is easier to not remember/use these formulae and to either use the definition of the group law, or just use computational software.

Let $n \in \mathbb{Z}$. Let $\mathfrak{G}[n]$ be the usual notation denoting the n-torsion subgroup. That is, $P \in \mathfrak{G}[n]$ if and only if $nP = \mathfrak{O}$. Additionally, write $\mathfrak{G}_{\text{tors}}$ as the group of all torsion points, $\mathfrak{G}_{\text{tors}} = \cup_n \mathfrak{G}[n]$.

Proposition 2.1.1
The 2-torsion are all points $(x, y) \in \mathfrak{G}$ such that $y = 0$ together with the identity. Thus $\mathfrak{G}[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{\times i}$ where $i \in \{0, 1, 2\}$.

Proof.
If $P \in \mathfrak{G}[2]$, then $2P = \mathfrak{O}$ and so $P = -P$. So either $P = \mathfrak{O}$ or $P = (x, 0)$. There are at most three such $x \in \mathbb{Q}$. □

2.2 Torsion

We now give a few standard results to aid in the classification of torsion points. Here, we consider elliptic curves over $\mathbb{Q}$. These can be found in various textbooks such as [3] and [5]. Many of these results also have higher genera analogues.

This theorem due to Hasse gives an estimate of the number of points on an elliptic curve C reduced modulo a prime. In fact, this also holds for higher genus as in Theorem 4.1 of [5].

Theorem 2.2.1 (Hasse)
Let E be an elliptic curve over $\mathbb{F}_p$ with p a prime. Then $||E(\mathbb{F}_p)| - (p + 1)| \leq 2\sqrt{p}$.

Hasse's theorem can be combined with the following proposition to find the structure of the torsion as in Section 4.3 of [5].

Proposition 2.2.2 (Reductions)
Let E ne an elliptic curve over $\mathbb{Q}$. If for a prime p, $E \mod p$ is non-singular, then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of $E'(\mathbb{F}_p)$ where E' is the reduced $E \mod p$.

The reduced curve is an elliptic curve when $p \neq 2$ and $p \nmid \Delta$. We call these p primes of good reduction. Note that furthermore, $|E(\mathbb{Q})_{\text{tors}}| \mid |E'(\mathbb{F}_p)|$ and the torsion is finite.

We then have a theorem that gives a necessary condition on the finite order points (Chapter 12 of [3]).

Theorem 2.2.3 (Nagell-Lutz)
Let E be an elliptic curve over $\mathbb{Q}$ and $(x, y) \in E(\mathbb{Q})_{\text{tors}} \setminus \{\mathfrak{O}\}$. Then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y^2 \mid \Delta$.

In fact, there are only a limited number of types of torsion of elliptic curves.

Theorem 2.2.4 (Mazur)
The torsion of an elliptic curve over $\mathbb{Q}$ must be isomorphic to one of these 15 groups

- $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq N \leq 10$,
- $\mathbb{Z}/12\mathbb{Z}$,
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ with $1 \leq n \leq 4$.

Example 2.2.5
Let $E \colon Y^2 = X(X-5)(X-7)$. Clearly E has three points of order 2 (namely, $(0,0), (5,0), (7,0)$). Thus $|E_{\text{tors}}(\mathbb{Q})| \geq 4$. Conversely, reducing E modulo 3,

$$\tilde{E} \colon Y^2 \equiv X^3 + 2X \equiv X(X+1)(X-1).$$

Thus, $\tilde{E}(\mathbb{F}_3) = \{\mathfrak{O}, (0,0), (0, \pm 1)\}$ and so $|\tilde{E}(\mathbb{F}_3)| = 4$. Since $E_{\text{tors}}(\mathbb{Q})$ injects into $\tilde{E}(\mathbb{F}_3)$, this means $|E_{\text{tors}}(\mathbb{Q})| \leq |\tilde{E}(\mathbb{F}_3)|$ and so $E_{\text{tors}}(\mathbb{Q})$ has exactly four points, namely the points of order 2 and the identity.

Example 2.2.6
When the lower bound for the torsion is not clear, we can find extra torsion points using Nagell-Lutz, then use reductions to prove that there are no other torsion points.

For example, consider $E \colon Y^2 = X^3 - X^2 - 4X + 4 = (X-1)(X-2)(X+2)$ with $\Delta = 2^8 \cdot 3^2$. Clearly, $E[2] = \{\mathfrak{O}, (1,0), (2,0), (-2,0)\}$.

Considering the reduction modulo 5, $E' \colon Y^2 = X^3 - X^2 + X - 1$ has the following possible right sides: $\{4, 0, 0, 0, 1\}$ which are all squares. Thus

$$E'(\mathbb{F}_5) = \{\mathfrak{O}, (0, \pm 2), (1,0), (2,0), (3,0), (4, \pm 1)\}.$$

It follows that $|E_{\text{tors}}(\mathbb{Q})| \leq 8$. Since $(0,2) + (4,1) = (0,-2) + (4,-1) = (3,0)$, $(0,2)$ and $(3,1)$ must be points of order 4, and so $E_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

By Nagell-Lutz, $(x, y) \notin E[2]$ is torsion only if $y^2 \mid \Delta = 2^8 \cdot 3^2$. So possible y values are $\{\pm 1, \pm 2 \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 16, \pm 24, \pm 48\}$. Of these, only $(0, \pm 2)$ and $(4, \pm 6)$ have integer coordinates. It is an easy computation using the group law to show that these are points of order 4. Since these give a total of 4 integer points giving a total of 8 known points, these must coincide with all 8 possible torsion points.

2.3 2-Isogeny Descent

Descent procedures give us a way to find the structure of $\mathfrak{G}$. Since the group is abelian and finitely generated (as we shall see from the Mordell-Weil Theorem), $\mathfrak{G} \simeq \mathfrak{G}_{\text{tors}} \times \mathbb{Z}^r$ where $r \geq 0$, $r \in \mathbb{Z}$. This r is called the rank of $\mathfrak{G}$. The standard way to find the rank (which is taught in courses) is to do a descent by 2-isogeny. A brief outline of this procedure is as follows.

For this section, suppose that the elliptic curve has at least one point of order 2 in $\mathbb{Q}$. Then we can birationally move this point to the origin. Thus consider elliptic curves of the form $E\colon Y^2 = X(X^2 + AX + B)$ with $\Delta = B(A^2 - 4B) \neq 0$ with corresponding group $\mathfrak{G}$.

Definition 2.3.1
An isogeny between two curves, is a morphism between them that preserves the identity.

Define another elliptic curve $E'\colon Y^2 = X(X^2 + A'X + B')$ where $A' = -2A$, $B' = A^2 - 4B$ with corresponding group $\mathfrak{G}'$. Then these cures are isogenous with corresponding isogeny

$$\varphi\colon E \to E'\colon (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2 - B)}{x^2}\right)$$

and $\varphi(\mathfrak{O}) = \mathfrak{O}$. An inverse isogeny is given by

$$\varphi'\colon E' \to E\colon (x, y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(x^2 - B')}{8x^2}\right).$$

These maps are surjective homomorphisms with kernels $\{\mathfrak{O}, (0,0)\}$. For any $P \in \mathfrak{G}$, $\varphi' \circ \varphi(P) = 2P$.

The following theorem tells us that the rank must indeed be finite, and the proof can give us an algorithm to find the rank using the isogenies.

Theorem 2.3.2 (Mordell-Weil)
$\mathfrak{G}/2\mathfrak{G}$ is finite. $\mathfrak{G}$ is finitely generated.

Since $\mathfrak{G}$ is finitely generated, the rank is an integer and so we can mod out by $2\mathfrak{G}$ to get that

$$\mathfrak{G}/2\mathfrak{G} \simeq \mathfrak{G}[2] \times (\mathbb{Z}/2\mathbb{Z})^{\times r}.$$

Thus, the problem reduces to finding out $\mathfrak{G}/2\mathfrak{G}$. But since $\varphi' \circ \varphi$ is the point doubling map, $\mathfrak{G}/2\mathfrak{G}$ is generated by $\mathfrak{G}/\varphi'(\mathfrak{G}')$ and $\varphi'(\mathfrak{G}'/\varphi(\mathfrak{G}))$.

Lemma 2.3.3
$(x, y) \in \varphi(\mathfrak{G}) \subseteq \mathfrak{G}'$ if and only if $x \in (\mathbb{Q}^*)^2$.

Define a map $q\colon \mathfrak{G}' \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ given by

$$q(P) = \begin{cases} B', & P = (0,0); \\ x, & P = (x,y), x \neq 0; \\ 1, & P = \mathfrak{O}. \end{cases}$$

This map is a homomorphism with kernel $\varphi(\mathfrak{G})$. We can similarly define $q'\colon \mathfrak{G} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$. By the first isomorphism theorem, $\mathfrak{G}/\varphi'(\mathfrak{G}') \simeq \operatorname{im}(q')$ and $\mathfrak{G}'/\varphi(\mathfrak{G}) \simeq \operatorname{im}(q)$. Thus, we need to find the image of q and q'.

To find these images, we can use homogeneous spaces. Let $r \in (\mathbb{Z}^*)/(\mathbb{Z}^*)^2$ (a square free integer). If $r \in \operatorname{im}(q)$ (respectively q') then $r \mid B'$ (resp. B).

Lemma 2.3.4
Define spaces

$$W_r\colon rl^4 + A'l^2m^2 + \frac{B'}{r}m^4 = n^2$$
$$W_r'\colon rl^4 + Al^2m^2 + \frac{B}{r}m^4 = n^2.$$

Then $r \in \operatorname{im}(q)$ (resp. q') if and only if W_r (resp. W_r') has a solution with $l, m, n \in \mathbb{Z}$, $(l, m, n) \neq (0, 0, 0)$ and $\gcd(l, m) = 1$.

Here is a summary of the whole descent process.

Proposition 2.3.5 (Descent by 2-isogeny)

- Let $E\colon Y^2 = X(X^2 + AX + B)$, $A, B \in \mathbb{Z}$, $B(A^2 - 4B) \neq 0$.
- $D\colon Y^2 = X(X^2 - 2AX + A^2 - 4B)$.
- Let $q\colon D(\mathbb{Q}) \to \mathbb{Q}/(\mathbb{Q}^*)^2$ given by $q(0,0) = A^2 - 4B$, $q(\mathfrak{O}) = 1$ and $q(x,y) = x$ (modulo squares). Similarly, $q'\colon E(\mathbb{Q}) \to \mathbb{Q}/(\mathbb{Q}^*)^2$ by $\hat{q}(0,0) = B$, $\hat{q}(\mathfrak{O}) = 1$ and $q(x,y) = x$.
- Find the image of q and q' using homogeneous spaces. That is, find the set of $r \in (\mathbb{Z}^*)/(\mathbb{Z}^*)^2$ such that $r \mid A^2 - 4B$ (resp. B) such that W_r (resp W_r') has a relevant solution.
- Combine the results to find the structure of $E(\mathbb{Q})/2E(\mathbb{Q})$.
- Find the 2-torsion $E(\mathbb{Q})[2]$.
- Use the fact that $E(\mathbb{Q}) \simeq E_{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^{\times r}$ iff $E(\mathbb{Q})/2E(\mathbb{Q}) \simeq E(\mathbb{Q})[2] \times (\mathbb{Z}/2\mathbb{Z})^{\times r}$, to solve for rank r.

2.3.1 An Example

Let $E\colon Y^2 = X(X-5)(X-7)$. Equivalently, $Y^2 = X^3 - 12X^2 + 35X = X(X^2 - 12X + 35)$.

We previously computed that this curve has four torsion points. We perform a descent by 2-isogeny to find the rank.

Let $D\colon Y^2 = X(X^2 + 24X + 4)$ be the curve isogenous to E. With the usual notation, let φ (respectively $\hat{\varphi}$) be the isogeny from $E(\mathbb{Q})$ to $D(\mathbb{Q})$ (resp. $D(\mathbb{Q}) \to E(\mathbb{Q})$) and q (resp. $\hat{q}$) be the homomorphism map to the first coordinate of a point on E (resp. D) to $\mathbb{Q}/(\mathbb{Q}^*)^2$. Let W_r (resp. $\hat{W}_r$) be the homogeneous space corresponding to $r \in q(E(\mathbb{Q}))$ (resp. $r \in \hat{q}(D(\mathbb{Q}))$).

Let us first consider the isogeny from E to D. Then $q(\mathfrak{O}) = 1$ and $q(0,0) = 4 \equiv 1$. Thus $\{1\} \subseteq \text{im}(q) \subseteq \{r \in \mathbb{Q}/(\mathbb{Q}^*)^2 : r \mid 4\} = \{\pm 1, \pm 2\}$. We now test for the triviality of each homogeneous space.

Consider the non-trivial integer solutions of $W_{-1}\colon -l^4 + 24l^2m^2 - 4m^4 = n^2$, and as usual, assume l and m are coprime. Completing the square, $-(l^2 - 12m^2)^2 + 156m^4 = n^2$. Taking this modulo 3, $-l^4 \equiv n^2$. Since -1 is not a quadratic residue modulo 3, it must be the case that $3 \mid n$ and $3 \mid l^2$, which also means $3 \mid l$. But then, $9 \mid (-l^4 - 24l^2m^2 - n^2) = -12m^4$ and so $3 \mid -4m^4$. It follows that $3 \mid m$ and $\gcd(l,m) \geq 3$. Thus W_{-1} cannot have any non-trivial integer solutions and $-1 \notin \text{im}(q)$.

Similarly, consider the solutions of $W_2\colon 2l^4 + 24l^2m^2 + 2m^4 = n^2$. Then clearly, $2 \mid n^2$, so $2 \mid n$, say $2n' = n$. Then $l^4 + 12l^2m^2 + m^4 = 2n'^2$ and completing the square, $(l^2 + 6m^2)^2 - 35m^4 = 2n'^2$. Modulo 5, $(l^2 + 6m^2)^2 \equiv 2n'^2$, since 2 is not a squre mod 5, $5 \mid n'$ and $5 \mid (l^2 + 6m^2)$. Thus, $25 \mid 2n'^2 - (l^2 + 6m^2)^2 = -35m^4$, so $5 \mid m$. But, then $5 \mid l^2 = ((l^2 + 6m^2) - 6m^2)$ and so $\gcd(l,m) \geq 5$. So W_2 has no non-trivial solutions and $2 \notin \text{im}(q)$.

Finally, consider $W_{-2}\colon -2l^4 + 24l^2m^2 - 2m^4 = n^2$. As before, write $n = 2n'$. Then $-l^4 + 12l^2m^2 - m^4 = n'^2$ and completing the square, $-(l^2 - 6m^2)^2 + 35m^4 = 2n'^2$. Since -2 is not a square modulo 5, $5 \mid (l^2 - 6m^2)$ and $5 \mid n'$. So $25 \mid 35m^4$ and $5 \mid m$. Thus $5 \mid l$ and there are no non-trivial integer solutions to W_{-2}. Hence $2 \notin \text{im}(q)$.

Thus $\text{im}(q) = \{1\}$ and $E(\mathbb{Q})/\varphi(D(\mathbb{Q})) \simeq \text{im}(q) = 1$.

Now let us consider the isogeny from D to E. Then $\hat{q}(\mathfrak{O}) = 1$ and $\hat{q}(0,0) = 35 \equiv 35$. Thus $\{1\} \subseteq \text{im}(\hat{q}) \subseteq \{r \in \mathbb{Q}/(\mathbb{Q}^*)^2 : r \mid 35\} = \{\pm 1, \pm 5, \pm 7, \pm 35\}$. As before, we test for the triviality of each homogeneous space.

First, $\hat{W}_{-1}\colon -l^4 - 12l^2m^2 - 35m^4 = n^2$. This clearly has no non-trivial solutions in $\mathbb{Z}$, since it has no non-trivial solutions in $\mathbb{R}$ (as $\sqrt{-1} \notin \mathbb{R}$).

Next consider $\hat{W}_3\colon 5l^4 - 12l^2m^2 + 7m^4 = n^2$. Then $l = m = 1$ and $n = 0$ is a non-trivial integer solution with $\gcd(l,m) = 1$.

Since $\operatorname{im}(\hat{q})$ is a group, it follows that $5 \cdot 35 \equiv 7 \in \operatorname{im}(\hat{q})$ and $r \cdot -1 \notin \operatorname{im}(\hat{q})$ for all $r \in \{1, 5, 7, 35\}$ (since otherwise, $-1 \in \operatorname{im}(\hat{q})$). Thus $\operatorname{im}(\hat{q}) = \{1, 5, 7, 35\}$ and $D(\mathbb{Q})/\hat{\varphi}(E(\mathbb{Q})) \simeq \operatorname{im}(\hat{q}) \simeq \langle (0,0), (5,0) \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now, $\hat{\varphi}(E(\mathbb{Q})/D(\mathbb{Q}))$ is trivial (since $E(\mathbb{Q})/D(\mathbb{Q})$ is trivial). So $E(\mathbb{Q})/2E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $E_{\text{tors}}(\mathbb{Q})$ is also $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, it follows that the rank must be trivial, and $E(\mathbb{Q}) = E_{\text{tors}}(\mathbb{Q})$.

2.4 Complete 2-descent

Complete 2-descent another method of finding the rank of an elliptic curve. Although it is slightly more complex to understand, it is much easier to generalise to higher genera. In this section, we shall describe complete 2-descent in the specific elliptic curve case, and later, we will describe complete 2-descent for Jacobians of higher genera.

Let $E \colon Y^2 = (X - A)(X - B)(X - C)$ where the roots are all in $\mathbb{Z}$ and distinct. As with 2-isogeny, finding $\mathfrak{G}/2\mathfrak{G}$ and the 2-torsion is sufficient to deduce the rank.

Instead of two maps to $\mathbb{Q}$ modulo squares, define a map $\mu' \colon G/2\mathfrak{G} \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ given by

$$\mu'(P) = \begin{cases} [\frac{A-C}{A-B}, A - B], & P = (A, 0); \\ [B - A, \frac{B-C}{B-A}], & P = (B, 0); \\ [1, 1], & P = \mathfrak{O}; \\ [x - A, x - B], & P = (x, y), x \neq A, B. \end{cases}$$

Then μ' is an injective homomorphism. Thus $\mathfrak{G}/2\mathfrak{G} \simeq \operatorname{im}(\mu')$. Thus it is sufficient to find the image of this map. Note also that

$$\operatorname{im}(\mu') \leq (\langle -1, 2, p \text{ prime} : p \mid (A - B)(B - C)(A - C) \rangle)^{\times 2}.$$

Thus $\mu'(A, 0)$ and $\mu'(B, 0)$ generate a lower bound for $\operatorname{im}(\mu')$. Any infinite order point (if one exists) will be independent from the previous subgroup, so can also be added on to get a bigger lower bound.

On the other hand, there are two ways to find an upper-bound for $\operatorname{im}(\mu')$. We can either use homogeneous spaces, or use a method presented by Cassels and Flynn. The latter of these methods is more practical for higher genus computations, though the first is easier to understand.

2.4.0.1 Using Homogeneous Spaces

From [2] X.1.1-1.4, we have the following result.

Proposition 2.4.1
$[r,s] \in (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ is the image of a point $P \in \mathfrak{G}/2\mathfrak{G}$ if and only if there is a solution $(l,m,n) \in \mathbb{Q}^{\times 3}$ with l,m non-zero to the system

$$\begin{aligned} rl^2 - sm^2 &= B - A \\ rl^2 - rsn^2 &= C - A. \end{aligned}$$

Furthermore, if a solution (l,m,n) for $[r,s]$ exists, then $P = (rl^2 + A, rslmn)$ is a point of $\mathfrak{G}$ that maps to $[r,s]$. Thus, this method is useful for finding generators of $\mathfrak{G}$. This is the biggest advantage of using homogeneous spaces, since the next method requires the knowledge of all generators to achieve a sharp bound.

2.4.0.2 Without Using Homogeneous Spaces

Let p be a prime. Denote $J(\mathbb{Q}_p)$ as $\mathfrak{G}_p$. Then there are inclusion maps i_p and j_p that map from global to local as in the following commutative diagram from [1] 11.2.

$$\begin{tikzcd}
\mathfrak{G}/2\mathfrak{G} \arrow[r, "\mu'"] \arrow[d, "i_p"] & M \leq (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2} \arrow[d, "j_p"] \\
\mathfrak{G}_p/2\mathfrak{G}_p \arrow[r, "\mu'_p"] & M_p \leq \left(\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2\right)^{\times 2}
\end{tikzcd}$$

Note that $\mu'_p = j_p \circ \mu' \circ i_p^{-1}$ is the map μ' on the relevant local fields. The general direction of this method is to choose a few primes p and look at the map μ'_p. Once we find the image of μ'_p, we can take the preimage of j_p to get an upper bound for the image of μ' since $\mathrm{im}(\mu') \leq \langle \mathrm{im}(\mu'_p), \ker(j_p) \rangle$. The hope is that taking intersections over a few p will give us a sharp upper bound and hence deduce the rank.

Since $M_p \leq \left(\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2\right)^{\times 2}$, we can take a set of representatives for $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ to generate the right. Thus [4] 3.3 can tell us the set of representatives.

Proposition 2.4.2
Let $x = p^n u \in \mathbb{Q}_p^*$ (written so $n \in \mathbb{Z}$ and $u \in \mathbb{Q}_p^*$). If p is an odd prime, then x is a square if and only if $u \mod p$ is a non-zero square and n is even. If $p = 2$, then $x = 2^n u \in \mathbb{Q}_2^*$ is a square if and only if n is even and $u \equiv 1 \mod 8$.

Proof.
Recall that every x can be written uniquely as $p^n u$ where u is a unit. So it's clear that n must be even if x was a square, in particular, x is a square if and only if n is even and

u is a square. If p is an odd prime, u is a square if and only if $u \mod p$ is a (non-zero) square by Hensel's lemma. If $p = 2$, then Hensel's lemma says that $u \mod 8$ is a square if and only if u is a square. □

Corollary 2.4.3
If $p \neq 2$, a set of representatives of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ is $\{1, p, u, up\}$ where $u \in \mathbb{Z}_p^*$ is a quadratic non-residue modulo p. If $p = 2$, then a set of representatives is $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.

Proof.
If $p \neq 2$, then clearly a non-square either has an odd power of p or the unit in the decomposition is a non-square and the set of representatives follows. If $p = 2$ then the squares in $\mathbb{Z}/8\mathbb{Z}$ are $\{\pm 1, \pm 5\}$, so the representatives also follow. □

These results easily give us the kernel of j_p.

Now we can use the fact ([1] 7.6) that

$$|\mathfrak{G}_p/2\mathfrak{G}_p| = \begin{cases} |\mathfrak{G}_p[2]|/2, & p = \infty; \\ |\mathfrak{G}_p[2]|, & p \neq 2, \infty; \\ 2|\mathfrak{G}_p[2]|, & p = 2. \end{cases}$$

This tells us how many generators we are looking for in the local field (since each element has order 2). We can find the lower bound of the image of M_p by taking the lower bound of M under j_p. After removing equivalent generators, we may be short of the required number.

To find extra generators, search for an x that lies in $\mathfrak{G}_p$ by using Proposition 2.4.2 and that under μ'_p maps to something outside the span of the existing generators. To do this, do trial and error on small x until we get a valid point in $\mathfrak{G}_p$ by checking that $(x-A)(x-B)(x-C)$ is indeed a square in $\mathbb{Q}_p$. Then apply the map μ' and check for independence. An implementation of this is given in the Appendix.

Here is a summary of the 2-descent procedure.

Proposition 2.4.4 (Complete 2-Descent)

- Let $E\colon Y^2 = (X-A)(X-B)(X-C)$, $A, B, C \in \mathbb{Z}$, $\Delta \neq 0$.
- Let $\mu'\colon \mathfrak{G}/2\mathfrak{G} \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ given by $\mu'(A, y) = [\frac{A-C}{A-B}, A-B]$, $\mu'(B, y) = [B-A, \frac{B-C}{B-A}]$, $\mu'(\mathfrak{O}) = [1, 1]$ and $\mu'(x, y) \mapsto [x-A, x-B]$ (modulo squares).
- Find the image of μ'_p. Consider the image of μ'_p, the map μ' on the local fields of $\mathbb{Q}$. Then find local generators for $\mathrm{im}(\mu'_p)$ by using existing generators of μ' and by finding new ones. Use the formula for $|\mathfrak{G}_p/2\mathfrak{G}_p|$ to verify that we have enough generators.
- Find $\ker(j_p)$.
- Take intersections of $\langle \mathrm{im}(\mu'_p), \ker(j_p) \rangle$ for a set of well chosen p to get back to the global image of μ'.
- The preimage of μ' is $\mathfrak{G}/2\mathfrak{G}$, so as with 2-isogeny, we can find the rank.

2.4.1 An Example

As with the 2-isogeny example, let $E\colon Y^2 = X(X-5)(X-7)$. Recall that $E_{\text{tors}}(\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^{\times 2}$ and that the rank is trivial. Instead of descent by 2-isogeny, let us use complete 2-descent.

Using the notation introduced before,

$$\mu'\colon E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}\colon (x,y) \mapsto [x, x-5].$$

Then the point $(0,0) \mapsto [35,-5]$ and $(5,0) \mapsto [5,-10]$. Finally, $(7,0)$ is dependent since $(7,0) = (0,0)(5,0) \mapsto [35,-5][5,-10] = [7,2]$. Thus

$$\begin{aligned}
&\langle [5,-10],[35,-5]\rangle\\
&\leq \operatorname{im}(\mu')\\
&\leq \langle \{1,-1,2,5,7\}^{\times 2}\rangle\\
&= \langle [1,-1],[-1,1],[2,1],[5,1],[7,1],[1,2],[1,5],[1,7]\rangle.
\end{aligned}$$

We check whether each element on the right are a possible image of μ'.

2.4.1.1 Using Homogeneous Spaces

Following Silverman's way of complete 2-descent, we need to determine if the equations

$$az_1^2 - bz_2^2 = 5, \qquad az_1^2 - abz_3^2 = 7$$

have solutions $z_1, z_2, z_3 \in \mathbb{Q}$ for every pair $[a,b] \in \langle \pm 2, \pm 5, \pm 7\rangle^{\times 2}$.

We shall consider multiple cases. For each case for some $[a,b]$, we consider whether the homogeneous spaces have no solutions in some $\mathbb{Q}_p$, thus no solutions in $\mathbb{Q}$.

- Clearly, if $a < 0$ then either $-b < 0$ or $-ab < 0$. Thus there are no solutions in $\mathbb{R}$ and so $[-a,b] \notin \operatorname{im}(\mu')$ for any $a,b \in \{1,2,5,7,10,14,35\}$.

- For $[1,-1]$, we have the equations $z_1^2 + z_2^2 = 5$ and $z_1^2 + z_3^2 = 7$. If there was an rational solution to this system, then there is certainly intgers y_1, y_2, y_3 such that $y_1^2 + y_2^2 = 7y_3^2$ by clearing denominators. But, by the sum of two squares theorem, this requires 7 to have an even exponent in the prime factorisation of $7y_3^2$, which is impossible. Thus $[1,-1] \notin \operatorname{im}(\mu')$.

- For $[2,1]$, we have $2z_1^2 - z_2^2 = 5$ and $2z_1^2 - 2z_3^2 = 7$. Clear denominators of the first equation to get $2y_1^2 - y_2^2 = 5y_3^2$. Since 2 is not a square modulo 5, $2y_1^2 \equiv y_2^2 \mod 5$ implies that $y_1 \equiv y_2 \equiv 0 \mod 5$, but then $v_5(2y_1^2 - y_2^2) = 5^{2n}$ for some positive integer n and so $v_5(v_3^2)$ is odd which is impossible. Thus, $[2,1] \notin \operatorname{im}(\mu')$.

  Similarly, $[1,2]$ gives $z_1^2 - 2z_2^2 = 5$ and $z_1^2 - 2z_3^2 = 7$. Considering the first equation modulo 5 gives that $[1,2] \notin \operatorname{im}(\mu')$. The same argument also works for $[1,7]$ and $[7,1]$. Noting that $-2 \equiv 3 \mod 5$ is also not a quadratic residue, $[1,-2]$, $[1,-7]$ also don't have solutions.

- If $a \equiv b \equiv 0 \mod 2$, say $a = 2a'$ and $b = 2b'$. Note that $2 \nmid a', b'$ since a and b are square free. The second homogeneous space gives $2a'z_1^2 - 4a'b'z_3^2 = 7$. Considering this modulo 2, we see that $v_2(z_1) \geq 0$. The first equation gives $2a'z_1^2 - 2b'z_2^2 = 5$. But $0 = v_2(5) = v_2(a'z_1^2 - 2b'z_2^2)$. If $v_2(z_2) \geq 0$, then $v_2(5) > 0$, a contradiction. So $v_2(z_2) < 0$, but then $v_2(-2b'z_2^2) < 0$, so $v_2(5) < 0$, also a contradiction. Hence none of these even pairs are in $\text{im}(\mu')$.

- For $[1, 5]$, we have $z_1^2 - 5z_2^2 = 5$ and $z_1^2 - 5z_3^2 = 7$. The second equation implies that $v_5(z_1) \geq 0$ and $v_5(z_3) \geq 0$ (otherwise $0 = v_5(7) < 0$). Furthermore the first equation says that $v_5(z_2) \geq 0$ and so in fact, $v_5(z_1) \geq 1$. But putting this back into the second equation gives $v_5(7) = v_5(z_1^2 - 5z_3^2) \geq 1$ which is impossible. Thus $[1, 5] \notin \text{im}(\mu')$.

  Clearly if $b \equiv 0 \mod 5$ and $a \not\equiv 0 \mod 5$ then the above argument also works.

- Now $[5, 1]$ gives $5z_1^2 - z_2^2 = 5$ and $5z_1^2 - 5z_3^2 = 7$. The first equation modulo 5 tells us that $v_5(z_2^2) \geq 1$, so $v_5(z_2) \geq 1$. Then $v_5(z_1) \geq 0$. The second equation modulo 5 with denominators cleared tells us that the common denominator y (the minimal integer that clears the denominators of z_1 and z_2, say $y_1 = yz_1$ and $y_2 = yz_2$ such that $y_1, y_2, y \in \mathbb{Z}$ and $\gcd(y_1, y_2, y) = 1$) must be divisible by 5. But then we have $v_5(z_1^2y^2 - z_3^2y^2) = v_5(7y^2) - 1 \geq 1$. Combining this with the result from the first equation, $v_5(z_1^2y^2) = v_5(z_1)^2 + v_5(y^2) \geq 2$, so $v_5(z_3^2y^2) \geq 1$. But then $\gcd(z_1y, z_3y, y) \geq 5$, which contradicts the fact that y was minimally chosen.

  It is clear that if $a \equiv 0 \mod 5$ and $b \not\equiv 0 \mod 5$ then the above argument still holds.

- Consider $[7, 7]$. Then we have $7z_1^2 - 7z_2^2 = 5$ and $7z_1^2 - 49z_3^2 = 7$. Then combining these, $49z_3^2 - 7z_2^2 = -2$. Let y be the minimal integer that clears the denominators of z_3 and z_2. Then modulo 7, we get that $7 \mid y$. So $49 \mid -7z_2^2$, and $7 \mid z_2$. Thus $z_3^2y^2 + 2(y/7)^2 \equiv 0 \mod 7$. But since -2 is not a quadratic residue, $z_3 \equiv 0 \mod 7$, a contradiction on the minimality of y. Thus $[7, 7] \notin \text{im}(\mu')$.

  If $a = 7$ and $b \equiv 0 \mod 7$ such that $b/7$ is not a quadratic residue modulo 7, then the argument above with the fact $-2(b/7)^{-1}$ is not a square says that $[7, -7]$ and $[7, 35]$ are not in $\text{im}(\mu')$.

- Since $[7, 2] \in \text{im}(\mu')$, $[1, 2] \notin \text{im}(\mu')$ and $[7, 1] = [7, 2][1, 2]$, then $[7, 1] \notin \text{im}(\mu')$. Similarly, if there is a non-image, multiplying by something in the image gives us another non-image.

Thus there exists no pairs outside the ones we already know such that $[a, b] \in \text{im}(\mu')$. Hence the rank is 0.

We summarise the previous calculation in the following table. If $[a, b] \in \text{im}(\mu')$ then we give a preimage, otherwise we write a local field of $\mathbb{Q}$ where the homogeneous equations do not have solutions. We say “grp” when the result is due to the group structure of the image. We omit $a < 0$ for space since all cases are covered by case 1 in $\mathbb{R}$.

$b \setminus a$	1	2	5	7	10	14	35	70
1	$\mathfrak{O}$	$\mathbb{Q}_5$	$\mathbb{Q}_5$	$\mathbb{Q}_5$	grp	grp	$\mathbb{Q}_5$	grp
2	$\mathbb{Q}_5$	$\mathbb{Q}_2$	$\mathbb{Q}_5$	$(7,0)$	$\mathbb{Q}_2$	grp	grp	$\mathbb{Q}_2$
5	$\mathbb{Q}_5$	grp	grp	$\mathbb{Q}_5$	grp	grp	grp	grp
7	$\mathbb{Q}_5$	grp	$\mathbb{Q}_5$	$\mathbb{Q}_7$	grp	grp	$\mathbb{Q}_5$	grp
10	grp	$\mathbb{Q}_2$	grp	grp	$\mathbb{Q}_2$	$\mathbb{Q}_2$	grp	$\mathbb{Q}_2$
14	grp	$\mathbb{Q}_2$	$\mathbb{Q}_5$	grp	$\mathbb{Q}_2$	$\mathbb{Q}_2$	grp	$\mathbb{Q}_2$
35	$\mathbb{Q}_5$	grp	grp	$\mathbb{Q}_5$	grp	grp	grp	grp
70	$\mathbb{Q}_5$	$\mathbb{Q}_2$	grp	$\mathbb{Q}_5$	$\mathbb{Q}_2$	$\mathbb{Q}_2$	grp	$\mathbb{Q}_2$
-1	$\mathbb{R}$	grp	grp	grp	grp	grp	grp	grp
-2	$\mathbb{Q}_5$	$\mathbb{Q}_2$	grp	grp	$\mathbb{Q}_2$	$\mathbb{Q}_2$	grp	$\mathbb{Q}_2$
-5	$\mathbb{Q}_5$	grp	grp	grp	grp	grp	$(0,0)$	grp
-7	$\mathbb{Q}_5$	grp	$\mathbb{Q}_5$	$\mathbb{Q}_7$	grp	grp	$\mathbb{Q}_5$	grp
-10	grp	$\mathbb{Q}_2$	$(5,0)$	$\mathbb{Q}_5$	grp	$\mathbb{Q}_2$	grp	$\mathbb{Q}_2$
-14	grp	$\mathbb{Q}_2$	$\mathbb{Q}_5$	grp	$\mathbb{Q}_2$	$\mathbb{Q}_2$	$\mathbb{Q}_5$	$\mathbb{Q}_2$
-35	$\mathbb{Q}_5$	grp	grp	$\mathbb{Q}_5$	grp	grp	grp	grp
-70	grp	$\mathbb{Q}_2$	grp	$\mathbb{Q}_5$	$\mathbb{Q}_2$	$\mathbb{Q}_2$	grp	$\mathbb{Q}_2$

2.4.1.2 Without using Homogeneous Spaces

Following Cassels and Flynn’s method.
Since there are four 2-torsion points, $|E_p(\mathbb{F}_p)[2]| = |E(\mathbb{Q})[2]| = 4$. So, we have that

$$|E_p(\mathbb{Q}_p)/2E_p(\mathbb{Q}_p)| = \begin{cases} 2, & p = \infty; \\ 4, & p \neq 2, \infty; \\ 8, & p = 2. \end{cases}$$

First consider $\mathbb{R}$. We have that $|E(\mathbb{R})/2E(\mathbb{R})| = 2$. A set of representatives for $\mathbb{R}^*/(\mathbb{R}^*)^2$ is $\{\pm 1\}$ and that $1 \not\equiv -1$. We already know that $[1,-1], [1,1] \equiv [5,-10], [7,2] \in \mathrm{im}(\mu')$. We already have two elements, so there are no others, in particular, $\mathrm{im}(\mu'_\infty) = \langle [1,-1] \rangle$. It follows that $\mathrm{im}(\mu) \leq \langle [1,-1], [2,1], [5,1], [7,1], [1,2], [1,5], [1,7] \rangle$

Next, consider $\mathbb{Q}_5$, so $|E(\mathbb{Q}_5)/2E(\mathbb{Q}_5)| = 4$. Then a set of representatives is $\{1, 5, 2, 10\}$. $M_5 = \langle [1,5], [5,1], [1,2], [2,1] \rangle$. Note that $7 \equiv 2 \mod 5$, so 7 is in the coset of 2; and -1 is a square in $\mathbb{Q}_5$, so is in the coset of 1. The points of order two map to $\langle [5,10], [10,5] \rangle$, which gives us the four distinct points. Thus these are sufficient generators. So, $\mathrm{im}(\mu'_5) = \langle [5,10], [10,5] \rangle$. Furthermore, $\ker(j_5) = \langle [1,-1], [-1,1], [14,1], [1,14] \rangle$. So

$$\mathrm{im}(\mu') \leq \langle [5,-10], [35,-5], [1,-1], [-1,1], [14,1], [1,14] \rangle.$$

Consider $\mathbb{Q}_7$ with representatives $\{1, 7, 5, 35\}$. $|E(\mathbb{Q}_7)/2E(\mathbb{Q}_7)| = 4$. Then $[5,-10] \equiv [5,1]$, $[35,-5] \equiv [35,1]$ are unique elements that generate a subgroup of order 4, so

$\mathrm{im}(\mu'_7) = \langle [5,-10],[35,-5] \rangle$. Furthermore, $\ker(j_7) = \langle [1,2],[2,1],[-5,1],[1,-5] \rangle$ and thus

$$\mathrm{im}(\mu') \leq \langle [5,-10],[35,-5],[1,2],[2,1],[-5,1],[1,-5] \rangle.$$

Taking intersections, we currently have $\mathrm{im}(\mu') \leq \langle [5,-10],[35,-5],[10,-5] \rangle$.

Finally, consider $\mathbb{Q}_2$ with representatives $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ and $\ker(j_2) = \langle \{1,-7\}^{\times 2} \rangle$. $|E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)| = 8$. Note $[5,-10]$ and $[35,-5] \equiv [-5,-5]$ are distinct generators of a subgroup of order 4. Consider a point $(x,y) \in E(\mathbb{Q}_2)$ with $x = 31$. Then $y^2 = 4^2 \cdot 1209$ and taking square roots is valid. This point maps to $[31,26] \equiv [-1,10]$ under μ'_2. This is unique from the other generators, and thus together, these three elements generate 8 elements. So

$$\mathrm{im}(\mu') \leq \{[5,-10],[35,-5],[-1,10],[7,-1],[1,-7]\}.$$

Taking the intersection, we get $\mathrm{im}(\mu') \leq \langle [5,-10],[35,-5] \rangle$. Thus the inequality is actually an equality and $\mathrm{rank}(E) = 0$.

Chapter 3

Genus 2 Curves

3.1 Definitions

Let k be a field with characteristic not 2.

Definition 3.1.1
A hyperelliptic curve over k is a non-singular curve such that $C\colon Y^2 = F(X)$ where $F(X) \in k[X]$ is a polynomial.

As mentioned before, we can define the genus of a hyperelliptic curve as follows.

Definition 3.1.2
A genus g hyperelliptic curve is birationally equivalent to a curve C where $C\colon Y^2 = F(X)$ such that F is of degree $2g+1$ or $2g+2$ and F has no repeated factors (so that the discriminant is nonzero). A more detailed discussion is in Section 3.2.1.

For the purpose of this dissertation, we will only consider examples of genus 2 curves that have the form

$$C\colon Y^2 = a_0 + a_1X + \cdots + a_5X^5 \in k[X],$$

where $a_5 \neq 0$ and where there are no multiple factors. We shall see in Section 3.2.2 that a curve $D\colon Y^2 =$ degree 6 in X is birationally equivalent to the above degree 5 case C if there exists a rational point on D.

As with the elliptic curve case, we actually treat C as a projective curve, so there is a point at infinity ∞.

Unlike elliptic curves, there is no non-trivial group structure on $C(k)$. Instead, we formally define the Jacobian which happens to be a group. This group can be thought of as pairs of points as we shall see.

Definition 3.1.3
The Jacobian $\mathfrak{G} = J(C)$ of a curve C is an algebraic variety which corresponds to Pic^0. This Jacobian is an abelian group.

In the sense of [2] II.3, a divisor group Div is the free abelian group generated by points in $C(k)$, i.e. $\sum_{\mathfrak{A}} n_{\mathfrak{A}}\mathfrak{A} \in \text{Div}$ where $\mathfrak{A} \in C(k)$ $n_{\mathfrak{A}} \in \mathbb{Z}$ and almost every $n_{\mathfrak{A}}$ is 0. An element $D \in \text{Div}$ is called principal if there exists a non-zero function f on $C(k)$ such that $f(\mathfrak{A})$ is a root/pole with multiplicity $n_{\mathfrak{A}}$.

The Picard group is the group of classes $\text{Div}/\sim$ where $\sim$ is the equivalence relation given by identifying principal divisors. Pic^0 are the elements of degree 0 in the Picard group Pic.

3.1.1 Group Law on the Jacobian

Let $C\colon Y^2 = F(X)$ be a genus 2 curve (so say $F(X)$ has degree 5). Then the Weierstrass points are the points invariant under $(x, y) \mapsto (x, -y)$ namely the zeros of F (of which there are at most five) and the point at infinity.

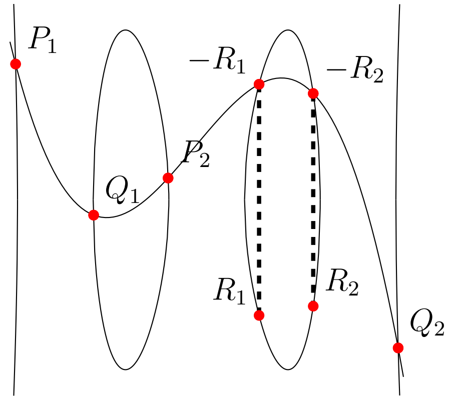
The identity is $\mathfrak{O}$ which is identified with all points of the form $\{(x, y), (x, -y)\}$ and $\{\infty, \infty\}$.

The Mordell-Weil group $J(\mathbb{Q})$ is given by the non-identity elements $\{(x, y), (u, v)\}$ modulo $\mathfrak{O}$ such that either $(x, y), (u, v) \in C(\mathbb{Q})$; or $(x, y), (u, v) \in C(\mathbb{Q}(\sqrt{d}))$ with (x, y) and (u, v) conjugates over $\mathbb{Q}$ and where $d \in \mathbb{Q}^* \setminus (\mathbb{Q}^*)^2$.

Negation is given by $\{(x, y), (u, v)\} \mapsto \{(x, -y), (u, -v)\}$.

The points of order two are pairs of distinct Weierstrass points, and these generate the full 2-torsion subgroup. Thus there are at most 15 order two elements.

Given two elements of $J(\mathbb{Q})$, $\mathfrak{A} = \{P_1, P_2\}$ and $\mathfrak{B} = \{Q_1, Q_2\}$, the sum of these elements involves finding the unique cubic $Y = \sum_{i=0}^{3} a_i X^i$ that goes through P_1, P_2, Q_1, Q_2 (which is analogous to the genus 1 case of a line). By substitution, this cubic meets C at six points (counting multiplicities), Let R_1, R_2 be the other two points. Then $\mathfrak{A} + \mathfrak{B} = -\{R_1, R_2\}$ where negation is as before. This is visually shown in the following diagram.



$$\{P_1, P_2\} + \{Q_1, Q_2\} = \{R_1, R_2\}$$

If two of P_1, P_2, Q_1, Q_2 are ∞ (say P_1 and Q_1), then the sum is $\{P_2, Q_2\}$. If one of them was ∞, then we ensure the projective cubic goes through ∞ by finding the affine quadratic through the other three points.

Example 3.1.4
Let $C\colon Y^2 = X(X-1)(X-2)(X-6)(X-9)$ be a genus 2 curve. Let us add the points $\{(2,0),(9,0)\}$ and $\{(9/4, 135/32), \infty\}$.

The cubic that goes through these four points must have a zero coefficent of X^3 (to make sure ∞ is on the projective cubic). This gives $Y = -\frac{5}{2}(X-2)(X-9)$. Substituting this into C (and cancelling the points corresponding to $X = 2$, $X = 9$ right away),

$$\begin{aligned}\frac{25}{4}(X-2)^2(X-9)^2 &= X(X-1)(X-2)(X-6)(X-9)\\ \frac{25}{4}(X^2-11X+18) &= X^3-7X^2+6X\\ 0 &= -X^3+15X^2-\frac{233}{2}X+\frac{225}{2}.\end{aligned}$$

The solutions are $X = 9/4$ (which we already know) and $X = \frac{1}{2}(11 \pm \sqrt{-79})$. Thus, the sum of these two points is $\left\{(\frac{1}{2}(11+\sqrt{-79}), 80), (\frac{1}{2}(11-\sqrt{-79}), 80)\right\}$.

3.1.2 Proof of Group Law

If we take the Picard definition of $\mathfrak{G}$, then we clearly inherit a group structure. But what if we defined the Jacobian and addition by the more concrete method of the previous subsection. Firstly, it is clear that negation is closed under the group law (since conjugation commutes with sign changes: $\overline{-x} = -\overline{x}$). And $\mathfrak{O}$ is indeed the identity by definition.

Let $\mathfrak{G}$ be the Jacobian of a genus 2 curve C and $\mathfrak{A}, \mathfrak{B} \in \mathfrak{G}$. If $\mathfrak{A}$ and $\mathfrak{B}$ were both rational, then clearly the unique cubic that goes through their pairs of points is rational. Since $C\colon Y^2 = F(X)$ is rational, the intersection with a rational cubic $Y = G(X)$ is given by the solutions of

$$G(X)^2 = F(X).$$

The left is a degree 6 polynomial in X and the right is a degree 5 (or degree 6 if F had degree 6). Thus the six intersection points are solutions to a rational sextic. Four of these solutions are already known rational points. Thus the final two solutions are solutions to a rational quadratic, of which roots are conjugate pairs as expected. If the X coordinates of two points on C are conjugate, then clearly their Y coordinates are conjugate too. Since negation is closed, $\mathfrak{A} + \mathfrak{B} \in \mathfrak{G}$.

Suppose instead that $\mathfrak{A}$ is rational but $\mathfrak{B}$ is not, say $\mathfrak{A} = \{P_1, P_2\}$ and $\mathfrak{B} = \{Q_1, Q_2\}$ so that Q_1, Q_2 are conjugates over a quadratic extension of $\mathbb{Q}$. By Lagrange polynomial interpolation, the unique cubic going through the points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $Q_1 = (x_3, y_3)$ and $Q_2 = (x_4, y_4) = (\overline{x_3}, \overline{y_3})$, is a sum

$$Y = G(X) = \sum_i y_i \frac{\sum_{j \neq i}(X - x_j)}{\sum_{j \neq i}(x_i - x_j)}.$$

If $i = 1$ the terms in the large sum looks like

$$y_1 \frac{(X - x_2)(X - x_3)(X - \overline{x_3})}{(x_1 - x_2)(x_1 - x_3)(x_1 - \overline{x_3})}.$$

Since the product $(X - x_3)(X - \overline{x_3})$ is rational, then the whole term is rational. Similarly the term $i = 2$ is also rational. The sum of the third and forth term is

$$\begin{aligned}&\frac{y_3(X - x_1)(X - x_2)(X - \overline{x_3})}{(x_3 - x_1)(x_3 - x_2)(x_3 - \overline{x_3})} + \frac{\overline{y_3}(X - x_1)(X - x_2)(X - x_3)}{(\overline{x_3} - x_1)(\overline{x_3} - x_2)(\overline{x_3} - x_3)} \\ &= \frac{y_3(X - x_1)(X - x_2)(X - \overline{x_3})(\overline{x_3} - x_1)(\overline{x_3} - x_2) - \overline{y_3}(X - x_1)(X - x_2)(X - x_3)(x_3 - x_1)(x_3 - x_2)}{(x_3 - x_1)(x_3 - x_2)(\overline{x_3} - x_1)(\overline{x_3} - x_2)(x_3 - \overline{x_3})}.\end{aligned}$$

In the denominator, $(x_3 - x_1)(\overline{x_3} - x_1)$ is rational (and similarly x_2). Suppose $x_3, y_3 \in \mathbb{Q}(\sqrt{d})$. Then $(x_3 - \overline{x_3})$ is some rational number times $\sqrt{d}$. The numerator is $y_3 z_1 - \overline{y_3 z_1}$ for some $z_1 \in \mathbb{Q}(\sqrt{d})$. But this simplifies to some rational multiple of $\sqrt{d}$. Thus we can cancel $\sqrt{d}$ from the numerator and denominator and be left with a rational cubic equation in X. As before, substituting $Y = G(X)$ into $Y^2 = F(X)$ yields a rational sextic. The roots corresponding to P_1 and P_2 can be factored out of $F(X) - G(X)^2 = 0$ as a rational linear factor, and the conjugate roots corresponding to Q_1 and Q_2 create a rational quadratic factor. Thus we are left with a rational quadratic that gives us the remaining two points of intersection. Thus $\mathfrak{A} + \mathfrak{B} \in \mathfrak{G}$.

Finally, if neither $\mathfrak{A}$ or $\mathfrak{B}$ are rational, then we can apply a similar argument to above to get that addition is truly closed.

The final part is showing that addition is associative. As usual, this is the hardest part. A similar proof to proving associativity in the elliptic curve case works. This involves a generalisation of Cayley–Bacharach theorem to higher degrees. Alternatively, we can get it for free by closely inspecting the Picard group definition of the Jacobian.

3.2 Discussion

3.2.1 Genus

One of the more general ways to define genus is Hurwitz's theorem (II.5.9 in [2]).

Theorem 3.2.1 (Hurwitz)
Let $\varphi\colon C_1 \to C_2$ be a non-constant separable map between smooth curves of genera g_1 and g_2 respectively. Then

$$2g_2 - 1 \geq (\deg \varphi)(2g_2 - 2) + \sum_{P \in C_1(k)} (e_\varphi(P) - 1).$$

Equality holds if and only if $\operatorname{char}(k) = 0$ or $\operatorname{char}(k) = p > 0$ where $p \nmid e_\varphi(P)$ for every $P \in C_1$.

Before proving that this definition of genus is consistent, we need a lemma (II.2.6 in [2]). For our needs, this lemma is sufficient as a defining feature of $e_\varphi(P)$.

Lemma 3.2.2
Let $\varphi\colon C_1 \to C_2$ as above. For every $Q \in C_2$,

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg(\varphi).$$

Corollary 3.2.3
The definition of genus in Hurwitz Theorem is the same as the definition as before.

Proof.
Let the genus of C be g. Let $\varphi\colon C \to \mathbb{P}^1$ (where $\mathbb{P}^1$ is the projective line, so has genus 0). This map is given by $(x, y) \mapsto (1, x)$. Since both $(x, y), (x, -y) \in C(k)$, φ has degree 2. Then Hurwitz's formula (assuming equality) becomes

$$2g + 2 = \sum_{P \in C(k)} (e_\varphi(P) - 1).$$

To resolve the right hand side, we note that the preimage of $(1, x) \in \mathbb{P}^1$ has two points if $y \neq 0$ and one point if $y = 0$ or the point is a single point at infinity. If we say the degree of the X part of C is d, then there are d points such that $y = 0$. Thus the latter case has $e_\varphi(P) = 2$, and the former is 1. If d is odd, there is a single point at infinity, otherwise when d is even, we have ∞^+ and ∞^- (which are two separate points at infinity). Thus, the right is d if d is even and $d + 1$ if d is odd. Hence $d = 2g + 1$ or $d = 2g + 2$ as desired. □

3.2.2 Degree 6

If instead we have the more general Y^2 = sextic in X of genus 2, we can always birationally transform this to a degree 5 whenever this sextic has a root in the base field. Let α be this root. Then take the map

$$(x, y) \mapsto \left(\frac{1}{x - \alpha}, \frac{y}{(x - \alpha)^3}\right) \quad \text{with inverse} \quad (x, y) \mapsto \left(\frac{1}{x} + 2, \frac{y}{x^3}\right).$$

Proof.
Write $C\colon Y^2 = (X-\alpha)(a_0 + a_1X + \cdots + a_5X^5)$. Then after the birational map, this becomes

$$\frac{Y^2}{X^6} = \left(\frac{1}{X} + \alpha - \alpha\right)\left(a_0 + a_1\left(\frac{1}{X}+\alpha\right) + \cdots + a_5\left(\frac{1}{X}+\alpha\right)^5\right),$$

and so,

$$Y^2 = a_0X^5 + a_1(1+\alpha X)X^4 + \cdots + a_5(1+\alpha X)^5,$$

which is of the desired degree 5 form given at the start of this chapter. □

Note that the points of infinity of $C\colon Y^2 =$ sextic are ∞^+ and ∞^-. These should be treated as points in $C(\mathbb{Q})$, so in the Jacobian, $\{\infty^+, \infty^+\} \neq \mathfrak{O} = \{\infty^+, \infty^-\}$.

3.2.3 The Jacobian

As mentioned, the proper way to construct the Jacobian is to use the Picard group. Knowing the computational aspect is enough for basic calculations, but there is some theory that is needed for proofs, which we will outline here (taken from main points of Chapter 2 and 3 of [1]).

Given a generic pair of points (x, y) and (u, v) on $C(\mathbb{Q})$, there are 16 functions (z_i) (given in 2.1.5, 2.1.6, 2.1.7, 2.1.8, 2.1.10, 2.12 of [1]) depending on x, y, u, v and the coefficients of C that generate a linear space L (in fact, they form a basis for L). Then the Jacobian $J(C)$ of C is the projective locus of these 16 functions (i.e. the vanishing set). By Hilbert's basis theorem, there exists a finite basis of this vanishing set. This basis involves 72 quadratic polynomials[1].

This description of the Jacobian is hard to use, so in Chapter 3 of [1], the Kummer surface $K(C)$ is introduced. $K(C)$ is defined to be four of the 16 basis elements (z_i) as given by ξ_i in 3.0.1 of [1]. These 4 functions give rise to biquadratic forms which allow us to fun either the sum or difference of two elements of $\mathfrak{G}$ (but these forms cannot differentiate between the sum or difference). These forms extend to bilinear forms[2] Φ_{ij}.

3.3 Torsion

As with elliptic curves, higher genus Jacobians have finite torsion.

[1] Which can be found here http://people.maths.ox.ac.uk/flynn/genus2/jacobian.variety/defining.equations

[2] Which can be found here http://people.maths.ox.ac.uk/flynn/genus2/jacobian.variety/bilinear.forms

Proposition 3.3.1 (Reductions)
Let $\mathfrak{G} = J(\mathbb{Q})$ be the Jacobian of a curve over $\mathbb{Q}$. If for a prime p, $C \mod p$ is non-singular, then $\mathfrak{G}_{\text{tors}}$ is isomorphic to a subgroup of $\tilde{\mathfrak{G}}_p = \tilde{J}(\mathbb{F}_p)$ which is the Jacobian of $\tilde{C}_p = C \mod p$.

The reduced curve is an elliptic curve when $p \neq 2$ and $p \nmid \Delta$. We call these p primes of good reduction. Note that furthermore, $|\mathfrak{G}_{\text{tors}}| \mid |\tilde{\mathfrak{G}}_p|$ and the torsion is finite.

For any p, finding the group $\tilde{\mathfrak{G}}_p$ is simple. For each $x \in \mathbb{F}_p$, find the square root of $F(x)$ (where the curve is $Y^2 = F(X)$) if it exists. The difference to the elliptic curves case is that we then need to check for points in quadratic extensions.

Example 3.3.2
Let $C\colon Y^2 = X(X-2)(X-3)(X-5)(X-8)$ be a genus-2 curve. The discriminant is $\Delta = 2^{12}3^8 5^4$. Note the six obvious Weierstrass points give rise to 16 elements in the 2-torsion.

First consider $p = 7$, the reduced curve is $\tilde{C}_7\colon Y^2 = X(X-1)(X-2)(X-3)(X-5)$, and so there are still 16 elements in the 2-torsion. Additional points in $\tilde{C}_7(\mathbb{F}_7)$ are $(4, \pm 2)$. Putting these points with the Weierstrass points give 6 points each, and with themselves 2 points. So we have counted 30 points.

Now, we need to look for points in the quadratic extensions. To do this, take any quadratic non-residue, say 3. We will find every point $(a + b\sqrt{3}, c + d\sqrt{3}) \in \tilde{C}_7(\mathbb{F}_4 9)$ where $a, b \in \mathbb{F}_7$ with $b \neq 0$ (since these are the existing points found before, or the identity). There are 36 such points. Pairing them together as conjugates gives 18 elements. Thus, in total, $|\tilde{\mathfrak{G}}_7| = 48$.

Similarly consider $p = 11$, the reduced curve is $Y^2 = X(X-2)(X-3)(X-5)(X-8)$, which also has 16 elements in 2-torsion. Additional points in $\tilde{C}_{11}(\mathbb{F}_{11})$ are $(1, \pm 1)$, $(9, \pm 4)$ and $(10, \pm 1)$. Adding in 58 pairs of conjugates in $\tilde{C}_{11}(\mathbb{F}_{11^2})$, we get $|\tilde{\mathfrak{G}}_{11}| = 128$.

The greatest common factor of these is 16, but we already have 16 points of order 2, so these are the only torsion points and $|\mathfrak{G}_{\text{tors}}| = |\mathfrak{G}[2]| = 16$.

As in [1] 2.2, we have the following equation,

$$|\tilde{\mathfrak{G}}_p| = 1 + \frac{1}{2}|W_p|(|W_p| - 1) + |W_p||R_p| + \frac{1}{2}|R_p|^2 + \frac{1}{2}|T_p|$$

where

$$\begin{aligned} W_p &= \{P \in \tilde{C}(\mathbb{F}_p) : P \text{ is a Weierstrass point}\}, \\ R_p &= \{P \in \tilde{C}(\mathbb{F}_p) : P \text{ is not a Weierstrass point}\}, \\ T_p &= \{(a + b\sqrt{\gamma}, c + d\sqrt{\gamma}) \in \tilde{C}(\mathbb{F}_{p^2}) : b \neq 0\} \end{aligned}$$

and γ is a fixed quadratic non-residue modulo p. In the formula, the first term accounts for members of $\tilde{\mathfrak{G}}_p$ of the form $\{P, Q\}$ where both P and Q are Weierstrass points. The second term is where $P \in W_p$ is a Weierstrass point and $Q \in R_p$ is not. The third term accounts for both components being in R_p, and the final term accounts for conjugate pairs in T_p.

3.4 Complete 2-descent

As with Elliptic curves, the Mordell-Weil theorem holds, that is, the rank of $\mathfrak{G}$ is finite. Thus, we can find this rank. Here, we shall give a full description of complete 2-descent for genus 2-curves.

Let $C\colon Y^2 = \prod_{i=1}^{5}(X - e_i)$ where the roots are all in $\mathbb{Z}$ and distinct. Let $\mathfrak{G} = J(\mathbb{Q})$. We aim to find $\mathfrak{G}/2\mathfrak{G}$.

Define a map $\mu\colon C(\mathbb{C}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 4}$ given by

$$\mu'(P) = \begin{cases} [\prod_{j\neq 1}(e_1 - e_j), e_1 - e_2, e_1, e_3, e_1 - e_4], & P = (e_1, 0); \\ [e_2 - e_1, \prod_{j\neq 2}(e_2 - e_j), e_2 - e_3, e_2 - e_4], & P = (e_2, 0); \\ [e_3 - e_1, e_3 - e_2, \prod_{j\neq 3}(e_3 - e_j), e_3 - e_4], & P = (e_3, 0); \\ [e_4 - e_1, e_4 - e_2, e_4 - e_3, \prod_{j\neq 4}(e_4 - e_j)], & P = (e_4, 0); \\ [1, 1, 1, 1], & P = \infty; \\ [x - e_1, \dots, x - e_5], & P = (x, y), x \neq e_1, \dots, e_4. \end{cases}$$

Then μ is a homomorphism. Further, define $\mu'\colon \mathfrak{G}/2\mathfrak{G} \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 4}$ given by $\mu'(\{P, Q\}) = \mu(P)\mu(Q)$. Then μ' is an injective homomorphism. Thus $\mathfrak{G}/2\mathfrak{G} \simeq \operatorname{im}(\mu')$. Thus it is sufficient to find the image of this map. Note also that

$$\operatorname{im}(\mu') \leq (\langle -1, 2, p \text{ prime} : p \mid \prod_{i\neq j}(e_i - e_j)\rangle)^{\times 4}.$$

Thus $\{\mu'(e_i, 0) : 1 \leq i \leq 5\}$ generate a lower bound for $\operatorname{im}(\mu')$. We also add any infinite generators to this list. We shall use Cassels and Flynn's method to find an upper bound.

Let p be a prime. Denote $J(\mathbb{Q}_p)$ as $\mathfrak{G}_p$. As in the genus 1 case, there are inclusion maps i_p and j_p that map from global to local as in the following commutative diagram.

$$\begin{tikzcd} \mathfrak{G}/2\mathfrak{G} \arrow[r, "\mu'"] \arrow[d, "i_p"] & M \leq (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 4} \arrow[d, "j_p"] \\ \mathfrak{G}_p/2\mathfrak{G}_p \arrow[r, "\mu'_p"] & M_p \leq \left(\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^4\right)^{\times 2} \end{tikzcd}$$

We will find an upper bound for $\operatorname{im}(\mu')$ as in the genus 1 case by taking intersections of $\langle \operatorname{im}(\mu'_p), \ker(j_p)\rangle$. To find the image in the local case we can use the fact that

$$|\mathfrak{G}_p/2\mathfrak{G}_p| = \begin{cases} |\mathfrak{G}_p[2]|/4, & p = \infty; \\ |\mathfrak{G}_p[2]|, & p \neq 2, \infty; \\ 4|\mathfrak{G}_p[2]|, & p = 2. \end{cases}$$

Here is a summary of the 2-descent procedure.

Proposition 3.4.1 (Complete 2-Descent)

- Let $E\colon Y^2 \prod_{i=1}^5 (X - e_i)$, $e_i \in \mathbb{Z}$, $\Delta \neq 0$.
- Find $\mu'\colon \mathfrak{G}/2\mathfrak{G} \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ as defined above.
- Find the image of μ'_p. Consider the image of μ'_p, the map μ' on the local fields of $\mathbb{Q}$. Then find local generators for $\operatorname{im}(\mu'_p)$ by using existing generators of μ' and by finding new ones. Use the formula for $|\mathfrak{G}_p/2\mathfrak{G}_p|$ to verify that we have enough generators.
- Find $\ker(j_p)$.
- Take intersections of $\langle \operatorname{im}(\mu'_p), \ker(j_p)\rangle$ for a set of well chosen p to get back to the global image of μ'.
- The preimage of μ' is $\mathfrak{G}/2\mathfrak{G}$ so we can find the rank.

3.4.1 An Example

Let $C\colon Y^2 = X(X-2)(X-3)(X-5)(X-8)$ be a genus 2 curve with Jacobian J. Write $\mathfrak{G} = J(\mathbb{Q})$.

We can take $\{(x,0), \infty\}$ for $x \in \{0,2,3,5\}$ as four independent generators of order 2. We aim to show that these are sufficient generators and that the rank is 0.

$$\mu'\colon \mathfrak{G}/2\mathfrak{G} \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 4}\colon (x,y) \mapsto [x, x-2, x-3, x-5].$$

(i) $x = 0 \mapsto [240, -2, -3, -5] \equiv [15, -2, -3, -5]$,

(ii) $x = 2 \mapsto [2, -36, -1, -3] \equiv [2, -1, -1, -3]$,

(iii) $x = 3 \mapsto [3, 1, 30, -2]$,

(iv) $x = 5 \mapsto [5, 3, 2, -90] \equiv [5, 3, 2, -10]$.

Let H be the subgroup generated by the above,

$$H = \langle [15,-2,-3,-5], [2,-1,-1,-3], [3,1,30,-2], [5,3,2,-10] \rangle.$$

Then we have

$$H \leq \operatorname{im}(\mu') \leq \langle \{1,-1,2,3,5\}^{\times 4} \rangle.$$

Additionally writing $\mathfrak{G}_p$ for $J_p(\mathbb{Q}_p)$, $|\mathfrak{G}_p[2]| = |\mathfrak{G}[2]| = 16$. It follows that

$$|\mathfrak{G}_p/2\mathfrak{G}_p| = \begin{cases} 4, & p = \infty; \\ 16, & p \neq 2, \infty; \\ 64, & p = 2. \end{cases}$$

First consider $\mathbb{R}$ where representatives for $\mathbb{R}^*/(\mathbb{R}^*)^2$ is $\{\pm 1\}$. We require two generators. Clearly $(i) \equiv (ii) \equiv [1, -1, -1, -1]$ is distinct from $(ii) = (iv) = [1, 1, 1, -1]$. The kernel is $\ker(j_\infty) = \langle \{1, 2, 3, 5\}^{\times 4} \rangle$. Thus

$$\mathrm{im}(\mu') \leq \langle H, \{1, 2, 3, 5\}^{\times 4} \rangle.$$

Next, consider $\mathbb{Q}_3$ with representatives $\{\pm 1, \pm 3\}$ and kernel $\ker(j_3) = \langle \{1, -2, -5\}^{\times 4} \rangle$. We require four generators. The ones we know from H are $(i) = [-3, 1, -3, 1]$, $(ii) = [-1, -1, -1, -3]$, $(iii) = [3, 1, 3, 1]$ and $(iv) = [-1, 3, -1, -1]$. These are sufficient since looking at the second entries, (iv) are not in the span of the other three; similarly the forth entry for (ii); and $(i), (iii)$ are clearly distinct. Thus

$$\mathrm{im}(\mu') \leq \langle H, \{1, -2, -5\}^{\times 4} \rangle.$$

Now, consider $\mathbb{Q}_5$ with representatives $\{1, 2, 5, 10\}$ and kernel $\ker(j_5) = \langle \{\pm 1, 6\}^{\times 4} \rangle$. The known generators reduce to $(i) = [10, 2, 2, 5]$, $(ii) = [2, 1, 1, 2]$, $(iii) = [2, 1, 5, 2]$, $(iv) = [5, 2, 2, 10] = (i) \cdot (ii)$. The first three elements generate a subgroup of order 8 since (i) is the only element with 5 in the first component, and clearly $(ii) \not\equiv (iii)$. To get the final required generator, note that $(1, \sqrt{56}) \in J(\mathbb{Q}_5)$ maps to $[1, -1, -2, -4] \equiv [1, 1, 2, 1]$. This is not in the span of the other generators because the only way to get 1 in the first coordinate is $(ii) \cdot (iii)$ which is not equivalent. Thus,

$$\mathrm{im}(\mu') \leq \langle H, \{\pm 1, 6\}^{\times 4}, [1, 1, 2, 1] \rangle.$$

Finally, consider $\mathbb{Q}_2$ with representatives $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ and $\ker(j_2) = \langle \{1, -15\}^{\times 4} \rangle$. Then $(i) = [-1, -2, -3, 3]$, $(ii) = [2, -1, -1, -3]$, $(iii) = [3, 1, -2, -2]$ and $(iv) = [-3, 3, 2, 6]$. Looking at the first entry, (i), (ii) and (iii) are all distinct and not the product of each other. And clearly, $(iv) \neq (i) \cdot (iii)$. Thus these four elements generate a subgroup of order 16, and we need to find two more generators. Firstly $(27, \sqrt{2^4 \cdot 423225}) \in J(\mathbb{Q}_2)$ and this maps to $[27, 25, 24, 22] \equiv [3, 1, 6, 6]$. This is not in the span of the other generators since it is not equivalent to (iii) or $(i) \cdot (iv)$ (which are sufficient observations because of the first entry). Secondly, $(-2, \sqrt{2^4 \cdot -175}) \in J(\mathbb{Q}_2)$ which maps to $[-2, -4, -5, -7] \equiv [-2, -1, 3, 1]$. Again, this is not in the span of the previous five generators, so we have the six required generators and

$$\mathrm{im}(\mu') \leq \langle H, \{1, -15\}^{\times 4}, [3, 1, 6, 6], [-2, -1, 3, 1] \rangle.$$

So $\mathrm{im}(\mu')$ is contained in the intersection of the above upper bounds. It remains to show that this intersection is equal to H.

The last entries of H are $\{-5, -3, -2, -10\}$ and the span is $\langle -1, 2, 3, 5 \rangle$. Note that inside the span, only $[1, 1, 1, 1]$ has a last entry of 1. We check for all possible elements of $\mathrm{im}(\mu')$ that have a last entry of 1.

First consider $p = 5$, we can only affect the last entry of an element in $\langle H \rangle$ by multiplying by ± 6. So the non-identity elements with last entry 1 in $\langle H, \{\pm 1, 6\}^{\times 4}, [1, 1, 2, 1] \rangle$

is $\alpha \cdot [a,b,c,d]$, $\alpha \cdot [1,1,2,1] \cdot [a,b,c,d]$ where $a,b,c \in \{\pm 1, \pm 6\}$ and $\alpha \in H$ with last entry $d \in \pm 1, \pm 6$. So we have $\alpha \in \{[6,-1,-30,6],[6,6,6,-6],[1,-6,-5,-1]\}$ and $\alpha \cdot [1,1,2,1] \in \{[6,-1,-15,6],[6,6,3,-6],[1,-6,-10,-1]\}$. Note, in particular, after multiplying by $[a,b,c,d]$, the first and second entry must be one of $\{\pm 1, \pm 6\}$.

For $p = 3$, since the kernel is $\{1,-2,-5,10\}$, for the last entry to be 1, the elements in H that we multiple by the kernel need to have last entry $\{1,-2,-5,10\}$; namely, $\{[15,-2,-3,-5],[3,1,30,-2],[5,-2,-10,10]\}$. The only ones that after multiplication give something with first and second entry $\{\pm 1, \pm 6\}$ are

$$\{[6,1,-3c,1],[-6,1,30c,1],[-1,1,-10c,1]\}, \quad \text{where} \quad c \in \{1,-2,-5,10\}.$$

Finally, considering $p = \infty$, the only reductions that have last entry 1 are $[1,-1,-1,1]$ and $[1,1,1,1]$. Since none of the 12 elements in the previous paragraphs have either of these forms, the only element in the intersection must be the identity.

Suppose for a contradiction that there exists $\alpha \in \operatorname{im}(\mu')$ such that $\alpha \notin H$. Then the last entry cannot be 1. Since the span of H can have any last entry, there exists $\beta \in H$ such that it has the same last entry as α. Then $\alpha \cdot \beta$ has last entry 1. But any element in $\operatorname{im}(\mu')$ with last entry 1 must be $[1,1,1,1]$, so $\alpha = \beta^{-1}$ and so $\alpha \in H$, a contradiction. Thus $\operatorname{im}(\mu') = H$ and the rank of $\mathfrak{G}$ is 0.

3.5 Descent by Richelot Isogeny

As with the elliptic curve case, instead of doing a complete 2-descent, we can do a descent by isogeny. The genus 2 case is due to Richelot. We also have that complete 2-descent is at least as good as descent by Richelot isogeny. We shall now describe the process of getting the rank using Richelot isogenies.

First, define $C\colon Y^2 = G_1(x)G_2(X)G_3(X)$ a genus 2 curve such that G_1 and G_2 are quadratics and G_3 is either linear or quadratic and let g_{ij} be the coefficient of X^j in G_i. Define $C''\colon \Delta Y^2 = L_1(X)L_2(X)L_3(X)$ where $\Delta = \det(g_{ij})$ and

$$\begin{aligned} L_1(X) &= G_2'(X)G_3(X) - G_2(X)G_3'(X), \\ L_2(X) &= G_3'(X)G_1(X) - G_3(X)G_1'(X), \\ L_3(X) &= G_1'(X)G_2(X) - G_1(X)G_2'(X). \end{aligned}$$

These two curves are isogenous with the maps $\varphi\colon J(C) \to J(C'')$ and $\varphi''\colon J(C'') \to J(C)$ as described in ([1] Ch10 1(ii) p103 and Ch9).

Now, birationally transform C'' to a curve C' such that the polynomial is monic (the coefficients of Y^2 and X^6 or X^5 are 1). Since these will be birationally equivalent, their Jacobians will be isomorphic. Let the Jacobian of C' be $\mathfrak{G}'$ and C be $\mathfrak{G}$. Let φ' be the composition of the birational transformation with the isogeny φ''.

As with the other methods of descent, we define a homomorphism onto the square free rationals: $\mu\colon \mathfrak{G}'/\varphi(\mathfrak{G}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ by

$$\mu(\{(x,y),(u,v)\}) = [L_1(x)L_1(u), L_2(x)L_2(u)],$$

and the dual $\mu'\colon \mathfrak{G}/\varphi'(\mathfrak{G}') \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ by

$$\mu'(\{(x,y),(u,v)\}) = [G_1(x)G_1(u), G_2(x)G_2(u)].$$

Sometimes, one of the entries may be undefined ($= 0$). One trick is to note that $L_1(x)L_1(u)L_2(x)L_2(u) \equiv L_3(x)L_3(u)$ (modulo squares). Another is to note that μ is a homomorphism.

Our goal is to find the images of μ and μ'. We know the solutions to L_i and G_i correspond to points of $\mathfrak{G}$ and $\mathfrak{G}'$, so these give us a lower bound (together with any free generators). To find an upper bound, we do the usual intersections of local reductions. To know that we have every generator in the local cases, we use the fact that

$$|\mathfrak{G}'_p/\varphi(\mathfrak{G}_p)| \cdot |\mathfrak{G}_p/\varphi'(\mathfrak{G}'_p)| = \begin{cases} 4, & p = \infty; \\ 16 & p \neq 64, \infty; \\ 16, & p = 2. \end{cases}$$

Once we know the images, we are able to deduce the structure of $\mathfrak{G}/2\mathfrak{G}$ and thus using the Mordell-Weil theorem, the rank.

3.5.1 An Example

We shall do a decent on the same curve as before, $C\colon Y^2 = X(X-2)(X-3)(X-5)(X-8) = (X^2-5X+6)(X^2-5X)(X-8)$.

Using the notation given before, $(X^2-5X+6)(X^2-5X)(X-8) = G_1(X)G_2(X)G_3(X)$ and $g_{10} = 6$, $g_{11} = -5$, $g_{12} = 1$, $g_{20} = 0$, $g_{21} = -5$, $g_{22} = -5$, $g_{30} = -9$, $g_{31} = 0$ and $g_{32} = 1$. So

$$\Delta = \det(g_{ij}) = \det\begin{pmatrix} 6 & -5 & 1 \\ 0 & -5 & -5 \\ -9 & 0 & 1 \end{pmatrix} = -300.$$

Furthermore, let

$$\begin{aligned} L_1 &= G_2'(X)G_3(X) - G_2(X)G_3'(X) = X^2 - 16X + 40, \\ L_2 &= G_3'(X)G_1(X) - G_3(X)G_1'(X) = -X^2 + 16X - 34, \\ L_3 &= G_1'(X)G_2(X) - G_1(X)G_2'(X) = -12X + 30. \end{aligned}$$

The the curve with isogenous Jacobian is

$$C''\colon \Delta Y^2 = (X^2 - 16X + 40)(-X^2 + 16X - 34)(-12X + 30).$$

We shall birationally map this curve to a monic curve. Firstly, multiply both sides by -300 then take the map $-300Y \mapsto Y$ to get the curve

$$Y^2 = -300(X^2 - 16X + 40)(-X^2 + 16X - 34)(-12X + 30).$$

Then, multiply by $(-300 \cdot 12)^4$ and use the maps $(-3600)^2 Y \mapsto Y$ and $-3600X \mapsto X$ to get

$$C' \colon Y^2 = (X^2 - 57600X + 518400000)(X^2 - 57600X + 440640000)(X - 9000) = L_1(X)L_2(X)L_3(X).$$

Denote the Jacobian of this curve by $\mathfrak{G}'$. Since C' is birational to C'', their Jacobians are isomorphic.

Define the usual homomorphism $\mu \colon \mathfrak{G}'/\varphi(\mathfrak{G}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ by

$$\mu(\{(x,y),(u,v)\}) = [L_1(x)L_1(u), L_2(x)L_2(u)],$$

and the dual $\mu' \colon \mathfrak{G}/\varphi'(\mathfrak{G}') \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ by

$$\mu'(\{(x,y),(u,v)\}) = [G_1(x)G_1(u), G_2(x)G_2(u)].$$

With μ', the five points $\{(x,0),\infty\}$ for $x \in \{0,2,3,5,8\}$ map to

1. $x = 0 \mapsto [6,-3]$ (where the second entry is found using the fact that $L_2(x) = L_1(x)L_3(x)$),
2. $x = 2 \mapsto [1,-6]$,
3. $x = 3 \mapsto [30,-6]$,
4. $x = 5 \mapsto [6,-2]$,
5. $x = 8 \mapsto [30,24] \equiv [30,6]$ (which is the product of the other four cases, so this point is redundant).

The first four elements are independent since clearly no two are equal, and the product of all four is neither trivial nor one of the four generators. Thus they generate a subgroup of order 16, $\langle [6,-3],[1,-6],[30,1],[1,6] \rangle = \langle [1,-1],[6,3],[1,6],[30,1] \rangle$. So, we know that

$$H' = \langle [1,-1],[6,3],[1,6],[30,1] \rangle \leq \operatorname{im}(\mu') \leq (\langle 1,-1,2,3,5 \rangle)^{\times 2}.$$

We aim to show that $\operatorname{im}(\mu')$ is exactly H.

For μ, we claim that the following three elements generate $\operatorname{im}(\mu) \leq (\langle -1,2,3,5 \rangle)^{\times 2}$:

1. $\{(28800 - 7200\sqrt{6}, 0), (28800 + 7200\sqrt{6}, 0)\} \mapsto [1,1]$,
2. $\{(28800 - 3600\sqrt{30}, 0), (28800 + 3600\sqrt{30}, 0)\} \mapsto [1,1]$,
3. $\{(9000,0),\infty\} \mapsto [1,1]$.

We shall resolve $\mathrm{im}(\mu)$ and $\mathrm{im}(\mu')$ using a similar method to that of complete 2-descent using the commutative diagram.

First, consider the local case $\mathbb{R}$. Then a set of representatives for $(\mathbb{R}^*/(\mathbb{R}^*))^2$ is $\{\pm 1\}$ and $\ker(j_\infty) = \langle \{1,2,3,5\}^{\times 2}\rangle$. We also have that $|\mathfrak{G}'_\infty/\varphi(\mathfrak{G}_\infty)| \cdot |\mathfrak{G}_\infty/\varphi'(\mathfrak{G}'_\infty)| = 4$, so we need a total of two generators. The four generators of H' map to $\langle [1,-1]\rangle$, a subgroup of order 2. The second generator comes from $\mathfrak{G}'_\infty$ - take $\{(x,y),\infty\}$ such that $x = 20000$ and $y^2 \geq 0$, then this maps to $[-1,-1]$. Thus $|\mathfrak{G}'_\infty/\varphi(\mathfrak{G}_\infty)| = |\mathfrak{G}_\infty/\varphi'(\mathfrak{G}'_\infty)| = 2$ and $\mathrm{im}(\mu') \leq \langle [1,-1], \ker(j_\infty)\rangle$ and $\mathrm{im}(\mu) \leq \langle [1,-1], \ker(j_\infty)\rangle$.

Next, consider $\mathbb{Q}_3$ with representatives $\{\pm 1, \pm 3\}$ and kernel $\ker(j_3) = \langle \{1,-2,-5\}^{\times 2}\rangle$. Then

$$H' \mapsto \langle [1,-1],[-3,3],[1,-3],[3,1]\rangle = \langle [1,-1],[-1,1],[1,3],[3,1]\rangle.$$

This has size 16, and since $|\mathfrak{G}'_3/\varphi(\mathfrak{G}_3)| \cdot |\mathfrak{G}_3/\varphi'(\mathfrak{G}'_3)| = 16$, then $|\mathfrak{G}'_3/\varphi(\mathfrak{G}_3)| = 1$. Thus $\mathrm{im}(\mu) \leq \ker(j_3)$ and $\mathrm{im}(\mu') \leq \langle H', \ker(j_3)\rangle$.

Now consider $\mathbb{Q}_2$ with representatives $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ and $\ker(j_2) = \langle \{1,-15\}^{\times 2}\rangle$. Since $|\mathfrak{G}'_2/\varphi(\mathfrak{G}_2)| \cdot |\mathfrak{G}_2/\varphi'(\mathfrak{G}'_2)| = 64$, we are looking for a total of 6 generators. H' gives us $[1,-1]$, $[6,3]$, $[1,6]$ and $[-2,1]$. These are independent since they are clearly all different and the product of the four is neither trivial nor one of the four. We require two extra generators. These both come from $\mathfrak{G}_2$. First, take the point $\{(-2,\sqrt{2^4 \cdot -175}),\infty\}$, this maps to $[20,14] \equiv [5,7] \equiv [-3,-1]$. This is independent since the only way to get -3 in the first entry is $[-2,1][6,3] = [-3,3]$ and multiplying by any combination of $[1,-1]$ and $[1,6]$ can never make the second entry -1. The second point is $\{(-3,\sqrt{2^4 \cdot -495}),\infty\}$ which maps to $[30,24] \equiv [7,6] \equiv [-1,6]$. This is independent to the other five generators since there is no way to get -1 in the first entry. Thus $|\mathfrak{G}'_3/\varphi(\mathfrak{G}_3)| = 1$ and $|\mathfrak{G}_3/\varphi'(\mathfrak{G}'_3)| = 64$. It follows that $\mathrm{im}(\mu) \leq \ker(j_2)$ and $\mathrm{im}(\mu') \leq \langle H', [-3,-1], [-1,6], \ker(j_2)\rangle$.

We now have enough information to determine $\mathrm{im}(\mu)$. We know that

$$H \leq \mathrm{im}(\mu) \leq \ker(j_3) \cap \ker(j_2) \cap \langle [1,-1], \ker(j_\infty)\rangle.$$

From $p = \infty$, we get that either both entries are positive or the first is positive and second negative. Then taking intersections with $p = 2$ tells us that $\mathrm{im}(\mu) \leq \langle [1,-15]\rangle$. But this isn't included in the $p = 3$ case since -15 is not a square in $\mathbb{Q}_3$. Thus $\mathrm{im}(\mu) = H$ is trivial.

Note that $p = 2,3$ don't give us any information about $\mathrm{im}(\mu')$ because $\{-1,2,3,5\}^{\times 2}$ is contained in $\langle \ker(j_3), H'\rangle$ and $\langle \ker(j_2), H', [1,-1], [-1,6]\rangle$. Since $p = \infty$ does not rule out $[1,5], [1,2] \in \mathrm{im}(\mu') \setminus H'$ (as an example), we require more information.

Consider $\mathbb{Q}_5$ with representatives $\{1,2,5,10\}$ and kernel $\ker(j_5) = \langle \{\pm 1, \pm 6\}^{\times 2}\rangle$. Since $|\mathfrak{G}'_5/\varphi(\mathfrak{G}_5)| \cdot |\mathfrak{G}_5/\varphi'(\mathfrak{G}'_5)| = 16$, we want 4 total generators. H' gives rise to two generators: $[1,2]$ and $[5,1]$. The point $\{(x,y),\infty\} \in \mathfrak{G}_5$ such that $x = 1$ maps to $[2,1]$, which is independent to the other two. The point $\{(x,y),\infty\} \in \mathfrak{G}'_5$ such that $x = 0$ maps to $[2,1]$, which is non-trivial. Thus $|\mathfrak{G}'_5/\varphi(\mathfrak{G}_5)| = 2$ and $|\mathfrak{G}_5/\varphi'(\mathfrak{G}'_5)| = 8$. It follows that

$\mathrm{im}(\mu') \leq \langle [1,2],[5,1],[2,1],\ker(k_5)\rangle$. This bound is the subgroup of everything except a multiple of 5 in the second entry. Together with $p=\infty$ (which says the first entry is positive), we now know that

$$\mathrm{im}(\mu') \leq \langle \{1,2,3,5\} \times \{\pm 1, \pm 2, \pm 3\}\rangle.$$

Since we already know that the rank of C is 0 by complete 2-descent, $\mathrm{im}(\mu')$ should be H. But clearly, we do not have enough information to deduce this when considering all primes of bad reduction. Thus C is a member of the Tate-Shafarevich group.

3.6 Proof of Descent by Richelot Isogeny

Chapter 9 of [1] explains the whole process of deriving the isogenies. The main idea is to define C and C' as before, then consider an isogeny between the Kummers which lifts to isogenies between C and C'. Now, 10.2.ii of [1] gives a concrete description of the isogenies, which involves matrices of the linear maps. The Richelot Isogeny is a 4-isogeny as in general, four divisors maps to the same divisor.

3.6.1 Proof of homomorphisms

Recall the map $\mu\colon \mathfrak{G}'/\varphi(\mathfrak{G}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ by

$$\mu(\{(x,y),(u,v)\}) = [L_1(x)L_1(u), L_2(x)L_2(u)].$$

Then this is equivalent to a map

$$\bar{\mu}\colon \mathfrak{G}'/\varphi(\mathfrak{G}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}\colon \{(x,y),(u,v)\} \mapsto [d_1,d_2]$$

where $x,y \in \mathbb{Q}(\sqrt{d_1})$ and $u,v \in \mathbb{Q}(\sqrt{d_2})$.

Proposition 3.6.1
$\bar{\mu}$ is a homomorphism.

Proof.
Let $\mathfrak{A} = \{(x,y),(u,v)\} \mapsto [d_1,d_2]$ and $\mathfrak{B}\{(x',y'),(u',v')\} \mapsto [d_1',d_2']$. Then clearly, $\bar{\mu}(\mathfrak{A}+\mathfrak{B}) \in \mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\sqrt{d_1'},\sqrt{d_2'})$. But after some algebra, we get that the first coordinate is in fact in $\mathbb{Q}(\sqrt{d_1 d_1'})$ and the second $\mathbb{Q}(\sqrt{d_2, d_2'})$. Noting that $\bar{\mu}$ preserves the identity and $\bar{\mu}$ is fixed under negation, we get that it is a homomorphism. □

Proposition 3.6.2
$\ker(\bar{\mu})$ is trivial and so $\bar{\mu}$ is injective.

Proof.
An element $\mathfrak{A}$ of $\mathfrak{G}'$ maps to $[1,1]$ when $\mathfrak{A} \in \varphi(\mathfrak{G})$, so by taking quotient, the map is injective. □

It follows that μ is also an injective homomorphism. These results also hold for the dual μ' with identical proofs.

3.6.2 The formula for $|\mathfrak{G}_p/2\mathfrak{G}_p|$

For simplicity, write $\mathfrak{G} = \mathfrak{G}_p$ for a prime p or ∞. Using the theory of formal groups in 7.5 and 7.6 of [1] gives

$$|\mathfrak{G}_p/2\mathfrak{G}_p| = \begin{cases} |\mathfrak{G}_p[2]|/4, & p = \infty; \\ |\mathfrak{G}_p[2]|, & p \neq 2, \infty; \\ 4|\mathfrak{G}_p[2]|, & p = 2, \end{cases}$$

which is the formula used in complete 2-descent. By considering isogenies (as in 10.4 of [1]), we also get the formula for descent by Richelot isogeny as follows.

The above shows that $\mathfrak{G}/2\mathfrak{G}$ and $\mathfrak{G}'/2\mathfrak{G}'$ and are finite, thus so are $\mathfrak{G}/\varphi'(\mathfrak{G}')$ and $\mathfrak{G}'/\varphi(\mathfrak{G})$. Note that $\varphi' \circ \varphi$ is the doubling map, so $\varphi'(\mathfrak{G}'/\varphi(\mathfrak{G})) = \varphi'(\mathfrak{G}')/2\mathfrak{G}$ with kernel $\ker(\varphi')/(\ker(\varphi') \cap \varphi(\mathfrak{G}))$ since the kernel of the doubling map is $\mathfrak{G}[2]$ and $\varphi(\mathfrak{G}[2]) = \ker(\varphi') \cap \varphi(\mathfrak{G})$. It follows from the isomorphism theorem that

$$|\mathfrak{G}'/\varphi(\mathfrak{G})| = |\varphi'(\mathfrak{G}')/2\mathfrak{G}| \cdot |\ker(\varphi')/(\ker(\varphi') \cap \varphi(\mathfrak{G}))|.$$

Additionally, the kernel of the restriction $\varphi(\mathfrak{G}[2])$ is $\ker(\varphi) = \ker(\varphi) \cap \mathfrak{G}[2]$ since $\ker(\varphi) \subseteq \mathfrak{G}[2]$. Thus

$$|\mathfrak{G}[2]| = |\ker(\varphi') \cap \varphi(\mathfrak{G})| \cdot |\ker(\varphi)|.$$

Combining the above with $|\mathfrak{G}/\varphi'(\mathfrak{G}')| \cdot |\varphi'(\mathfrak{G}')/2\mathfrak{G}| = |\mathfrak{G}/2\mathfrak{G}|$ gives

$$|\mathfrak{G}'/\varphi(\mathfrak{G})| \cdot |\mathfrak{G}/\varphi'(\mathfrak{G}')| \cdot |\mathfrak{G}[2]| = |\ker(\varphi)| \cdot |\ker(\varphi')| \cdot |\mathfrak{G}/2\mathfrak{G}|.$$

Substituting $|\mathfrak{G}/2\mathfrak{G}|$ from before and the fact that $|\ker(\varphi)| = |\ker(\varphi)| = 4$,

$$|\mathfrak{G}'_p/\varphi(\mathfrak{G}_p)| \cdot |\mathfrak{G}_p/\varphi'(\mathfrak{G}'_p)| = \begin{cases} 4, & p = \infty; \\ 8 & p \neq 2, \infty; \\ 64, & p = 2. \end{cases}$$

3.7 Proof of Mordell-Weil

We outline a proof of Mordell-Weil theorem which is central to all the descent techniques. It states that $\mathfrak{G}$ is finitely generated. This is based on [1] Ch11.

Let C be a genus 2 curve written as a product $C\colon Y^2 = G_1(X)G_2(X)G_3(X)$ as in the Richelot section.

Lemma 3.7.1
The $\mu\colon \mathfrak{G}'/\varphi(\mathfrak{G}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ given in the Richelot isogeny section has finite image. Similarly, $\mathrm{im}(\mu')$ is finite. In particular, these images are subgroups of $\mathbb{Q}(\mathcal{S}) = (\langle -1, p_i : p_i \in \mathcal{S}\rangle)^{\times 2}$ where $\mathcal{S} = \{2, p : p \mid \Delta b_1 b_2 b_3 b'_1 b'_2 b'_3\}$. Note that in the case that C has all it's roots e_i inside $\mathbb{Z}$, then $\mathbb{Q}(\mathcal{S})$ coincides with the set

$$(\langle -1, 2, p \text{ prime} : p \mid \prod_{i \neq j}(e_i - e_j)\rangle)^{\times 2}.$$

Proof.
Suppose for a contradiction that there exists $[d_1, d_2] \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ such that there exists $p \notin \mathbb{Q}(\mathcal{S})$ that does not divide either d_1 or d_2. Without loss of generality, suppose $p \nmid d_1$ (otherwise, renumber the functions G_i).

Let $\mathfrak{p}$ be the prime ideal above p. Write (z_i) so that $\max |z_i|_{\mathfrak{p}} = 1$ by scaling. Let $(\tilde{z_i})$ be the reduction modulo $\mathfrak{p}$. Since $|\sqrt{d_1}| < 1$, $\sigma(\tilde{z_i}) = (\tilde{z_i})$. So $\tilde{\mathbf{W}}_i(\tilde{\mathbf{z}}) = \tilde{\mathbf{z}}$ on $\tilde{\mathfrak{G}}$, the reduction of J modulo $\mathfrak{p}$. But this means one of the points of order 2 map to $\tilde{\mathfrak{O}}$ under the reduction map. This means two roots of the reduced curves are equal. This implies the reduced curve has a repeated root, so p is not a prime of good reduction, a contradiction. □

Theorem 3.7.2 (Weak Mordell-Weil)
$\mathfrak{G}/2\mathfrak{G}$ is finite.

Proof.
Since the image of μ is finite, $\mathfrak{G}'/\varphi(\mathfrak{G})$ is finite. Similarly, $\text{im}(\mu')$ and $\mathfrak{G}/\varphi'(\mathfrak{G}')$ is finite. Now, $\varphi' \circ \varphi$ is the point doubling map, so $\mathfrak{G}/2\mathfrak{G}$ is finite. □

To prove the full form of Mrdell-Weil, we need to look at heights ([1] Ch12).

Definition 3.7.3 (Height of a point)
Let $P = (x_i) \in \mathbb{P}^n(\mathbb{Q})$. Choose a representatives for P such that $x_i \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. Then define the height function $H \colon \mathbb{P}^n(\mathbb{Q}) \mapsto \mathbb{Z}^+$ as $H(P) = \max_i\{|x_i|\}$.

Definition 3.7.4 (Height on the Jacobian)
Define the height of an element in $\mathfrak{G}$ as $H_H \colon \mathfrak{G} \to \mathbb{Z}^+$ as $H_j(\mathfrak{A}) = H((z_i(\mathfrak{A})))$.

Definition 3.7.5 (Height on Kummer surface)
Define $H_\kappa \colon \mathbb{Z}^+ \colon \mathfrak{A} \mapsto H((\xi_i(\mathfrak{A})))$.

Now, we need to show that these functions are indeed height functions $F \colon \mathfrak{G} \to \mathbb{Z}^+$ that satisfy the following three conditions.

1. For any $C \in \mathbb{Z}^+$, $\{\mathfrak{A} \in \mathfrak{G} : F(\mathfrak{A}) \leq C\}$ is finite.
2. There exists $C_1 \in \mathbb{Z}^+$ such that for every $\mathfrak{A}, \mathfrak{B} \in \mathfrak{G}$, $F(\mathfrak{A} + \mathfrak{B})F(\mathfrak{A} - \mathfrak{B}) \leq C_1 F(\mathfrak{A})^2 F(\mathfrak{B})^2$.
3. There exists $C_2 \in \mathbb{Z}^+$ such that for any $\mathfrak{A} \in \mathfrak{G}$, $F(2\mathfrak{A}) \geq F(\mathfrak{A})^4/C_2$.

Proof of 3.7.3.
H satisfies the three conditions since H is the height map described in Chapter 17 of [3]. □

Proof of 3.7.4.
H_J is equivalent to H_κ^2 (ie. the same up to scalar multiplication). If H_k indeed satisfies the three conditions, then clearly for all C, $\{\mathfrak{A} \in \mathfrak{G} : H_\kappa^2(\mathfrak{A}) \leq C\}$ is finite, so the first condition is satisfied for H_J. It is also clear that squaring does not affect the second or third propeties. Thus, we are reduced to proving the Kummer case. □

Proof of 3.7.5.
This is given from the middle of 12.1 of [1] using the properties of the bilinear forms. □

Given that $\mathfrak{G}/2\mathfrak{G}$ is finite and H_κ satisfies the three properties of heights, we can now prove Mordell-Weil.

Theorem 3.7.6 (Mordell-Weil)
$\mathfrak{G}$ is finitely generated.

Proof.
We shall imitate [1] 12.2.

Since $\mathfrak{G}/2\mathfrak{G}$ is finite, write $\mathfrak{G}/2\mathfrak{G} = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_s\}$. Let $\mathfrak{A}_0 \in \mathfrak{G}$. Then $\mathfrak{A}_0 = 2\mathfrak{A}_1 + \mathfrak{B}_{i_0}$ for some $\mathfrak{B}_{i_0} \in \mathfrak{G}/2\mathfrak{G}$ and $\mathfrak{A}_1 \in \mathfrak{G}$. We may iteratively continue this by defining $\mathfrak{A}_j = 2\mathfrak{A}_{j+1} + \mathfrak{B}_{i_j}$ for some $\mathfrak{B}_{i_j} \in \mathfrak{G}/2\mathfrak{G}$ and $\mathfrak{A}_{j+1} \in \mathfrak{G}$.

At each index j,

$$\begin{aligned} H_\kappa(\mathfrak{A}_j)^4 &\le C_2 H_\kappa(2\mathfrak{A}_j) \\ &= C_2 H_\kappa(\mathfrak{A}_{j-1} - \mathfrak{B}_{i_{j-1}}) \\ &\le C_1 C_2 H_\kappa(\mathfrak{A}_{j-1})^2 H_\kappa(\mathfrak{B}_{j-1})^2 \\ &= H_\kappa(\mathfrak{A}_{j-1})^4 \left(\sqrt{C_1 C_2} \frac{H_\kappa(\mathfrak{B}_{i_{j-1}})}{H_\kappa(\mathfrak{A}_{j-1})} \right)^2 . \end{aligned}$$

Thus if $H_\kappa(\mathfrak{A}_{j-1}) > C_3 = \sqrt{C_1 C_2} \max\{H_\kappa(\mathfrak{G}/2\mathfrak{G})\}$, then $H_\kappa(\mathfrak{A}_j) < H_\kappa(\mathfrak{A}_{j-1})$.

Suppose for a contradiction that $H_\kappa(\mathfrak{A}_j) > C_3$ for all j. Then $H_\kappa(\mathfrak{A}_j) < H_\kappa(\mathfrak{A}_1)$. But since H_κ is a function on the positive integers, this cannot be true for all j, a contradiction. Thus, for some (minimal) j, $H_\kappa(\mathfrak{A}_j) \le C_3$. Hence,

$$\mathfrak{A}_1 = \mathfrak{B}_{i_1} + 2\mathfrak{A}_2 = \cdots = \mathfrak{B}_{i_1} + 2(\mathfrak{B}_{i_2} + 2(\cdots + 2\mathfrak{A}_j)),$$

so $\mathfrak{A}_1$ is a linear combination of $\mathfrak{A}_j$ and $\mathfrak{B}_i$s. Since $\{\mathfrak{A} \in \mathfrak{G} : H_\kappa(\mathfrak{A}) \le C_3\}$ is finite, there are only a finite number of choices of $\mathfrak{A}_j$. So $\mathfrak{G} = \langle \mathfrak{B}_1, \ldots, \mathfrak{B}_s, \{\mathfrak{A} \in \mathfrak{G} : H_\kappa(\mathfrak{A}) \le C_3\} \rangle$ is finitely generated. □

3.8 Chabauty's Theorem

Chabauty's Theorem gives us a bound on the number of points on $C(\mathbb{Q})$ for a curve C. A theorem by Falting says that this bound is finite if the genus of C is greater than or equal to 2. We shall give a brief description of the method of Chabauty, as well as an example and computer code in the Appendix. This follows [1] Chapter 13 and makes use of existing calculations by Flynn[3].

[3] `http://people.maths.ox.ac.uk/flynn/genus2`

Let $C\colon Y^2 = F(X)$ be a curve of genus 2 with discriminant Δ and Jacobian $\mathfrak{G}$. Suppose that we already know $\mathfrak{G}_{\text{tors}}$ and $\mathfrak{G}/2\mathfrak{G}$, and that we can find that the rank of C is 1 using one of the descent techniques. Suppose additionally that we have found a free generator $\mathfrak{D}$ such that $\mathfrak{G} = \langle \mathfrak{G}_{\text{tors}}, \mathfrak{D} \rangle$. Then we can use Chabauty's method to fully resolve all the rational points of C as follows.

Let p be any prime that doesn't divide Δ. Let $\tilde{\mathbb{C}}$ be the reduction $\mathbb{C}$ modulo p. We then find $\tilde{\mathfrak{G}}$ as discussed in the torsion section. Let d be the order of $\tilde{\mathfrak{D}}$ the image of $\mathfrak{D}$ under reduction. Then $\mathfrak{E} = d \cdot \mathfrak{D}$ maps to the identity under reduction modulo p. Thus, any element of $\mathfrak{G}$ can be written in the form

$$\mathfrak{B} = \mathfrak{A} + n \cdot \mathfrak{E}; \quad n \in \mathbb{Z},\ \mathfrak{A} \in \mathcal{U} = \{\mathfrak{B} + i \cdot \mathfrak{D} : \mathfrak{B} \in \mathfrak{G}_{\text{tors}},\ 0 \le i \le p\}.$$

Now, for each $\mathfrak{A} \in \mathcal{U}$, we wish to bound the number of values $n \in \mathbb{Z}$ such that $\mathfrak{B} = \{P, P\}$. Since $\tilde{\mathfrak{B}} = \tilde{\mathfrak{A}}$, we can look for points $\tilde{\mathfrak{A}}$ of the form $\{\tilde{P}, \tilde{P}\}$ (including the identity).

The next step is to analyse $E(n \cdot L(\mathbf{s}))$. For the divisor $\mathfrak{E}$, find

$$\mathbf{s} = \mathbf{s}(\mathfrak{E}) = \begin{pmatrix} s_1(\mathfrak{E}) \\ s_2(\mathfrak{E}) \end{pmatrix} = \begin{pmatrix} z_1(\mathfrak{E})/z_0(\mathfrak{E}) \\ z_2(\mathfrak{E})/z_0(\mathfrak{E}) \end{pmatrix},$$

given as follows. Write $F(X) = f_0 + f_1 X + \cdots + f_6 X^6$ and $\mathfrak{A} = \{(x, y), (u, v)\}$. From 2.1 of [1], we have

$$\begin{aligned}
F_0(x,u) &= 2f_0 + f_1(x+u) + 2f_2xu + f_3xu(x+u) + 2f_4x^2u^2 + f_5x^2u^2(x+u) + 2f_6x^3u^3 \\
\beta_0 &= \frac{F_0(x,u) - 2yv}{(x-u)^2} \\
G(x,u) &= 4f_0 + f_1(x+3u) + f_2(2xu+2u^2) + f_3(3xu^2+u^3) + 4f_4xu^3 + f_5(x^2u^3+3xu^4) + f_6(2x^2u^4+2xu^5) \\
H(x,u) &= f_0(2x+2u) + f_1(3xu+u^2) + 4f_2xu^2 + f_3(x^2u^2+3xu^3) + f_4(2x^2u^3+2xu^4) + f_5(3x^2u^4+xu^5) + 4f_6x^2u^5 \\
z_2 &= \frac{G(x,u)y - G(u,x)v}{(x-u)^3} \\
z_1 &= \frac{H(x,u)y - H(u,x)v}{(x-u)^3} \\
z_0 &= \beta_0^2.
\end{aligned}$$

Next, $E(n \cdot L(\mathbf{s}))$ is given by the formal power series of exponentials and logarithms as in 7.2 of [1]:

$$\begin{aligned}
L_2(\mathbf{s}) &= s_1 + \frac{1}{3}(-2f_4s_1^3 + f_1s_2^3) + \cdots \\
E_2(\mathbf{s}) &= s_1 + \frac{1}{3}(2f_4s_1^3 - f_1s_2^3) + \cdots \\
L_2(\mathbf{s}) &= s_2 + \frac{1}{3}(-2f_2s_2^3 + f_5s_1^3) + \cdots \\
E_2(\mathbf{s}) &= s_2 + \frac{1}{3}(2f_2s_2^3 - f_5s_1^3) + \cdots \\
E(n \cdot L(\mathbf{s})) &= \begin{pmatrix} E_1(n \cdot L_1(\mathbf{s})) \\ E_2(n \cdot L_2(\mathbf{s})) \end{pmatrix}.
\end{aligned}$$

Now, let $t_1 \equiv E_1(n \cdot L_1(\mathbf{s}))$ and $t_2 \equiv E_2(n \cdot L_2(\mathbf{s}))$.

For each $\mathfrak{A}$ found above, define for an arbitrarily well chosen power p^i

$$\theta(n) \equiv (\Phi_{42}(\mathbf{a}, \sigma(\mathbf{t})))^2 - 4\Phi_{41}(\mathbf{a}, \sigma(\mathbf{t})) \cdot \Phi_{43}(\mathbf{a}, \sigma(\mathbf{t})) \mod p^i,$$

where we have

$$\mathbf{t} = \begin{pmatrix} t_1 \\ t_2 \end{pmatrix}$$

and Φ_{ij} are bilinear forms described in 9.9 of [1][4]. The explicit form depends on $(a_i) \in \mathbb{P}^{15}(\mathbb{Q})$ given by $(z_i(\mathfrak{A}))$ chosen so $a_i \in \mathbb{Z}$ and $\gcd(a_i) = 1$, the usual equations don't work right of the bat since $x = u$, so we rewrite these 15 coordinates as a multiple of

$$\begin{aligned}
a_{15} &= ((x-u)^2)\\
a_{14} &= 1\\
a_{13} &= (x+u)\\
a_{12} &= (x*u)\\
a_{11} &= (x*u*(x+u))\\
a_{10} &= ((x*u)^2)\\
a_9 &= ((Fx-Fu)/((x-u)*(y+v)))\\
a_8 &= ((u^2*Fx-x^2*Fu)/((x-u)*(u*y+x*v)))\\
a_7 &= ((u^4*Fx-x^4*Fu)/((x-u)*(u^2*y+x^2*v)))\\
a_6 &= ((u^6*Fx-x^6*Fu)/((x-u)*(u^3*y+x^3*v)))\\
a_5 &= ((f0xu^2-4*Fx*Fu)/((x-u)^2*(f0xu+2*y*v)))\\
a_4 &= ((f1xu^2-(x+u)^2*Fx*Fu)/((x-u)^2*(f1xu+(x+u)*v*y)))\\
a_3 &= ((x*u)*a_5)\\
a_2 &= ((gxu^2*Fx-gux^2*Fu)/((x-u)^3*(gxu*y+gux*v)))\\
a_1 &= ((hxu^2*Fx-hux^2*Fu)/((x-u)^3*(hxu*y+hux*v)))\\
a_0 &= (a_5^2)
\end{aligned}$$

where $Fx = y^2$ and $Fu = v^2$, and terms gxu, gux, hxu, hux, $f1xu$ and $f0xu$ are as described in the code in the Appendix. If $\mathfrak{A} = \mathfrak{O}$, then $a_0 = 1$ and $a_i = 0$ for the other coordinates. The second input of Φ_{ij} are local coordinates (b_i) corresponding to $\mathbf{t}$ as describe in `http://people.maths.ox.ac.uk/flynn/genus2/local/local.coordinates` with $s_1 = t_1$ and $s_2 = t_2$.

Once we have found $\theta(n) \mod p^n$, we wish to use the following theorem (13.1.1 in [1]).

Theorem 3.8.1 (Strassman)
Let $\theta(X) = c_0 + c_1X + \cdots \in \mathbb{Z}_p[[X]]$ and eventually $c_j \to 0$ in $\mathbb{Z}_p$. Define a unique l give by $|c_l|_p \geq |c_j|_p$ for all $j \geq 0$ and $|c_l|_p > |c_j|_p$ for all $j > l$. Then there are at most l values of $x \in \mathbb{Z}_p$ such that $\theta(x) = 0$ and $|x|_p \leq 1$.

[4] `http://people.maths.ox.ac.uk/flynn/genus2/jacobian.variety/bilinear.forms`

This theorem puts a bound on the possible number of n such that $\mathfrak{A} + n \cdot \mathfrak{E}$ is of the form $\{P, P\}$. In the case a bound cannot be found, choose a larger power n of $p^n i$. Once we've created such a bound for every $\mathfrak{A}$, we have found every non-Weierstrass points on $C(\mathbb{Q})$.

In general, we have the following result.

Theorem 3.8.2 (Chabauty)
Let C be a curve of genus greater g greater than 1 over $\mathbb{Q}$ (or in fact any number field). If the Jacobian of C has rank less than g, then $C(\mathbb{Q})$ is finite.

So when $g = 2$, then we require the rank to be 1 and we can do what we did before to find $C(\mathbb{Q})$. Chabauty's theorem gives us a constructive way to find rational points. The stronger theorem by Falting does not yet have a constructive proof.

Theorem 3.8.3 (Falting)
Let C be a curve of genus greater than 1. Then $C(k)$ is finite for any number field k.

3.8.1 An Example

Let $C\colon Y^2 = X(X-1)(X-2)(X-6)(X-9)$ be a genus 2 curve. We first prove that this has rank 1, then find the entirety of $C(\mathbb{Q})$ using Chabauty's Theorem. We start with a complete 2-descent.

We have the maximal number of order 2 points. We also have an infinite generator $\{(9/4, 135/32), \infty\}$. We claim that these generate $\mathfrak{G}$.

Let μ' be the usual map

$$\tilde{\mu}'\colon J(\mathbb{Q})/2J(\mathbb{Q}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 4}\colon (x,y) \mapsto [x, x-1, x-2, x-6] \leq \langle \{-1, 2, 3, 5, 7\}^{\times 4} \rangle.$$

For the lower bound, consider $\{(x, 0), \infty\}$ for $x \in \{0, 1, 2, 6\}$ as four independent generators of order 2, as well as the infinite generator.

(i) $x = 0 \mapsto [3, -1, -2, -6]$,

(ii) $x = 1 \mapsto [1, -10, -1, -5]$,

(iii) $x = 2 \mapsto [2, 1, 14, -1]$,

(iv) $x = 6 \mapsto [6, 5, 1, -10]$,

(v) $\{(9/4, 135/32), \infty\} \mapsto [1, 5, 1, -15]$.

Let H be generated by the above

$$H = \langle [3, -1, -2, -6], [1, -10, -1, -5], [2, 1, 14, -1], [6, 5, 1, -10], [1, 5, 1, -15] \rangle$$

so that

$$H \leq \operatorname{im}(\mu') \leq \langle \{-1, 2, 3, 5, 7\}^{\times 4} \rangle.$$

First, consider $\mathbb{R}$. Clearly $H \mapsto \langle [1,-1,-1,-1],[1,1,1,-1]\rangle$ which gives us the 2 required generators and so

$$\operatorname{im}(\mu') \leq \langle H, \{1,2,3,5,7\}^{\times 4}\rangle).$$

In $\mathbb{Q}_3$, $H \mapsto \langle [3,-1,1,3],[1,-1,-1,1],[-1,1,-1,-1],[-3,-1,1,-1],[1,-1,1,3]\rangle$. This generates a subgroup of order 16 (since the last 4 are independent). Thus

$$\operatorname{im}(\mu') \leq \langle H, \{1,-2,-5,7\}^{\times 4}\rangle.$$

Next consider $\mathbb{Q}_5$. $H \mapsto \langle [2,1,2,1],[1,10,1,5],[2,1,1,1],[1,5,1,10]\rangle$ and all four are independent generators of a subgroup of order 16. Hence

$$\operatorname{im}(\mu') \leq \langle H, \{\pm 1,6,14\}^{\times 4}\rangle.$$

For $\mathbb{Q}_7$, $H \mapsto \langle [-1,-1,-1,1],[1,1,-1,1],[1,1,7,-1],[-1,-1,1,1],[1,-1,1,-1]\rangle$. The last four are sufficient generators for a subgroup of order 16. Thus

$$\operatorname{im}(\mu') \leq \langle H, \{1,2,-5,-3\}^{\times 4}\rangle.$$

Finally, in $\mathbb{Q}_2$, $H \mapsto \langle [3,-1,-2,-6],[1,6,-1,3],[2,1,-2,-1],[6,-3,1,6],[1,-3,1,1]\rangle$. These are all independent, so we require one more generator to reach $|\mathfrak{G}_p/2\mathfrak{G}_p| = 64$. There exists a point $(x,y) \in C(\mathbb{Z}_2)$ such that $x = 28$. This maps to $[-1,3,-6,6]$ which is clearly independent from the other five generators (by looking at the first entry). Hence

$$\operatorname{im}(\mu') \leq \langle H, [-1,3,-6,6], \{1,-7,-15\}^{\times 4}\rangle.$$

We now take the intersection of the upper bounds. Considering the last entries of H, they span $\langle -1,2,3,5\rangle$. The only elements of H that has last entry 1 are $[1,1,1,1]$ and $[1,-1,-7,1]$. From the $\mathbb{Q}_7$ case, it is clear that the intersection does not have a multiple of 7 in the last entry. As with the previous complete 2-descent example, it is sufficient to show that the aforementioned elements of H with last entry 1 are the only elements with last entry 1 in the upper bound of $\operatorname{im}(\mu')$.

If the last entry was 1, then $\mathbb{Q}_7$ says that the first entry cannot be a multiple of 7, and $\mathbb{R}$ says it must be positive. Considering $\mathbb{Q}_3$, the first entry must be in $\langle -2,3,-5,7\rangle$ and combining this with the information before, we get the first entry is in $\langle 3,10\rangle$. But we can rule out multiples of 10 by looking at $\mathbb{Q}_5$. So the first entry of any element $[a,b,c,1] \in \operatorname{im}(\mu')$ must have $a \in \{1,3\}$. Finally, looking at $\mathbb{Q}_2$, in order to get $a = 3$, we must have some multiple of $[3,-1,-2,-6]$ with $[1,6,-1,3]$ or $[1,-3,1,1]$, but neither of these gives rise to the last entry being 1. So $a = 1$.

Now, considering second entry, $\mathbb{Q}_7$ says that the second entry has no multiple of 7, so together with $\mathbb{Q}_5$, in order to have an element $[a,b,c,1]$ with $a \in \{1,3\}$ must have $b \in \{\pm 1, \pm 6\}$. But we cannot have multiples of 3 by looking at $\mathbb{Q}_3$, so in fact, $b \in \{\pm 1\}$. None of the non-kernel of the $\operatorname{im} \mu'_2$ give an element of the form $[1,-1,c,1]$ by noting that the only elements in $\operatorname{im}\mu_2'$ with last entry 1 is in the span of $[1,-3,1,1]$, $[1,3,1,1]$ and $[-6,-3,-6,1]$. Hence $b=1$

Finally, looking at the third entry, $\mathbb{Q}_5$ says that $c \in \langle -1,2,3,7\rangle$. Now in $\mathbb{Q}_3$, the sign of b and c must be the same and $c \in \langle -1,-2,-5,-7\rangle$ which gives an intersection of $\langle -1,-2,7\rangle$. Finally, an element of the form $[1,1,c,1]$ must map to the indentity under the reduction to $\mathbb{Q}_2$, so $c \in \langle 1,-7,-15\rangle$. The intersection thus gives $c \in \{1,-7\}$ which means that the only elements with last entry 1 in $\operatorname{im}(\mu')$ are $[1,1,1,1]$ and $[1,1,-7,1]$ as desired. Thus $\mathfrak{G}$ has rank 1.

Let $\mathfrak{D} = \{(9/4, 135/32), \infty\}$. We know that $\mathfrak{G} = \langle \mathfrak{G}_{\text{tors}}, \mathfrak{D}\rangle$ (where the torsion are the order 2 points). The discriminant is $\Delta = 2^{14}3^8 5^2 7^2$. So consider $p = 13 \nmid \Delta$. Let $\tilde{G}$ be the Jacobian of $\tilde{C}\colon Y^2 = X^5 + 8X^4 + 10X^3 + 3X^2 + 4X \mod 13$ be the reduction of $\tilde{C}$ modulo 13. The points on $\tilde{C}(\mathbb{F}_{13})$ are, $(0,0)$, $(1,0)$, $(2,0)$, $(3,\pm 2)$, $(6,0)$, $(7,\pm 3)$,$(8,\pm 2)$, $(9,0)$ and $(12,\pm 3)$. The point $\mathfrak{D}$ maps to $\tilde{\mathfrak{D}} = \{(12,3),\infty\}$ which has order 6.

Let $\mathfrak{E} = 6\cdot\mathfrak{D}$. Then this maps to the identity in $\tilde{\mathfrak{G}}$. Thus anything in $\mathfrak{G}$ can be written in the form

$$\mathfrak{A} + n\cdot\mathfrak{E}; \quad n \in \mathbb{Z},\ \mathfrak{A} \in \mathcal{U} = \{\mathfrak{B} + i\cdot\mathfrak{D} : \mathfrak{B} \in \mathfrak{G}_{\text{tors}},\ 0 \le i \le 5\}.$$

For each $\mathfrak{A} \in \mathcal{U}$, we wish to bound the number of n such that $\mathfrak{A} + n\cdot\mathfrak{E} = \{P,P\}$ for some $P \in C(\mathbb{Q})$. Since this element maps to $\mathfrak{A}$ under the reduction map, we only need to consider $\mathfrak{A} \in U$ such that the reduction $\tilde{\mathfrak{A}}$ is of the form $\{\tilde{P},\tilde{P}\}$. We have the following five cases.

1. $\tilde{\mathfrak{A}} = \mathfrak{O} + 0\cdot\mathfrak{D} = \mathfrak{O}$.
2. $\tilde{\mathfrak{A}} = \mathfrak{O} + 2\cdot\mathfrak{D} = \{(12,3),(12,3)\}$.
3. $\tilde{\mathfrak{A}} = \mathfrak{O} + 4\cdot\mathfrak{D} = \{(12,3),(12,3)\}$.
4. $\tilde{\mathfrak{A}} = \{(0,0),(9,0)\} + 1\cdot\mathfrak{D} = \{(12,3),(12,3)\}$.
5. $\tilde{\mathfrak{A}} = \{(0,0),(9,0)\} + 5\cdot\mathfrak{D} = \{(12,3),(12,3)\}$.

These points were found using MAGMA code as in the appendix. Of these, only the first three cases lift back to a point of the form $\{P,P\}$. These correspond to $\{(9/4,135/32),(9/4,135/32)\}$, $\{(9/4,-135/32),(9/4,-135/32)\}$ and $\mathfrak{O}$.

Now we find $E(n\cdot L(\mathbf{s}))$. Firstly (using Sage),

$$\mathbf{s} = \begin{pmatrix} \begin{matrix} 56583292739976842432297097662790629690764708391248659059829860387798941947660/ \\ 1553808132581617195083978115837544710530555239651242589881923745161720450996961 \end{matrix} \\ \\ \begin{matrix} -44859319762464961791713235585743308195018639601161989980285909365481460300720/ \\ 1553808132581617195083978115837544710530555239651242589881923745161720450996961 \end{matrix} \end{pmatrix}.$$

Thus $|s_1|_{13} = 13^{-1}$ and $|s_2|_{13} = 13^{-1}$.

Arbitrarily pick a power, say 13^4 and consider $E(n\cdot L(\mathbf{s})) \mod 13^4$. Note that we can ignore all terms with degree greater or equal to 4 since these will always be $0 \mod 13^4$

(since we shall only begin dividing by 13 in the factorial part when we get to terms with degree ≥ 13). Using sage, we get

$$\mathbf{s} \equiv \begin{pmatrix} 16081 \\ 18044 \end{pmatrix}, \quad L(\mathbf{s}) \equiv \begin{pmatrix} 5096 \\ 9256 \end{pmatrix}, \quad E(n \cdot L(\mathbf{s})) \equiv \begin{pmatrix} 5096n + 10985n^3 \\ 9256n + 8788n^3 \end{pmatrix},$$

where these are all modulo 13^4.

Writing $\mathbf{t}$ as the local parameter for $n \cdot \mathfrak{C}$, t_1 and t_2 are power series in n over $\mathbb{Z}_{13}$ given by

$$t_1 \equiv 5096n + 10985n^3, \quad t_2 \equiv 9256n + 8788n^3 \mod 13^4.$$

Note that any monomial in t_1 and t_2 with a degree greater or equal to 4 vanishes modulo 13^4. We now consider the three cases arising from different choices of $\mathfrak{A}$.

Case 1

$\mathfrak{A} = \{(9/4, 135/32), (9/4, 135/32)\}$. Finding integers (a_i) such that $\gcd(a_i) = 1$ and $(a_i) = (z_i(\mathfrak{A}))$,

$$\begin{aligned}(a_i) = (&1237984225, 157653252, 31836016, 45599760, -866880, 9007360, 3405888, \\ &2135808, 1225728, 667648, 1679616, 1492992, 331776, 294912, 65536, 0).\end{aligned}$$

Thus, plugging this all into the formulae for Φ_{ij}, we get

$$\begin{aligned}\theta(n) &\equiv (\Phi_{42}(\mathbf{a}, \sigma(\mathbf{t})))^2 - 4\Phi_{41}(\mathbf{a}, \sigma(\mathbf{t})) \cdot \Phi_{43}(\mathbf{a}, \sigma(\mathbf{t})) \\ &\equiv 25116n + 17238n^2 + 17576n^3 \mod 13^4.\end{aligned}$$

Since $|25116|_{13} = 13^{-1}$, $|17238|_{13} = 13^{-2}$, $|17576|_{13} = 13^{-3}$ and $|c_j|_{13} \leq 13^{-4}$ for all coefficients of terms of degree $j \geq 4$. By Strassman's Theorem on the 1th term, there is one solution to $n \in \mathbb{Z}_{13}$, namely $n = 0$.

Case 2

The case $\mathfrak{A} = \{(9/4, -135/32), (9/4, -135/32)\}$ is identical to the first case with the change $n \mapsto -n$. So there is again only one solution, $n = 0$.

Case 3

$\mathfrak{A} = \mathfrak{O}$. Considering 13^4 is not enough to deduce anything useful from Strassman (since $\theta \mod 13^4$ is trivial). So consider 13^8. We get

$$\theta(n) = 704714114n^6.$$

Since $|704714114|_{13} = 13^{-7}$, and every other coefficient has absolute value $\leq p^{-8}$, we can use Strassman on the 6th term to bound the number of solutions of θ to ≤ 6.

Observing that $\theta(n) \mod \mathbb{Z}_{13}$ has a leading term of degree 6, we can factor out n^6 in $\theta(n)$, and so $n = 0$ is a solution of multiplicity 6 and is the only solution of θ by Strassman.

Hence after considering all three cases, we have that $(9/4, 135/32)$ and the Weierstrass points are the only rational points.

Chapter 4

Advanced Topics

4.1 Genus 3 Hyperelliptic Curves

From our previous discussion on genera, a genus 3 hyperelliptic curve is a curve $C\colon Y^2 = F(X)$ where F is of degree 7 or 8 with no repeated factors. Note that not all genus 3 curves are birational to a hyperelliptic curve (but there is an equivalence in genus 1 and 2 cases).

Let J be the Jacobian of C and $\mathfrak{G} = J(\mathbb{Q})$. Then the creation of $\mathfrak{G}$ can be done in a similar way to genus 2 curves. At the end of such a derivation, an element of $\mathfrak{G}$ is a triple of points. In particular, Mordell-Weil holds, and so complete 2-descent on genus 3 hyperelliptic curves can be done in a similar way to before as shown in [6].

4.2 Example of Complete 2-Descent on Genus 3 Curves

Consider the genus 3 curve $C\colon Y^2 = X(X-2)(X-4)(X-5)(X-6)(X-8)(X-10)$ with Jacobian J. We shall prove that $\mathfrak{G} = J(\mathbb{Q})$ has trivial rank.

For each element given by a Weierstrass point and the point at infinity for the other two defining points, the map $\mu'\colon \mathfrak{G}/2\mathfrak{G} \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 6}$ maps

(i) $x = 0 \mapsto [3, -2, -1, -5, -6, -2]$,

(ii) $x = 2 \mapsto [2, -1, -2, -3, -1, -6]$,

(iii) $x = 4 \mapsto [1, 2, 6, -1, -2, -1]$,

(iv) $x = 5 \mapsto [5, 3, 1, -1, -1, -3]$,

(v) $x = 6 \mapsto [6, 1, 2, 1, 6, -2]$,

(vi) $x = 8 \mapsto [2, 6, 1, 3, 2, -1]$,

(vii) and $x = 10 \mapsto [10, 2, 6, 5, 1, 2]$ which is the product of the previous six.

The first six elements of $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 6}$ are clearly independent (the only way to get 1 in the first two entries is $(i) \cdot (ii) \cdot (iii) \cdot (v)$ which isn't the identity). Let these first six elements generate H of order 2^6. Then

$$H \leq \mathrm{im}(\mu') \leq \langle \{1, -1, 2, 3, 5\}^{\times 6} \rangle.$$

Writing $\mathfrak{G}_p$ for $J_p(\mathbb{Q}_p)$, we have the similar result to the genus 2 case that

$$|\mathfrak{G}_p/2\mathfrak{G}_p| = \begin{cases} 2^3, & p = \infty \\ 2^6, & p \neq 2, \infty \\ 2^9, & p = 2 \end{cases}.$$

If $p = \infty$, then the generators of H map to $[1, -1, -1, -1, -1, -1]$, $[1, 1, 1, -1, -1, -1]$ and $[1, 1, 1, 1, 1, 1, -1]$ which are clearly independent and generate a subgroup of order 2^3 as needed. So

$$\mathrm{im}(\mu') \leq \langle H, \{1, 2, 3, 5\}^{\times 6} \rangle.$$

Next consider $p = 3$, where the generators map to $[3, 1, -1, 1, 3, 1]$, $[-1, -1, 1, -3, -1, 3]$, $[1, -1, -3, -1, 1, -1]$, $[-1, 3, 1, -1, -1, -3]$, $[-3, 1, -1, 1, -3, 1]$, $[-1, -3, 1, 3, -1, -1]$ respectively. We have that (i) $\cdot$ (v) $\equiv$ (ii) $\cdot$ (iv) $\cdot$ (vi) so that the elements of H generate a subgroup of order 2^5, and so we need one more generator. There exists a point $(7, y) \in C(\mathbb{Q}_3)$. Under μ', this maps to $[1, -1, -1, 1, -1, -3]$ which is independent to the previous. Hence

$$\mathrm{im}(\mu') \leq \langle H, [1, -1, -1, 1, -1, -3], \{1, -2, -5\}^{\times 6} \rangle.$$

Now for $p = 5$, the generators of H map to $[2, 2, 1, 5, 1, 2]$, $[2, 1, 2, 2, 1, 1]$, $[1, 2, 1, 1, 2, 1]$, $[5, 2, 1, 1, 1, 2]$, $[1, 1, 2, 1, 1, 2]$ and $[2, 1, 1, 2, 2, 1]$. These are all independent and thus generate a subgroup of order 2^6 as required. Hence

$$\mathrm{im}(\mu') \leq \langle H, \{1, -1, 6\}^{\times 6} \rangle.$$

Finally if $p = 2$, the generators map to $[3, -2, -1, 3, -6, -2]$, $[2, -1, -2, -3, -1, -6]$, $[1, 2, 6, -1, -2, -1]$, $[-3, 3, 1, -1, -1, -3]$, $[6, 1, 2, 1, 6, -2]$ and $[2, 6, 1, 3, 2, -1]$. It is easy to check that these are all independent, so we require three more generators. Then, there exists points $(1, y_1), (16, y_2), (28, y_3) \in C(\mathbb{Q}_2)$ that map to $[1, -1, -3, -1, 3, 1]$, $[1, -2, 3, 3, -6, 2]$ and $[-1, -6, 6, -1, 6, -3]$ respectively. These are all independent and generate a subgroup of order 2^9, so

$$\mathrm{im}(\mu') \leq \langle H, [1, -1, -3, -1, 3, 1], [1, -2, 3, 3, -6, 2], [-1, -6, 6, -1, 6, -3], \{1, -15\}^{\times 6} \rangle.$$

Looking at the second entry of elements of H, we have $\langle -1, 2, 3 \rangle$. Now by looking at $\mathbb{Q}_5$, the second entry of $\mathrm{im}(\mu')$ cannot be a multiple of 5. Thus, it is sufficient to show that the elements of $\mathrm{im}(\mu')$ with second entry 1 are in H. There are 2^3 such elements in H, namely

$$\langle (\mathrm{v}), (\mathrm{i}) \cdot (\mathrm{ii}) \cdot (\mathrm{iii}), (\mathrm{iii}) \cdot (\mathrm{iv}) \cdot (\mathrm{vi}) \rangle = \langle [6, 1, 2, 1, 6, -2], [6, 1, 3, -15, -3, -3], [10, 1, 6, 3, 1, -3] \rangle.$$

Looking at the third entry, $\mathbb{R}$ tells us that the third entry $\mathrm{im}(\mu')$ must be positive, and $\mathbb{Q}_5$ that it is not a multiple of 5, thus we have $\langle 2, 3\rangle$. Since the third entry of the three elements of H given before with second entry 1 generate $\langle 2, 3\rangle$, it is sufficient to show that elements with second and third entry 1 of H and $\mathrm{im}(\mu')$ coincide. The elements of H that have this property are

$$\{[1, 1, 1, 1, 1, 1], [10, 1, 1, -5, -2, -2]\}.$$

Now, in $\mathbb{Q}_3$, the elements with ones in the second and third entry are generated by $[-1, 1, 1, 1, -1, 1]$ and $[3, 1, 1, -3, -3, -1]$; which can be lifted back up by taking into account the kernel of the projection $\langle\{1, -2, -5\}^{\times 6}\rangle$. Thus the possible forth entries are $\langle -2, -3, -5\rangle$. Similarly, in $\mathbb{Q}_5$ we have these generators: $[2, 1, 1, 2, 2, 1]$, $[2, 1, 1, 2, 1, 2]$, $[2, 1, 1, 5, 2, 2]$ and $[10, 1, 1, 5, 1, 1]$ together with kernel $\langle\{1, -1, 6\}^{\times 6}\rangle$ which has the possible forth entries $\langle -1, 5, 6\rangle$. Putting these two together, we thus have $\langle -5, 6\rangle$ as the possible forth entry in $\mathrm{im}(\mu')$. But taking $\mathbb{Q}_2$ into account, it is clear that no multiple of 2 is possible, so in fact, only $\{1, -5\}$ is possible.

Note that $\mathbb{Q}_5$ tells us that $\mathrm{im}(\mu')$ does not contain elements with fifth and sixth entries that are divisible by 5. Now, elements with second and third entries 1, forth in $\{1, -5\}$ and fifth and sixth not a multiple of 5 in the upper bound of $\mathrm{im}(\mu')$ given by considering $\mathbb{Q}_3$ must be generated by $[-1, 1, 1, -1, 1]$ and the kernel. Namely $[\langle 2, 5\rangle, 1, 1, \langle -5\rangle, \langle -1, 2\rangle, \langle -2\rangle]$.

Consider the upper bound given by $\mathbb{Q}_2$ generated by nine elements (label these (i) up to (ix) in the order presented) together with kernel $\{1, -15\}$. Taking intersections with the previous paragraph, the last entry must be in $\{1, -2\}$, so we must eliminate anything that divides 3, namely (ii), (iv) and (ix). Multiplying these pairwise will eliminate multiples of 3, so we can reduce these three elements to two elements by replacing them with (x) = (ii) · (iv) and (xi) = (ii) · (ix).

Continuing in a similar fashion, to get $\langle -1, 2\rangle$ in the 5th entry requires us to eliminate multiples of 3 which are present in (i), (v), (vii), (viii) and (xi). Multiplying (i) with the others reduces these five elements to four. The next steps are to eliminate the two elements with negative 4th entry, then three elements with negative 3rd entry, two elements with non-trivial 3rd entry and finally the two elements with non-trivial second entry. This leaves us with two elements: $[1, 1, 1, 1, 1, -1]$ and $[-6, 1, 1, 3, -2, -2]$. The first is not possible since the last entry must be 1 or -2. Thus we are left with $[-6, 1, 1, 3, -2, -2]$ which, after appropriately multiplying by a kernel element (made up of 1s and -15s), leaves us with the only option:

$$\langle [10, 1, 1, -5, -2, -2]\rangle.$$

These are the only elements of $\mathrm{im}(\mu')$ with second and third entry 1. Since this coincides with those of H, we have proved that $\mathrm{im}(\mu') = H$. Hence $\mathrm{rank}(\mathfrak{G}) = 0$.

4.3 Finding Large Torsion

In the elliptic curves case, Mazur's theorem gives a bound on the size of the torsion. But in higher genera, there is currently no known analogous result. In this section, we find a family of genus 2 curves with an element of order 14 in the Jacobian.

Following Example 8.3.3 of [1], let C be a genus 2 curve of the form

$$C\colon Y^2 = (A(X))^2 - \lambda X(X-1)^4,$$

where $A(X) \in \mathbb{Q}(t)[X]$ is a quadratic and $\lambda \in \mathbb{Q}(t)$. Let $P_0 = \{(0, A(0)), \infty\}$ and $P_1 = \{(1, A(1)), \infty\}$. Then the divisor of $Y - A(X)$ gives

$$1 \cdot P_0 + 4 \cdot P_1 = \mathfrak{O}.$$

Suppose we have the relation that

$$4 \cdot P_0 + 2 \cdot P_1 = \mathfrak{O}.$$

Then

$$M \cdot \begin{pmatrix} P_0 \\ P_1 \end{pmatrix} = \begin{pmatrix} \mathfrak{O} \\ \mathfrak{O} \end{pmatrix}, \quad M = \begin{pmatrix} 1 & 4 \\ 4 & 2 \end{pmatrix}.$$

Note that $\det(M) = -14$, so clearly, $|P_0|, |P_1| \mid 14$. But these two elements are clearly not the identity, and if we ensure that $A(0) \neq 0$ and $A(1) \neq 0$, then both of these elements cannot have order 2 either. So they either have order 7 or 14.

We wish to find a function $Y - v(X)$, where v is a cubic in $\mathbb{Q}(t)[X]$, whose divsor gives rise to the above conditions on P_0 and P_1. Subsituting this relation into the relation of C, the difference of the two sides of C must be $X^4(X-1)^2$, that is,

$$v(x)^2 - A^2 + \lambda X(X-1)^4 = X^4(X-1)^2.$$

Rearranging gives

$$(v + A)(v - A) = X(X-1)^2(X^3 - \lambda(X-1)^2).$$

Letting $\lambda = t$ and finding the difference of

$$\begin{aligned} (v - A) &= X(X-1)^2 \\ (v + A) &= (X^3 - \lambda(X - 1^2)) \end{aligned}$$

gives that

$$A(X) = \frac{1}{2}((t-2)X^2 + (1-2t)X + t), \quad \lambda = t.$$

This gives a family of genus 2 curves with a genus containing at least a 7 torsion element, since $A(1) = -1/2$ and $A(0) = -t$ (both non-zero).

Proposition 4.3.1
For any $t \in \mathbb{Q}$ and $t \neq 0$, the Jacobian of the genus 2 curve

$$C_t \colon Y^2 = \frac{1}{4}((t-2)X^2 + (1-2t)X + t)^2 - tX(X-1)^4$$

has an order 7 element.

Using Magma code (Section A.5), we see that for $|t| \leq 100$, the torsion of $J(C_t)$ is 14 most of the time, except 28 for $t \in \{2, 3, 6, 12, 18, 24, 30, 42, 45, 56, 72, 90\}$ and 56 for $t = 20$. Emperical data also suggests that $|P_0| = 7$ and $|P_1| = 14$.

In fact, $|P_1|$ is always 14. Suppose for a contradiction that P_1 had order 7 instead. Then the first relation of M says $1 \cdot P_0 - 3 \cdot P_1 = \mathfrak{O}$. But this means that $\{(0, A(0)), (1, A(1))\} = \{(1, A(1)), (1, A(1))\}$ which is a contradiction.

Similarly, $|P_0|$ is always 7. Suppose $14 \cdot P_0 = \mathfrak{O}$. Then the second relation of M gives $-2 \cdot P_0 + 6 \cdot P_1 = \mathfrak{O}$. Using the first relation five times, $-7 \cdot P_0 - 14 \cdot P_1 = \mathfrak{O}$. Simplifying, we see that $|P_0| = 7$.

Thus we instead have the following more specific statement.

Corollary 4.3.2
For any $t \in \mathbb{Q}$ and $t \neq 0$, define the following genus 2 curve

$$C_t \colon Y^2 = \frac{1}{4}((t-2)X^2 + (1-2t)X + t)^2 - tX(X-1)^4.$$

Let J_t be the Jacobian of C_t and $\mathfrak{G}_t = J_t(\mathbb{Q})$. Let $P_0 = \{(0, A(0)), \infty\}$ and $P_1 = \{(1, A(1)), \infty\}$. Then $P_0, P_1 \in \mathfrak{G}$, $|P_0| = 7$ and $|P_1| = 14$.

In general, one way to easily find such a series of genus g curves starts with finding a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a+b = 2g+1$, $c+d = 2g+2$ and $\min\{a, c\} + \min\{b, d\} = g+1$. Now we construct the curve

$$C_t \colon Y^2 = (A(X))^2 - tX^a(X-1)^b.$$

Write $e = \min\{a, c\}$ and $f = \min\{b, d\}$; and define

$$A(X) = \frac{1}{2}\left((X^e(X-1)^f) - (X^{a-e}(X-1)^{b-f} - tX^{c-e}(X-1)^{d-f})\right)$$

which has the required degree g (since we have cancellation of X^{g+1}). Write J as the Jacobian of C_t and $\mathfrak{G} = J(\mathbb{Q})$. Then two elements of the Jacobian are P_0 given by the divisor $(0, A(0))$ with ∞ and P_1 as $(1, A(1))$ with ∞. At this stage, once we check that C_t does not decrease in genus, we can deduce that C_t is indeed a genus g hyperelliptic curve and that

$$1 < |P_0|, |P_1| \mid \det(M).$$

If $\det(M)$ is prime, then clearly the elements have order equal to this prime. Otherwise, we require some extra observations (such as the ones given in the genus 2 example) to deduce the exact order of P_0 and P_1, though we always know that the order is at least the smallest prime dividing the determinant.

Appendix A

Code

In this dissertation, I used three programming languages: Python[1], Sage[2] and Magma[3]. Maple[4] is also widely used but is under a paywall and the previous three languages are sufficient for the purpose of this dissertation. Pros and cons of the following are as follows.

- Python is easy to learn, open source and widely used and documented. But it not handle symbolic calculations well and is mainly useful here for brute force calculations.
- Sage has identical syntax to Python and so basic Python code works in Sage (in particular the Python code snippet given later on). It is also open source. Sage is good at symbolic calculations and has basic elliptic curve functionality.
- Magma is good at more complex arithmetic geometry. But it is closed source and behind a pay-wall, though there is an online calculator available on their website which is sufficient for this dissertation.

In Python and Sage, a comment line suceeds `#`. In Magma, comments are given by `//`. In Magma, every line ends with `;` and this character prints any variable given before it. To print in Python and Sage, use `print()`. Multiplication in all cases is `*`. Powers are `**` in Python and Sage, and `^` in Sage and Magma.

We shall go through useful snippets of code in a similar order to the main body of this dissertation.

A.1 Elliptic Curves

Let us use the example $E\colon Y^2 = X(X-5)(X-7) = X^3 - 12X^2 + 35X$. Using Sage, we can find information about this curve.

[1] https://www.python.org/

[2] https://sagecell.sagemath.org/

[3] http://magma.maths.usyd.edu.au/calc/

[4] https://www.maplesoft.com/

```
E=EllipticCurve([0,-12,0,35,0]) # Defines the ec E
print(E)                        # Prints E
print(factor(E.discriminant())) # The discriminant of E
print(E.rank())                 # The rank of E
print(E.torsion_points())       # The torsion of E
```

This tells us that the elliptic curve E has descriminant $2^6 5^2 7^2$, rank 0 and torsion $E_{\text{tors}}(\mathbb{Q}) = \{\mathfrak{O}, (0,0), (5,0), (7,0)\} = E(\mathbb{Q})[2]$. Note that `EllipticCurve([0,a,0,b,c])` defines an elliptic curve $Y^2 = X^3 + aX^2 + bX + c$, the other two entries are for cross terms with Y. And, `E.torsion_points()` gives points in projective form.

A.2 p-adic point search

Using Python, we can brute force whether a polynomial in X has a non-zero p-adic square root at a point x. This is useful for finding extra generators of $\mathfrak{G}_p$.

```
p=2  # Prime p
X=28 # Specific value of x
F=X*(X-1)*(X-2)*(X-6)*(X-9) # Polynomial in X

# Function to list squares modulo p
def squares(p):
    sq=[]
    i=0
    while i<p: # For every i<p add i^2 to the list of
   squares
        sq.append(i**2%p)
        i=i+1
    return(sq)

# Function to find the largest power of p in an integer
   k and output k/p^n and power n
def largestpower(k):
    n=0
    k=k+0.0
    k1=k
    while (k1.is_integer()):
        k1=k/p**n
        n=n+1
        if k1==0:
            break
    k=k1*p
    n=n-2
    return(k,n)

sq=squares(p) # Squares mod p
k,n=largestpower(F) # Decomposition of F(x)

if p==2: # Catches the case of p=2 so we can apply mod 8
    q=8
else:
    q=p

print(F)       # Print F(x)
print(n,k,k%q) # Print n=v_p(F(x)), k=F(x)/v_p(F(x))p^n
   and k mod p (or mod 8 if p=2)

# Use Prop 2.4.2
if k%q in sq and n%2==0:
    print(F,"is a non-zero square in Z_"+str(p))
```

A.3 Genus 2 Curves

We can do calculations on genus 2 curves using Magma. Let us use the curve $C\colon Y^2 = X(X-2)(X-3)(X-5)(X-8)$.

```
_<x>:=PolynomialRing(Rationals()); //Base field
pol:=x*(x-2)*(x-3)*(x-5)*(x-8);
C:=HyperellipticCurve(pol); //Our Curve
J:=Jacobian(C); //Jacobian
RankBounds(J); //Rank Bound
```

This outputs the rank bound as two numbers, the lower and upper bounds for the rank. In this case, both are 0, so we definitely have a rank 0 curve. As long as we are able to do complete 2-descent, the upper and lower bounds will be equal. We can then find rational points and elements of the Jacobian respectively, up to a certain bound.

```
Pts:=Points(C:Bound:=100); Pts; // Rational points
PtsJ:=Points(J:Bound:=100); PtsJ; // Elements of
   Jacobian
```

The rational points are outputed as a projective point. The Jacobian is outputted as projective polynomials, so if the last coordinate is 0, that point is the identity. Otherwise, the roots of the first polynomial give the x, u of the divisor $\{(x, y), (u, v)\}$ as discussed here https://magma.maths.usyd.edu.au/magma/handbook/text/1560.

We can define elements of the Jacobian using rational points as follows.

```
A:=Pts[2]-Pts[1];A; // {(0,0),id}
B:=Pts[2]-Pts[3];B; // {(0,0),(2,0)}
```

And addition is obvious.

```
A+B; // {(2,0),id}
```

We can also find the torsion points and the discriminant.

```
TorsionSubgroup(J); // Torsion
Discriminant(C); // Discriminant
```

A.4 Chabauty's Method

We shall present the code used for the previous example. We first use Magma to find out the rank of the curve.

```
_<x>:=PolynomialRing(Rationals()); //Base field
pol:=x*(x-1)*(x-2)*(x-6)*(x-9);
C:=HyperellipticCurve(pol); //Our Curve
J:=Jacobian(C); //Jacobian
RankBounds(J); //Rank Bound
```

We get a rank of 1. We can then use Magma to find rational points on C up to a bound and define the divisor $\mathfrak{D}$ of infinite order.

```
Pts:=Points(C:Bound:=100); Pts; //Rational points
D:=(Pts[8]-Pts[1]);D;Order(D); //D
```

Magma already has Chabuty built in, so we may run `Chabauty(D);` to get a list of all rational points. Instead, let us do it "by-hand". The first step is to consider C modulo a good prime (13 in this case).

```
_<x>:=PolynomialRing(FiniteField(13)); //Base field
pol:=x*(x-1)*(x-2)*(x-6)*(x-9);
C:=HyperellipticCurve(pol); //Our Curve
J:=Jacobian(C); //Jacobian
Pts:=Points(C); //Points
D:=Pts[13]-Pts[1]; //Point corresponding to D mod 13
```

Then we find every $\mathfrak{A}$ that reduces to a point of the form $\{\tilde{P}, \tilde{P}\}$.

```
     //List all 2-torsion
orderPoints:=[Order(Points(J)[i]) eq 2 select i else 0:i
    in [1..#Points(J)]];
twoTor:=[Points(J)[1]];
for i in orderPoints do
    if not(i eq 0) then
```

```
        twoTor:=Append(twoTor,Points(J)[i]);
        end if;
    end for;

     //Iterate over all choices for P=B+i*D
for B in twoTor do
    for i in [0..5] do
        P:=B+i*D;
        //check if defining polynomial of the x-
   coordinate of P has exactly 1 root of multiplicity 2
        if #Roots(P[1]) eq 1 and Roots(P[1])[1][2] eq 2
   then
            Roots(P[1]);
            B; i; P; //Output B, then i, then P
            end if;
        end for;
    end for;
```

Bringing these back up to $\mathbb{Q}$, we can find the two non-identity points of the form $\{P, P\}$.

```
     //Define objects
_<x>:=PolynomialRing(Rationals()); //Base field
pol:=x*(x-1)*(x-2)*(x-6)*(x-9);
C:=HyperellipticCurve(pol); //Our Curve
J:=Jacobian(C); //Jacobian
Pts:=Points(C:Bound:=100^2); Pts; //Points

D:=(Pts[8]-Pts[1]); D; //Point corresponding to D

     //Four points found before
B2:=(Pts[1]-Pts[1]);B2+2*D;
B3:=(Pts[1]-Pts[1]);B3+4*D;B3-2*D;
B4:=(Pts[2]-Pts[1])-(Pts[1]-Pts[6]);B4+1*D;
B5:=(Pts[2]-Pts[1])+(Pts[6]-Pts[1]);B5+5*D; B4-D;
```

We can now move on to computing the local parameters. For this, we use Sage. First define $\{(x, y), (u, v)\} = \mathfrak{E}$.

```
x = (3*145940556273707085441196519099/592834428929026720148888341476) -
    (3*2340/592834428929026720148888341476)*sqrt
    (-3182434692678204560739929758205767407808798573246230)
u = (3*145940556273707085441196519099/592834428929026720148888341476) +
    (3*2340/592834428929026720148888341476)*sqrt
    (-3182434692678204560739929758205767407808798573246230)
y=1/1711447333809472145468719630736594643349338724948367240309298312164333248
    *(2*155406215716448164939712279680108237163975878095358229703839535871809063735
    +1928194356507392461844527917380068711252339505148*sqrt
    (-2*1591217346339102280369964879102883703904399286623115))
v=1/1711447333809472145468719630736594643349338724948367240309298312164333248
    *(2*155406215716448164939712279680108237163975878095358229703839535871809063735
    -1928194356507392461844527917380068711252339505148*sqrt
    (-2*1591217346339102280369964879102883703904399286623115))
```

Now we calculate s_1 and s_2 according to page 7 of [1]. Note the use of `full_simplify` which simplifies a symbolic expression (in terms of roots etc).

```
f0,f1,f2,f3,f4,f5,f6=0,108,-192,101,-19,1,0 # Coefficients of F(X)

F0=2*f0+f1*(x+u)+2*f2*x*u+f3*x*u*(x+u)+2*f4*x^2*u^2+f5*x^2*u^2*(x+u)+2*f6*x^3*u^3
B0=(F0-2*y*v)/(x-u)^2
delta=B0^2

a,b=x,u
Gxu=4*f0+f1*(a+3*b)+f2*(2*a*b+2*b^2)+f3*(3*a*b^2+b^3)+4*f4*a*b^3+f5*(a^2*b^3+3*a*b^4)
    +f6*(2*a^2*b^4+2*a*b^5)
a,b=u,x
Gux=4*f0+f1*(a+3*b)+f2*(2*a*b+2*b^2)+f3*(3*a*b^2+b^3)+4*f4*a*b^3+f5*(a^2*b^3+3*a*b^4)
    +f6*(2*a^2*b^4+2*a*b^5)
gamma0=(Gxu*y-Gux*v)/(x-u)^3

a,b=x,u
Hxu=f0*(2*a+2*b)+f1*(3*a*b+b^2)+4*f2*a*b^2+f3*(a^2*b^2+3*a*b^3)+f4*(2*a^2*b^3+2*a*b
    ^4)+f5*(3*a^2*b^4+a*b^5)+4*f6*a^2*b^5
a,b=u,x
Hux=f0*(2*a+2*b)+f1*(3*a*b+b^2)+4*f2*a*b^2+f3*(a^2*b^2+3*a*b^3)+f4*(2*a^2*b^3+2*a*b
    ^4)+f5*(3*a^2*b^4+a*b^5)+4*f6*a^2*b^5
gamma1=(Hxu*y-Hux*v)/(x-u)^3

z0=delta
z1=gamma1
z2=gamma0

s1=(z1/z0).full_simplify()
s2=(z2/z0).full_simplify()

print(s1)
print(s2)
```

We first define our base field and get $s_1, s_2 \mod 13^4$.

```
Zp=Integers(13^4)
print(Zp(s1))
print(Zp(s2))
```

Then we compute $E(n \cdot L(\mathbf{s})) \mod 13^4$. Note that in the following, the formal logarithm and exponential are defined here up to powers of 7 (from [5] and [6] respectively), though we only need them up to powers of 4 as higher powers vanish. The only modification needed from the Maple code on those webpages is to get rid of the colon in `:=` and at the end of the line.

```
# From http://people.maths.ox.ac.uk/flynn/genus2/local/
  log
Log1=
Log2=
```

[5] http://people.maths.ox.ac.uk/flynn/genus2/local/log

[6] http://people.maths.ox.ac.uk/flynn/genus2/local/exp

```
# Define the variable n
var(’n’)
s1=n*Log1
s2=n*Log2
Zpn.<n>=PolynomialRing(Zp) # (Z/(13^4 Z))[n]

# From http://people.maths.ox.ac.uk/flynn/genus2/local/
   exp
Exp1=
Exp2=

print(Zpn(Exp1)) # Reducing the function Exp1 modulo
   13^4
print(Zpn(Exp2)) # Reducing the function Exp2 modulo
   13^4
```

Now, with the goal of computing the polynomial θ for the point $\mathfrak{A} = 2 \cdot \mathfrak{D}$ modulo 13^4, we first find (a_i). As $\mathfrak{A}$ is of the form $\{P, P\}$ where $P = (x, y) = (u, v)$, we multiply each fraction by 1 represented as the conjugate of its numerator so that Sage simplifes before performing subsitutions to avoid divison by $(x - u)$.

```
var(’x y u v’) # Define variables
x0,y0,u0,v0=9/4,135/32,9/4,135/32 # Values of x,y,u,v for
   subsitution

# Intermediate functions
f0xu=2*f0+f1*(x+u)+2*f2*(x*u)+f3*(x+u)*(x*u)+2*f4*(x*u)^2+f5*(x+u)*(
   x*u)^2+2*f6*(x*u)^3
f1xu=f0*(x+u)+2*f1*(x*u)+f2*(x+u)*(x*u)+2*f3*(x*u)^2+f4*(x+u)*(x*u)
   ^2+2*f5*(x*u)^3+f6*(x+u)*(x*u)^3
gxu=f0*4+f1*(x+3*u)+f2*(2*x*u+2*u^2)+f3*(3*x*u^2+u^3)+f4*(4*x*u^3)+
   f5*x*(x*u^3+3*u^4)+f6*2*x*(x*u^4+u^5)
gux=f0*4+f1*(u+3*x)+f2*(2*u*x+2*x^2)+f3*(3*u*x^2+x^3)+f4*(4*u*x^3)+
   f5*u*(u*x^3+3*x^4)+f6*2*u*(u*x^4+x^5)
hxu=f0*2*(x+u)+f1*u*(3*x+u)+f2*4*x*u^2+f3*x*u^2*(x+3*u)+f4*2*x*u^3*(
   x+u)+f5*x*u^4*(3*x+u)+f6*4*x^2*u^5
hux=f0*2*(u+x)+f1*x*(3*u+x)+f2*4*u*x^2+f3*u*x^2*(u+3*x)+f4*2*u*x^3*(
   u+x)+f5*u*x^4*(3*u+x)+f6*4*u^2*x^5
Fx=f0+f1*x+f2*x^2+f3*x^3+f4*x^4+f5*x^5+f6*x^6 # y^2
Fu=f0+f1*u+f2*u^2+f3*u^3+f4*u^4+f5*u^5+f6*u^6 # v^2

# (a_i)
a15=((x-u)^2).full_simplify().subs(x=x0,y=y0,u=u0,v=v0)
a14=1
a13=(x+u).full_simplify().subs(x=x0,y=y0,u=u0,v=v0)
a12=(x*u).full_simplify().subs(x=x0,y=y0,u=u0,v=v0)
a11=(x*u*(x+u)).full_simplify().subs(x=x0,y=y0,u=u0,v=v0)
a10=((x*u)^2).full_simplify().subs(x=x0,y=y0,u=u0,v=v0)
a9=((Fx-Fu)/((x-u)*(y+v))).full_simplify().subs(x=x0,y=y0,u=u0,v=v0)
a8=((u^2*Fx-x^2*Fu)/((x-u)*(u*y+x*v))).full_simplify().subs(x=x0,y=
   y0,u=u0,v=v0)
a7=((u^4*Fx-x^4*Fu)/((x-u)*(u^2*y+x^2*v))).full_simplify().subs(x=x0
   ,y=y0,u=u0,v=v0)
a6=((u^6*Fx-x^6*Fu)/((x-u)*(u^3*y+x^3*v))).full_simplify().subs(x=x0
   ,y=y0,u=u0,v=v0)
a5=((f0xu^2-4*Fx*Fu)/((x-u)^2*(f0xu+2*y*v))).full_simplify().subs(x=
   x0,y=y0,u=u0,v=v0)
a4=((f1xu^2-(x+u)^2*Fx*Fu)/((x-u)^2*(f1xu+(x+u)*v*y))).full_simplify
   ().subs(x=x0,y=y0,u=u0,v=v0)
a3=((x*u)*a5).full_simplify().subs(x=x0,y=y0,u=u0,v=v0)
a2=((gxu^2*Fx-gux^2*Fu)/((x-u)^3*(gxu*y+gux*v))).full_simplify().
   subs(x=x0,y=y0,u=u0,v=v0)
a1=((hxu^2*Fx-hux^2*Fu)/((x-u)^3*(hxu*y+hux*v))).full_simplify().
   subs(x=x0,y=y0,u=u0,v=v0)
a0=(a5^2).full_simplify().subs(x=x0,y=y0,u=u0,v=v0)

# ensure gcd(a_i)=1
a=[a0,a1,a2,a3,a4,a5,a6,a7,a8,a9,a10,a11,a12,a13,a14,a15]
aLcm=lcm([denominator(ai) for ai in a])
a=[ai*aLcm for ai in a]
a0,a1,a2,a3,a4,a5,a6,a7,a8,a9,a10,a11,a12,a13,a14,a15 = a
print(a)
```

If $\mathfrak{A} = \infty$ then we would have this instead.

```
a0,a1,a2,a3,a4,a5,a6,a7,a8,a9,a10,a11,a12,a13,a14,a15 =
   1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
```

Recall that the Φ_{ij} depend on the coefficients f_i, a_i from above, and b_i arrising from t_1 and t_2. We now compute b_i. We use the formule from `http://people.maths.ox.ac.uk/flynn/genus2/local/local.coordinates` with the name changes $s_i \to b_i$ and $s_1, s_2 \to t_1, t_2$.

```
var(’t1 t2’) # Define variables

# (b_i)
b0=1
b1=t1
b2=t2
# http://people.maths.ox.ac.uk/flynn/genus2/local/local.coordinates
b3=
b4=
b5=
b6=
b7=
b8=
b9=
b10=
b11=
b12=
b13=
b14=
b15=
```

We can now use the formulae for Φ_{ij} (from `http://people.maths.ox.ac.uk/flynn/genus2/jacobian.variety/bilinear.forms`) to arrive at $\theta(n)$.

```
# http://people.maths.ox.ac.uk/flynn/genus2/jacobian.variety/
   bilinear.forms}
phi41=
phi42=
phi43=
```

Finally, we are in a position to compute $\theta(n)$.

```
# Symbolically find theta(n)
theta=(phi42^2-4*phi41*phi43).full_simplify()

# Simplify theta modulo 13^4
Zpt.<t1,t2>=PolynomialRing(Zp)
print(Zpt(theta))

# Substitute our expressions for t_1 and t_2 to get the
   final theta(n)
print(Zpt(theta).subs(t1=Zpn(Exp1), t2=Zpn(Exp2)))
```

If our original power of p (here 13^4) does not give us a $\theta(n)$ that Strassman's Theorem works on, we can go back and redefine `Zp=Integers(...)` to a larger power of p, provided that considering the formal exponential and logarithm up to degree 7 is enough. This happens here when we consider $\mathfrak{A} = \mathfrak{O}$ where we need to consider 13^7 instead (`Zp=Integers(13^7)`).

A.5 Large Torsion

Note that Magma requires hyperelliptic curves to have integer coefficients, so we multiply the right by 4 (which is a birational transformation $Y \mapsto 2Y$). This prints the size of the torsion of $J(C_t)$ for $-n \leq t \leq n$ where $n = 100$.

```
_<x>:=PolynomialRing(Rationals()); //Base field
n:=100; //Max t to try

for t in [-n..n] do
    if not(t eq 0) then
        A:=(1/2)*((t-2)*x^2+(1-2*t)*x+t);
        pol:=A^2-t*x*(x-1)^4;
        pol:=pol*4; //Make integer coefficients
        C:=HyperellipticCurve(pol); //Curve C_t
        J:=Jacobian(C); //Jacobian

    //Size of Torsion
        printf "%o: %o\n",t,#(TorsionSubgroup(J));

    //Order of P_0 and P_1 resp
        Order(C![0,Evaluate(A,0)*2]-C![1,0,0]);
        Order(C![1,Evaluate(A,1)*2]-C![1,0,0]);
        end if;
    end for;
```

References

[1] Cassels, J. W. S., & Flynn, E. V. (1996). Prolegomena to a middlebrow arithmetic of curves of genus 2 (Vol. 230). Cambridge University Press.

[2] Silverman, J. H. (2009). The arithmetic of elliptic curves (Vol. 106). Springer Science & Business Media.

[3] Cassels, J. W. S. (1991). LMSST: 24 Lectures on Elliptic Curves (No. 24). Cambridge University Press.

[4] Serre, J. P. (2013). Local fields (Vol. 67). Springer Science & Business Media.

[5] Silverman, J. H., & Tate, J. T. (1992). Rational points on elliptic curves (Vol. 9). New York: Springer-Verlag.

[6] Schaefer, E. F. (1995). 2-descent on the Jacobians of hyperelliptic curves. Journal of number theory, 51(2), 219-232.