Height Bounds for n-Coverings

Graham Sills*
Trinity College, Cambridge

June 11, 2010

A thesis submitted for the
degree of Doctor of Philosophy
at the University of Cambridge.

*Email: gs300@cam.ac.uk

Summary

This thesis aims to develop the theory of height bounds between points on an elliptic curve E and corresponding points on n-descendant curves C_n. We concentrate on 2- and 4-descendants and, in general, work over $\mathbb{Q}$.

We start by discussing the basics of descent and explain that the objects obtained can be viewed as n-coverings of E. We explain the theory of how height comparisons can be made between E and C_n and give a crude bound using the theory of resultants.

The majority of the work then splits into two parts; 2-coverings, which amounts to the study of binary quartic forms, and 4-coverings, which amounts to the study of quadric intersections in $\mathbb{P}^3$. In each section, after discussing the known theory, we define a bound as the sum of local contributions ε_p, calculated at all primes and ∞. We discuss some properties of the ε_p and show how they can be computed. A slightly 'brute force' approach is required at $p = \infty$ and the primes 2 and 3 require special consideration. We give an algorithm which has been implemented using MAGMA and also give some examples.

The study of 4-coverings gives the more powerful bound, so we investigate this more deeply, showing that the best bounds can be found at the 'centre' of a certain graph. Section 4 then investigates this graph in detail for curves with multiplicative reduction, which is in some ways the most complicated case. We then give a few more examples and directions for further study.

Declaration

I hereby declare that this thesis is the result of my own work and includes nothing which is the outcome of work done in collaboration. I also declare that this thesis is not substantially the same as any other that I have submitted for a degree or diploma at any other university.

Acknowledgments

Primarily, I would like to thank my supervisor Tom Fisher for his guidance and helpful comments. He showed immense patience whenever I failed to grasp anything and I am somewhat surprised that I never caused him to raise his voice. I would also like to thank Trinity College for their financial support.

I would like to thank the friends I have made through mathematics; Mohammad Sadek, Chris Taylor, Vicky Neale, Jack Waldron, Chris Cawthorn, Johnny Evans, Allan Lo, Mike Shuter, Jon Middleton, James Griffin and Tim Henshaw deserve particular mention for their helpful mathematical comments and (more usually) for their social distraction around lunch times. The Guardian crossword and Cambridge Snooker Centre also deserve a mention for their therapeutic effect on my sanity.

Finally, I would like to thank my girlfriend Hilde, my parents and my brother for their supportive nods and smiles.

Contents

1 Introduction

Elliptic curves date back to Diophantus in 250AD and were initially studied by mathematicians trying to find solutions to puzzles involving sums of cubes, areas of right angled triangles or stacks of cannonballs (to name but a few). Many people still study them for practical purposes such as elliptic curve cryptography, but I think there is a deeper reason why they continue to get so much attention. This reason is that they are still so mysterious when compared to other arithmetical objects.

To explain, we must understand that one of the most important problems in studying a particular curve is being able to describe its rational points. In some sense everything is known if the curve has genus 0; i.e. we can parametrise the solutions to show there are either no rational points or an infinite number. If a curve has genus 2 or higher, then a theorem of Faltings tells us that there are only a finite number of rational points. But for elliptic curves (which have genus 1), we cannot say any such thing. We can realise the rational points as a finitely generated abelian group (by the Mordell-Weil Theorem), but in general we have no way of determining whether there are any (non-trivial) rational points at all.

It is somewhat surprising that so little is known, since they have far more apparent structure than other Diophantine equations. They also exist in an area of mathematics where number theory, analysis and algebraic geometry converge, so we should have more angles for attack in trying to understand them.

We want to write down explicitly the group of rational points on an elliptic curve E and this group is given by the Mordell-Weil Theorem as

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

for T the torsion subgroup and an integer r known as the rank. Theorems of Nagell and Lutz and of Mazur explain the torsion subgroup and this is in some sense dealt with. But that still leaves two problems; to determine the rank and to write down the generators of E, i.e. the set of r points which generate the infinite part of $E(\mathbb{Q})$.

Methods have become fairly effective using L-series to compute r, although for $r > 1$ they rely on unproved parts of the Birch and Swinnerton-Dyer Conjecture. To find the generators, there is a good method using Heegner points for

$r = 1$, but for higher ranks the best methods involve quadratic sieves modulo prime powers and various p-adic arguments. These methods have been made fast, but they are still exponential in the height of the point being searched for, so they eventually become impractical.

What we will instead investigate is the possibility of searching on n-descendant curves C_n, known as n-coverings of E. The term 'descent' dates back to Fermat (who approached the problem of 2-descent) and it involves algorithms for finding what is called the n-Selmer group of E. This group is written as $S_n(E)$ and its elements are n-coverings, which we can view as genus one curves that are equivalent to E over $\overline{\mathbb{Q}}$ and have points everywhere locally (i.e. $C_n(\mathbb{Q}_p) \neq \emptyset$ for all p). It turns out that we are then interested in those elements of $S_n(E)$ that have a point over $\mathbb{Q}$, since these correspond to generators of E. This then allows us to get a bound for the rank of E.

The height of a point is closely related to how much time it takes to search for it. It is known that points on n-coverings should have smaller height than their image on the elliptic curve; in fact the height $h(q_n)$ of a point on C_n should be approximately $h(P)/(2n)$, for P the corresponding point on E. We know that constants exist bounding the difference between these two heights and computing these bounds precisely will be the main aim of this thesis. Having this bound on the difference is useful; for example, there are reasons why we may know that there should be a point on E of height $h(P) < 500$, say. This point would be impractical to search for directly, but it means than we would only need to search up to a height of about $250/n$ on an n-covering. Searching on a 4-covering would then be quite feasible and the fact that these heights are logarithmic makes the improvement considerable.

In fact only 2-,3- and 4-descent work efficiently, although work has been done by Fisher on 6- and 12-descent ([Fis08]) and by Stamminger on 8-descent ([Sta05]). The group $S_2(E)$ consists of binary quartics:

$$C_2 : y^2 = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

and $S_4(E)$ consists of quadric intersections in $\mathbb{P}^3$:

$$\begin{aligned} C_4 : \; & a_{11}x_1^2 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{14}x_1x_4 + a_{22}x_2^2 + a_{23}x_2x_3 + a_{24}x_2x_4 + \\ & a_{33}x_3^2 + a_{34}x_3x_4 + a_{44}x_4^2 = 0, \\ & b_{11}x_1^2 + b_{12}x_1x_2 + b_{13}x_1x_3 + b_{14}x_1x_4 + b_{22}x_2^2 + b_{23}x_2x_3 + b_{24}x_2x_4 + \\ & b_{33}x_3^2 + b_{34}x_3x_4 + b_{44}x_4^2 = 0. \end{aligned}$$

To demonstrate that the points are smaller on these curves than on E, take the elliptic curve given by

$$y^2 = x^3 - 59643.$$

We get a single binary quartic from 2-descent:

$$y^2 = -15x^4 + 39x^3z + 9x^2z^2 + 33xz^3 - 21z^4$$

and a single quadric intersection from 4-descent[1]:

$$\begin{aligned} 4x_1x_2 + 2x_1x_3 - 2x_2x_3 - 2x_2x_4 + x_3^2 - 2x_3x_4 + 2x_4^2 = 0, \\ x_1^2 - 2x_1x_2 - 3x_2^2 - 2x_2x_3 - 2x_2x_4 + 4x_3^2 + x_4^2 = 0. \end{aligned} \tag{1}$$

The quadric intersection contains the point $(-1 : 1 : 0 : 2)$, which corresponds to $(119, 4725, 40)$ on the binary quartic and

$$\left(\frac{62511752209}{9922500}, \frac{15629405421521177}{31255875000}\right)$$

on E. This is the smallest point on E of infinite order, but would have taken a very long time to find directly. We will investigate exactly how the sizes of these points change by examining the maps from C_4 and C_2 down to E.

When trying to discover things about n-coverings over $\mathbb{Q}$, we will work over $\mathbb{Q}_p$ instead of directly over $\mathbb{Q}$. This is because we can break up the height of a point into its local contributions and consider them individually. We then also make use of the fact that $\mathbb{Z}_p$ is compact.

It is possible to define the notion of equivalence of n-coverings and we will be interested in them up to $\mathbb{Q}_p$-equivalence. However, it will become apparent

[1] We use the computer algebra package MAGMA (see [BCP97]) for all computations.

that the height bound between $\mathbb{Q}_p$-equivalent n-coverings and E actually differs depending on the $\mathbb{Z}_p$-equivalence class in which our n-covering lies. For example, it would have been better to have considered the reduced (in the sense below) quadric intersection

$$\begin{aligned} x_1x_2 + x_1x_4 + x_2^2 - x_2x_3 + x_3^2 + 2x_4^2 &= 0, \\ -3x_1x_2 + 4x_1x_3 + 2x_1x_4 + x_2^2 - x_2x_3 - 4x_2x_4 - x_3^2 - 3x_3x_4 - x_4^2 &= 0, \end{aligned}$$

in the above example. This is equivalent to the quadric intersection (1) over $\mathbb{Q}_p$ for all p, but not over $\mathbb{Z}_{47}$, and it contains the point $(1 : 0 : 0 : 0)$, which is of even smaller height than the one previously found. We will give more extreme examples in later sections.

To demonstrate this in general, we will show how to construct a graph whose vertices represent $\mathbb{Z}_p$-equivalence classes. For $n = 2$, the graph is not complicated and is often just a string of vertices, but for $n = 4$ it usually has many more vertices and has weighted edges. We show how to generate the largest graphs in section 4. The best bounds are found at the central vertices of these graphs, so we can choose which n-covering is most likely to be the quickest on which to search. Alternatively, if we are prepared to search on a few different n-coverings simultaneously, then we can give the set which is best to use. Even in the worst instances, these bounds turn out to be relatively small and workable.

To demonstrate that the bounds we calculate are better than previous methods, take the elliptic curve and 2-covering given by

$$\begin{aligned} E &: y^2 + xy = x^3 + x^2 - 2x + 1, \\ C_2 &: y^2 + (x^2 + xz + z^2)y = -x^3z - x^2z^2 + 2xz^3 + z^4. \end{aligned}$$

The current method to bound the difference between the height of a point $P_2 \in C_2$ and a quarter of the height of the corresponding point $P \in E$ is to use a method of resultants, which gives a bound of

$$h(P_2) - h(P)/4 \leq 4.8201...$$

However by our methods, we can find a bound of 0.1234..., which is a marked improvement. The improvements are even more obvious for 4-coverings, where

the bound using resultants can become quite unworkable.

It should also be noted that this work is only possible thanks to recent developments in the theories of minimisation and reduction. See sections 2.2 and 3.2 for the definitions of these terms, but roughly speaking, minimisation allows us to write equations for n-coverings such that the valuation of the discriminant $v_p(\Delta(C_n))$ is as small as possible. Roughly speaking, the reduction process tries to get the n-coverings as near as possible to being Hesse forms[2] and to have small coefficients (over $\mathbb{R}$). If the operations of minimisation and reduction were not possible, then the bounds we produce would be meaningless, or at best very large. Our results are a good way of seeing the benefits of these operations.

[2]For binary quartics, Hesse forms are $y^2 = a(x^4 + z^4) + bx^2z^2$ for $a, b \in \mathbb{C}$ and for quadric intersections they are $a(x_0^2 + x_2^2) + bx_1x_3 = a(x_1^2 + x_3^2) + bx_0x_2 = 0$ for $a, b \in \mathbb{C}$.

1.1 Notation

Let K be a number field with ring of integers O_K and let M_K be the set of standard absolute values on K. For $v \in M_K$, let $n_v = [K_v : \mathbb{Q}_v]$. Throughout, E/K will be an elliptic curve defined over K with point at infinity O. The field K will usually be $\mathbb{Q}$ and we will fix a Weierstrass equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in \mathbb{Q}$. When not working in characteristic 2 or 3, we will usually assume our elliptic curve is given in shorter Weierstrass form.

We will assume E is minimal and we will then write $\Delta(E)$ for its discriminant (called the minimal discriminant of E), calculated as a polynomial[3] in the coefficients of E.

For a curve C defined over $\mathbb{Q}$ or $\mathbb{Q}_p$, we will write $\overline{C}$ for its reduction modulo a prime p and the context will make it clear whether this is a general prime or a specific one. The valuation at p and the absolute value at p will be denoted v_p and $|.|_p$, respectively. We write $C(\mathcal{R})$ for the set of points on C defined over a ring $\mathcal{R}$.

Also, for two real-valued functions f and g defined on a set of points $\mathcal{S}$, we write

$$f = g + O(1),$$

if there exist constants c_1 and c_2 such that $c_1 \leq f(P) - g(P) \leq c_2$ for all $P \in \mathcal{S}$.

1.2 Height Functions

The purpose of height functions is to get some idea of the 'arithmetic size' of a point in projective space and the height of a point will be closely related to the amount of time required to search for it, starting from 0. However, a height function for elliptic curves was first required not for computation, but in order to prove the Mordell-Weil Theorem. Good references for the theory of heights are chapters VIII.5 and VIII.6 in [Sil09] and chapter 5 in [SZ03]. Let us start by defining a height in projective space.

[3] Given on p46 of [Sil09].

Definition 1 *Let $P \in \mathbb{P}^N(K)$ be the point given by $(x_0 : \ldots : x_N)$ for $x_i \in K$. The height of P relative to K, written as the product of local heights, is*

$$H_K(P) = \prod_{v \in M_K} \max_i \{|x_i|_v\}^{n_v}.$$

The global absolute (or naive) height of P is then

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]}.$$

Note that this is ≥ 1, it is independent of the ground field and it can be shown that it is independent of the choice of homogeneous co-ordinates for P. In later chapters, K will usually be $\mathbb{Q}$ and we will be interested in calculating $\max\{|x_i|_p\}$ at all primes p and ∞.

Definition 2 *For P as in the previous definition, the absolute logarithmic height of P is given by*

$$h(P) = \frac{1}{[K : \mathbb{Q}]} \log H_K(P).$$

Note that this is ≥ 0 and it can be shown that for any constant c,

$$\{P \in \mathbb{P}^N(K) : h(P) \leq c\}$$

is a finite set. We will also want to apply functions to points and calculate their heights.

Definition 3 *For f a morphism and $P \in \mathbb{P}^N(K)$, we write $h_f(P) = h(f(P))$.*

A more complicated type of height function, with many benefits when working on elliptic curves is the canonical height.

Definition 4 *For E an elliptic curve over K and $P \in E(\overline{K})$, the canonical (or Neron-Tate) height is the function defined by*

$$\begin{aligned} \hat{h} \colon E(\overline{K}) &\to \mathbb{R} \\ P &\mapsto \lim_{N \to \infty} 4^{-N} h([2^N]P). \end{aligned}$$

This has the following properties for all $P, Q \in E(\overline{K})$ and $m \in \mathbb{Z}$:

1. $\hat{h}(P + Q) + \hat{h}(P - Q) = 2(\hat{h}(P) + \hat{h}(Q))$.
2. $\hat{h}([m]P) = m^2 \hat{h}(P)$.

3. $\hat{h}$ is a quadratic form on E.

4. $\hat{h}(P) = 0 \Leftrightarrow P$ is a torsion point.

5. Let $f \in K(E)$ be an even function of degree d, then $d\hat{h} = h_f + O(1)$.

There are clear advantages to having a height function with these properties[4], but unfortunately it requires the group structure of an elliptic curve. This means it is difficult to come up with a sensible definition for a canonical height function on other curves and we will generally just use the naive height $H(P)$.

It is worth noting that the canonical height does not depend on a choice of Weierstrass equation, whereas the naive height does since it requires specific co-ordinates.

1.3 General Selmer Groups

The elements of the 2- and 4-Selmer groups will be the focus of our study in later sections, but it is worth discussing their general structure first.

Let us assume we have an elliptic curve E/K for a number field K and let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. From the multiplication by n map on the elliptic curve, we have the following straightforward exact sequence of Galois modules:

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{\times n} E \longrightarrow 0.$$

We then pass to the long exact sequence of cohomology[5]:

$$0 \to E(K)[n] \to E(K) \xrightarrow{\times n} E(K) \to H^1(G_K, E[n]) \to ...$$

from which we obtain the widely used Kummer exact sequence:

$$0 \longrightarrow \frac{E(K)}{nE(K)} \longrightarrow H^1(G_K, E[n]) \longrightarrow H^1(G_K, E)[n] \longrightarrow 0,$$

[4]Indeed somewhat weaker properties are used to prove the Mordell-Weil Theorem.
[5]See for example Proposition 38 in [Ser02]

which we can specialise to all the completions K_v of K:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E(K)}{nE(K)} & \longrightarrow & H^1(G_K, E[n]) & \longrightarrow & H^1(G_K, E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle j_v} & \searrow^{\gamma} & \downarrow & & \\ 0 & \longrightarrow & \prod_v \frac{E(K_v)}{nE(K_v)} & \xrightarrow{\prod_v \mu_v} & \prod_v H^1(G_{K_v}, E[n]) & \longrightarrow & \prod_v H^1(G_{K_v}, E)[n] & \longrightarrow & 0. \end{array}$$

Definition 5 *The n-Selmer Group $S_n(E/K) \subset H^1(G_K, E[n])$ is given by* $\ker(\gamma)$ *in the above diagram, i.e. the elements $X \in H^1(G_K, E[n])$ such that $j_v(X) \in \mathrm{im}(\mu_v)$ for all places v.*

This is a finite set (see for example page 4 of [Sto]). We can also define in passing the mysterious Tate-Shafarevich Group.

$$Ш(E/K) = \ker\left\{H^1(G_K, E) \to \prod_v H^1(G_{K_v}, E)\right\}$$

and in particular,

$$Ш(E/K)[n] = \frac{S_n(E/K)}{(E(K)/nE(K))}.$$

The goal of n-descent is to understand the elements of $S_n(E/K)$ explicitly, since this will give us an upper bound for the size of $E(K)/nE(K)$. Note that the bound will be slack whenever $Ш[n] \neq \emptyset$. This in turn gives us the rank of E, although we would need to take into account the torsion subgroup first.

As we shall see in the next section, n-descent is performed by looking for objects that can be viewed as twists of the multiplication by n map on E. We also see that $S_2(E/K)$ consists of curves $C_2 : y^2 = g(x, z)$ for integral binary quartic forms g and that $S_4(E/K)$ consists of pairs of quaternary quadratic forms[6]

$$C_4 : Q_1(x_1, x_2, x_3, x_4) = Q_2(x_1, x_2, x_3, x_4) = 0.$$

It is also the case that $S_3(E/K)$ consists of elements $C_3 : h(x, y, z) = 0$ for h a ternary cubic form and that for $n \geq 5$, elements of $S_n(E/K)$ can be realised as a set of $\frac{1}{2}n(n-3)$ quadrics in $\mathbb{P}^{n-1}$, but we will be focusing on $n = 2$ and 4. A good reference for the theory of binary quartics is [Cre01], although there are now many treatments of the subject. For ternary cubics, there is a good overview

[6] Geometrically the intersection of two quadrics in $\mathbb{P}^3$.

in [AKM$^+$01] and a more detailed approach in [Fis06]. For 4-descent and quadric intersections, most people use [MSS96] as a first reference, but [Wom03] gives a very readable account and [Sta05] gives a detailed description on his way to an investigation of 8-coverings.

1.3.1 n-Coverings

Before understanding the output of n-descent, let us recall the following arithmetical objects.

Definition 6 *A principal homogeneous space for an elliptic curve E/K is a smooth curve C/K together with a simply transitive group action of E on C. i.e. a pair (C, μ) where $\mu\colon C \times E \to C$ is a morphism satisfying*

1. *$\mu(p, O) = p$ for all $p \in C$,*
2. *$\mu(\mu(p, P), Q) = \mu(p, P + Q)$ for all $P, Q \in E$,*
3. *for all $p, q \in C$, there exists a unique $P \in E$ such that $\mu(p, P) = q$.*

Then we have the following notion of equivalence of two principal homogeneous spaces.

Definition 7 *Two homogeneous spaces (C, μ) and (C', μ') are isomorphic if there exists an isomorphism $\phi\colon C \to C'$ which is compatible with the action of E.*

Choose $p_0 \in C$ and then define $\nu\colon C \to E$ such that $\nu(p) = P$ (the unique point on E with $\mu(p_0, P) = p$). This is an isomorphism over $\overline{K}$. Now let us introduce the idea of an n-covering which will form the focus of our study in later chapters.

Definition 8 *A pair (C, π) consisting of a curve C and a morphism π is an n-covering of E for some n if there exists an isomorphism ν defined over $\overline{K}$ such that the following diagram commutes:*

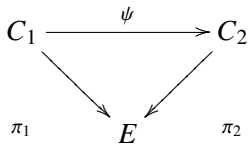
$$\begin{array}{ccc} C & & \\ {\scriptstyle \nu}\downarrow & \searrow^{\pi} & \\ E & \xrightarrow[[n]]{} & E \end{array}$$

We say that an n-covering is defined over K if the curve C and the morphism μ are both defined over K. So, (E, ϕ) for

$$\begin{aligned} \phi \colon E &\longrightarrow E \\ X &\longmapsto nX + P \end{aligned}$$

and some $P \in E(K)$ is an example of an n-covering of E defined over K. We can also define what it means for two n-coverings to be isomorphic.

Definition 9 *Two n-coverings (C_1, π_1) and (C_2, π_2) are isomorphic if there exists an isomorphism of curves ψ such that the following diagram commutes.*



Then, in order to try and understand the Selmer group (as defined in the previous section), we have the following result which appears as Proposition 1.3 in [Sto]. We refer to the twists of X as the objects Y defined over K such that X and Y are isomorphic over $\overline{K}$.

Lemma 10 *Let X be some sort of algebraic or geometric object defined over K. Then the set of twists of X, up to K-isomorphism, are parametrised by $H^1(G_K, \mathrm{Aut}_{\overline{K}}(X))$*

If we let X be the trivial n-covering defined by the pair $(E, [n])$, then the twists of X are precisely the n-coverings of E. An automorphism of X is 'translation by an n-torsion point on E', hence by applying the above lemma, we see that the n-coverings up to K-isomorphism are parametrised by $H^1(G_K, E[n])$. So, all elements of $S_n(E/K)$, together with the n-descent map (which takes a point on C_n to a point on E) are n-coverings. It is also true[7] that principal homogeneous spaces are parametrised by the group $H^1(G_K, E)$ and the map $H^1(G_K, E[n]) \to H^1(G_K, E)[n]$ takes the n-covering (C, π) to the principal homogeneous space (C, μ) for some morphism μ and this allows us to realise $S_n(E/K)$ as the set of 'everywhere locally soluble' n-coverings of E.

Definition 11 *An alternative definition of $S_n(E/K)$ is the set of n-coverings (C, π) (up to K-isomorphism) such that $C(K_v) \neq \emptyset$ for all places v.*

[7] See [Cas67] for these facts, in particular Theorem 10.1 and Lemma 19.3.

Now let us see how the heights of points on C compare to those on E. To embed the curve C in $\mathbb{P}^3$, we need a K-rational divisor.

Lemma 12 *Let $(C, \pi) \in S_n(E/K)$ be such that ν (in the diagram for an n-covering) gives an isomorphism $C \to E$ over $\overline{K}$ and let O be the 'point at infinity' on E, then there exists a divisor $D_1 \sim \nu^*([n.O])$ defined over K.*

Proof: This argument can be seen in section 2 of [CM00], but was proved earlier by Cassels in chapter 7 of [Cas62]. The divisor $\nu^*([n.O])$ on C is of degree n and is defined over $\overline{K}$, so we have a linear equivalence class $\mathcal{D}$ of divisors of degree n on C which is K-rational [8]. Now consider the variety V/K of effective divisors on C which are in $\mathcal{D}$. Over $\overline{K}$, this is a projective space, therefore V is a twist of projective space over K. Since C is everywhere locally soluble, it follows that V has a K_v-rational point for all completions K_v and therefore, by the Hasse Principle for Brauer-Severi varieties, that V has a K-rational point, i.e. there is a K-rational divisor $D_1 \sim \nu^*([n.O])$ on C.

□

Let ψ be a morphism defined by the complete linear system $|D_1|$. We then have the following diagram for x denoting the map which takes the x co-ordinate of a point on E and $\phi = x \circ \pi$:

$$\begin{array}{ccc} & \overset{\psi}{} & \\ C & \longrightarrow & \mathbb{P}^{n-1} \\ {\scriptstyle\pi}\downarrow & \searrow^{\phi} & \\ E & \longrightarrow & \mathbb{P}^1 \\ & {\scriptstyle x} & \end{array}$$

The next lemma can be found in an altered form on page 11 of [Sto] and in some sense it motivates our study of n-coverings.

Lemma 13 $h_x \circ \pi = 2nh_\psi + O(1)$.

Proof : Let $H \subset \mathbb{P}^{n-1}$ and $H' \subset \mathbb{P}^1$ be hyperplane sections. Then we have $D_1 = \psi^*(H)$ a divisor of degree n on C as defined above and let $D_2 = \phi^*(H')$ a divisor of

[8] To see this, take $\sigma \in G_K$, then $\sigma(\nu)^*$ differs from ν^* by the pullback of an n-torsion point, but this would still give us a linearly equivalent divisor, so $\mathcal{D}$ is K-rational.

degree $2n^2$ on C. Then, for p a point on C, from the general theory of heights on divisor classes we have:

$$h_{[D_1]}(p) = h_\psi(p) + O(1),$$
$$h_{[D_2]}(p) = h_\phi(p) + O(1),$$

for all $p \in C(K)$. Now if we have $D_2 \sim 2nD_1$, then we are done, since then

$$\begin{aligned} h_x(\pi(p)) = h_\phi(p) &= h_{[D_2]}(p) + O(1) \\ &= 2nh_{[D_1]}(p) + O(1) \\ &= 2nh_\psi(p) + O(1). \end{aligned}$$

This uses two results from the theory of heights, which can be found as Theorems B.2.5(b) and B.3.1. in [HS00]. Now two divisors on E are linearly equivalent if and only if they have the same degree and the same sum. Here the degrees are clearly the same, so it is enough to show equivalence of the sum. We are free to replace C by any n-covering which is isomorphic over $\overline{K}$, so let us choose $C = E$ and ν the identity. Then $[D_1]$ is just $[n.O]$ and we have

$$\begin{array}{ccc} E & \xrightarrow{[n.O]} & \mathbb{P}^{n-1} \\ {\scriptstyle [n]}\downarrow & & \\ E & \xrightarrow{[2.O]} & \mathbb{P}^1. \end{array}$$

So $D_2 = 2[n]^*.O = 2\sum_{T\in E[n]}(T)$ and so it is enough to prove $\sum_{T\in E[n]}(T) \sim n^2.O$, but it is a standard fact from group theory that elements of a group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ sum to the identity[9], so we are done.

□

This makes our question of finding the difference between the heights of points on C and E look approachable, since we now know that constants do exist to bound this difference. Our goal will now be to gain some machinery and intuition at the smallest case $n = 2$ to calculate the bound there and then be able to say something about larger n, but first we have a discussion on resultants.

[9]The elements with inverses sum to zero and if n is even, there are three non trivial 2-torsion elements which also sum to zero

1.4 An Overview of Resultants

Resultants can be a powerful tool in the computation of heights and they have been studied extensively since the 19th century. [GKZ08] is a detailed treatment of some of the algebra required for resultants and [CLO05] has a slightly more applicable slant. We will not give a full treatment here, but it is important to establish some facts that will be used later.

For $f, g \in K[x]$ and

$$f = a_0 x^n + ... + a_n,$$
$$g = b_0 x^m + ... + b_m,$$

then the resultant of f and g is given by

$$\mathrm{Res}(f,g) = \det \begin{pmatrix} a_0 & & & b_0 & & & \\ . & . & & . & . & & \\ . & & a_0 & . & & . & \\ . & & . & . & & & b_0 \\ . & & . & b_m & & & . \\ a_n & & . & & . & & . \\ & . & . & & & . & . \\ & & a_n & & & & b_m \end{pmatrix},$$

where the matrix above has m columns with the coefficients of f and n columns with the coefficients of g. It is an integer polynomial in the coefficients of f and g.

Lemma 14 *For $f, g \in K[x]$ as above with roots in $\overline{K}$ given by $(\eta_j)_{j=1}^n$ and $(\zeta_i)_{i=1}^m$ respectively, then* $\mathrm{Res}(f,g)$ *is given by*

$$a_0^m b_0^n \prod_{i=1}^{m} \prod_{j=1}^{n} (\zeta_i - \eta_j).$$

Proof : This is given as Exercise 10 on p83 of [CLO05].

□

This shows us the following important fact; $\mathrm{Res}(f,g) = 0$ if and only if f and g have a common root. Also, there exist polynomials $\alpha, \beta \in K[x]$, whose coefficients

are integer polynomials in the coefficients of f and g such that

$$\alpha f + \beta g = Res(f, g). \tag{2}$$

This is shown in Proposition 9 on p152 of [CLO97] and we will use this fact in sections 1.5 and 2.3.

1.4.1 Multi-Dimensional Resultants and Computation

The situation becomes a bit more complicated with more than one variable. Suppose we have the following system of equations:

$$F_1(x_1, ..., x_{n+1}) = ... = F_{n+1}(x_1, ..., x_{n+1}) = 0, \tag{3}$$

for $F_i = \sum_{|\alpha|=d_i} c_{i,\alpha} x^\alpha \in K[x_1, ..., x_{n+1}]$. For simplicity, we will assume that the degrees d_i are all equal: $d_1 = ... = d_{n+1} = d$, but we could proceed with more generality if required. We have the following theorem to introduce the resultant.

Theorem 15 *Fix $d > 0$, then there exists a unique polynomial* Res *(integral in the coefficients of the F_i) with the following properties:*

- *If $F_1, ..., F_{n+1} \in K[x_1, ..., x_{n+1}]$ are homogeneous of degree d, then equation (3) has a solution in $\overline{K}[x_1, ..., x_{n+1}]$ if and only if* $\text{Res}(F_1, ..., F_{n+1}) = 0$.
- $\text{Res}(x_1^d, ..., x_{n+1}^d) = 1$.
- Res *is irreducible, even over $\overline{K}$.*

Proof : See section 13.1A of [GKZ08].

□

The following lemma will eventually help us achieve a height bound using resultants.

Lemma 16 *For F_j as above, there exist non-trivial polynomials $g_{ij} \in K[x_1, ..., x_{n+1}]$ for $i \in \{1, ..., n+1\}$, such that*

$$\sum_{j=1}^{n+1} g_{ij} F_j = c_i x_i^k,$$

for some integers c_i and k.

Proof : Let us consider F_{n+1} and F_j as polynomials in x_{n+1} only, with coefficients in $K[x_1, ..., x_{j-1}, x_{j+1}, ..., x_n]$. Then using the resultant from the last subsection, we can get n equations of the form

$$\text{Res}(F_j, F_{n+1})x_j^k = f_j(x_j, x_{n+1})F_{n+1} + g_j(x_j, x_{n+1})F_j,$$

for some polynomials f_j and g_j. The left hand sides of all these equations do not involve x_{n+1}, so they provide us with the same setting only one dimension lower, i.e. we have equations

$$G_1(x_1, ...x_n) = ... = G_n(x_1, ...x_n) = 0.$$

So now

$$\begin{aligned}\text{Res}(G_j, G_n)x_j^l &= f_j'(x_j, x_n)G_n + g_j'(x_j, x_n)G_j \\ &= f_j''(x_j, x_n, x_{n+1})F_{n+1} + g_j''(x_j, x_n, x_{n+1})F_n + h_j''(x_j, x_n, x_{n+1})F_j.\end{aligned}$$

And we get $n-1$ equations like this, which eliminate x_n. Therefore by induction we get to one equation.

$$\sum_{j=1}^{n+1} g_{1j}F_j = c_1 x_1^k,$$

for some integer k and constant c_1. We could carry out the same procedure for the other co-ordinates, hence the lemma is proved.

□

These constants c_i almost have the desired properties of the resultant given in the above theorem and in practice it appears that the resultant divides c_i for all i. However, we will only be interested in finding constants such that we can write $d_i x_i^k$ as a combination of the F_j and the resultant provides these, so we will use the observed fact that there exist polynomials g_{ij}' in the coefficients of the F_j such that

$$\sum_{j=1}^{n+1} g_{ij}'F_j = \text{Res}(F_1, ..., F_{n+1})x_i^k,$$

for all i.

Let us now outline an algorithm to compute Res. This method can be found on

page 103 of [CLO05] and we will take $d = 2$ and $n = 3$, since this will be useful in later sections.

Let us define e to be the sum of the degrees of the polynomials F_i minus n, i.e. in our case $e = 5$. Note that all monomials of degree e are divisible by x_i^d for some i. We then divide the monomials $x^\alpha = x_1^{\alpha_1}...x_{n+1}^{\alpha_{n+1}}$ of total degree e into $n+1$ sets as follows:

$$\begin{aligned} S_1 =& \{x^\alpha : x_1^d \mid x^\alpha\}, \\ S_2 =& \{x^\alpha : x_1^d \nmid x^\alpha, \text{ but } x_2^d \mid x^\alpha\}, \\ & ..., \\ S_{n+1} =& \{x^\alpha : x_1^d, ...x_n^d \nmid x^\alpha, \text{ but } x_{n+1}^d \mid x^\alpha\}. \end{aligned}$$

In our case, we have

$$\begin{aligned} S_1 =& \{x_1^5, x_1^4x_2, x_1^4x_3, x_1^4x_4, x_1^3x_2^2, x_1^3x_2x_3, x_1^3x_2x_4, x_1^3x_3^2, x_1^3x_3x_4, x_1^3x_4^2, x_1^2x_2^3, x_1^2x_2^2x_3, \\ & x_1^2x_2^2x_4, x_1^2x_2x_3^2, x_1^2x_2x_3x_4, x_1^2x_2x_4^2, x_1^2x_3^3, x_1^2x_3^2x_4, x_1^2x_3x_4^2, x_1^2x_4^3\}, \\ S_2 =& \{x_1x_2^4, x_1x_2^3x_3, x_1x_2^3x_4, x_1x_2^2x_3^2, x_1x_2^2x_3x_4, x_1x_2^2x_4^2, x_2^5, x_2^4x_3, x_2^4x_4, x_2^3x_3^2, x_2^3x_3x_4, \\ & x_2^3x_4^2, x_2^2x_3^3, x_2^2x_3^2x_4, x_2^2x_3x_4^2, x_2^2x_4^3\}, \\ S_3 =& \{x_1x_2x_3^3, x_1x_2x_3^2x_4, x_1x_3^4, x_1x_3^3x_4, x_1x_3^2x_4^2, x_2x_3^4, x_2x_3^3x_4, x_2x_3^2x_4^2, x_3^5, x_3^4x_4, x_3^3x_4^2, \\ & x_3^2x_4^3\}, \\ S_4 =& \{x_1x_2x_3x_4^2, x_1x_2x_4^3, x_1x_3x_4^3, x_2x_3x_4^3, x_1x_4^4, x_2x_4^4, x_3x_4^4, x_4^5\}. \end{aligned}$$

Now, if we let $N = |S_1 \cup ... \cup S_{n+1}| = \begin{pmatrix} d+n \\ n \end{pmatrix}$, then we can write the following system of N equations in N variables:

$$(x^\alpha / x_i^d)F_i = 0,$$

for all $x^\alpha \in S_i$. So, if we let D be the determinant of the $N \times N$ coefficient matrix formed from these equations, then we have $\text{Res}(F_1, ...F_{n+1}) \mid D$, but clearly we have created some redundancy here by expanding the number of equations we are dealing with. In fact (see Theorem 4.9 on page 108 of [CLO05]) we have

$$\text{Res}(F_1, ...F_{n+1}) = \pm D/D',$$

for D' the determinant of the sub-matrix formed by deleting all the rows and columns corresponding to monomials where $x_i^d \mid x^\alpha$ for exactly one i. This means we can explicitly calculate the resultant for our example by considering the following sets:

$$\begin{aligned}
S'_1 =&\{x_1^3x_2^2, x_1^3x_3^2, x_1^3x_4^2, x_1^2x_2^3, x_1^2x_2^2x_3, x_1^2x_2^2x_4, x_1^2x_2x_3^2, x_1^2x_2x_4^2, x_1^2x_3^3, x_1^2x_3^2x_4, x_1^2x_3x_4^2,\\
&x_1^2x_4^3\},\\
S'_2 =&\{x_1x_2^2x_3^2, x_1x_2^2x_4^2, x_2^3x_3^2, x_2^3x_4^2, x_2^2x_3^3, x_2^2x_3^2x_4, x_2^2x_3x_4^2, x_2^2x_4^3\},\\
S'_3 =&\{x_1x_3^2x_4^2, x_2x_3^2x_4^2, x_3^3x_4^2, x_3^2x_4^3\},\\
S'_4 =&\emptyset.
\end{aligned}$$

These then allow us to calculate D and D'.

1.5 Bounding Height Differences

In this section we will see how people have approached the problem of bounding $|\hat{h} - h|$ on E. The simplest approach uses the ideas of the previous section. We use the duplication formula for a point $P = (x\colon y\colon z)$ (scaled so that x and z are coprime) on $E\colon y^2z = 4x^3 + b_2x^2z + 2b_4xz^2 + b_6z^3$. For convenience we will write this as the affine co-ordinate $x(2P)$, so

$$x(2P) = \frac{x^4 - b_4x^2z^2 - 2b_6xz^3 - b_8z^4}{4x^3z + b_2x^2z^2 + 2b_4xz^3 + b_6z^4} = \frac{f_1(x,z)}{f_2(x,z)},$$

where $b_8 = (b_2b_6 - b_4^2)/4$ and f_1 and f_2 are coprime polynomials. Then we know from section 1.4 that there exist polynomials p_1, p_2, p_3 and p_4 of degree α such that

$$\begin{aligned}
p_1(x,z)f_1(x,z) + p_2(x,z)f_2(x,z) &= kz^{4+\alpha},\\
p_3(x,z)f_1(x,z) + p_4(x,z)f_2(x,z) &= kx^{4+\alpha},
\end{aligned}$$

for k the resultant of f_1 and f_2. We can ensure $\alpha \leq 3$. Now if f_1 and f_2 were to have a common factor, then this factor would divide $\gcd(kx^4, kz^4) = k$, so

$$kH(2P) \geq \max(|f_1(x,z)|, |f_2(x,z)|).$$

If we then assume $z > x$, we have $H(P) = z$ and

$$kH(2P) \geq \max(|f_1(x,z)|, |f_2(x,z)|) \geq \frac{kH(P)^4 z^\alpha}{|p_1(x,z) \pm p_2(x,z)|}$$

and so

$$H(2P) \geq c_1 H(P)^4,$$

for some constant c_1 depending on the coefficients of p_1 and p_2. We also have the following upper bound.

$$H(2P) \leq \max((1 + |b_4| + 2|b_6| + |b_8|), (4 + |b_2| + 2|b_4| + |b_6|))H(P)^4 = c_2 H(P)^4.$$

Obtaining a third constant from these, $c_3 = \max(\log(c_1), \log(c_2))/4$, we have

$$\left|\frac{1}{4}h(2P) - h(P)\right| < c_3 \text{ and } |\hat{h}(P) - h(P)| < 4c_3/3,$$

by iteration of the triangle law. This method could be found in many introductions to elliptic curves[10] and is really just showing that a bound exists. It is clear that more work can be done and a more serious attempt at a bound was made by Zimmer (see [Zim76] and [SZ03]), which we will summarise in the next subsection.

1.5.1 Zimmer's Bound

First let us make some definitions before we can state Zimmer's theorem. For K a number field, fix the completion K_ν of K at the place ν, let $\nu(x) = -\log(|x|_\nu)$ and let $n_\nu = [K_\nu \colon \mathbb{Q}_\nu]$. Define:

$$\begin{aligned}
d(P) &= -\frac{1}{2[K\colon \mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \max\left(\nu(x), \nu(b_2), \frac{\nu(b_4)}{2}, \frac{\nu(b_6)}{3}, \frac{\nu(b_8)}{4}\right), \\
\lambda &= \frac{1}{[K\colon \mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \max\left(\nu(b_2), \frac{\nu(b_4)}{2}, \frac{\nu(b_6)}{3}, \frac{\nu(b_8)}{4}\right), \\
\mu_l &= \frac{1}{[K\colon \mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \min\left(0, \nu(b_2), \frac{\nu(b_4)}{2}, \frac{\nu(b_6)}{3}, \frac{\nu(b_8)}{4}\right), \\
\mu_h &= \frac{1}{[K\colon \mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \max\left(0, \min\left(\nu(b_2), \frac{\nu(b_4)}{2}, \frac{\nu(b_6)}{3}, \frac{\nu(b_8)}{4}\right)\right),
\end{aligned}$$

for $P = (x, y) \in E(K)$. Then he proves two theorems.

[10] For example Theorem 5.6 in [Sil09]

Theorem 17 *(5.18 (a) in [SZ03]) For all $P \in E(K)$,*

$$\frac{1}{2}\mu_l \leq \frac{1}{2}h(P) - d(P) \leq \frac{1}{2}\mu_h.$$

Theorem 18 *(5.35 (c) in [SZ03])*

$$-(\lambda + \frac{4}{3}\log 2) \leq \frac{1}{2}\hat{h}(P) - d(P) \leq \frac{1}{2}\log 2.$$

This leads to the result, which is nicely stated in [Uch06]:

$$-2\mu_l + \mu_h - \frac{8}{3}\log 2 \leq \hat{h}(P) - h(P) \leq \mu_l + \log 2.$$

1.5.2 Silverman's Bound

Silverman, in his paper [Sil90], then goes on to make improvements to the bounds above. He defines as usual:

$$h(x) = \frac{1}{[K\colon \mathbb{Q}]} \sum_{v \in M_K} n_v \log(\max(1, |x|_v)),$$
$$h_\infty = \frac{1}{[K\colon \mathbb{Q}]} \sum_{v \in M_K^\infty} n_v \log(\max(1, |x|_v)).$$

He also defines 2^* to be 2 if $b_2 \neq 0$ and 1 if $b_2 = 0$ and

$$\mu(E) = \frac{1}{12}h(\Delta) + \frac{1}{12}h_\infty(j) + \frac{1}{2}h_\infty\left(\frac{b_2}{12}\right) + \frac{1}{2}2^*.$$

He then proves the following theorem.

Theorem 19 *For all $P \in E(\overline{K})$, we have*

$$-\frac{1}{24}h(j) - \mu(E) - 0.973... \leq \hat{h}(P) - h(P) \leq \mu(E) + 1.07...$$

As a corollary, if E is written in shorter Weierstrass form $y^2 = x^3 + ax + b$, by replacing $h_\infty(j)$ with the larger quantity $h(j)$, we can get the following simpler bound.

$$-\frac{1}{8}h(j) - \frac{1}{12}h(\Delta) - 0.973... \leq \hat{h}(P) - h(P) \leq \frac{1}{12}h(j) + \frac{1}{12}h(\Delta) + 1.07...$$

As an example, Silverman goes further to say that if we work over $\mathbb{Q}$, if E is in shorter Weierstrass form and if we are in the following special case: $a, b \in \mathbb{Z}$,

$4a^3 + 27b^2$ square-free, $\gcd(a, 3b) = \gcd(2, b) = 1$ and $a > 0$, then in particular the theorem implies

$$h(P) \leq \hat{h}(P) + 2.137...$$

Even without these specialisations, this bound is much better since the constants are vastly improved. There are examples in the paper to demonstrate that his method is better than that of Zimmer.

1.5.3 Siksek's Bound

Siksek (in [Sik95]) goes about bounding $|h(P) - \hat{h}(P)|$ by estimating $h(2P) - 4h(P)$ at each place. Let ν be a valuation on K (with π a prime element for ν) and let $f(X) = 4X^3 + b_2X^2 + 2b_4X + b_6$ and $g(X) = X^4 - b_4X^2 - 2b_6X - b_8$. He defines

$$\begin{aligned} D_\nu &= \{X \in K_\nu \colon |X|_p \leq 1, f(X) \in K_\nu^2\}, \\ d_\nu &= \inf_{X \in D_\nu} \max(|f(X)|_\nu, |g(X)|_\nu), \\ \varepsilon_\nu &= \inf_{(X,Y) \in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1, |x|_\nu)^4}. \end{aligned}$$

Also, letting $f'(X) = X^4 f(1/X)$ and $g'(X) = X^4 g(1/X)$ be the 'reversals' of f and g, he defines D'_ν and d'_ν in the natural way[11]. Then he proves the following theorem

Theorem 20 *The following are properties of ε_ν:*

- *ε_ν exists and $\varepsilon_\nu = \min(d_\nu, d'_\nu)$.*
- *$\varepsilon_\nu < 1$.*
- *If ν is non-archimedean, E is minimal at ν and the Tamagawa number $c_\nu = 1$, then $\varepsilon_\nu = 1$.*
- *If ν is non-archimedean, then $\varepsilon_\nu = d'_\nu$.*
- *If ν is non-archimedean and $n = [\frac{\nu(4\Delta)}{2}]$, then $\varepsilon_\nu \geq |\pi|_\nu^{2n}$.*

[11] Note that we have used the reciprocal of Siksek's quantity ε_ν here, but this will reduce confusion when certain notation is introduced in Section 2.3.

After proving this, he defines μ_v as follows (for $E^0(K_v) = \{P \in E(K_v) : \overline{P} \text{ is non-singular}\}$).

$$\begin{aligned}
\mu_v = 1/3 &\quad \text{for archimedean } v,\\
1/3 &\quad v \text{ non-arch, } E \text{ not minimal},\\
0 &\quad v \text{ non-arch, } E \text{ minimal, } c_v = 1,\\
1/4 &\quad v \text{ non-arch, } E \text{ minimal, } E(K_v)/E^0(K_v) \cong \mathbb{Z}/2\mathbb{Z} \text{ or } (\mathbb{Z}/2\mathbb{Z})^2,\\
(1 - 1/4^\alpha)/3 &\quad v \text{ non-arch, } E \text{ minimal, } E(K_v)/E^0(K_v) \cong \mathbb{Z}/2^\alpha\mathbb{Z} \text{ for some } \alpha > 1,\\
1/3 &\quad v \text{ non-arch, } E \text{ minimal, } c_v \neq 2^k \text{ for some k.}
\end{aligned}$$

Then he proves the following theorem.

Theorem 21 *For all $P \in E(K)$,*

$$h(P) - \hat{h}(P) \leq -\frac{1}{[K : \mathbb{Q}]}\left(\sum_{v \in M_K} \mu_v n_v \log(\varepsilon_v)\right).$$

This work of Siksek is then improved (especially at the complex achimedean places) in his joint paper with Prickett and Cremona, [CPS06].

Due to previous work in the theory of binary quartics (see for example [Cre01] and section 2.2), the existence of a new method becomes apparent using similar ideas to those of Siksek. As we shall see, by fixing a Weierstrass equation for E and an n-covering (C_n, π), we can bound the expression $|\frac{1}{2n}h(\pi(P)) - h(P)|$ by a constant B_3, say. This factor of $2n$ will improve on the previous methods greatly.

For example, suppose the bound on the right hand side in Theorem 21 is given by B_1 and suppose we want to prove there are no points P on E with $\hat{h}(P) < 1000$, then using current methods we would have to search for points on E of naive height up to $1000 + B_1$. Each generator of E comes from some covering curve, so if we were to calculate all the 2-coverings say, and compute the bound B_3 (above), then we would only need to search on each one up to naive height $250 + B_1/4 + B_3$. The fact these are logarithmic heights means that even if we have to search on several different curves, the time required would be much smaller.

In the above example, this method only really becomes more efficient when the bound B_3 is small compared to 1000, but we have methods for writing (for

example) binary quartics 'nicely,' i.e. in minimised and reduced form and this will ensure B_3 remains fairly small. See [SC02] and [SC03] for how minimisation and reduction work for binary quartic forms. We will define exactly what we mean by these terms in sections 2.2 and 3.2.

The above methods concentrate on improving the lower bound for the canonical height, which is often more useful since it gives us an upper bound for how far we would need to search for points. It is worth noting that work is being done on the upper bound too; see for example [Tho08], which investigates this bound over totally real number fields, not just over $\mathbb{Q}$.

2 Binary Quartic Forms

It seems sensible to start our investigation with $n = 2$, since this will give us the easiest equations to handle, so let us introduce the setup for 2-coverings in detail.

2.1 Two Descent

By conducting 2-descent, we aim to compute all the 'everywhere locally soluble' 2-coverings of E. We will work over $\mathbb{Q}$ here, letting $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and referring to $S_2(E/\mathbb{Q})$ as $S_2(E)$.

Definition 22 *The $\mathbb{Q}$-algebra associated to E is given by*

$$\mathbb{Q}[\theta] = \frac{\mathbb{Q}(T)}{(f(T))},$$

for $E\colon y^2 = f(x)$.

This can be expanded as the direct sum of at most three fields (one for each irreducible factor of f). Note here that the field norm $N_{\frac{\mathbb{Q}[\theta]}{\mathbb{Q}}}((x-\theta)) = f(x)$. Now we define the following map[12]

Definition 23

$$\begin{aligned} \mu\colon E(\mathbb{Q}) &\longrightarrow \frac{\mathbb{Q}[\theta]^*}{(\mathbb{Q}[\theta]^*)^2}, \\ O &\longmapsto 1, \\ (x,y), \quad y \neq 0 &\longmapsto (x-\theta)\ mod\ (\mathbb{Q}[\theta]^*)^2, \\ (x,0) &\longmapsto (x-\theta)^{\sim}\ mod\ (\mathbb{Q}[\theta]^*)^2. \end{aligned}$$

In the last part of the definition, $f(x) = 0$, so one component of the sum of fields becomes just $\mathbb{Q}$. Therefore $\sim$ refers to the fact that we replace this component in the image with $b \in \mathbb{Q}^*$, chosen such that $N_{\frac{\mathbb{Q}[\theta]}{\mathbb{Q}}}(\mu(x,0)) \in \mathbb{Q}^{*^2}$, rather than being 0.

Some calculation can now show that this is a homomorphism, with kernel $2E(\mathbb{Q})$ (see lecture 15 in [Cas91] for details). In fact, we can view $H^1(G, E[2])$ as a subgroup of $\mathbb{Q}[\theta]^*/(\mathbb{Q}[\theta]^*)^2$ and μ gives us the connecting map in the diagram from section 1.3 (which we will still refer to as μ). We specialise the diagram to

[12] Sometimes referred to as 'Cassels' map'.

$K = \mathbb{Q}$ and the places $p \leq \infty$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} & \xrightarrow{\mu} & H^1(G, E[2]) & \longrightarrow & H^1(G, E)[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle j_p} & & \downarrow & & \\ 0 & \longrightarrow & \prod_p \frac{E(\mathbb{Q}_p)}{2E(\mathbb{Q}_p)} & \xrightarrow{\prod_p \mu_p} & \prod_p H^1(G_p, E[2]) & \longrightarrow & \prod_p H^1(G_p, E)[2] & \longrightarrow & 0. \end{array}$$

We are interested in calculating the image of μ, in particular, recall the definition of the Selmer group.

Definition 24 *The 2-Selmer group of E over $\mathbb{Q}$ is given by*

$$S_2(E) = \{X \in H^1(G, E[2]) \text{ such that } j_p(X) \in im(\mu_p) \text{ for all } p \leq \infty\}.$$

To discover more about the structure of the Selmer group, suppose we have an element $\delta \in \mathrm{im}(\mu)$. This must come from a point on E, i.e. there exists $(x, y) \in E(\mathbb{Q})$ such that $x - \theta = \delta d^2$ with $d \in \mathbb{Q}[\theta]^*$, so it can be represented as a polynomial in θ with coefficients in $\mathbb{Q}$ and no term higher than θ^2 (since $f(\theta) = 0$ allows us to remove those). So we have

$$\begin{aligned} x - \theta &= \delta(u_0 + u_1\theta + u_2\theta^2)^2 \\ &= Q_0(u_0, u_1, u_2) + Q_1(u_0, u_1, u_2)\theta + Q_2(u_0, u_1, u_2)\theta^2, \end{aligned}$$

where the Q_i are quadratic forms over $\mathbb{Q}$ depending on δ. Now, equating coefficients of θ and θ^2, we get a solution to

$$Q_1(u_0, u_1, u_2) = -1, \qquad Q_2(u_0, u_1, u_2) = 0. \tag{4}$$

Since we necessarily have a solution everywhere locally, we must have that the conic $Q_2(u_0, u_1, u_2) = 0$ is soluble over $\mathbb{Q}_p$ for all p. It is a well known fact that the Hasse Principle holds for conics (see chapter 3 of [Cas91]), so therefore it must have a point over $\mathbb{Q}$. Now we can parametrise the conic giving $(u_1 : u_2 : u_3)$ as $(f_1(s,t) : f_2(s,t) : f_3(s,t))$ for three quadratic forms f_i. Putting these in the left hand equation in (4) and homogenising gives an equation of the form

$$\alpha^2 = g(s, t),$$

for some $\alpha \in \mathbb{Q}^*$ and binary quartic g. Indeed one way of visualising elements of $S_2(E)$ is as 'everywhere locally soluble' binary quartics

$$C_2 \colon y^2 = g(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4. \tag{5}$$

These (up to $\mathbb{Q}$-equivalence), together with the 2-covering map which will be discussed in the next section are the required 2-coverings predicted by the discussion in section 1.3.1.

2.2 Definitions and Invariant Theory

In this section, (C_2, π) will be a 2-covering obtained as an element of the 2-Selmer group from conducting 2-descent. As we have seen, C_2 can be represented by a binary quartic given in (5) above. This is a curve in projective space where the y co-ordinate is given a double weighting, i.e. the points $(x\colon y\colon z)$ and $(\lambda x\colon \lambda^2 y\colon \lambda z)$ are equivalent for all $\lambda \neq 0$. We will sometimes think of the projective curve $y^2 = g(x,z)$ as two affine pieces

$$y_1^2 = g(x,1), \qquad y_2^2 = g(1,z)$$

glued together. We will now discuss some of the basic properties of binary quartics.

If K is a field, $\mathrm{GL}_2(K)$ acts on the space of binary quartics via:

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \colon g(x,z) \quad \longmapsto g(\alpha x + \beta z, \gamma x + \delta z)$$

and we will write that the coefficients a, b, c, d and e map to a^*, b^*, c^*, d^* and e^* under this action. We will sometimes write $A(C_2)$ for $A(g)$.

We also have the action of K^* on binary quartics via simply multiplying $g(x,z)$ by some constant λ^2 and therefore a general action can be viewed as a pair $< \lambda, A >$ for $\lambda \in K^*$, $A \in \mathrm{GL}_2(K)$. We refer to two binary quartics as K-equivalent if they are related by such a pair (recall that $S_2(E)$ consists of binary quartics up to $\mathbb{Q}$-equivalence). Now let us define the notion of an invariant for g.

Definition 25 *An invariant of g of weight w and degree n is a homogeneous polynomial f of degree n such that*

$$f(a^*, b^*, c^*, d^*, e^*) = det(A)^w f(a, b, c, d, e)$$

for all $A \in \mathrm{GL}_2(\mathbb{Q})$.

It can be shown that any invariant of g is a combination of the following two:

$$I = 12ae - 3bd + c^2, \qquad J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3 \tag{6}$$

and the Jacobian elliptic curve can be written as[13]

$$E_{IJ} : y^2z = x^3 - 27Ixz^2 - 27Jz^3.$$

The discriminant of C_2 is then given by $\Delta(C_2) = \frac{1}{27}(J^2 - 4I^3)$.

Definition 26 *An integral binary quartic given in the equation for C_2 is minimal at p if $v_p(\Delta(C_2))$ is minimal among all integral binary quartics $\mathbb{Q}_p$-equivalent to it.*

The reduction process tries to get an n-covering as near as possible to being a Hesse form with small coefficients (over $\mathbb{R}$); i.e. one of the form $y^2 = a(x^4 + z^4) + bx^2z^2$ for $a, b \in \mathbb{C}$. For a full treatment, see section 9 of [CFS09], but it amounts to conducting reduction on a certain lattice.

For simplicity, we will always assume that our binary quartic is minimised and reduced. In particular, this means that p^2 cannot divide all the coefficients of a minimal binary quartic, since then

$$\Delta\left(< \frac{1}{p}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} > (C_2)\right)$$

has smaller valuation.

[13] Weil explained how we can write the Jacobian in this form in [Wei54] using formulae of Hermite, but later he realised that these formulae had been known to Euler and he explains this in [Wei83].

Theorem 27 *If C_2 is minimal and has Jacobian E, then $v_p(\Delta(C_2)) = v_p(\Delta(E))$ for all $p > 2$.*

Proof : This is a consequence of Proposition 4.2 in [SC02].

□

We will also use the notion of a covariant function.

Definition 28 *A covariant of g of weight w is a polynomial M such that*

$$M(a^*, b^*, c^*, d^*, e^*; x, z) = \det(A)^w M(a, b, c, d, e; \alpha x + \beta z, \gamma x + \delta z)$$

for all $A \in \mathrm{GL}_2(\mathbb{Q})$.

Note that g is trivially a covariant and we also have two other covariants of weights 2 and 3 respectively:

$$\begin{aligned}
g_4(x,z) = \; & (3b^2 - 8ac)x^4 + 4(bc - 6ad)x^3z + 2(2c^2 - 24ae - 3bd)x^2z^2 \\
& + 4(cd - 6be)xz^3 + (3d^2 - 8ce)z^4, \\
g_6(x,z) = \; & (b^3 + 8a^2d - 4abc)x^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)x^5z \\
& + 5(8abe + b^2d - 4acd)x^4z^2 + 20(b^2e - ad^2)x^3z^3 \\
& - 5(8ade + bd^2 - 4bce)x^2z^4 - 2(16ae^2 + 2bde - 4c^2e + cd^2)xz^5 \\
& - (d^3 + 8be^2 - 4cde)z^6.
\end{aligned}$$

Note that if g and g_4 have a common root then (by an SL_2 action) we may assume it is at $(0, 1)$, so $e = d = 0$. Therefore $I = c^2$, $J = -2c^3$ and $\Delta(C_2) = 0$ and this would mean C_2 is singular. Now one may check that the following relation (or syzygy) is satisfied:

$$27g_6^2 = g_4^3 - 48Ig^2g_4 - 64Jg^3.$$

After some manipulation, we see

$$(27g_6(x,z))^2 = (4g(x,z))^3 \left(\left(\frac{3g_4(x,z)}{4g(x,z)} \right)^3 - 27I \left(\frac{3g_4(x,z)}{4g(x,z)} \right) - 27J \right)$$

and replacing $g(x, z)$ by y^2, we get

$$\left(\frac{27g_6(x,z)}{(2y)^3} \right)^2 = \left(\frac{3g_4(x,z)}{(2y)^2} \right)^3 - 27I \left(\frac{3g_4(x,z)}{(2y)^2} \right) - 27J.$$

So the following is a morphism from C_2 to E_{IJ}:

$$\pi\colon (x : y : z) \longmapsto \left(6yg_4(x,z) : 27g_6(x,z) : (2y)^3\right),$$

which we will take as our covering map. Replacing y^2 by $g(x,z)$ and rescaling, we can write this as

$$\pi\colon (x : y : z) \longmapsto \left(3g_4(x,z) : \frac{27g_6(x,z)}{2y} : 4g(x,z)\right). \tag{7}$$

We will use this map when calculating heights and we will do this by summing local contributions, i.e. $H(\pi(P))$ will be given by

$$\prod_{p\in M_{\mathbb{Q}}} \max(|3g_4(x,z)|_p, |4g(x,z)|_p),$$

for $P = (x\colon y\colon z)$. Before discussing this further, there are some adjustments we must make at the awkward primes 2 and 3.

2.2.1 Characteristic 3

In characteristic 3, a problem arises because the formula for the Jacobian $\overline{E}_{IJ}$ is always singular, which means we must find a different covering map. Note that

$$\pi_3\colon \quad (x\colon y\colon z) \mapsto (9x + 3cz\colon\ -27y\colon z)$$

maps E_{IJ} to an elliptic curve which is in general non-singular at 3. Here c is (as usual) the third coefficient of g. Now $\pi_3^{-1}\pi$ is a map to E_3 defined in characteristic 3, for

$$E_3\colon y^2z = x^3 + cx^2z + (-4ae + bd)xz^2 + (-4ace + ad^2 + b^2e)z^3.$$

Therefore in projective co-ordinates (recall that we will only be interested in the x and z co-ordinates), we instead consider the covering map given by

$$(x,z) \mapsto (\widetilde{g}(x,z), 4g(x,z)) = \left(\frac{g_4(x,z) - 4cg(x,z)}{3}, 4g(x,z)\right). \tag{8}$$

2.2.2 Characteristic 2

A further problem occurs in characteristic 2, which is that C_2 may not be minimal[14]. In fact the general form for a 2-covering in characteristic 2 is

$$\begin{aligned} C_2 &: y^2 + P(x,z)y = Q(x,z), \\ & y^2 + (\alpha_0 x^2 + \alpha_1 xz + \alpha_2 z^2)y = a_2x^4 + b_2x^3z + c_2x^2z^2 + d_2xz^3 + e_2z^4. \end{aligned}$$

Now, if we are given a generalised binary quartic (i.e. one in the above form) that is minimal everywhere, this may mean it has cross terms. In fact we have a new action to consider on these quartics; that of a y-substitution.

$$y \mapsto y - (\beta_0 x^2 + \beta_1 xz + \beta_2 z^2),$$

for integers β_i. We will now write an action on a generalised binary quartic as

$$< \lambda, [\beta_0, \beta_1, \beta_2], M >,$$

for $\lambda \neq 0$ and $M \in \mathrm{SL}_2$ as before. Note that the first argument now acts by mapping $y^2 + P(x,z)y = Q(x,z)$ to

$$y^2 + \lambda P(x,z)y = \lambda^2 Q(x,z).$$

Minimal at 2 now means that the valuation of the discriminant is smallest amongst all *generalised* binary quartics $\mathbb{Q}_2$ equivalent to it. When C_2 is written as a generalised binary quartic, Theorem 27 holds for $p = 2$.

Completing the square on a generalised binary quartic, i.e. using the map

$$(x\colon y\colon z) \mapsto (x\colon y - \frac{1}{2}P(x,z)\colon z),$$

would give us a binary quartic in the sense of section 2.2 and we could calculate the covariants and invariants as usual. This gives us a natural expression for the covariant g_4 which makes sense in characteristic 2, that is

$$y^2 + (\alpha_0\alpha_1 x^2 + \alpha_1^2 xz + \alpha_1\alpha_2 z^2)y = A_2x^4 + B_2x^3z + C_2x^2z^2 + D_2xz^3 + E_2z^4,$$

[14] Fisher, in [Fis07], shows how to minimise binary quartics (and ternary cubics) at the primes 2 and 3.

where A_2, B_2, C_2, D_2 and E_2 have complicated expressions defined over $\mathbb{Z}$ given by

$$\begin{aligned}
A_2 =& 3b_2^2 + 3b_2\alpha_0\alpha_1 - 8a_2c_2 - 2\alpha_0^2c_2 - 2\alpha_1^2a_2 - 4\alpha_0\alpha_2a_2 - \alpha_0^3\alpha_2,\\
B_2 =& 4b_2c_2 + 2\alpha_0\alpha_1c_2 + \alpha_1^2b_2 + 2\alpha_0\alpha_2b_2 - 24a_2d_2\\
&- 12\alpha_1\alpha_2a_2 - 6\alpha_0^2d_2 - 2\alpha_0^2\alpha_1\alpha_2,\\
C_2 =& 4c_2^2 + 2\alpha_1^2c_2 + 4\alpha_0\alpha_2c_2 - 48a_2e_2 - 12\alpha_0^2e_2 - 12\alpha_2^2a_2\\
&- 6b_2d_2 - 3\alpha_0\alpha_1d_2 - 3\alpha_1\alpha_2b_2 - 2\alpha_0^2\alpha_2^2 - \alpha_0\alpha_1^2\alpha_2,\\
D_2 =& 4c_2d_2 + 2\alpha_1\alpha_2c_2 + \alpha_1^2d_2 + 2\alpha_0\alpha_2d_2 - 24b_2e_2\\
&- 12\alpha_0\alpha_1e_2 - 6\alpha_2^2b_2 - 2\alpha_0\alpha_1\alpha_2^2,\\
E_2 =& 3d_2^2 + 3d_2\alpha_1\alpha_2 - 8c_2e_2 - 2\alpha_2^2c_2 - 2\alpha_1^2e_2 - 4\alpha_0\alpha_2e_2 - \alpha_0\alpha_2^3.
\end{aligned}$$

We will call the binary quartics obtained by completing the square G and G_4 respectively. They are not defined over $\mathbb{Z}_2$, but will be useful in discovering a map that is. We will refer to the coefficients of G as a to e in the usual way, so for example $c = c_2 + \frac{1}{2}\alpha_0\alpha_2 + \frac{1}{4}\alpha_1^2$.

Considering $((G_4 - 4cG)/3, 4G)$ mentioned in the characteristic 3 case will still not work, since the first argument will often have terms in $\frac{1}{2}$ or $\frac{1}{4}$. However, if we add $\frac{1}{2}\alpha_0\alpha_2G(x,z)$ from the first argument (i.e. a multiple of the second argument) then we get a well defined map in $\mathbb{Z}_2$ to the following elliptic curve:

$$\begin{aligned}
E_2\colon\ & y^2z + \alpha_1xyz + (\alpha_0d_2 + \alpha_2b_2)yz^2 = x^3 + (-\alpha_0\alpha_2 + c_2)x^2z +\\
& (-\alpha_0^2e_2 - \alpha_0\alpha_2c_2 - \alpha_2^2a_2 - 4a_2e_2 + b_2d_2)xz^2 + (-\alpha_0^2c_2e_2 + \alpha_0\alpha_1b_2e_2 -\\
& \alpha_0\alpha_2b_2d_2 - \alpha_1^2a_2e_2 + \alpha_1\alpha_2a_2d_2 - \alpha_2^2a_2c_2 - 4a_2c_2e_2 + a_2d_2^2 + b_2^2e_2)z^3.
\end{aligned}$$

This means that in projective co-ordinates, we consider

$$\pi_2\colon (x,z) \mapsto (\widetilde{G}(x,z), 4G(x,z)), \tag{9}$$

for

$$\begin{aligned}
G(x,z) &= \frac{1}{4}P(x,z)^2 + Q(x,z),\\
\widetilde{G}(x,z) &= \frac{G_4(x,z) - G(x,z)(4c_2 - 4\alpha_0\alpha_2 + \alpha_1^2)}{3}.
\end{aligned}$$

It is worth writing out the expressions for $4G$ and $\widetilde{G}$ in full, since we will be referring back to them in the following section.

$$\begin{aligned}
4G(x,z) =&(4a_2+\alpha_0^2)x^4+(4b_2+2\alpha_0\alpha_1)x^3z+(4c_2+2\alpha_0\alpha_2+\alpha_1^2)x^2z^2+\\
&(4d_2+2\alpha_1\alpha_2)xz^3+(4e_2+\alpha_2^2)z^4,\\
\widetilde{G}(x,z) =&(b_2^2-4a_2c_2-\alpha_0^2c_2+\alpha_0\alpha_1b_2-\alpha_1^2a_2)x^4+\\
&(-8a_2d_2-2\alpha_0^2d_2-2\alpha_0\alpha_2b_2-4\alpha_1\alpha_2a_2)x^3z+\\
&(-16a_2e_2-2b_2d_2-4\alpha_0^2e_2-\alpha_0\alpha_1d_2+2\alpha_0\alpha_2c_2-\alpha_1\alpha_2b_2-4\alpha_2^2a_2)x^2z^2+\\
&(-8b_2e_2-2\alpha_2^2b_2-2\alpha_0\alpha_2d_2-4\alpha_0\alpha_1e_2)xz^3+\\
&(d_2^2-4c_2e_2-\alpha_2^2c+\alpha_1\alpha_2d_2-\alpha_1^2e_2)z^4.
\end{aligned}$$

2.3 Bounding Heights on 2-coverings

First note that we can obtain a bound for $|\frac{1}{4}h(\pi(P))-h(P)|$ using the methods of resultants by replacing f and g in section 1.4 with $4G$ and $\widetilde{G}$. In fact, if we let $|f|$ be the maximum size of the coefficients of the polynomial f, then Lemma 3.2 in [Sil88] gives

$$\max\left(\frac{|4G(x,z)|}{|4G|},\frac{|\widetilde{G}(x,z)|}{|\widetilde{G}|}\right)\geq\frac{|\mathrm{Res}(4G,\widetilde{G})|\max(|z^4|,|x^4|)}{2^{20}5^3|4G|^4|\widetilde{G}|^4}$$

and this allows us to form a bound. However, we will demonstrate a better method based on Siksek's bound and show that this gives smaller constants in section 2.8.

Let us define the quantity ε_p, the details of which will form the focus of the next few sections.

Definition 29 *Let $C_2\colon y^2+P(x,z)y=Q(x,z)$ be defined over $\mathbb{Q}_p$ and let G and $\widetilde{G}$ be as given in the previous section. Then define*

$$\varepsilon_p(C_2)=\inf_{(x:y:z)\in C_2(\mathbb{Q}_p)}\frac{\max(|4G(x,z)|_p,|\widetilde{G}(x,z)|_p)}{\max(|x|_p,|z|_p)^4}.$$

We have the freedom to scale a point $(x\colon y\colon z)$ in projective co-ordinates, but the numerator and denominator in the above expression are both homogeneous of degree 4, so ε_p is independent of this scaling. We will use this quantity in the following theorem, which will be proved at the end of the next section. This will be our main theorem for 2-coverings.

Theorem 30 *Let $C_2 : y^2 + P(x,z) = Q(x,z)$ be minimal for all primes p. Then for $P \in C_2$ and π the 2-covering map given in equation (9),*

$$h(P) \leq \frac{1}{4}h(\pi(P)) - \frac{1}{4}\sum_{p\in\mathcal{B}} \log(\varepsilon_p(C_2)).$$

Here $\mathcal{B} \subset M_{\mathbb{Q}}$ is the set consisting of all primes dividing the discriminant $\Delta(E)$ as well as ∞. Since C_2 has been minimised, the primes dividing $\Delta(C_2)$ are the same as those dividing $\Delta(E)$. We shall see that the ε_p are computable, making it possible to determine the bound.

2.4 Properties of ε_p

In this section we shall attempt to learn more about this quantity ε_p. Some of the ideas and proofs are similar to those in [Sik95], although there it was applied to the multiplication-by-2 map on the elliptic curve, rather than the 2-covering map. The following lemma will show us how the various actions affect $4G$ and $\widetilde{G}$, via some algebra.

Lemma 31 *Let G and $\widetilde{G}$ be as given above and let $\lambda, \beta_0, \beta_1, \beta_2 \in \mathbb{Z}_p$ and $M \in \mathrm{GL}_2(\mathbb{Z}_p)$. Then the following three transformations have the following effects.*

$$\begin{aligned}
< \lambda, [0,0,0], \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} > :\ & 4G(x,z) \mapsto 4\lambda^2 G(x,z), \\
& \widetilde{G}(x,z) \mapsto \lambda^4 \widetilde{G}(x,z), \\
< 1, [\beta_0,\beta_1,\beta_2], \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} > :\ & 4G(x,z) \mapsto 4G(x,z), \\
& \widetilde{G}(x,z) \mapsto \widetilde{G}(x,z) + 4(\alpha_0\beta_2 + 2\beta_0\beta_2 + \alpha_2\beta_0)G(x,z), \\
< 1, [0,0,0], M > :\ & 4G(x,z) \mapsto 4G(M(x,z)^T), \\
& \widetilde{G}(x,z) \mapsto \det(M)^2(\widetilde{G}(M(x,z)^T) + 4kG(M(x,z)^T)),
\end{aligned}$$

for some integer k.

Proof : After the first transformation, our binary quartic is given by

$$y^2 + \lambda P(x,z)y = \lambda^2 Q(x,z),$$

so by examining the formula for $4G$, we can see that every term has either two coefficients from $P(x,z)$ or one from $Q(x,z)$. Therefore we get $4\lambda^2 G$ after this

transformation. Similarly, by examining the formula for $\widetilde{G}$, we can see that every term gets multiplied by λ^4.

For the second transformation, if we let $R(x,z) = \beta_0 x^2 + \beta_1 xz + \beta_2 z^2$, then after this transformation $P(x,z)$ becomes $(P + 2R)(x,z)$ and $Q(x,z)$ becomes $(Q - PR - R^2)(x,z)$. Then $4G(x,z) = (P^2 + 4Q)(x,z)$ becomes

$$(P^2 + 4PR + 4R^2 + 4Q - 4PR - 4R^2)(x,z) = 4G(x,z),$$

so this remains unchanged. For $\widetilde{G}$, recall that G_4 was formed as a covariant of G, so is also unchanged and

$$\widetilde{G}(x,z) = (G_4 - (4c_2 - 4\alpha_0\alpha_2 + \alpha_1^2)G)(x,z)/3,$$

which becomes

$$(G_4 - (4(c_2 - \beta_0(\alpha_2 + \beta_2) - \beta_2(\alpha_0 + \beta_0) - \beta_1(\alpha_1 + \beta_1)) - 4(\alpha_0 + 2\beta_0)(\alpha_2 + 2\beta_2) + (\alpha_1 + 2\beta_1)^2)G)(x,z)/3 = (\widetilde{G} + 4(\alpha_0\beta_2 + 2\beta_0\beta_2 + \alpha_2\beta_0)G)(x,z),$$

as required.

For the $\mathrm{GL}_2(\mathbb{Z}_p)$ transformation, it is enough to prove the lemma for the two matrices

$$D = \begin{pmatrix} \mu & 0 \\ 0 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

For the matrix D, if we replace x by μx in the formula for $4G(x,z)$, then we get the same as replacing $\{\alpha_0, \alpha_1, \alpha_2, a_2, b_2, c_2, d_2, e_2\}$ by $\{\mu^2\alpha_0, \mu\alpha_1, \alpha_2, \mu^4 a_2, \mu^3 b_2, \mu^2 c_2, \mu d_2, e_2\}$. The only difference in $\widetilde{G}$ is that we get a factor of μ^2 in every term. Hence the claim is true for this matrix.

For the matrix T, we will spare the reader the details, but a lengthy calculation shows that $4G(x,z)$ becomes $4G(x+z,z)$ and $\widetilde{G}(x,z)$ becomes

$$(\widetilde{G} - 4(b_2 + 2a_2)G)(x+z,z),$$

hence the lemma is proved.

□

The following lemma will give us some freedom in later discussion.

Lemma 32 *$\varepsilon_p(C_2)$ is invariant under $\mathbb{Z}_p$ transformations, i.e. for a transformation t defined over $\mathbb{Z}_p$ and C_2 defining a 2-covering over $\mathbb{Q}_p$, we have*

$$\varepsilon_p(t(C_2)) = \varepsilon_p(C_2).$$

Proof : We may assume

$$t =< 1, [\beta_0, \beta_1, \beta_2], M >,$$

for $\beta_i \in \mathbb{Z}_p$ and $M \in \mathrm{SL}_2(\mathbb{Z}_p)$. We will use the previous lemma to show how ε_p changes. Let $\max(|4G(x,z)|_p, |\widetilde{G}(x,z)|_p) = k$, for $x, z \in \mathbb{Z}_p$ and not both in $p\mathbb{Z}_p$. Then using the second and third transformations in Lemma 31, $t\colon 4G \mapsto 4G$ and $t\colon \widetilde{G} \mapsto \widetilde{G} - 4lG$ (for some integer l) and

$$\max(|4G(M^{-1}(x,z)^T)|_p, |(\widetilde{G} - 4lG)(M^{-1}(x,z)^T)|_p) = \\ \max(|4G(M^{-1}(x,z)^T)|_p, |\widetilde{G}(M^{-1}(x,z)^T)|_p) = k.$$

Therefore, the set of all values taken by $\max(|4G(x,z)|_p, |\widetilde{G}(x,z)|_p)$ is the same as the set of values after we have transformed by t (for $x, z \in \mathbb{Z}_p$ and not both in $p\mathbb{Z}_p$).

Also, $\max(|x|_p, |z|_p)$ stays the same after we have transformed by t, so when we take the infimum over $\mathbb{Q}_p$ points of all values taken by $\frac{\max(|4G(x,z)|_p, |\widetilde{G}(x,z)|_p)}{\max(|x|_p, |z|_p)}$, namely ε_p, this is unchanged and we are done.

□

Now we have a couple of lemmas which will show us that there are only certain points to consider when we are calculating ε_p.

Lemma 33 *Let K be any field and C_2 a curve defined by a generalised binary quartic over K. Also let G and $\widetilde{G}$ be as given above, then*

$$(x\colon y\colon z) \in C_2(K) \text{ is singular } \Leftrightarrow 4G(x,z) = \widetilde{G}(x,z) = 0.$$

Proof : Using Lemma 31, we may assume $(x\colon y\colon z) = (0\colon 0\colon 1)$. Since this is a point on C_2, we must have $e_2 = 0$. Therefore, from the equations for $4G$ and $\widetilde{G}$, we have

$$\alpha_2^2 = \alpha_1\alpha_2 d_2 - \alpha_2^2 c_2 + d_2^2 = 0,$$

i.e. $\alpha_2 = d_2 = 0$. These are exactly the criteria for a singular point.

□

Lemma 34 *Let C_2 have $\mathbb{Z}_p$ coefficients and let a and A be the leading coefficients of $4G(x,1)$ and $\widetilde{G}(x,1)$ respectively. Let $p < \infty$ be a prime such that $p \nmid \gcd(a, A)$. If $P = (x : y : 1) \in C_2(\mathbb{Q}_p)$, with $\overline{P} = (\overline{x} : \overline{y} : 1) \in \overline{C}_2(\mathbb{F}_p)$ a non-singular point, then*

$$\max(|4G(x,1)|_p, |\widetilde{G}(x,1)|_p) = \max(1, |x|_p)^4.$$

Proof : If $|x|_p > 1$, then

$$|4G(x,1)|_p \leq |x|_p^4 \text{ and } |\widetilde{G}(x,1)|_p \leq |x|_p^4,$$

but p does not divide both A and a, so $\max(|4G(x,1)|_p, |\widetilde{G}(x,1)|_p) = |x|_p^4$ and in this case we are done.

If $|x|_p \leq 1$, we need to show that $\max(|4G(x,1)|_p, |\widetilde{G}(x,1)|_p) = 1$. So it is enough to show that if $4G(x,1) \equiv \widetilde{G}(x,1) \equiv 0 \bmod p$, then $\overline{P}$ is singular for a contradiction. This is simply applying Lemma 33 with $K = \mathbb{F}_p$.

□

Corollary 35 *Let $\mathcal{B}$ be as in Theorem 30. Then $\varepsilon_p(C_2) = 1$ for all $p \notin \mathcal{B}$.*

Proof : From the above lemma, if $\varepsilon_p \neq 1$ then there are two possibilities. We need a singular point of C_2 modulo p or we need $p \mid \gcd(a, A)$. The latter implies that $(1 : 0 : 0)$ is a singular point of C_2 modulo p using Lemma 33 and both mean that $p \in \mathcal{B}$, so we are done.

□

Now, the following compact sets and infima will be important in the next lemma:

$$\begin{aligned}
D_p &= \{x \in \mathbb{Q}_p : |x|_p \leq 1, G(x,1) \text{ is a square in } \mathbb{Q}_p\},\\
D'_p &= \{z \in \mathbb{Q}_p : |z|_p \leq 1, G(1,z) \text{ is a square in } \mathbb{Q}_p\},\\
d_p &= \inf_{x \in D_p} \max(|4G(x,1)|_p, |\widetilde{G}(x,1)|_p),\\
d'_p &= \inf_{z \in D'_p} \max(|4G(1,z)|_p, |\widetilde{G}(1,z)|_p).
\end{aligned}$$

Note that the following two lemmas also hold for $p = \infty$, where $\mathbb{Q}_p = \mathbb{R}$.

Lemma 36 *d_p and d'_p, as defined above, are non-zero.*

Proof : First note that D_p and D'_p are compact subsets of $\mathbb{Q}_p$ (with respect to the p-adic topology), so the infima will be attained. Now suppose $d_p = 0$, then there exists an $x \in D_p$ such that $|4G(x,1)|_p = |\widetilde{G}(x,1)|_p = 0$, i.e. $4G(x,1) = \widetilde{G}(x,1) = 0$. Using Lemma 33 with $K = \mathbb{Q}_p$, this means C_2 is singular, which is a contradiction. Similarly for d'_p.

□

Lemma 37 *$\varepsilon_p(C_2) = \min(d_p, d'_p)$, which is non-zero.*

Proof : Let $P = (x\colon y\colon z) \in C_2(\mathbb{Q}_p)$. Since $\varepsilon_p(C_2)$ is independent of the scaling of points, we may assume $z = 1$. If $|x|_p \leq 1$, then $x \in D_p$ and we have $\varepsilon_p = d_p$. If $|x|_p > 1$, then $x^{-1} \in D'_p$ and $\frac{\max(|4G(x,1)|_p, |\widetilde{G}(x,1)|_p)}{|x|_p^4} = \max(|4G(1,x^{-1})|_p, |\widetilde{G}(1,x^{-1})|_p)$, so $\varepsilon_p(C_2) = d'_p$. Therefore $\varepsilon_p(C_2) = \min(d_p, d'_p)$, which is non-zero by Lemma 36.

□

This means

$$0 < \varepsilon_p(C_2) \leq 1$$

and we are now ready to put the pieces together and prove Theorem 30.

Proof : Recall for a general point $P = (x : y : z) \in C_2(\mathbb{Q}_p)$, we have

$$H(P) = \prod_{p \in M_{\mathbb{Q}}} \max(|x|_p, |z|_p)$$

and

$$H(\pi(P)) = \prod_{p \in M_{\mathbb{Q}}} \max(|4G(x,z)|_p, |\widetilde{G}(x,z)|_p).$$

Now Definition 29 states

$$\varepsilon_p(C_2) \leq \frac{\max(|4G(x,z)|_p, |\widetilde{G}(x,z)|_p)}{\max(|x|_p, |z|_p)^4},$$

so

$$\begin{aligned} H(\pi(P)) &\geq \prod_{p \in M_{\mathbb{Q}}} (\varepsilon_p(C_2) \max(|x|_p, |z|_p)^4) \\ &= H(P)^4 \prod_{p \in M_{\mathbb{Q}}} \varepsilon_p(C_2). \end{aligned}$$

Therefore, by Lemma 37 and Corollary 35 we have

$$h(\pi(P)) - 4h(P) \geq \sum_{p \in \mathcal{B}} \log(\varepsilon_p(C_2)),$$

by taking logs, which achieves the result.

□

2.5 Calculation at the Infinite Place

The case for $p = \infty$ requires a slightly inelegant approach, but the method lends itself easily to an algorithm for computation. Here $\mathbb{Q}_p = \mathbb{R}$, so $4G$ and $\widetilde{G}$ are real polynomials and $|.|_p$ is the usual real absolute value. We need to find

$$d_\infty = \inf_{X \in D_\infty} \max(|4G(X,1)|, |\widetilde{G}(X,1)|),$$
$$d'_\infty = \inf_{X \in D'_\infty} \max(|4G(1,X)|, |\widetilde{G}(1,X)|),$$

where

$$D_\infty = \{X \in \mathbb{R} \colon |X| \leq 1 \text{ and } G(X,1) \geq 0\},$$
$$D'_\infty = \{X \in \mathbb{R} \colon |X| \leq 1 \text{ and } G(1,X) \geq 0\}.$$

Now we have the following routine lemma for infima.

Lemma 38 *Let f_1 and f_2 be continuous real valued functions on a closed and bounded interval I. Then the infimum over I of the continuous function $s(X) = \max(|f_1(X), |f_2(X)|)$ occurs at one of the following points:*

- *An end point of I.*
- *A root of f_1, f_2, $f_1 + f_2$ or $f_1 - f_2$ in I.*
- *A turning point of f_1 or f_2 in I.*

Proof : At any point which is not an end point of I or one of the roots mentioned above, then (in a neighbourhood of that point) $s = f_1, -f_1, f_2$ or $-f_2$. This means that the infimum of these points must be a local supremum or infimum of f_1 or f_2.

□

Thus, in order to compute $\varepsilon_\infty(C_2)$, we need to use the following algorithm:

- D_∞ is a finite union of closed and bounded intervals (since g is a real polynomial), so we need to find these intervals. Call them I_i.
- For each I_i, find the value of $\max(|4G(X,1)|, |\widetilde{G}(X,1)|)$ at each of the roots, turning points and end points as mentioned in Lemma 38 (for $f_1 = 4G$ and $f_2 = \widetilde{G}$).
- Find the minimum of all of these values over all intervals I_i. This is d_∞.
- Repeat the process for I_i' and D_∞' in order to find d_∞'.
- Calculate $\varepsilon_\infty(C_2) = \min(d_\infty, d_\infty')$.

While this seems like a laborious algorithm, it is actually relatively easy for a computer to carry out all the steps. For example, take the curve (whose Jacobian has reference '988b1' in [Cre97])

$$C_2 : y^2 + x^2y = 268x^4 - 965x^3z + 1530x^2z^2 - 292xz^3 - 127z^4.$$

In order to calculate ε_∞, we calculate $4G$ and $\widetilde{G}$ and then find the roots of $4G(x,1)$ between -1 and 1. This gives us two intervals for D_∞, namely

$$[-1, -0.1993...] \text{ and } [0.4912..., 1].$$

We then look within these intervals for roots or turning points of $4G, \widetilde{G}, 4G+\widetilde{G}$ and $4G - \widetilde{G}$, which yields the points $0.8700..., 0.8716...$ and $-0.5322....$ The smallest value of

$$\max(|4G(x,1)|, |\widetilde{G}(x,1)|)$$

over these seven points (the three above and the four end points of the intervals) comes out to be $1180.8957....$ Then we proceed with $4G(1,z)$; this has no roots between -1 and 1, therefore there is only one interval to consider. However, searching this interval for roots and turning points of $4G, \widetilde{G}, 4G + \widetilde{G}$ and $4G - \widetilde{G}$ yields four points to consider:

$$-0.9044..., -0.8997..., -0.3871..., 0.3603...$$

plus the two end points. The minimum of $\max(|4G(1,z)|, |\widetilde{G}(1,z)|)$ over these eight points comes out as $10017.5914...$, therefore the value of ε_∞ is $1180.8957...$

We expect that having our binary quartic in reduced form will give a smaller value for ε_∞ in general.

2.6 The Finite Places

Now let us investigate what happens when $p < \infty$. Recall that we have $\varepsilon_p(C_2) = \min(d_p, d'_p)$.

Definition 39 *For C_2 a binary quartic with coefficients $\alpha_0, \alpha_1, \alpha_2, a_2, b_2, c_2, d_2$ and e_2 and v_p the p-adic valuation, define the valuation of C_2 to be*

$$v_p(C_2) = \min(v_p(\alpha_0), v_p(\alpha_1), v_p(\alpha_2), v_p(a_2), v_p(b_2), v_p(c_2), v_p(d_2), v_p(e_2)).$$

Definition 40 *For C_2 with coefficients $\alpha_0, \alpha_1, \alpha_2, a_2, b_2, c_2, d_2, e_2 \in \mathbb{Z}_p$ and $P = (0 : 0 : 1)$ a singular point of C_2 modulo p. Then P is a non-regular point if $p^2 \mid e_2$.*

Lemma 41 *For C_2 given by $y^2 + P(x, z)y = Q(x, z)$, if $v_p(C_2) = 1$, then $\varepsilon_p(C_2) \leq 1/p^2$ if $4G(x, z)/p$ has a root over $\mathbb{F}_p$ and $\varepsilon_p(C_2) = 1$ if not. If $v_p(C_2) = 0$, then $\varepsilon_p(C_2) \leq 1/p^2$ if C_2 contains a non-regular point over $\mathbb{F}_p$ and $\varepsilon_p(C_2) = 1$ if not.*

Proof : If $v_p(C_2) = 1$ then $v_p(\widetilde{G}) = 2$, so any root of $4G/p$ modulo p could be moved by an $\mathrm{SL}_2(\mathbb{Z}_p)$ transformation to $(0 : 0 : 1)$, after which $p^2 \mid e_2$ and therefore $\varepsilon_p(C_2) \leq 1/p^2$. If $4G/p$ has no roots modulo p, then $|4G(x, z)|_p$ is always $1/p$, but by consideration modulo p^2, we can see that if $p^2 \nmid e_2$, then $(0 : 0 : 1)$ cannot lift to a $\mathbb{Q}_p$ point and so may be ignored. Therefore $\varepsilon_p(C_2) = 1$.

If $v_p(C_2) = 0$, we only need to take the infimum over the $\mathbb{Q}_p$ points reducing to singular points of C_2 over $\mathbb{F}_p$, because of the proof of Lemma 34. We do not need to consider all singular points over $\overline{\mathbb{F}}_p$, since $\varepsilon_p(C_2)$ is defined as the maximum over $\mathbb{Q}_p$ points. Now, if $p^2 \nmid e_2$, then consideration modulo p^2 shows that the point $(0 : 0 : 1)$ cannot lift to a $\mathbb{Q}_p$ point. So, for a contribution we need $p^2 \mid e_2$ and then we also have $p \mid \alpha_2$ and d_2, since the point is singular. Therefore, p^2 divides the last coefficient of $\widetilde{G}$, which is given by

$$-\alpha_1^2 e_2 + \alpha_1\alpha_2 d_2 - \alpha_2^2 c_2 - 4c_2 e_2 + d_2^2$$

and therefore $\varepsilon_p(C_2) \leq 1/p^2$. Hence the lemma is proved.

□

2.6.1 $\mathbb{F}_p$ Points Not Lifting Uniquely

Restricting our discussion to those quartics which give a contribution to $\varepsilon_p(C_2)$, from above we have seen that these are those with points whose reduction modulo p is a non-regular point defined over $\mathbb{F}_p$ (including those where $v_p(C_2) = 1$). However, two different $\mathbb{Q}_p$ points above the same $\mathbb{F}_p$ point could give a different value for ε_p. For example, when we take the quartic

$$C_2 \colon y^2 + x^2y = 268x^4 - 965x^3z + 1530x^2z^2 - 292xz^3 - 127z^4,$$

$4G(x, 1)$ has repeated roots at 6 and 10 over $\mathbb{F}_{19}$. Simply using $x = 10$ would yield a contribution of 19^{-2} to $\varepsilon_{19}(C_2)$. However, $106714 \equiv 10 \bmod 19$ and we have 19^6 dividing both $4G(106714, 1)$ and $\widetilde{G}(106714, 1)$ and in fact $\varepsilon_{19}(C_2) = 19^{-6}$.

Before tackling this problem, we need to make some definitions.

Definition 42 *The contribution to $\varepsilon_p(C_2)$ from the set of $\mathbb{Q}_p$ points X' reducing to the set $X \subset \overline{C}_2(\mathbb{F}_p)$ is denoted*

$$\varepsilon_p(C_2, X) = \inf_{(x:y:z)\in X'} \frac{\max(|4G(x,z)|_p, |\widetilde{G}(x,z)|_p)}{\max(|x|_p, |z|_p)^4}.$$

For example, Lemma 41 shows that

$$\varepsilon_p(C_2) = \varepsilon_p(C_2, N),$$

for N the set of non-regular points of C_2 over $\mathbb{F}_p$. To make our task simpler, we will move points that we want to consider to somewhere convenient (which will not affect ε_p, because of Lemma 32), i.e. to $(0 : 0 : 1)$. So our task is now to calculate $\varepsilon_p(C_2, \{(0 : 0 : 1)\})$. This then only has a contribution if we have $p \mid \alpha_2, d_2$ and $p^2 \mid e_2$.

At this point we can note that curves with Tamagawa number 1 can yield a contribution[15].

[15]Recall the definition of the Tamagawa number at p, $c_p = [E(\mathbb{Q}) : E^0(\mathbb{Q})]$. Note that this is not as strong as the analogue in Siksek's paper [Sik95], where he proves that there is no contribution to his version of ε_p when the Tamagawa number is 1.

2.6.2 Operating To Evaluate ε_p

Definition 43 *A 2-covering C_2 defines an 'end quartic' either if it has only one non-regular point over $\mathbb{F}_p$ and this is at $(1:0:0)$ or if it has no non-regular points over $\mathbb{F}_p$.*

Definition 44 *For a prime p and C_2 given by $y^2 + P(x,z)y = Q(x,z)$, the following is the 'flip' operation on C_2*

$$\Upsilon\colon C_2 \longmapsto C_2',$$

for C_2' given by

$$C_2'\colon y^2 + \frac{1}{p}P(px,z)y = \frac{1}{p^2}Q(px,z).$$

The new quartic obtained has $\mathbb{Z}_p$ coefficients as long as $p \mid \alpha_2, d_2$ and $p^2 \mid e_2$. This means that if C_2 is not an end quartic then we can move[16] a non-regular point (one not at $(1:0:0)$) to $(0:0:1)$ and apply Υ. Note that 'flipping' preserves the invariants I and J. It does however move the quartic to a different $\mathbb{Z}_p$-equivalence class.

We can also define Υ^{-1} whenever we have a non-regular point at $(1:0:0)$. When applying Υ (or Υ^{-1}), the translation of any singular points to $(0:0:1)$ (or $(1:0:0)$) is understood.

Lemma 45 *If C_2 defines an end quartic, then $\varepsilon_p(C_2, \overline{C}_2(\mathbb{F}_p) \setminus \{(1:0:0)\}) = 1$.*

Proof : If $v_p(C_2) = 1$, then $4G(x,1)/p$ has no roots modulo p for an end quartic (if it did, we could move the root to 0 and have $p^2 \mid e_2$, i.e. we would have a non-regular point of $\overline{C}_2$), so $\varepsilon_p(C_2, \overline{C}_2(\mathbb{F}_p) \setminus \{(1:0:0)\}) = 1$ (by considering Lemma 41) and we are done.

If $v_p(g) = 0$, then only a non-regular point of C_2 could give a contribution by Lemma 41. But we have assumed that if C_2 has a non-regular point then this is at $(1:0:0)$ and there are no others, so $\varepsilon_p(C_2, \overline{C}_2(\mathbb{F}_p) \setminus \{(1:0:0)\}) = 1$.

□

Lemma 46 *Let C_2 define an integral generalised binary quartic with a non-regular point at $(x\colon y\colon z) = (0:0:1)$ and let $C_2' = \Upsilon(C_2)$. Then we have*

$$\varepsilon_p(C_2, \{(0:0:1)\}) = p^{-2}\varepsilon_p(C_2', \overline{C}_2'(\mathbb{F}_p) \setminus \{(1:0:0)\}).$$

[16] Using an $\mathrm{SL}_2(\mathbb{Z}_p)$ transformation of the form $x \mapsto x + \lambda z$ and possibly a y substitution.

Proof : Suppose $\varepsilon_p(C_2, \{(0:0:1)\}) = p^{-k}$, then k is the greatest integer such that there exists an $x_0 \in \mathbb{Z}_p$ with $p^k \mid 4G(x_0 p, 1)$ and $p^k \mid \widetilde{G}(x_0 p, 1)$. This means that $k-2$ is the greatest integer such that there exists an $x_0 \in \mathbb{Z}_p$ with $p^{k-2} \mid p^{-2}4G(x_0 p, 1)$ and $p^{k-2} \mid p^{-2}\widetilde{G}(x_0 p, 1)$. Using Lemma 31, we can see that after the transformation

$$< \frac{1}{p}, [0,0,0], \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} >,$$

i.e. Υ, these are what $4G(x_0, 1)$ and $\widetilde{G}(x_0, 1)$ become. Therefore $\varepsilon_p(C_2', \overline{C}_2'(\mathbb{F}_p) \setminus \{(1,0,0)\}) = p^{2-k}$.

□

It now helps to break into cases according to the reduction type of the elliptic curve E_2.

2.6.3 A Classification

For simplicity in computation, notice that if $3 < p < \infty$, then we can complete the square and apply the map π_3 from section 2.2.1 without changing ε_p, so in that case

$$\varepsilon_p(C_2) = \inf_{(x:y:z) \in C_2'(\mathbb{Q}_p)} \frac{\max(|g(x,z)|_p, |g_4(x,z)|_p)}{\max(|x|_p, |z|_p)^4},$$

for C_2' a minimal (and $\mathbb{Z}_p$-equivalent) 2-covering for $p > 3$ given by $y^2 = g(x,z)$. This makes our computations simpler for $p > 3$ and although the picture is the same in this section for $p = 2$ or 3, for simplicity we will avoid these cases, so let

$$g(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + z^4.$$

If E has multiplicative reduction and C_2 is minimal at p, then $v_p(C_2) = 0$, since otherwise $p \mid I$ and $p \mid J$. We can have up to two singular points on C_2 over $\mathbb{F}_p$ and if one is at $(x,z) = (0,1)$, then $p \mid d, e$, but $p \nmid c$ since again this would mean that I and J both vanish modulo p. In other words, we have pictures for $\overline{C}_2(\mathbb{F}_p)$ consisting of either one component with a node or two components meeting at two nodes. These nodes are allowed to be regular or non-regular and the only case where we do not have an end quartic is where we have two components and two non-regular points defined over $\mathbb{F}_p$.

If lines represent applications of Υ or its inverse and if we assume we start

at a quartic with two non-regular points, we could view this as a one dimensional graph whose edges have weighting two:

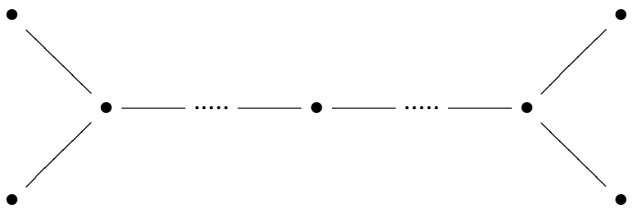
$$\Upsilon^{-1} \longleftarrow (C_2) \longrightarrow \Upsilon$$

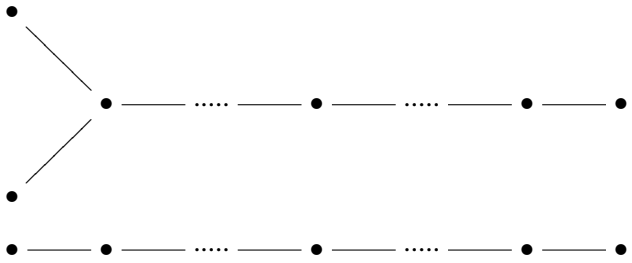
We can view all the vertices apart from those at the two ends (via an $\overline{\mathbb{F}}_p$ transformation) by an equation of the form $y^2 = x^2z^2$, with both intersection points being non-regular. Those at the ends are either the same as above with only one of the singular points being non-regular or they are represented (via an $\overline{\mathbb{F}}_p$ transformation) by an equation of the form $y^2 = (x^2 + z^2)x^2$. As shown in Lemma 45, end quartics do not yield a contribution away from the non-regular point.

For additive reduction, the diagrams are different. If $v_p(C_2) = 0$ and we have a singular point at $(x, z) = (0, 1)$, then we need $p \mid c$ for both the invariants to vanish, so we either have a cusp (given by an equation of the form $y^2 = (x + z)x^3$) or a root of order 4, sometimes called a swallowtail (given by an equation of the form $y^2 = x^4$).

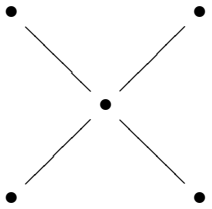
If $v_p(C_2) = 1$, then every point is singular and we represent this by a singular line. We could move any root of g/p modulo p to $(0, 1)$ and apply Υ. Now g/p could have up to four roots, but at most two repeated roots, where (when moved to $(0, 1)$) $p^2 \mid d, e$. In fact, if we do not have $p^2 \mid d$ and $p^3 \mid e$, then $v_p(\Upsilon(C_2)) = 0$. The end quartics are those where $v_p(C_2) = 0$ or where $v_p(C_2) = 1$ and g/p has only one root over $\mathbb{F}_p$.

We have the following three possible graphs:

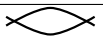




Here the vertices of degree more than two represent a singular line with g/p having more than two roots. These can only happen in vertices adjacent to the end quartics. If an end of the graph splits, this represents two cuspidal quartics. If it does not, this represents either a swallowtail quartic or a singular line. Note that the following special case of the first graph does exist:



Let r be the number of non-regular points over $\mathbb{F}_p$. The table below indicates the possible cases we can have. The third column gives the form of the equation modulo p via an $\overline{\mathbb{F}}_p$ transformation and the fifth column records whether this gives an end quartic.

Reduction	Diagram	Equation over $\mathbb{F}_p$	r	End quartic?
Multiplicative		$y^2 = x^2z^2$	2	No
		$y^2 = x^2z^2$	0 or 1	Yes
		$y^2 = (x^2 + z^2)x^2$	0 or 1	Yes
Additive		$y^2 = pg'(x, z)$	2,3 or 4	No
		$y^2 = pg'(x, z)$	0 or 1	Yes
		$y^2 = (x + z)x^3$	0 or 1	Yes
		$y^2 = x^4$	0 or 1	Yes

In the above graphs, the vertices represent different $\mathbb{Z}_p$-equivalence classes of binary quartic. Sadek has shown that there are only a finite number of such classes and gives expressions for these depending on the reduction type

(see [Sad10a], Table 1) and Liu also gives a detailed classification in [Liu94]. For our purposes however, we can say that after m applications of Υ, we have $p^{2m} \mid a$ and $p^m \mid b$, so $p^{2m} \mid \Delta(C_2)$ and therefore m is bounded.

Now let us remove our assumption of $p > 3$ and consider a general prime. If C_2 has a non-regular point at $(0 : 0 : 1)$, then let $i_0(C_2)$ be the smallest non-negative integer such that $\Upsilon^{i_0}(C_2)$ defines an end quartic. Iterating Lemma 46 and using Lemma 45 gives

$$\varepsilon_p(C_2, \{(0 : 0 : 1)\}) = p^{-2i_0}.$$

And we could write down a similar expression for any other non-regular points, so now let us consider the graphs discussed above. If we let i be the maximum number of edges from the starting vertex to a vertex of degree one, then we have the following simple and useful expression

$$\varepsilon_p(C_2) = p^{-2i}.$$

2.6.4 An Algorithm for ε_p

The investigations in the previous sections allow us to describe an algorithm for calculating ε_p.

1. Choose a prime p. Set $i_1 = i_2 = c = 0$ and $j = 1$.
2. Find the non-regular points of C_2 and call them $\{P_i\}$. If there are none, then $\varepsilon_p(C_2) = 1$.
3. If there are 4, then $\varepsilon_p(C_2) = p^{-2}$.
4. If there are 3, find which point does not take us to an end quartic using Υ and move this point to $(0 : 0 : 1)$.
5. If there are 2, set $c = 1$ and move P_1 to $(0 : 0 : 1)$.
6. If there is only one, move it to $(0 : 0 : 1)$.
7. Apply Υ, add one to i_j.
8. If we have an end quartic, then we have $\varepsilon_p(C_2, \{P_j\}) = p^{-2i_j}$.

9. If we do not have an end quartic, move any non-regular point (that is not at $(1:0:0)$) to $(0:0:1)$ and return to step 7.

10. If $c = 1$, set $c = 0$, $j = 2$ and consider the original quartic. Move P_2 to $(0:0:1)$ and return to step 7.

11. Then $\varepsilon_p(C_2) = \min_i(\varepsilon_p(C_2, \{P_i\}))$.

2.7 Worked Examples

In this section we will illustrate the calculation of ε_p on three examples.

1. Firstly, consider the binary quartic given by

$$C_2 : y^2 + (2xz + 2z^2)y = 24x^4 - 116x^2z^2 - 2xz^3 - 26z^4.$$

   This occurs in the 2-Selmer group of the elliptic curve with reference '600a6' in [Cre97]. It has bad reduction at $p = 2, 3$ and 5 of types II^*, I_1 and I_8^*, respectively.

2. Next consider

$$C_2 : y^2 + xyz = -53x^4 + 486x^3z + 531x^2z^2 + 486xz^3 - 53z^4.$$

   This occurs in the 2-Selmer group of the elliptic curve with reference '897d1' in [Cre97]. It has bad reduction at $p = 3, 13$ and 23 of types I_{12}, I_{10} and I_1, respectively.

3. And finally consider

$$C_2 : y^2 + x^2y = 268x^4 - 965x^3z + 1530x^2z^2 - 292xz^3 - 127z^4.$$

   This occurs in the 2-Selmer group of the elliptic curve with reference '988b1' in [Cre97]. It has bad reduction at $p = 2, 13$ and 19 of types IV, I_1 and I_{13}, respectively.

2.7.1 Local Contributions

Let us compute ε_p for $p < \infty$ on the above examples.

1. At $p = 2$ in the first example, we do not initially have $p^2 \mid e_2$, but we do after moving the point $(1 : 0 : 1)$ to $(0 : 0 : 1)$. Then we can apply Υ, giving the new quartic

$$y^2 + 2xyz = 96x^4 + 192x^3z + 28x^2z^2 - 67xz^3 - 29z^4.$$

   We cannot however apply Υ any further here so this is an end quartic.

   Returning to the original quartic, if we consider the point $(1 : 0 : 0)$ (by switching x and z, say), then we can apply Υ and get the quartic

$$y^2 + (4x^2 + 2xz)y = -104x^4 - 4x^3z - 116x^2z^2 + 6z^4.$$

   We cannot apply Υ again, so this means that we have a contribution of 2^2 on the original quartic and therefore $\varepsilon_2 = 2^{-2}$.

   We can then complete the square to consider the remaining primes, so let

$$C_2' \colon y^2 = g(x, z) = 96x^4 - 460x^2z^2 - 100z^4.$$

   At $p = 3$, this has one singular point at $(1, 0)$, but it is regular and this is an end quartic, therefore $\varepsilon_3 = 1$.

   Taking $p = 5$, we notice that g has a swallowtail point at $(x, z) = (0, 1)$, since $g \equiv x^4$. Then, applying Υ to C_2, we get

$$(5^2 \times 96)x^4 - (5 \times 92)x^2z^2 - 4z^4.$$

   By considering this modulo 5, we can see that it is an end quartic so it has no contribution. Thus $\varepsilon_5(C_2) = 5^{-2}$.

2. We have good reduction at 2, so we can complete the square immediately, giving

$$C_2 \colon y^2 = -212x^4 + 1944x^3z + 2125x^2z^2 + 1944xz^3 - 212z^4.$$

At $p = 3$, this has non-regular points at $(1,1)$ and $(2,1)$. We can apply Υ twice on the first point and three times on the second to get to end quartics, so we get $\varepsilon_3(C_2) = 3^{-6}$.

At $p = 23$, the only singular point of g is at $(1,1)$, but this turns out to be a regular point. Therefore there is no contribution, i.e. $\varepsilon_{23}(C_2) = 1$.

At $p = 13$, we have non-regular points at $(2,1)$ and $(7,1)$. If we move the first to $(0,1)$ and apply Υ, we get the quartic

$$-(13^2 \times 212)x^4 + (13 \times 248)x^3z + 8701x^2z^2 + 2076x^3z + 144z^4,$$

which still has a non-regular point at $(7,1)$[17]. Carrying out a further 'flip' on this gives

$$-(13^4 \times 212)x^4 - (13^2 \times 76920)x^3z - 10457027x^2z^2 - 3735246x^3z - 499859z^4.$$

This now has no non-regular points modulo 13 (apart from $(1,0)$) and is therefore an end quartic[18]. Returning to the original quartic and considering the other singular point at $(7,1)$, we 'flip' to get

$$-(13^2 \times 212)x^4 - (13 \times 3992)x^3z - 19379x^2z^2 + 2046x^3z + 1629z^4$$

and 'flip' this on $(1,1)$ to get

$$-(13^4 \times 212)x^4 - (13^2 \times 15016)x^3z - 390035x^2z^2 - 25824x^3z - 612z^4.$$

This is now an end quartic, so we have shown that we can carry out two 'flips' in each direction from the original quartic and therefore $\varepsilon_{13}(C_2) = \min(13^{-4}, 13^{-4}) = 13^{-4}$.

3. For $p = 2$, we have one non-regular point at $(0:1:1)$, but if we apply Υ, there are no more on the new quartic. Therefore $\varepsilon_2(C_2) = 2^{-2}$. We then complete the square and get

$$C_2 \colon y^2 = 1073x^4 - 3860x^3z + 6120x^2z^2 - 1168xz^3 - 508z^4.$$

[17] This bears no relation to the $(7,1)$ in the original quartic.

[18] I have chosen not to reduce the binary quartics at each stage, since although it would provide nicer equations, I feel it makes the situation less clear.

This has no non-regular points at $p = 13$ (although it does have a regular singular point at $(3, 1)$), so $\varepsilon_{13}(C_2) = 1$.

At $p = 19$, we have non-regular points at $(6, 1)$ and $(10, 1)$. We can 'flip' three times on the first and three times on the second to reach end quartics. This means $\varepsilon_{19}(C_2, \overline{C}_2(\mathbb{F}_{19}) \setminus \{(6, 1)\}) = 19^{-6}$ and $\varepsilon_{19}(C_2, \overline{C}_2(\mathbb{F}_{19}) \setminus \{(10, 1)\}) = 19^{-6}$, so $\varepsilon_{19}(C_2) = 19^{-6}$.

As we can see, there appears to be a connection between the m in reduction type I_m and the size of the contribution to ε_p. This is no coincidence, since the larger m is, the more $\mathbb{Z}_p$-equivalence classes of binary quartics there are[19] and so the more operations of Υ we are able to carry out.

2.7.2 Putting the Contributions Together

We now have all the ingredients to calculate a bound between the curves C_2 and E_2. We use the formula from Theorem 30:

$$h(P) - \frac{1}{4}h(\pi(P)) \leq -\frac{1}{4}\sum_{p \in \mathcal{B}} \log(\varepsilon_p(C_2)),$$

for $P \in C_2$. To summarise the three examples above, we have

1. $\varepsilon_2 = 2^{-2}$, $\varepsilon_3 = 1$, $\varepsilon_5 = 5^{-2}$ and it can be shown that $\varepsilon_\infty = 11040$. The overall bound is then

$$\frac{1}{4}(2\log 2 + 2\log 5 - 9.3093...) = -1.1760...$$

2. Here $\varepsilon_3 = 3^{-6}$, $\varepsilon_{13} = 13^{-4}$, $\varepsilon_{23} = 1$ and it can be shown that $\varepsilon_\infty = 364238.9969....$ The overall bound is then

$$\frac{1}{4}(6\log 3 + 4\log 13 - 12.8056...) = 1.0115...$$

3. Finally, ε_∞ comes out to be 1180.8957... (from the example in section 2.5) and we also have $\varepsilon_2 = 2^{-2}$, $\varepsilon_{13} = 1$ and $\varepsilon_{19} = 19^{-6}$. Thus the overall bound is calculated as

$$\frac{1}{4}(2\log 2 + 6\log 19 - 7.0740...) = 2.9947...$$

[19] Table 1 in [Sad10a] shows that the relationship is linear.

2.8 Final Remarks and Examples on Binary Quartics

Note that we are forcing the choice of E that we use for height comparisons to be E_2 given above, so that all the local contributions match up. If we had a different elliptic curve in mind then we could in principle bound the height difference between them, but it is expected that we would not mind too much searching on this equivalent elliptic curve.

Also we should note that for ease we would want to search for points on a quartic after completing the square rather than a generalised binary quartic, but fortunately this does not change x or z, so is no problem.

The first thing to note about the examples in the previous section is that they seem to be pleasingly small (sometimes even negative), so for points of fairly large height on E, their corresponding points on C_2 will be significantly smaller.

Next let us turn our attention to choosing an equivalence class of quartics on which to search so as to give the smallest bound. Let n be the number of $\mathbb{Z}_p$-equivalence classes and let i_1 and i_2 be the number of steps from our quartic to each end of the graph of equivalence classes. Then $n = i_1 + i_2 + 1$ if C_2 has multiplicative reduction and $n = i_1 + i_2 + 1 + l$ for $l = 0, 1$ or 2 if C_2 has additive reduction (recalling that the ends of the graph can split in this case). If we are allowed to choose our quartic C_2, then we can obtain a better bound by choosing it to be in the 'middle' equivalence class, i.e. so that $i_0 = i^0$ or $i^0 + 1$. Then for multiplicative reduction we get $\varepsilon_p(C_2) = p^{-k}$ for $k = n - 1$ if n is odd and $k = n$ if n is even. For additive reduction, we have a number of possibilities; if l is the number of split ends of the graph, then we can choose C_2 so that k is given in the following table.

Parity of n	Mult. Red.	Add. Red:	$l = 0$	$l = 1$	$l = 2$
Odd	$n - 1$		$n - 1$	$n - 1$	$n - 3$
Even	n		n	$n - 2$	$n - 2$

To illustrate this, consider the third example above

$$C_2 : y^2 + x^2 y = 268x^4 - 965x^3 z + 1530x^2 z^2 - 292xz^3 - 127z^4.$$

This lies in the fourth (out of 7) $\mathbb{Z}_{19}$-equivalence class. The following are reduced representatives[20] for each of the equivalence classes

$$\begin{aligned}
y^2 &= 49x^4 - 720x^3z - 774x^2z^2 + 3064xz^3 + 17297z^4,\\
y^2 &= 68x^4 + 352x^3z + 4608x^2z^2 + 20xz^3 - 4687z^4,\\
y^2 &= x^4 - 544x^3z + 1122x^2z^2 + 9672xz^3 + 28697z^4,\\
y^2 &= 1073x^4 - 3860x^3z + 6120x^2z^2 - 1168xz^3 - 508z^4,\\
y^2 &= 161x^4 + 2312x^3z - 270x^2z^2 - 1968xz^3 + 1897z^4,\\
y^2 &= 4x^4 - 368x^3z + 312x^2z^2 + 12548xz^3 + 71617z^4,\\
y^2 &= 233x^4 - 636x^3z - 768x^2z^2 + 6688xz^3 + 1444z^4.
\end{aligned}$$

The values of ε_∞ do not vary greatly amongst these curves and are given by

$$5.0603..., 5.9943..., 4.5879..., 7.0740..., 7.2197..., 3.6740..., 5.1523...,$$

respectively. However, although there is no change in ε_p other than at $p = 19$ (where consecutive classes differ by $2\log 19$), this has a large effect on the overall bounds for $h(P) - \frac{1}{4}h(\pi(P))$, which are given by

$$7.9148..., 6.2091..., 5.0885..., 2.9947..., 4.4305..., 6.7892..., 7.8918...,$$

respectively.

So we can see that we give ourselves the best chance of finding a point if we search on the middle equivalence class for each prime and the benefit of this dominates any change at the infinite place. However this does not guarantee that any particular point will always be smallest on a quartic in the middle equivalence class. For example, the representative of the first equivalence class contains the point $(1:7:0)$, but this has a much larger height on the other representatives. We will expand on this idea in the section on 4-coverings.

The bound we compute seems to be considerably better than that achieved using the resultant method in section 2.3. This is most extreme when there is little or no contribution from the finite primes. Take for example the elliptic curve and

[20] Note that we have completed the square and therefore these are not minimal at 2, but we know ε_2 will remain unchanged.

binary quartic below.

$$E_2 : y^2 + xy = x^3 + x^2 - 2x + 1,$$
$$C_2 : y^2 + (x^2 + xz + z^2)y = -x^3z - x^2z^2 + 2xz^3 + z^4.$$

Even though this has bad primes at $p = 5, 7$ and 19, there is no contribution from any of them. The bound therefore comes out to be 0.1234... If instead, we use the formula at the start of section 2.3, then we would get a bound of:

$$-\frac{1}{4}\log\left(\frac{\min(|4G|, |\widetilde{G}|)|\mathrm{Res}(4G, \widetilde{G})|}{2^{20}5^3|4G|^4|\widetilde{G}|^4}\right) = -\frac{1}{4}\log\left(\frac{5^2 7^2 19^2}{2^{27}5^7}\right) = 4.8210...$$

This shows that we make a marked improvement on previous methods.

3 The Intersection of Two Quadrics

Although the equations are a bit more complicated, we will now look at 4-coverings instead of 3-coverings, since we can make use of the fact that to get to the elliptic curve from a 4-covering, we can map via a 2-covering.

3.1 4-Descent

Four descent is effectively a second 2-descent carried out on a 2-covering. Because of Lemma 13 in section 1.3.1, it should be more powerful, i.e. points will be easier to find on 4-coverings if they exist. We will assume where necessary that we have not found a point via 2-descent. We will follow closely the methods of [MSS96], so for this section let C_2 be given by the binary quartic $y^2 = g(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$ with integer coefficients. The reader should bear in mind the sections 1.3 and 2.1 since the method bears many similarities to the $n = 2$ case. Here we define our algebra $\mathbb{Q}[\theta]$ in terms of elements of the 2-Selmer group rather than the elliptic curve, so it now has degree 4. It is a field or product of fields as before.

Definition 47 *The algebra associated to C_2 is given by*

$$\mathbb{Q}[\theta] = \frac{\mathbb{Q}(T)}{(g(T))} = L_1 \oplus ... \oplus L_t,$$

where the L_i are number fields given by $\mathbb{Q}(\theta_i)$ for θ_i non-pairwise-conjugate roots of g. Let us define the map μ:

$$\begin{aligned} \mu\colon \quad C_2(\mathbb{Q}) &\longrightarrow \frac{\mathbb{Q}[\theta]^*}{(\mathbb{Q}[\theta]^*)^2\mathbb{Q}^*} \\ (x,y,z) &\longmapsto x - \theta z \mod (\mathbb{Q}[\theta]^*)^2\mathbb{Q}^*. \end{aligned}$$

We have to quotient out by $\mathbb{Q}^*$ in the image, since now C_2 is unramified above infinity as a covering of $\mathbb{P}^1$. We may assume $(x,z) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ and that x and z are coprime.

Writing $(x - \theta_i z)\mathcal{O}_{L_i} = \mathfrak{a}_i\mathfrak{b}_i^2$ as a product of ideals with $\mathfrak{a}_i$ square-free and so that $\prod_{i=1}^t N_{L_i/\mathbb{Q}}(\mathfrak{a}_i) \in a\mathbb{Q}^{*^2}$, and letting S_i be the set of prime ideals $\mathfrak{p}$ of L_i such that $\mathfrak{p} \mid a\Delta(g)$, we have the following lemma.

Lemma 48 *For $L_i, \mathfrak{a}_i$ and S_i defined as above, if $\mathfrak{p} \mid \mathfrak{a}_i$ is a prime ideal of L_i, then $\mathfrak{p} \in S_i$.*

Proof : This can be found on page 9 of [MSS96].

□

Definition 49

$$L_i(S_i, 2) = \{\xi \in L_i^*/(L_i^*)^2 \text{ such that } L_i(\sqrt{\xi})/L_i \text{ is unramified away from } S_i\}.$$

To see that this is a finite set, see Proposition 1.6 on p194 of [Sil09]. Now suppose we have an element $\delta_i \in \mathrm{im}(\mu)$. Then it must come from a point $(x : y : z) \in C_2(\mathbb{Q})$ such that

$$x - \theta_i z = \delta_i \gamma_i^2,$$

for $\delta_i \in L_i(S_i, 2)$ and $\gamma_i \in L_i^*$. We reject all sets of equations for which we get $\prod_{i=1}^{t} N_{L_i/\mathbb{Q}}(\delta_i) \notin a\mathbb{Q}^{*^2}$.

If $g(x, z)$ is irreducible, then since we can remove coefficients of θ^4 and above using the equation for $g(x, 1)$, we have

$$\begin{aligned} x - \theta z &= \delta(u_0 + u_1\theta + u_2\theta^2 + u_3\theta^3)^2 \\ &= Q_3(u_0, u_1, u_2, u_3) + Q_4(u_0, u_1, u_2, u_3)\theta + Q_1(u_0, u_1, u_2, u_3)\theta^2 + Q_2(u_0, u_1, u_2, u_3)\theta^3. \end{aligned}$$

Thus, equating coefficients of θ^2 and θ^3, we must have a point on the curve

$$C_4 \colon Q_1(u_0, u_1, u_2, u_3) = Q_2(u_0, u_1, u_2, u_3) = 0,$$

for two quaternary quadratic forms Q_1 and Q_2 depending on δ, i.e.

$$\begin{aligned} C_4 \colon\ & a_{11}x_1^2 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{14}x_1x_4 + a_{22}x_2^2 + a_{23}x_2x_3 + a_{24}x_2x_4 + \\ & a_{33}x_3^2 + a_{34}x_3x_4 + a_{44}x_4^2 = 0, \\ & b_{11}x_1^2 + b_{12}x_1x_2 + b_{13}x_1x_3 + b_{14}x_1x_4 + b_{22}x_2^2 + b_{23}x_2x_3 + b_{24}x_2x_4 + \\ & b_{33}x_3^2 + b_{34}x_3x_4 + b_{44}x_4^2 = 0. \end{aligned}$$

If $g(x, z)$ is not irreducible, then it is either the product of two irreducible quadratic factors or it has a linear term. We will ignore the latter case, since this would mean

we had found a point and that 2-descent had been successful, so let us suppose we obtain equations

$$x - \theta_1 z = \delta_1(u_1 + \theta_1 u_2)^2,$$
$$x - \theta_2 z = \delta_2(u_3 + \theta_2 u_4)^2.$$

Then equating constant and linear coefficients (replacing θ_i^2 terms by linear expressions from their minimal polynomials), we obtain

$$q_1(u_1, u_2) = x = q_2(u_3, u_4),$$
$$q_3(u_1, u_2) = z = q_4(u_3, u_4),$$

for quadratic forms q_1, q_2, q_3 and q_4. These again give us the intersection of two equations in the same form as C_4 above. We will refer to these objects as quadric intersections and investigate their properties in the following section.

3.2 Quadric Intersections and Their Invariant Theory

A good place to start for the theory of quadric intersections is [AKM$^+$01], where the authors aim to give an overview of 4-coverings in a similar manner to the way in which they treat 2- and 3-coverings.

Definition 50 *A quadric intersection (or QI) is a pair of homogeneous equations (Q_1, Q_2) of degree two in four variables. The curve C_4 defined by (Q_1, Q_2) in $\mathbb{P}^3$ is given by*

$$C_4 \colon Q_1(x_1, x_2, x_3, x_4) = Q_2(x_1, x_2, x_3, x_4) = 0.$$

We will say C_4 is integral if it has integer coefficients and we will denote by $C_4(K)$ the set of K-rational points on C_4. As we saw at the end of the previous section, these objects have 20 coefficients a_{ij}, b_{ij} for $i, j \in \{1, 2, 3, 4\}$ and $i \leq j$. They can often be more easily managed in the form of two 4×4 symmetric matrices

$$(x_1, x_2, x_3, x_4)^T V_1(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4)^T V_2(x_1, x_2, x_3, x_4) = 0,$$

for

$$V_1 = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} & a_{14} \\ a_{12} & 2a_{22} & a_{23} & a_{24} \\ a_{13} & a_{23} & 2a_{33} & a_{34} \\ a_{14} & a_{24} & a_{34} & 2a_{44} \end{pmatrix}, \qquad V_2 = \begin{pmatrix} 2b_{11} & b_{12} & b_{13} & b_{14} \\ b_{12} & 2b_{22} & b_{23} & b_{24} \\ b_{13} & b_{23} & 2b_{33} & b_{34} \\ b_{14} & b_{24} & b_{34} & 2b_{44} \end{pmatrix}.$$

Note that the matrices V_1 and V_2 only define the QI with coefficients in a ring $\mathcal{R}$ if $\mathrm{char}(\mathcal{R}) \neq 2$. For convenience, if we wish to specify the equations involved, we may write the QI as (Q_1, Q_2) or (V_1, V_2) interchangeably.

There are two actions on the space of QIs; the first by GL_2 to move through the pencil of quadrics and the second by GL_4 to change co-ordinates.

Definition 51 *Given a QI over a ring $\mathcal{R}$ given by matrices (V_1, V_2),*

$$S(V_1, V_2) = (aV_1 + bV_2, cV_1 + dV_2), \quad \textit{for } S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{R})$$

$$\textit{and } M(V_1, V_2) = (M^T V_1 M, M^T V_2 M), \quad \textit{for } M \in \mathrm{GL}_4(\mathcal{R}).$$

We usually amalgamate these into one transformation, so for $S \in \mathrm{GL}_2(\mathcal{R})$ and $M \in \mathrm{GL}_4(\mathcal{R})$, the transformation $t =< S, M >$ acts on C_4 by giving the curve $t(C_4)$ defined by

$$t(Q_1, Q_2) = t(V_1, V_2) = S(M(V_1, V_2)).$$

Let $a_{ij}^{(M)}$, $b_{ij}^{(M)}$ be the coefficients of $M(Q_1, Q_2)$ and similarly for the action of S or even of the transformation $t =< S, M >$. We say that two 4-coverings are K-equivalent if they are related by such a transformation t defined over K. Given the GL_4 action, it now makes sense to change co-ordinates to ensure that if our QI contains a point, then it is at $(1\colon 0\colon 0\colon 0)$, which will be useful in later sections. Now, the underlying 2-covering (in $(1\colon 2\colon 1)$-weighted projective space) is given by

$$C_2\colon y^2 = g(x, z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4 = \det(V_1 x + V_2 z), \qquad (10)$$

the coefficients of which are invariant under the action of SL_4 on the QI. Note that this is not a generalised binary quartic, but these will come into play in section 3.5.2. In general, we have the following definition of an invariant.

Definition 52 *An invariant of C_4 (with coefficients a_{ij}, b_{ij}) of weight w and degree n is a homogeneous polynomial f of degree n such that*

$$f(a_{ij}^{(t)}, b_{ij}^{(t)}) = \det(S)^w \det(M)^w f(a_{ij}, b_{ij}),$$

for all $t =< S, M >$ with $S \in \mathrm{GL}_2(K), M \in \mathrm{GL}_4(K)$.

The only expressions which remain invariant under this definition are those which are polynomials in I and J (as defined in section 2.2, but now in terms of the coefficients of the QI via equation (10)). In fact, for a general transformation $t =< S, M >$ acting on C_4, the discriminant becomes $\det(S)^{12} \det(M)^{12} \Delta(C_4)$. This means that working over $\mathbb{Q}$, t only acts on minimal 4-coverings if $\det(S) \det(M) = \pm 1$.

Then we have the following definition of a covariant of a QI.

Definition 53 *Fix $R = (x_1 : x_2 : x_3 : x_4)$. A covariant of weight w of a QI given by (Q_1, Q_2) is a polynomial N such that*

$$N(a_{ij}^{(M)}, b_{ij}^{(M)}, R) = \det(M)^w N(a_{ij}, b_{ij}, M(R)), \tag{11}$$

for all $M \in \mathrm{GL}_4(K)$.

This allows us to introduce two important examples.

Definition 54 *Let (V_1, V_2) be the matrices defining a QI and let $\det(V_1 x + V_2 z) = ax^4 + bx^3 z + cx^2 z^2 + dxz^3 + ez^4$. The two 4×4 matrices U_1 and U_2 in the following equation*

$$\mathrm{adj}(\mathrm{adj}(V_1)x + \mathrm{adj}(V_2)z) = a^2 V_1 x^3 + ax^2 z U_1 + exz^2 U_2 + e^2 V_2 z^3 \tag{12}$$

define the two covariant quadratic forms

$$T_i(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4)^T U_i (x_1, x_2, x_3, x_4),$$

for $i \in \{1, 2\}$.

To check that these are indeed covariants and that they are of weight 2, we replace V_1 and V_2 in equation (12) by $M^T V_1 M$ and $M^T V_2 M$, and U_1 and U_2 are now given in terms of the coefficients $a_{ij}^{(M)}$, $b_{ij}^{(M)}$. Note also that a and e are replaced

by $\det(M)^4 a$ and $\det(M)^4 e$. Some calculation then gives us an expression like equation (11) with $w = 2$, so they are indeed covariants.

Another lengthy calculation (see [AKM$^+$01]) then shows that for $\mathcal{H} = \frac{\partial(Q_1,Q_2,T_1,T_2)}{\partial(x_1,x_2,x_3,x_4)}$ (a covariant of weight 5), we have the following syzygy whenever $Q_1 = Q_2 = 0$.

$$\mathcal{H}^2 = aT_1^4 - bT_1^3T_2 + cT_1^2T_2^2 - dT_1T_2^3 + eT_2^4.$$

Comparing this with (10), we have the map

$$\begin{aligned} \phi\colon C_4 &\longrightarrow C_2 \\ (x_1 : x_2 : x_3 : x_4) &\longmapsto (T_1, \mathcal{H}, -T_2) \end{aligned} \tag{13}$$

and therefore the following diagram

$$\begin{array}{ccc} C_4 & \hookrightarrow & \mathbb{P}^3 \\ {\scriptstyle\phi}\downarrow & & \\ C_2 & \xrightarrow{x} & \mathbb{P}^1 \\ {\scriptstyle\pi}\downarrow & & \\ E & \xrightarrow{x} & \mathbb{P}^1 \end{array}$$

Here π is the usual 2-covering map and x refers to taking the x co-ordinate of a point on E or C_2. It is then a fact that $\pi \circ \phi$ is the required 4-covering map.

Now recall that a general action on the 2-covering is given by $< \lambda, A >$ for $\lambda \in K^*$ and $A \in \mathrm{GL}_2(K)$. We have the following lemma.

Lemma 55 *Let (V_1, V_2) be a QI over K and $g(x, z)$ be its underlying binary quartic as described above. Also let $M \in \mathrm{GL}_4(K)$, $S \in \mathrm{GL}_2(K)$ and $t =< S, M >$. Then the underlying binary quartic of $t(V_1, V_2)$ is given by $s(g(x, z))$ for s the transformation $< \det(M), S^T >$.*

Proof : For $M \in \mathrm{GL}_4(K)$, the underlying binary quartic is given by

$$\begin{aligned}\det(M^T V_1 M x + M^T V_2 M z) &= \det(M^T (V_1 x + V_2 z) M) \\ &= \det(M)^2 \det(V_1 x + V_2 z) \\ &= \det(M)^2 g(x, z).\end{aligned}$$

The underlying binary quartic for $S(V_1, V_2)$ is given by

$$\det((aV_1 + bV_2)x + (cV_1 + dV_2)z) = \det((ax + cz)V_1 + (bx + dz)V_2),$$

so the effect is to replace $\begin{pmatrix} x \\ z \end{pmatrix}$ with $S^T \begin{pmatrix} x \\ z \end{pmatrix}$, i.e. the effect of the transformation t is to act by $< \det(M), S^T >$ on the underlying binary quartic.

□

Definition 56 *A 4-covering C_4 is said to be minimal at p if $v_p(\Delta(C_4))$ is minimal amongst all integral 4-coverings $\mathbb{Q}_p$-equivalent to C_4.*

In particular, this means that if C_4 is minimal at p, then $\overline{C}_4$ is a curve. The paper [CFS09] is the culmination of a collection of papers by the authors (often individually) and gives a complete treatment of the minimisation and reduction of both binary quartics and QIs.

The reduction process tries to get the 4-covering as near as possible to being a Hesse form with small coefficients (over $\mathbb{R}$); i.e. one of the form $a(x_0^2 + x_2^2) + bx_1x_3 = a(x_1^2 + x_3^2) + bx_0x_2 = 0$ for $a, b \in \mathbb{C}$. As in the case of 2-coverings, this amounts to reducing a lattice. The following lemma will show that having a point on C_4 which is a root of the covariants means that C_4 is singular.

Lemma 57 *Let C_4 be a 4-covering with equations given by (Q_1, Q_2) and let T_1 and T_2 be the covariants defined above. If we have*

$$Q_1(R) = Q_2(R) = T_1(R) = T_2(R) = 0,$$

for some point $R \in C_4$, then the discriminant $\Delta(C_4) = 0$.

Proof : Since T_1 and T_2 are covariants, let us first assume that $R = (1 : 0 : 0 : 0)$, which we can do by an SL_4 transformation (that does not affect Δ). By an SL_2

transformation, we may assume $a_{14} = 0$, say. Then by further transformations on x_2, x_3 and x_4, we may also assume that $a_{12} = b_{12} = 0$ and a final SL_2 transformation ensures $b_{13} = 0$, so we have matrices for C_4 in the following form:

$$V_1 = \begin{pmatrix} 0 & 0 & a_{13} & 0 \\ 0 & 2a_{22} & a_{23} & a_{24} \\ a_{13} & a_{23} & 2a_{33} & a_{34} \\ 0 & a_{24} & a_{34} & 2a_{44} \end{pmatrix}, \qquad V_2 = \begin{pmatrix} 0 & 0 & 0 & b_{14} \\ 0 & 2b_{22} & b_{23} & b_{24} \\ 0 & b_{23} & 2b_{33} & b_{34} \\ b_{14} & b_{24} & b_{34} & 2b_{44} \end{pmatrix}.$$

Some calculation then shows that the leading coefficients of T_1 and T_2 are given by $a_{13}^2 b_{14}^2 b_{22}$ and $a_{13}^2 b_{14}^2 a_{22}$ respectively. Since $T_1(R) = T_2(R) = 0$, we have at least one of the following three possibilities; either $a_{13} = 0$, $b_{14} = 0$ or $a_{22} = b_{22} = 0$. From equation (10), we know that in our case a_{13} divides the first column of the matrix V_1, so it divides a and (since $b_{11} = 0$) b in the two covering. Similarly b_{14} divides d and (since $a_{11} = 0$) e. Then, by considering the equations for the invariants (equation (6)), we can see that if either were 0, then $\Delta = 0$. For the other case, if we assume $a_{13} = b_{14} = 1$ and $a_{22} = b_{22} = 0$, then the invariants are given by $2^4 I = ((a_{23} - b_{24})^2 + 4a_{24}b_{23})^2$ and $2^5 J = -((a_{23} - b_{24})^2 + 4a_{24}b_{23})^3$, so $\Delta = \frac{1}{27}(4I^3 - J^2) = 0$ and the lemma is proved.

□

Indeed this proof shows not only that $\Delta = 0$, but also that C_4 contains either the line $\{x_3 = x_4 = 0\}$ or the singular point R.

3.3 Reduction Diagrams

In this section, we will assume our QI is defined over $\mathbb{Z}_p$. If we suppose E has bad reduction at some prime p, then $\overline{C}_4$ is singular and it will be useful to know its structure over $\mathbb{F}_p$.

Definition 58 *A point $P \in \overline{C}_4$ is singular if and only if the matrix given by*

$$\mathcal{J}(P) = \frac{\partial(\overline{Q}_1, \overline{Q}_2)}{\partial(x_1, x_2, x_3, x_4)}(P)$$

has rank at most 1 over $\mathbb{F}_p$.

To gain a more intuitive grasp of these points, suppose $P = (1 : 0 : 0 : 0) \in \overline{C}_4$ is singular, so the leading coefficients of Q_1 and Q_2 are both divisible by p. By a

change of co-ordinates (not involving x_1), we may assume $p \mid a_{12}, a_{13}$ and then $\mathcal{J}(P)$ looks like

$$\begin{pmatrix} 0 & 0 & 0 & a_{14} \\ 0 & b_{12} & b_{13} & b_{14} \end{pmatrix}$$

over $\mathbb{F}_p$. So for this to have rank at most 1, we would need $p \mid b_{12}$ and $p \mid b_{13}$ or we would need $p \mid a_{14}$. Either way (by an $\mathrm{SL}_2(\mathbb{F}_p)$ transformation if necessary) we can write the matrices for $\overline{C}_4$ in the form

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2a_{22} & a_{23} & a_{24} \\ 0 & a_{23} & 2a_{33} & a_{34} \\ 0 & a_{24} & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & b_{12} & b_{13} & b_{14} \\ b_{12} & 2b_{22} & b_{23} & b_{24} \\ b_{13} & b_{23} & 2b_{33} & b_{34} \\ b_{14} & b_{24} & b_{34} & 2b_{44} \end{pmatrix}.$$

Definition 59 *Let $P = (1 : 0 : 0 : 0) \in \overline{C}_4(\mathbb{F}_p)$ be a singular point. Then P is a non-regular point if we can write the matrices for $\overline{C}_4$ in the above form with $p^2 \mid a_{11}$.*

The curve $\overline{C}_4$ could contain more than one singular point over $\mathbb{F}_p$, in which case it can be viewed as a number of irreducible components.

Definition 60 *A component Γ is a smooth (or multiplicity 1) component if it contains only a finite number of singular points over $\overline{\mathbb{F}}_p$.*

We only ever have a finite number of non-regular points; in fact at most 4.

Definition 61 *The degree $\mathrm{d}(\Gamma)$ of a component Γ is the number of its points of intersection with a generic hyperplane.*

A component of degree 1 is a line $L \subset \mathbb{P}^3(\mathbb{F}_p)$ given by two linear equations

$$l_1x_1 + l_2x_2 + l_3x_3 + l_4x_4 = l_5x_1 + l_6x_2 + l_7x_3 + l_8x_4 = 0.$$

Up to permutation of co-ordinates, this can be rewritten as

$$m_1x_1 + m_2x_2 + x_3 = m_3x_1 + m_4x_2 + x_4 = 0,$$

so by a change of co-ordinates, we may assume it is given by $L = \{x_3 = x_4 = 0\}$. If $L \subset \overline{C}_4$, then we need $\overline{Q}_1(x_1, x_2, 0, 0) \equiv \overline{Q}_2(x_1, x_2, 0, 0) \equiv 0$ for all x_1, x_2, so $\overline{C}_4$

can be written as

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & a_{13} & a_{14} \\ 0 & 0 & a_{23} & a_{24} \\ a_{13} & a_{23} & 2a_{33} & a_{34} \\ a_{14} & a_{24} & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & 0 & b_{13} & b_{14} \\ 0 & 0 & b_{23} & b_{24} \\ b_{13} & b_{23} & 2b_{33} & b_{34} \\ b_{14} & b_{24} & b_{34} & 2b_{44} \end{pmatrix}.$$

A component of degree two is a conic $C \subset \mathbb{P}^3(\mathbb{F}_p)$ given by a linear and a degree two equation which, by a change of coordinates, can be written as

$$x_1 = f(x_2, x_3, x_4) = 0,$$

for some quadratic form f. If f has rank less than 3, then we refer to C as a 'degenerate' conic. If $C \subset \overline{C}_4$, then we can write $\overline{V}_1$ as

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{12} & 0 & 0 & 0 \\ a_{13} & 0 & 0 & 0 \\ a_{14} & 0 & 0 & 0 \end{pmatrix}$$

and $\overline{Q}_2$ is given by $x_1 l(x_2, x_3, x_4) + f(x_2, x_3, x_4)$ for some linear form l. The reduction $\overline{C}_4$ can contain components of degree three or four (a twisted cubic or a singular quartic), but their matrix forms do not simplify nicely.

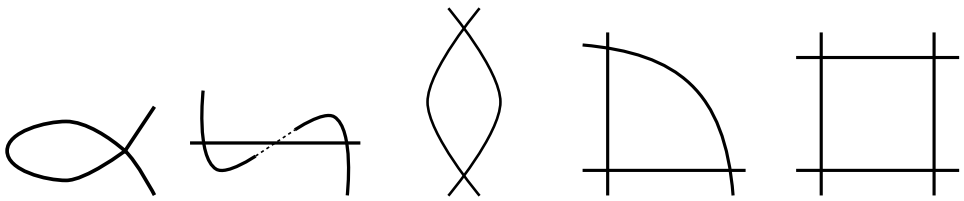
There are a finite number of possibilities for describing the components of $\overline{C}_4$ [21]. A complete classification of singular QIs is given in [HP94] (see also [DLLP08] for a very readable modern classification) containing fourteen different combinations of lines, conics and components of higher degree, distinguishing between cases where there are a different number of intersection points between the components.

We will now mention the special case of multiplicative reduction. In many ways split multiplicative reduction is the most interesting form of reduction, since the component group $E(K)/E^0(K)$ (studied in a computational setting in [Cre08]) is largest[22]. Some calculation shows that if $\overline{C}_4$ contains a singular (multiplicity

[21] If we were to suitably define the multiplicity $m(\Gamma)$ of a component, then an application of Bezout's Theorem can show we must have $\sum_\Gamma d(\Gamma)m(\Gamma) = 4$, giving a finite number of possibilities.

[22] It is isomorphic to $\mathbb{Z}/N\mathbb{Z}$, whereas for other reduction types, the group has order at most 4.

> 1) line or conic, then p divides both of the invariants I and J, so we have additive reduction. Therefore the classification of possible combinations for multiplicative reduction is much shorter, since all the components are smooth. Furthermore, all the singular points are nodes, so none of the components meet tangentially. Now we have the following five possibilities[23]:



Quartic. Cubic, line. Two conics. Conic, two lines. Four lines.

Eventually, these will form five different vertices in a graph of equivalence classes, but first let us discover how to bound heights on 4-coverings.

3.4 Bounding Heights on Four Coverings

Let us reiterate the definition of height from section 1.2.

Definition 62 *Let the point P be given by $(x_1 : x_2 : x_3 : x_4) \in \mathbb{P}^3(\mathbb{Q})$. Then the height of P is defined as the product of local contributions from the finite places and ∞, i.e.*

$$H(P) = \prod_{p \in M_{\mathbb{Q}}} \max(|x_1|_p, |x_2|_p, |x_3|_p, |x_4|_p).$$

Using the diagram from section 3.2 to calculate the height difference, we will now show how a naive approach to a bound between the height on E and the height on the 4-covering can be achieved via the theory of resultants.

3.4.1 A Bound Using Resultants

Lemma 63 *For ϕ the 4-to-2-covering map in equation (13) and any $R = (x_1 : x_2 : x_3 : x_4) \in C_4(\mathbb{Q})$, we can find (using the theory of resultants) a constant β such that*

$$H(\phi(R)) \geq \beta H(R)^2.$$

[23]For reduction type I_n, the special fibre of the minimal proper regular model can be viewed as an n-gon (see Corollary 15.2.1 in [Sil09]). Here some of the components are contained above the singular points, which give us the five possibilities.

Proof : Recall the definition of the 4-covering map in section 3.2, let (Q_1, Q_2) be the equations for C_4 and let R be scaled so that the co-ordinates are coprime integers. Now, there exist polynomials f_1, f_2, f_3 and f_4 of degree 3 such that

$$|f_1(\underline{x})Q_1(\underline{x}) + f_2(\underline{x})Q_2(\underline{x}) + f_3(\underline{x})T_1(\underline{x}) + f_4(\underline{x})T_2(\underline{x})| = c|x_l|^5,$$

for c the resultant of Q_1, Q_2, T_1 and T_2 (the f_i depend on the choice of co-ordinate, so we have an equation like this for each $l \in \{1, 2, 3, 4\}$; see section 1.4.1). This means that if $T_1(R)$ and $T_2(R)$ have a common factor for some point on C_4, then this would divide $\gcd(cx_1^5, cx_2^5, cx_3^5, cx_4^5) = c$ and so we have

$$cH(\phi(R)) \geq \max(|T_1(R)|, |T_2(R)|) = \max(|T_1(R)|, |T_2(R)|, |Q_1(R)|, |Q_2(R)|)$$

and

$$\max(|T_1(R)|, |T_2(R)|, |Q_1(R)|, |Q_2(R)|) \max(|f_1(R) \pm f_2(R) \pm f_3(R) \pm f_4(R)|) \geq c|x_l(R)|^5,$$

where the second maximum is over all combinations of $\pm$. So

$$H(\phi(R)) \geq \frac{|x_l(R)|^5}{\max(|f_1(R) \pm f_2(R) \pm f_3(R) \pm f_4(R)|)}$$

and if $q_m(R) = \sum_{i,j,k \in \{1,2,3,4\}} q_{mijk} x_i x_j x_k$ is one of the polynomials $f_1(R) \pm f_2(R) \pm f_3(R) \pm f_4(R)$, then

$$|q_m(R)| \leq \sum_{i,j,k} |q_{mijk}||x_i x_j x_k| \leq \max(|x_1|, |x_2|, |x_3|, |x_4|)^3 \sum_{i,j,k} |q_{mijk}| = H(R)^3 s(q_m),$$

for $s(q_m)$ the function summing the coefficients of the polynomial $q_m(R)$. Therefore

$$\max_m(|q_m(R)|) \leq H(R)^3 \max_m(s(q_m)) = H(R)^3 M,$$

for some $M > 0$ and we have (for $i = 1$ to 4)

$$\begin{aligned} H(\phi(R)) &\geq \frac{|x_l|^5}{MH(R)^3} && \text{for each } l \\ &\geq \frac{H(R)^2}{M} \\ &\geq \beta H(R)^2. \end{aligned}$$

□

We will show an example of a bound using the resultant method in section 3.7.

3.4.2 The Natural Analogue of ε_p

Recall the definition of ε_p used in the sections on 2-coverings, which we will now refer to as:

$$\varepsilon_p^{(2)}(C_2) = \inf_{(x:y:z)\in C_2(\mathbb{Q}_p)} \left(\frac{\max(|4G(x,z)|_p, |\widetilde{G}(x,z)|_p)}{\max(|x|_p, |z|_p)^4} \right),$$

for C_2 defining a generalised binary quartic and G and $\widetilde{G}$ given in section 2.2.1. Now let us define a new quantity.

Definition 64

$$\varepsilon_p^{(4)}(C_4) = \inf_{R\in C_4(\mathbb{Q}_p)} \left(\frac{\max(|T_1(R)|_p, |T_2(R)|_p)}{\max_i(|x_i|_p^2)} \right),$$

for the covariants T_1 and T_2.

This provides us with a bound for the height difference between a point on a 4-covering and its image on the elliptic curve.

Lemma 65 *The infimum in the definition for $\varepsilon_p^{(4)}$ exists and is non-zero.*

Proof : Let us consider four compact subsets:

$$H_{p,i} = \{(x_1 : x_2 : x_3 : x_4) \in \mathbb{P}^3(\mathbb{Q}_p) \colon |x_i|_p = 1, |x_j|_p \leq |x_i|_p \text{ for all } j\}.$$

These are compact, since they are isomorphic to $\mathbb{Z}_p^3$. This allows us to define four infima,

$$e_{p,i} = \inf_{R\in H_{p,i}} \max(|T_1(R)|_p, |T_2(R)|_p).$$

Now, if the infimum in the definition of $\varepsilon_p^{(4)}$ is 0, then $\min_i(e_{p,i}) = 0$. Assuming $e_{p,i} = 0$ for some i, then in a similar way to the proof of Lemma 37 we have $T_1(R) = T_2(R) = Q_1(R) = Q_2(R) = 0$ for some $R \in \mathbb{P}^3(\mathbb{Q}_p)$, which in turn would imply C_4 is singular by Lemma 57, so we are done.

□

Lemma 66 *For a fixed $R = (x_1 : x_2 : x_3 : x_4) \in C_4(\mathbb{Q})$ and C_2 the underlying 2-covering, we have*

$$h(R) - \frac{1}{8}h_{\pi\phi}(R) \leq -\frac{1}{2}\sum_p \log \varepsilon_p^{(4)}(C_4) - \frac{1}{8}\sum_p \log \varepsilon_p^{(2)}(C_2), \tag{14}$$

with the sums taken over all primes and ∞.

Proof : Treating $\phi(R)$ as a point on a 2-covering, we have

$$\begin{aligned} H(\pi(\phi(R))) &\geq H(\phi(R))^4 \prod_p \varepsilon_p^{(2)}(C_2) \\ &= \left(\prod_p \varepsilon_p^{(2)}(C_2)\right) \prod_p \max(|T_1(R)|_p, |T_2(R)|_p)^4 \\ &\geq \prod_p \varepsilon_p^{(2)}(C_2)(\varepsilon_p^{(4)}(C_4))^4 \quad \max(|x_1|_p^2, |x_2|_p^2, |x_3|_p^2, |x_4|_p^2)^4 \\ &= H(R)^8 \prod_p \varepsilon_p^{(2)}(C_2)(\varepsilon_p^{(4)}(C_4))^4, \end{aligned}$$

which together with Lemma 65 gives us the result by taking logs.

□

3.4.3 The Infinite Place

Now, taking p to be ∞,

$$\varepsilon_\infty^{(4)}(C_4) = \inf_{R \in C_4(\mathbb{R})} \left(\frac{\max(|T_1(R)|, |T_2(R)|)}{\max_i(|x_i(R)|^2)} \right).$$

Without loss of generality, let us assume $x_4 = 1$ gives the largest $|x_i|$ for a given point $R = (x_1 : x_2 : x_3 : 1)$ and let $T(R) = \max(|T_1(R)|, |T_2(R)|)$. Then we are looking for the infimum of the function $T(R)$ on the curve given by $Q_1(R) = Q_2(R) = 0$. So we have the following Lagrangian to solve:

$$\mathcal{L} = T - \lambda_1 Q_1 - \lambda_2 Q_2.$$

Using $\frac{\partial \mathcal{L}}{\partial x_i} = \frac{\partial \mathcal{L}}{\partial \lambda_j} = 0$ for $i \in \{1, 2, 3\}$, $j \in \{1, 2\}$, we can solve for λ_1 and λ_2 in the first three equations and substitute back in to the others. Some rearrangement gives:

$$Q_1(R) = Q_2(R) = \frac{\partial(Q_1, Q_2, T)}{\partial(x_1, x_2, x_3)}(R) = 0.$$

This only fails when T is not differentiable at R or when R lies on the boundary of the box $|x_i| \leq 1$ for $i \in \{1, 2, 3\}$. Note that if one component of C_4 lies completely within the box, then it must have a turning point and so it will be counted. Therefore in order to find the infimum, we must include some exceptional points, i.e. we are finding all solutions in $\mathbb{R}^3$ with co-ordinates ≤ 1 to

$$\begin{aligned} Q_1(R) = Q_2(R) = 0 \text{ and either } & \frac{\partial(Q_1, Q_2, T)}{\partial(x_1, x_2, x_3)}(R) = 0, \\ \text{or } & T_1(R) \pm T_2(R) = 0, \\ \text{or } & x_i = 1 \qquad \text{for } i \in \{1, 2, 3\}. \end{aligned}$$

Lemma 67 *The above system of equations has only a finite number of solutions for $R \in \mathbb{R}^3$ with all co-ordinates ≤ 1.*

Proof : Firstly note that we are done if we can show that we only have a finite number of solutions over $\mathbb{C}^3$ to

$$\begin{aligned} Q_1(R) = Q_2(R) = 0 \text{ and either } & \frac{\partial(Q_1, Q_2, T_1)}{\partial(x_1, x_2, x_3)}(R) = 0, \\ \text{or } & \frac{\partial(Q_1, Q_2, T_2)}{\partial(x_1, x_2, x_3)}(R) = 0, \\ \text{or } & T_1(R) \pm T_2(R) = 0, \\ \text{or } & x_i = 1 \qquad \text{for } i \in \{1, 2, 3\}. \end{aligned}$$

To prove this, we will need Lemma 57 and the following lemma.

Lemma 68 *For a hyperplane H and a 4-covering C_4, the intersection of C_4 with H contains a finite number of points.*

Proof : This is a consequence of Bezout's Theorem (see p47 of [Har77]), which states that two plane curves (in our case $Q_1 \cap H$ and $Q_2 \cap H$) without a common component (which these do not, else C_4 would be singular) have as many solutions over $\mathbb{C}$ as the product of their degrees.

□

Tackling the last set of equations first, we have the hyperplane $H = \{x_i = 1\}$ intersecting the curve given by $Q_1(R) = Q_2(R) = 0$, so this has a finite number of points by Lemma 68.

For the other equations, since T_1 and T_2 are covariants, we may act by transformations and may assume[24] that Q_1 and Q_2 are given projectively by

$$b(x_1^2 + x_3^2) + x_2x_4 = b(x_2^2 + x_4^2) + x_1x_3 = 0,$$

for some non-zero $b \in \mathbb{C}$. Some calculation then shows that

$$\begin{aligned} T_1 =& b(x_2^2 + x_4^2) + 16b^4x_1x_3, \\ T_2 =& b(x_1^2 + x_3^2) + 16b^4x_2x_4. \end{aligned}$$

Now we pass back to affine co-ordinates by letting $x_4 = 1$. We can substitute $x_2 = -b(x_1^2 + x_3^2)$ into the equation for Q_2 and also into each of the four equations $\frac{\partial(Q_1,Q_2,T_1)}{\partial(x_1,x_2,x_3)}$, $\frac{\partial(Q_1,Q_2,T_2)}{\partial(x_1,x_2,x_3)}$, T_1+T_2 and T_1-T_2 respectively, which gives us the following four sets of equations:

$$\begin{aligned} b^3(x_1^2 + x_3^2)^2 + x_1x_3 + b =& 8b^3(1 - 16b^4)(x_1^4 - x_3^4) = 0, \\ b^3(x_1^2 + x_3^2)^2 + x_1x_3 + b =& 2b(1 - 16b^4)(x_1^2 - x_3^2) = 0, \\ b^3(x_1^2 + x_3^2)^2 + x_1x_3 + b =& b^3(x_1^2 + x_3^2)^2 + 16b^4x_1x_3 + b + b(16b^4 - 1)(x_1^2 + x_3^2) = 0, \\ b^3(x_1^2 + x_3^2)^2 + x_1x_3 + b =& b^3(x_1^2 + x_3^2)^2 + 16b^4x_1x_3 + b + b(1 - 16b^4)(x_1^2 + x_3^2) = 0. \end{aligned}$$

If we assume $16b^4 \neq 1$, then we can get $x_1^2 = \pm x_3^2$ in the first two sets of equations, which is a collection of hyperplanes and this yields a finite number of points by Lemma 68. The remaining sets reduce to

$$\begin{aligned} b^3(x_1^2 + x_3^2)^2 + x_1x_3 + b =& x_1x_3 + b(x_1^2 + x_3^2) = 0, \\ b^3(x_1^2 + x_3^2)^2 + x_1x_3 + b =& x_1x_3 - b(x_1^2 + x_3^2) = 0. \end{aligned}$$

By substituting $b^2(x_1^2 + x_3^2)^2 = x_1^2x_3^2$ into the left hand equation, we see that these are solved whenever $bx_1^2x_3^2 + x_1x_3 + b = 0$, so substituting $x_1 = \frac{1}{2bx_3}(-1 \pm \sqrt{b-4})$ into $x_1x_3 - b(x_1^2 + x_3^2) = 0$ say, gives at most 4 solutions for x_3 and therefore a finite set of solutions for R.

Here, the discriminant of C_4 is given by $b^4(16b^4 - 1)^4$, so if $16b^4 = 1$ then C_4 is singular, so the lemma is proved.

□

[24] See p28 of [Hul86] for how to attain this form.

Once Gröbner bases have been called upon, solving a system of three equations like this is simply a case of finding the roots of various univariate polynomials. Having found these solutions when we set $x_4 = 1$, we also need to solve a system of equations for each of $x_1 = 1$, $x_2 = 1$ and $x_3 = 1$ and find the infimum of these.

Now, let us demonstrate the calculation at the infinite place on a particular example. Consider the elliptic curve given by reference '897f2' in [Cre97]. This has two 4-descendant curves and we will consider the one given by

$$\begin{aligned} Q_1 &= -2x_1x_2 - 2x_1x_4 + x_2^2 - 2x_2x_4 + 4x_3^2 + 2x_3x_4 + x_4^2, \\ Q_2 &= 2x_1x_2 + 2x_1x_3 + 2x_1x_4 - 2x_2x_3 - 2x_2x_4 + x_3^2 - 2x_3x_4 + 2x_4^2. \end{aligned}$$

First we set $x_1 = 1$ in $Q_1, Q_2, T_1 + T_2$ and $T_1 - T_2$ and we calculate $\frac{\partial(Q_1,Q_2,T_1)}{\partial(x_2,x_3,x_4)}$ and $\frac{\partial(Q_1,Q_2,T_2)}{\partial(x_2,x_3,x_4)}$. Then we can calculate the seven ideals $I_l \subset \mathbb{Z}_p[x_2, x_3, x_4]$ given by Q_1, Q_2 and either $T_1 \pm T_2$, $x_i = 1$ or one of the partial derivatives. For example,

$$\begin{aligned} I_1 =< Q_1, Q_2, T_1 + T_2 >=< Q_1, Q_2, 128 + 192x_2 + 384x_3 + 320x_4 + 288x_2^2 \\ - 384x_2x_3 - 576x_2x_4 + 1024x_3^2 - 64x_3x_4 + x_4^2 > . \end{aligned}$$

Then we compute the Gröbner basis of each ideal, which is a basis given by

$$< x_2 + p_1(x_4), x_3 + p_2(x_4), p_3(x_4) >,$$

for polynomials p_1, p_2 and p_3. We find the roots X_i of p_3 and evaluate the polynomials p_1 and p_2 there to give us points $(1, -p_2(X_i), -p_3(X_i), X_i)$ to consider. We discard all points that do not have all values ≤ 1.

After performing this routine on the seven ideals, we have a list of points with $x_1 = 1$ (in our example we get 12 such points). Repeating the process for the affine spaces when $x_2 = 1$, $x_3 = 1$ and $x_4 = 1$ gives us an even larger set of points (in our case 19). Then we find the value of $\max(|T_1(R)|, |T_2(R)|)$ for each R in the list and compute the minimum of these values. This is our desired $\varepsilon_\infty^{(4)}$.

In our case, the minimum is 64 at the root of $(T_1(1, x_2, x_3, x_4) - T_2(1, x_2, x_3, x_4))$ given by $(0, 0, 0)$. Then $\frac{1}{2}\log \varepsilon_\infty^{(4)} = 2.0794...$

Now let us turn our attention to $p < \infty$.

3.5 A New Definition for the Finite Places

When calculating the effect of certain operations (defined later) on $\varepsilon_p^{(4)}(Q_1, Q_2)$, unfortunately we cannot get an exact answer, since the covariants T_1 and T_2 behave differently under these transformations. So, in the search for precision, we are motivated to go back a step and make the following definition (for Q_1 and Q_2 the equations for C_4 with integer coefficients).

Definition 69 *Let $p > 3$ be a prime and $X' \subset C_4(\mathbb{Q}_p)$ be the set of points above $X \subseteq \overline{C}_4(\mathbb{F}_p)$, then define*

$$\begin{aligned}\varepsilon_p(Q_1, Q_2; X) &= \inf_{R \in X'} \left(\frac{\max(\gamma_p(R), \delta_p(R))}{\max(|x_i(R)|_p)^8} \right), \\ \textit{for } \gamma_p(R) &= |4g(T_1(R), T_2(R))|_p, \\ \delta_p(R) &= |3g_4(T_1(R), T_2(R))|_p.\end{aligned}$$

The inputs for this quantity will make it easy to distinguish from the ε_p for $n = 2$. The definition will be extended to $p = 2$ and 3 in the next section, but this uses different γ_p and δ_p. In projective space, we have freedom to choose how we scale a point R, so for this definition to make sense we must fix the co-ordinates of R before we enter them in the equations for T_1 and T_2. Then ε_p is independent of scaling by virtue of the fact that the top and bottom of the infimum are both homogeneous of degree 8. By convention, we also set $\varepsilon_p(Q_1, Q_2; \emptyset) = 1$. This means that if we have $\overline{C}_4(\mathbb{F}_p) = \coprod X_i$ for some finite union of components $\{X_i\}$, then

$$\varepsilon_p(Q_1, Q_2; C_4(\mathbb{Q}_p)) = \min_i \varepsilon_p(Q_1, Q_2; X_i)$$

and we write $\varepsilon_p(Q_1, Q_2)$ for $\varepsilon_p(Q_1, Q_2; C_4(\mathbb{Q}_p))$. By the same argument as in the proof of Theorem 30, this gives us the following bound.

Theorem 70 *For $R \in C_4(\mathbb{Q})$ and $\pi\phi$ the 4-covering map taking C_4 to its Jacobian E_{IJ}, we have*

$$h(R) - \frac{1}{8} h_{\pi\phi}(R) \leq -\frac{1}{8} \sum_p \log \varepsilon_p(Q_1, Q_2).$$

3.5.1 Properties of ε_p.

Still working with $p > 3$, we shall prove some results about this new quantity.

Lemma 71 *For ε_p defined as above, let C_4 be given by (Q_1, Q_2) with integer coefficients and let $X \subseteq \overline{C}_4(\mathbb{F}_p)$ be any subset. Then we have $\varepsilon_p(Q_1, Q_2; X) \leq 1$.*

Proof : From Lemma 37, we have

$$\inf_{P \in C_2(\mathbb{Q}_p)} \left(\frac{\max(|4g(P)|_p, |3g_4(P)|_p)}{\max(|x(P)|_p, |z(P)|_p)^4} \right) \leq 1,$$

since g and g_4 have integer coefficients. We can apply this to $P = (T_1(R), T_2(R)) \in C_2(\mathbb{Q}_p)$, so we are left to check that for a point $R \in C_4(\mathbb{Q}_p)$, we have

$$\frac{\max(|T_1(R)|_p, |T_2(R)|_p)}{\max(|x_1(R)|_p, |x_2(R)|_p, |x_3(R)|_p, |x_4(R)|_p)^2} \leq 1.$$

But this is clear, since if we scale to ensure that the maximum on the bottom is 1, then all the co-ordinates are integers and since the T_i have integer coefficients, the top is an integer and therefore has p-adic absolute value ≤ 1.

□

Lemma 72 *The infimum in the definition for ε_p exists and is non-zero.*

Proof : From Lemma 37, we have

$$0 < \varepsilon_p^{(2)} \leq 1$$

and from Lemma 65, we have

$$0 < \varepsilon_p^{(4)} \leq 1.$$

Since (by considering their definitions) we also have

$$\left(\varepsilon_p^{(4)}\right)^4 \varepsilon_p^{(2)} \leq \varepsilon_p \leq 1,$$

we can deduce that

$$0 < \varepsilon_p \leq 1.$$

□

As we have seen in section 3.3, $\overline{C}_4$ looks like a finite number of components over $\mathbb{F}_p$, so the above notation allows us to consider the contribution from a single component or even from a point.

Definition 73 *A component or point $X \subseteq \overline{C}_4(\mathbb{F}_p)$ is said to contribute to ε_p if*

$$\varepsilon_p(Q_1, Q_2; X) < 1.$$

The following lemma shows us that we are free to adjust our QI by an $\mathrm{SL}_4(\mathbb{Z}_p)$ or $\mathrm{GL}_2(\mathbb{Z}_p)$ transformation before doing calculations. This will mean we can often deal with the point $(1 : 0 : 0 : 0)$, for example, instead of a more complicated point.

Lemma 74 *For a transformation $t \in \mathrm{SL}_4(\mathbb{Z}_p) \times \mathrm{GL}_2(\mathbb{Z}_p)$ (whose action on (Q_1, Q_2) and X has been defined in section 3.2), we have $\varepsilon_p(t(Q_1, Q_2), t(X)) = \varepsilon_p(Q_1, Q_2, X)$.*

Proof : Let $R = (x_1 : x_2 : x_3 : x_4)$ with $\max |x_i|_p = 1$. If we consider two matrices $M_2 \in \mathrm{GL}_2(\mathbb{Z}_p)$ and $M_4 \in \mathrm{SL}_4(\mathbb{Z}_p)$ and act by the transformation $< M_2, M_4 >$ on the QI, then the effect on the underlying binary quartic is to act by $(\det M_4^2, M_2^T) = (1, M_2^T)$. Considering first the $\mathrm{SL}_4(\mathbb{Z}_p)$ action, let $t =< I, M_4 >$. The equations for g and g_4 do not change (see Lemma 55) and since T_1 and T_2 are covariants, we have

$$\begin{aligned}
&\varepsilon_p(t(Q_1, Q_2); t(X)) \\
=&\inf_{R \in t(X): R \in t(C_4)} \max(|4g(M_4T_1(R), M_4T_2(R))|_p, |3g_4(M_4T_1(R), M_4T_2(R))|_p) \\
=&\inf_{R' \in X: R' \in C_4} \max(|4g(T_1(R'), T_2(R'))|_p, |3g_4(T_1(R'), T_2(R'))|_p) \\
=&\varepsilon_p(Q_1, Q_2; X),
\end{aligned}$$

since we still have $\max |x_i'|_p = 1$ for $R' = (x_1' : x_2' : x_3' : x_4')$. For the $\mathrm{GL}_2(\mathbb{Z}_p)$ action, we know that the equations for g and g_4 change by the action of M_2, but Lemma 32 from section 2.3 tells us that this does not have an effect on ε_p. The point R in the infimum does not change if we act by $\mathrm{GL}_2(\mathbb{Z}_p)$, so we can see that ε_p remains unchanged.

□

The following lemma shows us there are only three types of component we need to worry about.

Lemma 75 *If C_4 is minimal, then $\overline{R} \in \overline{C}_4(\mathbb{F}_p)$ contributes to ε_p only if*

1. *$\overline{R}$ is a non-regular point defined over $\mathbb{F}_p$.*
2. *$\overline{R}$ lies on a straight line defined over $\mathbb{F}_p$ that is a component in $\overline{C}_4$.*
3. *$\overline{R}$ lies on a plane conic defined over $\mathbb{F}_p$ that is a component in $\overline{C}_4$.*

Proof: Let $R = (x_1 : x_2 : x_3 : x_4)$ with $\max(|x_i|_p) = 1$. For a contribution we have two cases; we either need $p \mid T_1(R)$ and $p \mid T_2(R)$ or (if we assume $P = (T_1(R) : T_2(R))$ is given by $(1 : 0)$ modulo p, say), then we need some condition on the coefficients of C_4 amounting to $p \mid a$ and $p \mid b$ in the coefficients of g.

If we assume $\overline{R}$ is a singular point, then we are in the first case and $T_1(R) \equiv T_2(R) \equiv 0 \bmod p$. We may assume that $R = (0 : 0 : 0 : 1)$, so

$$Q_1 = p(ax_1 + bx_2 + cx_3 + dx_4)x_4 + f_1(x_1, x_2, x_3),$$
$$Q_2 = \alpha p x_4^2 + f_2(x_1, x_2, x_3, x_4),$$

where the polynomial f_2 has no x_4^2 term and $a, b, c, d, \alpha \in \mathbb{Z}_p$. Now if $p \nmid d$, then looking modulo p^2, we see that $\overline{R}$ does not lift to a point on $C_4(\mathbb{Q}_p)$ and can therefore be ignored. So we only need to consider points where $p^2 \mid a_{44}$, which is precisely the definition of $\overline{R}$ being a non-regular point.

If instead $\overline{R}$ is a smooth point, then it lifts to a $\mathbb{Q}_p$ point (by Hensel's Lemma) and we can then use an $\mathrm{SL}_4(\mathbb{Z}_p)$ transformation to move R to $(0 : 0 : 0 : 1)$. By suitable $\mathrm{SL}_4(\mathbb{Z}_p)$ and $\mathrm{GL}_2(\mathbb{Z}_p)$ transformations we can eliminate a_{24}, a_{34}, b_{14} and b_{34}, say (this is effectively moving the tangent line at R to $\{x_1 = x_2 = 0\}$). Then by scaling each equation (effectively another $\mathrm{GL}_2(\mathbb{Z}_p)$ transformation), we may assume our QI is given by $Q_1 = x_1x_4 + f_1(x_1, x_2, x_3)$ and $Q_2 = x_2x_4 + f_2(x_1, x_2, x_3)$. A calculation shows that the coefficients of x_4^2 in $\overline{T}_1$ and $\overline{T}_2$ are $a_{14}^2 b_{24}^2 b_{33}$ and $a_{14}^2 b_{24}^2 a_{33}$ respectively, i.e. b_{33} and a_{33}. If we are in the first case where $p \mid T_1(R)$ and $p \mid T_2(R)$, this means $a_{33} \equiv b_{33} \equiv 0 \bmod p$. In other words[25], we have the

[25]Note that the argument thus far has been similar to that in the proof of Lemma 57.

matrices

$$\overline{V}_1 = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} & 1 \\ a_{12} & 2a_{22} & a_{23} & 0 \\ a_{13} & a_{23} & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 2b_{11} & b_{12} & b_{13} & 0 \\ b_{12} & 2b_{22} & b_{23} & 1 \\ b_{13} & b_{23} & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

and $\{x_1 = x_2 = 0\}$ is a line on the reduction $\overline{C}_4$.

Now if instead we are in the second case, by considering when $p \mid T_2(R)$, $p \nmid T_1(R)$ and again conducting suitable $\mathrm{GL}_2(\mathbb{Z}_p)$ and $\mathrm{SL}_4(\mathbb{Z}_p)$ transformations, we may assume that Q_1 and Q_2 are represented modulo p by the following matrices:

$$\overline{V}_1 = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} & 1 \\ a_{12} & 2a_{22} & a_{23} & 0 \\ a_{13} & a_{23} & 2a_{33} & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 2b_{11} & b_{12} & b_{13} & 0 \\ b_{12} & 2b_{22} & b_{23} & 1 \\ b_{13} & b_{23} & 2b_{33} & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

where $p \mid a_{33}$, but $p \nmid b_{33}$. Now, recalling what it meant for the point $(1:0)$ to contribute in the $n = 2$ case, some calculation shows:

$$\begin{aligned} g(x,z) &= \det(V_1 x + V_2 z) = ax^4 + bx^3 z + cx^2 z^2 + dxz^3 + ez^4, \\ p \mid a &= 4a_{22}a_{33} - a_{23}^2 \Rightarrow p \mid a_{23}, \\ p \mid b &= 4a_{12}a_{33} - 2a_{13}a_{23} - 4a_{22}b_{33} + 2a_{23}b_{23} - 4a_{33}b_{22}, \\ &\Rightarrow p \mid 4a_{22}b_{33} \Rightarrow p \mid a_{22}, \end{aligned}$$

since we are assuming $p > 3$. In other words we have the following matrices:

$$\overline{V}_1 = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} & 1 \\ a_{12} & 0 & 0 & 0 \\ a_{13} & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 2b_{11} & b_{12} & b_{13} & 0 \\ b_{12} & 2b_{22} & b_{23} & 1 \\ b_{13} & b_{23} & 2b_{33} & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

and $\overline{R}$ lies on the hyperplane $\{x_1 = 0\}$ and the conic given by $b_{22}x_2^2 + b_{23}x_2x_3 + x_2x_4 + b_{33}x_3^2 = 0$.

□

We remark here that if the reduction contains a non-degenerate conic, then we treat this as item 3 in the statement of the lemma, but if we have a degenerate conic, we are free to treat it as item 2 or item 3.

Now we will define three operations which will help us deal with the types of components coming out of the above lemma. As usual, C_4 will have integral equations $Q_1(x_1, x_2, x_3, x_4) = Q_2(x_1, x_2, x_3, x_4) = 0$.

1. First let $L \subset \overline{C}_4$ be a smooth line defined over $\mathbb{F}_p$, then

$$\Phi\colon (Q_1, Q_2, L) \mapsto (Q_3, Q_4),$$

where (Q_3, Q_4) is formed from (Q_1, Q_2) by applying the transformation

$$< \begin{pmatrix} \frac{1}{p} & 0 \\ 0 & \frac{1}{p} \end{pmatrix}, D_1 M_1 > .$$

Here $M_1 \in \mathrm{SL}_4(\mathbb{Z}_p)$ is the transformation which moves the line L to $\{x_3 = x_4 = 0\}$ and

$$D_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix}.$$

Notice that the image always contains the line $\{x_1 = x_2 = 0\}$ and applying Φ to this is the inverse operation and returns us to the original QI.

2. Then for $P \in \overline{C}_4(\mathbb{F}_p)$ a non-regular point,

$$\chi\colon (Q_1, Q_2, P) \mapsto (Q_3, Q_4),$$

where (Q_3, Q_4) is formed using

$$< \begin{pmatrix} \frac{1}{p^2} & 0 \\ 0 & \frac{1}{p} \end{pmatrix} S_2, D_2 M_2 > .$$

Here $M_2 \in \mathrm{SL}_4(\mathbb{Z}_p)$ is the transformation which moves P to $(0\colon 0\colon 0\colon 1)$, $S_2 \in \mathrm{SL}_2(\mathbb{Z}_p)$ is the transformation which ensures we have $p \mid a_{14}, a_{24}, a_{34}$

and

$$D_2 = \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

3. Note that we can now also define another operation which behaves like the inverse of χ, for $C \subset \overline{C}_4$ a conic defined over $\mathbb{F}_p$. We write

$$\chi^{-1} : (Q_1, Q_2, C) \mapsto (Q_3, Q_4),$$

for (Q_3, Q_4) formed using

$$< \begin{pmatrix} \frac{1}{p} & 0 \\ 0 & 1 \end{pmatrix} S_3, D_3 M_3 > .$$

Here $M_3 \in \mathrm{SL}_4(\mathbb{Z}_p)$ is the transformation which moves the conic into the plane $\{x_1 = 0\}$, $S_3 \in \mathrm{SL}_2(\mathbb{Z}_p)$ is the transformation which ensures we have $p \mid b_{22}, b_{23}, b_{24}, b_{33}, b_{34}$ and

$$D_3 = \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that we can choose to operate on a degenerate conic using either Φ (in one of two ways) or χ^{-1}.

These operations also all preserve minimality. We will refer back to the definitions frequently in the following sections.

Lemma 76 *The operation Φ is well defined up to $\mathbb{Z}_p$-equivalence, i.e. if (Q_1, Q_2) and (Q_3, Q_4) are $\mathbb{Z}_p$-equivalent QIs (and this $\mathbb{Z}_p$ transformation modulo p identifies the lines L_1 and L_2 on the respective reductions of the QIs), then $\Phi(Q_1, Q_2, L_1)$ and $\Phi(Q_3, Q_4, L_2)$ are also $\mathbb{Z}_p$-equivalent.*

Proof : Firstly, since the same $\mathrm{GL}_4(\mathbb{Z}_p)$ transformation is used to move the lines L_1 and L_2, we may assume $L_1 = L_2 = \{x_3 = x_4 = 0\}$. Let (V_1, V_2) and (V_3, V_4) be the respective matrix representations for the $\mathbb{Z}_p$-equivalent QIs. We have that for

some matrix $M \in \mathrm{GL}_4(\mathbb{Z}_p)$,

$$V_1 = M^T V_3 M, \quad V_2 = M^T V_4 M.$$

So, by replacing (V_1, V_2) by the transformed QI given by (V_1', V_2') and similarly for (V_3, V_4), we get

$$(D_1^{-1})^T V_1' D_1^{-1} = M^T (D_1^{-1})^T V_3' D_1^{-1} M, \quad (D_1^{-1})^T V_2' D_1^{-1} = M^T (D_1^{-1})^T V_4' D_1^{-1} M,$$

i.e.

$$V_1' = (D_1^{-1} M D_1)^T V_3' (D_1^{-1} M D_1), \quad V_2' = (D_2^{-1} M D_1)^T V_4' (D_1^{-1} M D_1).$$

Now, the matrix M preserves the line $\{x_3 = x_4 = 0\}$, i.e. we can view this as a matrix which preserves $D_1(\mathbb{Z}_p^4)$. Thus M has the form[26]

$$M = D_1 M' D_1^{-1},$$

for some $M' \in \mathrm{GL}_4(\mathbb{Z}_p)$. So we have

$$V_1' = (M')^T V_3' M' \quad \text{and} \quad V_2' = (M')^T V_4' M',$$

which is the required result.

□

We can perform similar proofs to show that the operations χ and χ^{-1} are also well defined up to $\mathbb{Z}_p$-equivalence.

Lemma 77 *1. The operation Φ leaves the underlying binary quartic $g(x, z)$ unchanged.*

2. The operations χ and χ^{-1} 'flip' $g(x, z)$ in the sense of Definition 44 (up to an SL_2 *transformation).*

Proof: Recall Lemma 55 from section 3.2, which gives the rule for how the underlying binary quartic changes for a given transformation $< A, B >$ on the QI. This is by $< \det(B), A^T >$, recalling that the action of the first argument is by multiplication by $\det(B)^2$. Since M_1, M_2 and M_3 in the definitions of the maps

[26] This is a special case of Lemma 4.1 in [CFS09].

have determinant 1, we may assume that $L = \{x_3 = x_4 = 0\}$, that $P = (0\colon 0\colon 0\colon 1)$ and that the conic C is in the plane $\{x_1 = 0\}$. S_2 and S_3 (in the definitions of the maps) act as a translation on the binary quartic, so we only need to consider the actions of the diagonal matrices. The effect on g_4 is the same as that on g, since it is a covariant.

For Φ, the transformation on the binary quartic is $< p^2, \begin{pmatrix} \frac{1}{p} & 0 \\ 0 & \frac{1}{p} \end{pmatrix} >$, so $g(x,z)$ changes to $p^4 g(\frac{1}{p}x, \frac{1}{p}z) = g(x,z)$. For χ we have $< p^3, \begin{pmatrix} \frac{1}{p^2} & 0 \\ 0 & \frac{1}{p} \end{pmatrix} >$ and we get $p^6 g(\frac{1}{p^2}x, \frac{1}{p}z) = p^2 g(\frac{1}{p}x, z)$, i.e. the 'flip' of $g(x,z)$, which is also what we get from the transformation $< p, \begin{pmatrix} \frac{1}{p} & 0 \\ 0 & 1 \end{pmatrix} >$ for χ^{-1}.

□

Now we are ready to put together the following theorem.

Theorem 78 *For a QI given by $C_4 = (Q_1, Q_2)$,*

1. *Let $C_4' = \Phi(Q_1, Q_2, L)$ for $L \subset \overline{C}_4$ a line defined over $\mathbb{F}_p$. Then we have $\varepsilon_p(Q_1, Q_2; L) = p^{-4}\varepsilon_p(C_4'; \overline{C}_4'(\mathbb{F}_p) \setminus L')$, for L' a line defined over $\mathbb{F}_p$ depending on L.*

2. *Let $C_4'' = \chi(Q_1, Q_2, P)$, for $P \in \overline{C}_4(\mathbb{F}_p)$ a non-regular point. Then we have $\varepsilon_p(Q_1, Q_2; P) = p^{-6}\varepsilon_p(C_4''; \overline{C}_4''(\mathbb{F}_p) \setminus C)$, for C a (possibly degenerate) conic defined over $\mathbb{F}_p$ depending on P.*

3. *Let $C_4''' = \chi^{-1}(Q_1, Q_2, C)$, for $C \subset \overline{C}_4$ a (possibly degenerate) conic defined over $\mathbb{F}_p$. Then we have $\varepsilon_p(Q_1, Q_2; C) = p^{-2}\varepsilon_p(C_4'''; \overline{C}_4'''(\mathbb{F}_p) \setminus P)$, for P a non-regular point depending on C.*

Proof: Firstly, since we know that the actions of $\mathrm{SL}_2(\mathbb{Z}_p)$ and $\mathrm{SL}_4(\mathbb{Z}_p)$ do not affect ε_p, we only need to consider the diagonal transformation. Let $R = (x_1\colon x_2\colon x_3\colon x_4)$ be a generic point. Now recall that for a 4×4 matrix M, we have

$$T_i(R, \{a_j^{(M)}\}) = \det(M)^2 T_i(M(R), \{a_j\}),$$

for the a_j running through the coefficients of Q_1 and Q_2 and the $a_j^{(M)}$ running through the coefficients after the application of the matrix M. So now, for the

matrix D_1 from the definition of Φ, we have

$$T_i(R, \{a_j^{(D_1)}\}) = \det(D_1)^2 T_i(D_1(R), \{a_j\}) = p^4 T_i(D_1(R), \{a_j\}).$$

Therefore, for a point on the line $\{x_1 = x_2 = 0\}$, we can take a factor of p from each co-ordinate of R and (because the T_i are quadratic) we get

$$T_i(R, \{a_j^{(D_1)}\}) = p^6 T_i(R', \{a_j\}),$$

for some $R' = (x_1' : x_2' : x_3' : x_4')$ with entries in $\mathbb{Z}_p$ such that $\max |x_i'|_p = 1$ (since we are in projective co-ordinates and therefore x_3 and x_4 are not both 0). Now we have to divide each of the Q_i through by p, which has the effect of dividing the T_i by p^5. So under application of Φ,

$$g(T_1(R), T_2(R)) \longmapsto g(pT_1(R'), pT_2(R')),$$
$$g_4(T_1(R), T_2(R)) \longmapsto g_4(pT_1(R'), pT_2(R'))$$

and so

$$\gamma_p(R) \longmapsto p^{-4}\gamma_p(R'),$$
$$\delta_p(R) \longmapsto p^{-4}\delta_p(R'),$$

for R such that $\overline{R} \in L = \{x_1 = x_2 = 0\}$ and some R' such that $\overline{R}' \in \overline{C}_4' \setminus L' = \overline{C}_4' \setminus \{x_3 = x_4 = 0\}$. If we let $R = (0 : 0 : 0 : 1)$, then $R' = (* : * : 0 : 1)$. By applying the same calculation to L', we obtain the equality

$$\varepsilon_p(Q_1, Q_2; L) = p^{-4}\varepsilon_p(C_4'; \overline{C}_4'(\mathbb{F}_p) \setminus L').$$

For χ it is slightly more complicated, because T_1 and T_2 behave differently. We use the matrix D_2 from the definition of χ and then consider a point R such that $x_4(R) \not\equiv 0$. In a similar way to the above, after dividing both quartics by p, we obtain

$$T_i(R, \{a_j^{(D_2)}/p\}) = pT_i(R', \{a_j\}),$$

for some $R' = (x_1' : x_2' : x_3' : x_4')$ with coefficients in $\mathbb{Z}_p$ such that $|x_4'|_p = 1$. Then, dividing Q_1 by a further p has the effect of dividing T_1 by p^2 and T_2 by p^3. When putting these into the $p^2 g(x/p, z)$ obtained in the previous lemma, $\gamma_p(R)$ becomes $p^6\gamma_p(R')$ and $\delta_p(R)$ becomes $p^6\delta_p(R')$ for R such that $\overline{R} \in \overline{C}_4''(\mathbb{F}_p) \setminus C$ and R' such

that $\overline{R}' = (0\colon 0\colon 0\colon 1)$.

Finally, for χ^{-1} we use D_3 and consider R such that $\overline{R} \not\equiv (1\colon 0\colon 0\colon 0)$. This gives $T_1(R', \{a_j\})$ and $\frac{1}{p}T_2(R', \{a_j\})$, meaning $\gamma_p(R)$ becomes $p^2\gamma_p(R')$ and $\delta_p(R)$ becomes $p^2\delta_p(R')$ for R' a point such that $x_4(R') = 0$. Putting this all together gives us the two equalities

$$\begin{aligned}\varepsilon_p(Q_1, Q_2; P) =& p^{-6}\varepsilon_p(C_4''; \overline{C}_4''(\mathbb{F}_p) \setminus C),\\ \varepsilon_p(Q_1, Q_2; C) =& p^{-2}\varepsilon_p(C_4'''; \overline{C}_4'''(\mathbb{F}_p) \setminus P),\end{aligned}$$

as required.

□

Note that in the statement of the lemma, L', C and P, respectively are the components we would have to operate on to take us back to the original QI. Also, note that we can always read off the contribution to ε_p as $2|\det M|_p$, for M the GL_4 transformation in the relevant operation. This will be made more precise later on.

This now gives us the machinery to calculate ε_p for $p > 3$. On a given QI, we can find all the singular points, lines and conics. Then we can apply the relevant operation, add a multiple of $\log(p)$ to ε_p and investigate the new QI (ignoring the relevant component or point which would send us back). We know there is only a finite number of $\mathbb{Z}_p$-equivalence classes of QIs, so as long as we can tell when we reach a QI that we have considered before, we will be able to calculate the maximum contribution from all points on the original QI. Hence we can compute ε_p. However, before discussing an algorithm in detail, we need to see what happens at $p = 2$ and 3.

3.5.2 The Awkward Primes 2 and 3

Let us generalise to the remaining finite places, recalling that we need to use different formulae for the 2-covering map. Hence, for $R \in C_4(\mathbb{Q}_p)$ and $p = 2$ or 3, define

$$\begin{aligned}\gamma_p(R) =& |4G(T_1(R), T_2(R))|_p,\\ \delta_p(R) =& |\widetilde{G}(T_1(R), T_2(R))|_p,\end{aligned}$$

where we recall G and $\widetilde{G}$ from section 2.2.1.

$$\begin{aligned}
G(x,z) =& \frac{1}{4}(\alpha_0 x^2 + \alpha_1 xz + \alpha_2 z^2)^2 + a_2 x^4 + b_2 x^3 z + c_2 x^2 z^2 + d_2 x z^3 + e_2 z^4, \\
\widetilde{G}(x,z) =& (b_2^2 - 4a_2c_2 - \alpha_0^2 c_2 + \alpha_0\alpha_1 b_2 - \alpha_1^2 a_2)x^4 + \\
& (-8a_2d_2 - 2\alpha_0^2 d_2 - 2\alpha_0\alpha_2 b_2 - 4\alpha_1\alpha_2 a_2)x^3 z + \\
& (-16a_2e_2 - 2b_2d_2 - 4\alpha_0^2 e_2 - \alpha_0\alpha_1 d_2 + 2\alpha_0\alpha_2 c_2 - \alpha_1\alpha_2 b_2 - 4\alpha_2^2 a_2)x^2 z^2 + \\
& (-8b_2e_2 - 2\alpha_2^2 b_2 - 2\alpha_0\alpha_2 d_2 - 4\alpha_0\alpha_1 e_2)x z^3 + \\
& (d_2^2 - 4c_2e_2 - \alpha_2^2 c + \alpha_1\alpha_2 d_2 - \alpha_1^2 e_2)z^4.
\end{aligned}$$

Here $a_2, b_2, c_2, d_2, e_2, \alpha_0, \alpha_1$ and α_2 now have expressions in terms of the coefficients of (Q_1, Q_2) and are integers. We calculate them following ideas of [CFS09] and modifying equation (10). The expressions for the first five are complicated, but the cross terms are quite manageable:

$$\begin{aligned}
\alpha_0 =& a_{12}a_{34} + a_{13}a_{24} + a_{14}a_{23}, \\
\alpha_1 =& a_{12}b_{34} + a_{13}b_{24} + a_{14}b_{23} + b_{12}a_{34} + b_{13}a_{24} + b_{14}a_{23}, \\
\alpha_2 =& b_{12}b_{34} + b_{13}b_{24} + b_{14}b_{23}.
\end{aligned}$$

Remember at $p = 2$ we have to be careful not to work with the matrix notation, since that is not well defined over $\mathbb{F}_2$ (it is safe over $\mathbb{Q}_2$ for the above calculation though), but many of the lemmas in the previous section do still hold.

Lemma 79 *The expressions within γ_p and δ_p are covariants for diagonal matrices.*

Proof : Recall the definition of a covariant (Definition 53). The easiest way to see this is by invoking MAGMA to ease some of the calculations. Let Δ_i be the four diagonal matrices with a in the i'th diagonal entry and 1's elsewhere.

We know that T_1 and T_2 are covariants of (Q_1, Q_2), so without loss of generality, we will work with Q_1 and Q_2 in our expressions for γ_2 and δ_2. Since $G(x,z) = \det(V_1 x + V_2 z)$ and we are effectively multiplying one row and column by a, we have $(\det M)^2 G(x,z) = \det(MV_1 x + MV_2 z)$ for M one of the matrices above. This is allowed at $p = 2$, since the determinant has a precise polynomial expression and we never actually have to pass to matrix notation.

It remains to check $\widetilde{G}$. For this we use MAGMA to do the calculations for all the Δ_i and we get that $\widetilde{G}$ is a covariant of weight 4.

□

A calculation shows that the relation also holds for swapping two co-ordinates and we can say something about general $\mathrm{SL}_4(\mathbb{Z}_p)$ transformations too. That is for one of the basis matrices for $\mathrm{SL}_4(\mathbb{Z}_2)$, e.g.

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

we get that the cross-terms (i.e. the α_i) after this transformation[27] are given by

$$\begin{aligned}
\alpha_0 =& a_{12}a_{34} + a_{13}a_{24} + a_{14}a_{23} + 2a_{22}a_{34} + 2a_{23}a_{24}, \\
\alpha_1 =& a_{12}b_{34} + a_{13}b_{24} + a_{14}b_{23} + 2a_{22}b_{34} + a_{23}b_{14} + 2a_{23}b_{24} + a_{24}b_{13} + 2a_{24}b_{23} + \\
& a_{34}b_{12} + 2a_{34}b_{22}, \\
\alpha_2 =& b_{12}b_{34} + b_{13}b_{24} + b_{14}b_{23} + 2b_{22}b_{34} + 2b_{23}b_{24}.
\end{aligned}$$

These are the same as the original α_i modulo 2. Thus the action of $\mathrm{SL}_4(\mathbb{Z}_p)$ only affects the underlying generalised binary quartic by a y-substitution.

Lemma 80 *For $p = 2$ or 3, $\varepsilon_p(C_4)$ is unaffected by $\mathbb{Z}_p$-transformations; i.e. for $t =< S, M >$, with $S \in \mathrm{GL}_2(\mathbb{Z}_p)$ and $M \in \mathrm{SL}_4(\mathbb{Z}_p)$, we have*

$$\varepsilon_p(t(C_4)) = \varepsilon_p(C_4).$$

Proof : From Lemma 55 and the calculations above, t affects C_2 using the transformation $t_1 =< 1, [\beta_0, \beta_1, \beta_2], S^T >$, for some $\beta_i \in \mathbb{Z}_p$. Therefore, since the T_i in the expressions for γ_p and δ_p are covariants, we just need to check that t_1 does not affect $\varepsilon_p(C_2)$, but this is a consequence of Lemma 32.

□

[27] We only use matrix notation here for convenience.

Lemma 81 *Lemma 75 holds for $p = 2$ and $p = 3$.*

Proof : Tackling $p = 3$ first, if we have $3 \mid T_1$ and $3 \mid T_2$, then the identical argument still implies that we either have a line or a non-regular singular point. If instead we are considering $P = (1\colon 0)$, then we need 3 to divide the first coefficient of the expressions in γ_3 and δ_3. Recall that we are assuming $3 \mid a_{24}, a_{33}, a_{34}, b_{14}, b_{34}, b_{44}$, $3 \nmid b_{33}$ and $a_{14} \equiv b_{24} \equiv 1 \bmod 3$, i.e.

$$\begin{aligned}\overline{Q}_1 =& a_{11}x_1^2 + a_{12}x_1x_2 + a_{13}x_1x_3 + x_1x_4 + a_{22}x_2^2 + a_{23}x_2x_3,\\ \overline{Q}_1 =& b_{11}x_1^2 + b_{12}x_1x_2 + b_{13}x_1x_3 + b_{22}x_2^2 + b_{23}x_2x_3 + x_2x_4 + b_{33}x_3^2.\end{aligned}$$

The expression for the first term of $4G$ is

$$\begin{aligned}&16a_{11}a_{22}a_{33}a_{44} - 4a_{11}a_{22}a_{34}^2 - 4a_{11}a_{23}^2a_{44} + 4a_{11}a_{23}a_{24}a_{34} -\\ &4a_{11}a_{24}^2a_{33} - 4a_{12}^2a_{33}a_{44} + a_{12}^2a_{34}^2 + 4a_{12}a_{13}a_{23}a_{44} -\\ &2a_{12}a_{13}a_{24}a_{34} - 2a_{12}a_{14}a_{23}a_{34} + 4a_{12}a_{14}a_{24}a_{33} - 4a_{13}^2a_{22}a_{44} +\\ &a_{13}^2a_{24}^2 + 4a_{13}a_{14}a_{22}a_{34} - 2a_{13}a_{14}a_{23}a_{24} - 4a_{14}^2a_{22}a_{33} + a_{14}^2a_{23}^2,\end{aligned}$$

so for 3 to divide this, we need $3 \mid a_{23}$. The expression for the first coefficient of $\widetilde{G}$ is even less inviting, but it reduces to

$$-2a_{13}a_{14}a_{23}b_{24} - 4a_{14}^2a_{22}b_{33} + 2a_{14}^2a_{23}b_{23}.$$

For 3 to divide this then means that $3 \mid a_{22}$, which means we have a conic as before.

For $p = 2$, again if we have $2 \mid T_1(R)$ and $2 \mid T_2(R)$, then (so long as we bypass any matrix notation by thinking about the equations for the quadric) we still get a line or a non-regular singular point. Otherwise we will need $2 \mid \alpha_0$ and 2 to divide the first coefficient of $\widetilde{G}$ from the expression for δ_2. Since we are again assuming $2 \mid a_{24}, a_{33}, a_{34}, b_{14}, b_{34}, b_{44}$ and that a_{14}, b_{24}, b_{33} are odd, from the expression for α_0 we must also have $2 \mid a_{23}$. We also have 2 dividing

$$\begin{aligned}((\alpha_0^2\alpha_2^2)/4 + 3b_2^2 + 3b_2\alpha_0\alpha_1 - 8a_2c_2 - 2\alpha_0^2c_2 - 2\alpha_1^2a_2 - 4\alpha_0\alpha_2a_2 - \alpha_0^3\alpha_2\\ - (a_2 + \alpha_0^2/4)(4c_2 - 4\alpha_0\alpha_2 + \alpha_1^2)),\end{aligned}$$

which means $2 \mid (b_2^2 - \alpha_1^2a_2)$. Since we now have $2 \mid a_{23}$, a calculation shows we must have $2 \mid a_2$, therefore we need $2 \mid b_2$, from above. Another calculation shows

that this implies $2 \mid a_{22}$ similarly. So we also still have a conic and the lemma is proved.

□

Lemma 82 *For $p = 2$ and 3,*

1. *Φ leaves γ_p and δ_p unchanged.*
2. *χ and χ^{-1} 'flip' the equations in γ_p and δ_p.*

Proof : This is identical to the proof of Lemma 77.

□

We can check that $\varepsilon_p > 0$ and the proof of Theorem 78 also follows through in the same way, since we only need to use the equations for T_1 and T_2 and know that the maps Φ and χ affect the coefficients of γ_p and δ_p for $p = 2, 3$ in the same way as a, b, c, d and e. Thus for the awkward primes there are no real difficulties beyond those encountered in the $n = 2$ case.

3.6 Implementation

The following result will be useful when we describe an algorithm for computing ε_p using the graph of equivalence classes.

Lemma 83 *The contribution to ε_p from a particular $\mathbb{Z}_p$-equivalence class can be read off as $-2|\det M|_p$, for M the GL_4 part of the transformation between the initial vertex and the vertex in question.*

Proof : From Theorem 78, we can see that the determinant gives the required value for a single transformation, so we only need to be careful to remove common factors from M (which will not affect $C_4(\mathbb{Q}_p)$) when we put several operations together to account for the possibility of going round in circles in the graph.

□

The routine we shall discuss will work on any reduction type, but it is useful to have the graph of I_n in mind (which will be discussed in section 4.1.1), since that is in some ways the most complicated case we will have to consider.

To calculate the bound given in section 3.5, we need three routines. One

for ε_p at the finite primes, one for $\varepsilon_\infty^{(4)}$ and one for $\varepsilon_\infty^{(2)}$. The latter two have already been discussed, so we will now look at the first.

The input will be $p > 2$ and F, a QI. The algorithm has been implemented for $p > 2$ and the method can be adapted for $p = 2$, but the changes are at every stage (since we use matrix notation) so would effectively be a parallel program. We will be careful in the next section to use examples where 2 is not a prime of bad reduction.

Let $Q1$ and $Q2$ be the equations for F and $V1$ and $V2$ be the matrix forms of these over $\mathbb{F}_p$. We also start with a list of the vertices ($\mathbb{Z}_p$-equivalence classes) that we have considered so far; call this list KK. Each element of the list contains the GL_2 and SL_2 transformations used to get there (from F), the equations of the QI and the last conic, line or (non-regular) point considered to get there. So KK starts off as $\{(I, Q1, Q2, -)\}$.

Now, given $V1$ and $V2$, we have three functions to find the conics, lines and singular points at this equivalence class.

- FindSP simply calculates the singular sub-scheme of the curve formed from $Q1$ and $Q2$ over $\mathbb{F}_p$ and lists the points there.
- FindLines calls MAGMA's 'PrimaryDecomposition' function on the ideal generated by $Q1$ and $Q2$ over $\mathbb{F}_p$. This returns the smooth components of the ideal and then we determine which of these have degree 1.
- FindConics does similarly, returning the degree 2 components, but we also have to consider the 'degenerate conics' - those formed by any two co-planar lines. We calculate the equations for these by taking the equations for two lines and finding the intersection of the vector spaces.

Once we have found these singular points, lines and conics, we temporarily move them to somewhere convenient and then have functions to determine whether they need to be considered.

- MoveSP will move the singular point to $(1 : 0 : 0 : 0)$ by calculating the Smith Normal Form (SNF) of the 1×4 matrix for the point. The transformation matrix to get it in SNF is what we want. We also use the GL_2 action to ensure

the output is two matrices of the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & * & \\ 0 & & & \end{pmatrix}, \qquad \begin{pmatrix} 0 & & \\ & & \\ & * & \\ & & \end{pmatrix}.$$

It also outputs the global transformation used to get there.

- MoveLine uses SNF in the same way to change the 2×4 matrix for the line into $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$, returning

$$\begin{pmatrix} * & & & \\ & 0 & 0 & \\ & 0 & 0 & \end{pmatrix}, \qquad \begin{pmatrix} * & & & \\ & 0 & 0 & \\ & 0 & 0 & \end{pmatrix}.$$

- MoveConic is essentially the same, but we must first ensure that the QI is in the form $x_4 = f(x_1, x_2, x_3) = 0$ and then find a point on the conic f. Once we have this, we use the same SNF trick to move this point to $(1\colon 0\colon 0\colon 0)$, returning

$$\begin{pmatrix} 0 & 0 & 0 & \\ 0 & 0 & 0 & \\ 0 & 0 & 0 & \\ & & & * \end{pmatrix}, \qquad \begin{pmatrix} 0 & & \\ & & \\ & * & \\ & & \end{pmatrix}.$$

Now we need to see whether this point, line or conic needs to be considered. For lines and conics, this just involves checking whether the relevant 'flip' lands us in an element of KK that we have already considered. For singular points, we also need to check that it is a non-regular point, i.e. that $p^2 \mid a_{11}$. To see whether a new QI is in the list already, we take the SL_4 transformation, T say, used to get there and calculate $M_i = TT_i^{-1}$ for T_i each of the transformations in KK. The SNF of M_i will then tell us whether we are in that ith equivalence class, since if its top left entry is divisible by p, then M_i contains a factor of pI, i.e. $\chi\chi^{-1}$ or $\Phi\Phi^{-1}$. If this is the case, then we could have got to this vertex via a shorter route.

We discard those which fail this test and carry out the relevant operation on

the others and add them to KK, keeping track of the transformation, which now includes one of

$$< \begin{pmatrix} \frac{1}{p^2} & 0 \\ 0 & \frac{1}{p} \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & p & & \\ & & p & \\ & & & p \end{pmatrix} >, \quad < \begin{pmatrix} \frac{1}{p} & 0 \\ 0 & \frac{1}{p} \end{pmatrix}, \begin{pmatrix} p & & & \\ & p & & \\ & & 1 & \\ & & & 1 \end{pmatrix} >$$

$$\text{or } < \begin{pmatrix} \frac{1}{p} & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & p \end{pmatrix} > .$$

We move through this list of QIs until no new $\mathbb{Z}_p$-equivalence classes are found, keeping track of the contribution to ε_p at each step. At the end, we look at contributions at all the vertices stored in KK and find the maximum, which is returned as ε_p for F.

Clearly this routine can also be used to generate a list of all the vertices in the graph as a list of their transformations from the starting vertex. We could pick out only those vertices where a component is seen with multiplicity at least 3. These (as a set) are the best on which to search for points, since a given $\mathbb{Q}_p$-point will be smooth on at least one of them. They are also the only ones that we need to consider for the bound (see Lemma 100). There are c_p of these equivalence classes, for c_p the Tamagawa number at p. It is then possible to meld[28] each of these transformations at every bad prime to get $\prod_p c_p$ global models on which to search.

We must also note that the above algorithm terminates, since there are only a finite number of equivalence classes.

3.7 Examples

How good are the bounds we are producing? Are there points on the elliptic curve which come close to achieving the bounds, which would show that they are in some sense 'best possible'?

[28] I.e. if we have T_p a transformation modulo p and T_q a transformation modulo q, we can find a transformation T which is congruent to T_p and T_q respectively modulo p and q.

Consider the elliptic curve given by '897f2' in [Cre97] and its reduced 4-covering given by

$$C_4 : x_1x_4 - x_2x_3 = x_1^2 + x_1x_3 + x_1x_4 + x_2^2 + x_2x_4 - 2x_3^2 - x_3x_4 - 5x_4^2 = 0.$$

This has reduction type I_4 at 3, I_1 at 13 and I_2 at 23. The bound for $h(R) - h(\pi(\phi(R)))/8$ comes out as 4.0268..., but the point on C_4 which maps to $73(-5 : 1 : 1)$ on E gives a value of 3.2209..., which is close to achieving the bound. This sort of proximity is often found in $\mathbb{Z}_p$-equivalence classes where the component on which the point lies cannot be seen as a smooth component in the reduction and where it would take many operations of χ and Φ before it can be seen as a smooth component.

Another question to answer is that of what makes up the major contributions to the bound. We will see in section 4.1.2 that the contributions at the finite places (certainly for multiplicative reductions) vary quite dramatically depending on the equivalence class in which we start. For reduction type I_2 for example, there could be three equivalence classes, two of which have $\varepsilon_p = p^{-8}$ and one of which has $\varepsilon_p = p^{-2}$. We will investigate this further in the next section.

For now, we can say that in general (if we ensure the coverings are reduced), the contribution at the finite primes dominates that at ∞. Consider the curve given by '777d2' in [Cre97]. In the following table, we list the contributions (to 3 significant figures) at the finite places compared to those at ∞. There are two equivalence classes at $p = 3$ and three at $p = 7$ and $p = 37$, so eighteen in all. This means that there end up being four possible values at the finite places and for each value, we list the various computations at ∞. Numbers in brackets give how many of the eighteen equivalence classes give each particular value.

$\sum_{p<\infty} \log(\varepsilon_p)/8$	$\log(\varepsilon_\infty^{(2)})/8$	$\log(\varepsilon_\infty^{(4)})/2$.
6.11 (8)	-0.195	-0.155, -0.264, 0.309 (2), 0.317 (2), -0.512 (2).
4.65 (4)	-0.195	0, 0.399, 0.236, 0.108.
3.40 (4)	-0.492	0.110, 0.154 (2), 0.185.
1.94 (2)	-0.0266	0.485, 0.445.

As we can see, the contribution at ∞ is fairly negligible, so it is more im-

portant to improve the value at the finite primes. We will now see how the contributions there can vary depending on the graph of equivalence classes.

To see that the bounds we obtain are better than those achieved using the theory of resultants, take the example at the end of section 2.8;

$$E_2 : y^2 + xy = x^3 + x^2 - 2x + 1.$$

This has a single 4-covering that is everywhere locally soluble, given in reduced form by

$$x_1x_4 + x_2x_3 = x_1x_2 - x_1x_4 - 2x_2x_4 + x_3^2 + x_3x_4 - x_4^2.$$

Using our methods, we get no contributions from the finite primes, therefore our bound is just from the infinite place and comes out as 0.5480... Using the resultant method found in section 3.5, we find that there are polynomials f_i such that

$$(f_1Q_1 + f_2Q_2 + f_3T_1 + f_4T_2)(x_1, x_2, x_3, x_4) = 133x_i^5,$$

for each i. This then leads to a bound of 3.8523...

4 Deeper Investigations for Curves with Multiplicative Reduction

4.1 Graphs of Equivalence Classes

When considering all the $\mathbb{Z}_p$-equivalence classes of quadric intersections, it is useful to have a picture in mind. Here I will discuss how one can generate such a picture for reduction type I_n, first with a naive example and then in a general setting. In principal, the ideas could be used on other reduction types, although there is less need when there are fewer smooth components. For a naive example, let us consider the QI given over $\mathbb{Q}$ by

$$\begin{aligned} Q_1 &= 2x_1x_3 + 6x_1x_4 + x_2^2 - 2x_2x_4 - 2x_3^2 + 3x_4^2, \\ Q_2 &= 2x_1x_2 + 2x_1x_4 + 2x_2x_4 + x_3^2 - 3x_4^2. \end{aligned}$$

This has Kodaira symbol I_3 at $p = 5$. It can be shown that the QI above contains two lines and a conic over $\mathbb{F}_p$:

$$\begin{aligned} L_1 &: x_1 + 2x_3 + x_4 = x_2 + x_3 + x_4 = 0, \\ L_2 &: x_1 + x_3 + x_4 = x_2 + 2x_3 + x_4 = 0, \\ \Gamma &: x_2 + 2x_3 + 2x_4 = x_1x_3 + 3x_1x_4 + x_3^2 + x_3x_4 + 3x_4^2 = 0. \end{aligned}$$

It also contains a degenerate conic (in the plane formed from the two lines), given by

$$\Gamma_{12} : x_1 + x_2 + 3x_3 + 2x_4 = x_2^2 + 3x_2x_3 + 2x_2x_4 + 2x_3^2 + 3x_3x_4 + x_4^2 = 0.$$

There are singular points at

$$(1:0:4:1), (4:4:0:1), (4:3:1:0),$$

but we can check that these are all regular. If we apply $\chi^{-1}(Q_1, Q_2, \Gamma)$, i.e. we use the following transformation:

$$< \begin{pmatrix} \frac{1}{5} & \frac{3}{5} \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -10 & 4 & 1 \\ 0 & -2 & 1 & 0 \\ 1 & -4 & 2 & 0 \\ 0 & -5 & 0 & 0 \end{pmatrix} >,$$

then we arrive in a new equivalence class with equations

$$\begin{aligned} Q_3 =& 6x_1^2 + 6x_1x_2 + 4x_1x_3 + 10x_1x_4 + 2x_2^2 + 2x_2x_3 + 4x_2x_4 + 2x_3x_4 + 5x_4^2, \\ Q_4 =& -25x_1^2 - 18x_1x_3 - 20x_1x_4 + 2x_2^2 - 4x_3^2 - 10x_3x_4. \end{aligned}$$

This has no lines or conics and only a singular point at $(0\colon 0\colon 0\colon 1)$ (which would return us to the first equivalence class), so we must be seeing one component four times.

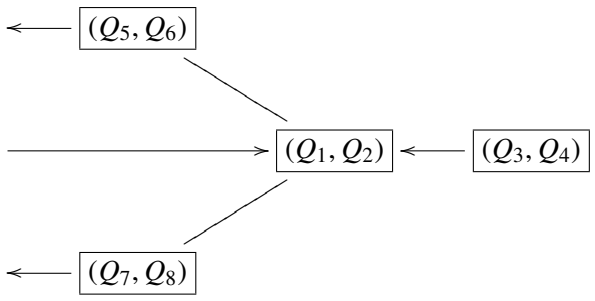
If instead we 'flipped' one of the lines using either

$$< \begin{pmatrix} \frac{1}{5} & 0 \\ 0 & \frac{1}{5} \end{pmatrix}, \quad \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ -1 & 0 & 1 & -1 \\ -1 & -1 & 0 & 1 \end{pmatrix} >$$

or

$$< \begin{pmatrix} \frac{1}{5} & 0 \\ 0 & \frac{1}{5} \end{pmatrix}, \quad \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & -1 & 1 & -1 \\ -1 & -1 & 0 & 1 \end{pmatrix} >,$$

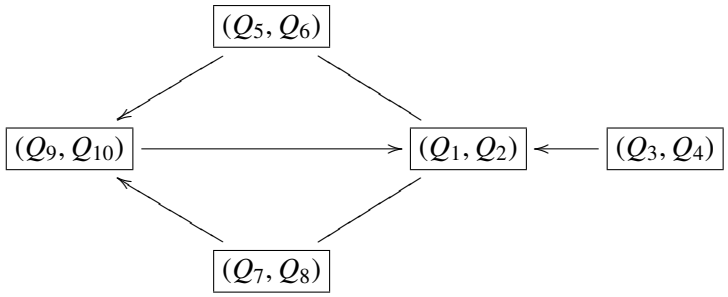
then we would arrive in a new equivalence class containing a line and a component of degree 3. Call the QIs we obtain (Q_5, Q_6) and (Q_7, Q_8) respectively. Each line would take us back to the original QI, but each of these two equivalence classes also has a non-regular point which we could blow up. So our graph of four vertices still has three loose ends (namely Γ_{12} on the original QI and a non-regular point on each of (Q_5, Q_6) and (Q_7, Q_8)), so thus far we have the following picture:



where the lines are applications of Φ and the arrows χ. Applying $\chi^{-1}(Q_1, Q_2, \Gamma)$, using

$$< \begin{pmatrix} \frac{1}{5} & \frac{3}{5} \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 12 & 1 & 1 & 2 \\ -3 & 0 & 0 & -1 \\ 5 & 0 & 1 & 1 \\ 5 & 0 & 0 & 0 \end{pmatrix} >,$$

brings us to a QI with equations (Q_9, Q_{10}) containing two conics and a non-regular point (which would take us back). By some computation of the matrices, it can be shown that this is also what we get (up to $\mathbb{Z}_p$-equivalence) after applying χ to singular points which represented the other two loose ends. So we have the following graph:



Again the lines are applications of Φ and the arrows χ. Recalling that an edge representing Φ has weight 4, χ weight 6 and χ^{-1} weight 2, we can read off that the maximum of the distances from (Q_1, Q_2) to any other vertex is 4. Therefore, $\varepsilon_5(Q_1, Q_2) = 5^{-4}$.

4.1.1 A Power Series Point of View

The goal of this section is to try to understand how many components of the special fibre are 'contained' in a singular point P (i.e. the components which, after blowing up, are found above P) and then how the transformations Φ and χ affect this. To do this, let us consider what happens at a singular point when we carry out one of the operations Φ or χ, so let us start with the ideal generated by the QI with coefficients in $\mathbb{Z}_p$ (which we will consider in affine co-ordinates by setting $x_4 = 1$, say) in the power series ring $\mathbb{Z}_p[[x_1, x_2, x_3]]$,

$$I = (Q_1(x_1, x_2, x_3), Q_2(x_1, x_2, x_3)) \subset_{\text{id}} \mathbb{Z}_p[[x_1, x_2, x_3]].$$

Since we have multiplicative reduction, the reduction of the QI modulo p has a node, i.e. a singular point with two distinct tangent directions (see [Har77] p.37 or [EH00] p 57). Now if we move the node to the origin and take the completion of the co-ordinate ring, we get a ring isomorphic to

$$\frac{\mathbb{F}_p[[x_1, x_2, x_3]]}{(x_1x_2, x_3)}.$$

In other words, we can make a substitution so that I is such that

$$\overline{I} = \{\overline{f} \colon f \in I\} = (x_1x_2, x_3),$$

with $\{x_1 = x_3 = 0\}$ and $\{x_2 = x_3 = 0\}$ being the two distinct tangents. Throughout this section, we will write w' for w/p for $w \in \mathbb{Z}_p$. Now let us utilise the following lemma from the theory of arithmetic geometry.

Lemma 84 *Let I be an ideal in $S = \mathbb{Z}_p[[x_1, x_2, ..., x_m]]$ and let the maximal ideal $\mathfrak{m}$ of S/I be given by $\mathfrak{m} = (p, w, z)$ for elements $w, z \in S/I$ such that $wz \in pS/I$. Then*

1. *There exists $\alpha \in p\mathbb{Z}_p$ and a surjective homomorphism*

$$\psi \colon \mathbb{Z}_p[[u, v]]/(uv - \alpha) \to S/I,$$

   such that $\psi(u) - w$, $\psi(v) - z \in pS/I$.

2. *If*

$$\mathbb{F}_p[[x_1, x_2, ..., x_m]]/\overline{I} \cong \mathbb{F}_p[[x, y]]/(xy),$$

   then any ψ in (1) *is an isomorphism.*

Proof : This is proved on p512 of [Liu02] with $A = \mathbb{Z}_p$, $\mathfrak{m}_A = p\mathbb{Z}_p$, $B = S/I$, $\mathfrak{m}_B = \mathfrak{m}$ and noting that the completion of $\mathbb{Z}_p$ is still $\mathbb{Z}_p$ and that S/I is Noetherian. The main idea in the proof is showing that there exist sequences $(w_n)_{n\geq 0}$, $(z_n)_{n\geq 0}$ and $(c_n)_{n\geq 0}$ with $w_0 = w$, $z_0 = z$, $w_n, z_n \in \mathfrak{m}$ and $c_n \in p\mathbb{Z}_p$ such that $w_{n+1} - w_n \in p^{n+1}S/I$, $z_{n+1} - z_n \in p^{n+1}S/I$, $c_{n+1} - c_n \in p^{n+1}\mathbb{Z}_p$ and $w_nz_n - c_n \in p^{n+1}S/I$. We also need S/I to be flat over $\mathbb{Z}_p$, which is a consequence of Corollary 2.14 on p11 of [Liu02] and the fact that we can inject $\mathbb{Z}_p$ into S/I.

□

We then use this in the following theorem, keeping in mind that we will be using I generated by the QI.

Corollary 85 *For S as above, suppose we have the ideal I of S such that*

$$\overline{I} = \{\overline{f} \colon f \in I\} = (x_1 x_2, x_3),$$

then for some k we have

$$S/I \cong \mathbb{Z}_p[[u, v]]/(uv - p^k).$$

Proof : If we apply the above lemma using $w = x_1$, $z = x_2$, so that $wz \equiv 0$ modulo (p, I), then the hypothesis of the second part of the lemma holds and

$$\psi \colon \mathbb{Z}_p[[u, v]]/(uv - \alpha) \to S/I$$

is an isomorphism for some $\alpha \in p\mathbb{Z}_p$. We have $\alpha \neq 0$ (since otherwise C_4 would be singular), so after multiplication by a unit, we may assume it is p^k for some k.

□

Definition 86 *Let P be a singular point defined over $\mathbb{F}_p$. We define the thickness $\tau(P)$ by first moving P to the origin and taking the completion of the co-ordinate ring there. Then $\tau(P)$ is defined as k in $\mathbb{Z}_p[[u, v]]/(uv - p^k)$ realised in the isomorphism in the above corollary.*

We say $\tau(P) = 0$ if P is a smooth point. We should also remark that $\tau(P)$ is equal to the number of components found above P (in the special fibre of the minimal desingularisation of C_4) plus one, which has the following two consequences:

$$P \text{ is a singular point } \Leftrightarrow \tau(P) \geq 1,$$
$$P \text{ is a regular singular point } \Leftrightarrow \tau(P) = 1.$$

This will prove a very useful tool in describing the graph of equivalence classes below. Note that we believe it is always possible to find a $\mathbb{Q}_p$-equivalent QI such that $\tau(P) = v_p(a_{11})$ by continually applying χ to the point P (which includes the intermediary transformations to get the point to $(1 \colon 0 \colon 0 \colon 0)$) and then reversing the process (which does not include the intermediary transformations). In principle, this could give another way of defining the thickness, but we will continue with the power series approach here.

Definition 87 *The elliptic curve E is said to have multiplicative reduction at p if $p \mid \Delta(E)$, but $p \nmid I, J$, for I and J the invariants given in section 2.2.*

The following lemma is partly an illustration to show how we can calculate the singular points. We will usually assume that they are at $(1:0:0:0)$ and $(0:1:0:0)$. It also shows that there are precisely two singular points on any given line in the reduction of C_4 so long as we have multiplicative reduction, in agreement with the classification mentioned in section 3.3.

Lemma 88 *If we have a singular point $P_1 = (1:0:0:0)$ lying on the line $\{x_3 = x_4 = 0\}$ in the reduction of C_4 over $\mathbb{F}_p$ and C_4 has multiplicative reduction at p, then there is another singular point at $P_2 = (k:1:0:0)$, for $k = \frac{a_{24}b_{23}-a_{23}b_{24}}{b_{14}a_{23}-a_{24}b_{13}}$.*

Proof : The singular points are those where $\text{rank}(\mathcal{J}) \leq 1$, for $\mathcal{J} = (\frac{\partial Q_i}{\partial x_j})$. In our situation, with coefficients in $\mathbb{F}_p$, we have $a_{11} = a_{12} = a_{22} = b_{11} = b_{12} = b_{22} = 0$ and $x_3 = x_4 = 0$, so

$$\mathcal{J} \equiv \begin{pmatrix} 0 & 0 & a_{13}x_1 + a_{23}x_2 & a_{14}x_1 + a_{24}x_2 \\ 0 & 0 & b_{13}x_1 + b_{23}x_2 & b_{14}x_1 + b_{24}x_2 \end{pmatrix}.$$

This has rank ≤ 1 if and only if

$$(a_{13}x_1 + a_{23}x_2)(b_{14}x_1 + b_{24}x_2) = (a_{14}x_1 + a_{24}x_2)(b_{13}x_1 + b_{23}x_2),$$

in other words, the singular points are $(x_1 : x_2 : 0 : 0)$, for (x_1, x_2) a solution to the following quadratic form:

$$q(s,t) = (a_{13}b_{14} - a_{14}b_{13})s^2 + (a_{13}b_{24} + a_{23}b_{14} - a_{14}b_{23} - a_{24}b_{13})st + (a_{23}b_{24} - a_{24}b_{23})t^2 = 0.$$

Now, the invariant I remains unchanged when we move from the elliptic curve to a 4-covering since C_4 is minimal (see [CFS09]). Recalling its equation from section 2.2 in terms of the coefficients of the binary quartic, some computation shows that I is given by

$$((a_{13}b_{24} + a_{23}b_{14} - a_{14}b_{23} - a_{24}b_{13})^2 - 4(a_{23}b_{24} - a_{24}b_{23})(a_{13}b_{14} - a_{14}b_{13}))^2. \quad (15)$$

This is the square of the discriminant of the quadratic form q. Since we have multiplicative reduction at p, we have $p \mid \Delta$, but $p \nmid I, J$, so the discriminant of q is non-zero. This means if we have roots, then they are distinct. One of our singular

points is P_1, so we have $a_{13} = a_{14} = 0$. Therefore the other is a solution to

$$(a_{23}b_{14} - a_{14}b_{23})st + (a_{23}b_{24} - a_{24}b_{23})t^2 = 0$$

and P_2 has $x_2 \neq 0$, so set $t = 1$ and then $x_1 = \frac{a_{24}b_{23} - a_{23}b_{24}}{b_{14}a_{23} - a_{24}b_{13}}$ as required.

□

For the rest of this section we will assume we have split multiplicative reduction and then we will see how the non-split case can be read off from this.

As mentioned in section 3.3, if we are in a particular $\mathbb{Z}_p$-equivalence class of QI, then we see up to four components of the special fibre. The components have multiplicity 1 (since we have multiplicative reduction) and we can see some of them more than once according to the degree of their equations. Let us number the components of the minimal proper regular model 1 to n (consecutively round the polygon of components). Suppose we can see components numbered a, b, c and d say (in ascending order and possibly including repeats), then we will write $[a, b, c, d]$ for this $\mathbb{Z}_p$-class (up to equivalence of cyclic permutations, i.e. $[a, b, c, d] = [b, c, d, a]$). For example, $[1, 1, 2, 4]$ would represent a conic and two lines. By work of Sadek (see Definition 2.4 in [Sad10b]), if C_4 is minimal at p, then the minimal proper regular model for E is the same as the minimal desingularisation[29] of C_4. This means that if our reduction of C_4 modulo p already contains a regular point, then the two components meeting there must be numbered consecutively. We also know (see [Sad10a]) that the sum $s = a + b + c + d$ is constant modulo n for a particular $\mathbb{Q}_p$-equivalence class of QI, which means we could write a list of all the potential equivalence classes for a given QI, knowing only n and s. In fact[30], if we know s modulo n and C_4 minimal, there is a bijection between sets:

$$\{[a, b, c, d] \colon s = a + b + c + d\} \leftrightarrow \{\mathbb{Z}_p\text{-equivalence classes for } C_4\}.$$

We will now define a graph, where the vertices are represented by $\mathbb{Z}_p$-classes in the form $[a, b, c, d]$ and the directed edges will be the maps χ and Φ (which change the $\mathbb{Z}_p$-equivalence class of the QI). We will construct the graph by realising χ

[29] See [Liu02] section 9.3 for definitions of minimal proper regular model and minimal desingularisation.

[30] This is Theorem 4.2 in [Sad10a].

and Φ as operations on the bracket $[a, b, c, d]$ in the following theorem, which transforms the geometric problem into something much more combinatorial.

Theorem 89 *1. If 'a' represents the line L for a QI given by (Q_1, Q_2) in the class $[a, b, c, d]$, i.e. if $a \neq b, d$, then we 'flip' the line using the operation*

$$\Phi\colon [a, b, c, d] \longmapsto [a, b-1, c, d+1].$$

2. If the singular point P between d and a is non-regular, i.e. $d \neq a - 1$, then

$$\chi\colon [a, b, c, d] \longmapsto [a-1, b, c, d+1].$$

3. Hence, the inverse of this gives the 'blow down' either of a conic C_1 (if $a = b$, $a \neq c$ and $a \neq d$):

$$\chi^{-1}\colon [a, a, c, d] \longmapsto [a-1, a+1, c, d],$$

or of a degenerate conic C_2 (if $a \neq b, d$ and $b \neq c$):

$$\chi^{-1}\colon [a, b, c, d] \longmapsto [a-1, b+1, c, d].$$

Before proving this, it is useful to remember what the various maps do to the coefficients of (Q_1, Q_2). Recall that the twenty coefficients are listed with $i \leq j$. We will assume the singular point is at $(1\colon 0\colon 0\colon 0)$, the line is at $\{x_3 = x_4 = 0\}$ and the conic is at $x_1 = f_2(x_2, x_3, x_4) = 0$ in the following table:

	$\frac{1}{p^2}$	$\frac{1}{p}$	No change	p	p^2
Φ		$a_{ij}, b_{ij}, j \leq 2$	$a_{ij}, b_{ij}, i \leq 2, j \geq 3$	$a_{ij}, b_{ij}, i \geq 3$	
χ	a_{11}	$b_{11}, a_{1j}, j \geq 2$	$a_{ij}, b_{1i}, i \geq 2$	$b_{ij}, i \geq 2$	
χ^{-1}		$b_{ij}, i \geq 2$	$a_{ij}, b_{1i}, i \geq 2$	$a_{1j}, j \geq 2, b_{11}$	a_{11}.

To prove the theorem, we need to put together a few lemmas. This one will show us that the line L is still present after the operation of Φ.

Lemma 90 *Let $P_1, P_2 \in \overline{C}_4(\mathbb{F}_p)$ be (distinct) singular points on the line $L \subset \overline{C}_4$, which is defined over $\mathbb{F}_p$ and let C_4' be given by $\Phi(Q_1, Q_2, L)$. Then*

$$\Phi\colon \{R \in C_4(\mathbb{Q}_p)\colon \overline{R} \in L \setminus \{P_1, P_2\}\} \mapsto \{R' \in C_4'(\mathbb{Q}_p)\colon \overline{R'} \in \Gamma' \setminus \{P_1', P_2'\}\},$$

for singular points $P_1', P_2' \in \overline{C}_4(\mathbb{F}_p)$ on some smooth component $\Gamma' \subset \overline{C}_4'$ (of degree 1, 2 or 3) defined over $\mathbb{F}_p$. Furthermore, we get an isomorphism $\rho\colon L \to \Gamma'$.

Proof : If we take $L = \{x_3 = x_4 = 0\}$ over $\mathbb{F}_p$, then a general point on the line can be parametrised by $(x_1\colon x_2\colon x_3\colon x_4) = (s\colon t\colon 0\colon 0)$. Assuming the point is smooth, then when we lift it to a $\mathbb{Q}_p$ point, apply Φ and look at the reduction of this modulo p, we get the point $(s\colon t\colon \xi_1\colon \xi_2)$ and

$$\begin{aligned}(a_{11}'s^2 + 2a_{12}'st + a_{22}'t^2) + a_{13}s\xi_1 + a_{14}s\xi_2 + a_{23}t\xi_1 + a_{24}t\xi_2 &= 0,\\ (b_{11}'s^2 + 2b_{12}'st + b_{22}'t^2) + b_{13}s\xi_1 + b_{14}s\xi_2 + b_{23}t\xi_1 + b_{24}t\xi_2 &= 0,\end{aligned}$$

for $a_{ij}' = \frac{a_{ij}}{p}$. This is linear in ξ_1 and ξ_2, so for $F_i(s,t) = -\frac{1}{p}Q_i(s,t,0,0)$, we can derive the following:

$$\begin{pmatrix} a_{13}s + a_{23}t & a_{14}s + a_{24}t \\ b_{13}s + b_{23}t & b_{14}s + b_{24}t \end{pmatrix}\begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \equiv \begin{pmatrix} F_1(s,t) \\ F_2(s,t) \end{pmatrix} \bmod p.$$

Now, the matrix on the left, M say, has $\det(M) = q(s,t)$, for q the quadratic form in the proof of Lemma 88. This is non-zero apart from at the two distinct singular points, since we have multiplicative reduction at p. So we can invert the matrix M, allowing us to define

$$\begin{pmatrix} G_1(s,t) \\ G_2(s,t) \end{pmatrix} = q(s,t)M^{-1}\begin{pmatrix} F_1(s,t) \\ F_2(s,t) \end{pmatrix}.$$

Substituting in the expressions for ξ_1 and ξ_2, we see the smooth points on the line L map to

$$(sq(s,t)\colon tq(s,t)\colon G_1(s,t)\colon G_2(s,t)).$$

Thus we have morphisms

$$\begin{array}{rccc} L \to & \mathbb{P}^1 \to & \Gamma' \\ (s\colon t\colon 0\colon 0) \mapsto & (s\colon t) \mapsto & (sq(s,t)\colon tq(s,t)\colon G_1(s,t)\colon G_2(s,t)), \end{array}$$

meaning that the smooth points on L map to a smooth component parametrised by the equation above. We then divide through by the greatest common divisor of the co-ordinates and the degree of the expression obtained is then the degree of Γ'. Note that we cannot have everything reducing to a point, since the first two entries in the parametrisation do not divide one another.

This also gives us a map for the singular points, so the two singular points on Γ', P'_1 and P'_2 (and there must be precisely two, since Γ' has degree at most 3 and at least 1) are defined to have come from P_1 and P_2. The isomorphism ρ is then the morphism above on the smooth points together with $\rho(P_1) = P'_1$ and $\rho(P_2) = P'_2$.

□

The following two lemmas explain how to choose co-ordinates in a sensible manner.

Lemma 91 *Let (Q_1, Q_2) be a QI with coefficients in $\mathbb{Z}_p$. Suppose $L \subset \overline{C}_4$ is a line defined over $\mathbb{F}_p$ and let $P, P_1 \in \overline{C}_4(\mathbb{F}_p)$ be singular points on L. Then, by replacing (Q_1, Q_2) with a $\mathbb{Z}_p$-equivalent QI, we may assume that $L = \{x_3 = x_4 = 0\}$, $P = (1 : 0 : 0 : 0)$, $P_1 = (0 : 1 : 0 : 0)$ and*

$$(\overline{Q}_1, \overline{Q}_2) = (x_2x_3 + x_4l(x_3, x_4), x_1x_4 + f(x_3, x_4)),$$

for some quadratic form f and linear form l.

Proof : Moving the line L and the points P and P_1 is just an $\mathrm{SL}_4(\mathbb{Z}_p)$ transformation. Since P is a singular point, an $\mathrm{SL}_2(\mathbb{Z}_p)$ transformation can ensure we have matrices of the form

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & a_{23} & a_{24} \\ 0 & a_{23} & 2a_{33} & a_{34} \\ 0 & a_{24} & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & 0 & b_{13} & b_{14} \\ 0 & 0 & b_{23} & b_{24} \\ b_{13} & b_{23} & 2b_{33} & b_{34} \\ b_{14} & b_{24} & b_{34} & 2b_{44} \end{pmatrix}.$$

If $p \mid a_{23}$ and a_{24}, then we would have a singular line in the reduction of C_4 modulo p (contradicting multiplicative reduction), so the fact that the point P_1 is singular means that we must be able to add a multiple of V_1 to V_2 to get $p \mid b_{23}$ and b_{24}. This can be viewed as an $\mathrm{SL}_2(\mathbb{Z}_p)$ transformation. Also, without loss of generality,

$p \nmid a_{23}$. Now, by adding a multiple of x_4 to x_3 (or equivalently, by subtracting a multiple of row (and column) three from row[31] (and column) four in the matrices above), we can ensure $p \mid a_{24}$. Rescaling can also ensure $a_{23} = 1$, so we have the following matrices:

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 2a_{33} & a_{34} \\ 0 & 0 & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & 0 & b_{13} & b_{14} \\ 0 & 0 & 0 & 0 \\ b_{13} & 0 & 2b_{33} & b_{34} \\ b_{14} & 0 & b_{34} & 2b_{44} \end{pmatrix}.$$

Now recall the quadratic form q from Lemma 88. In our situation,

$$q(s,t) = b_{14}st,$$

so we must have $p \nmid b_{14}$ to ensure q has two distinct solutions. Then by subtracting a multiple of row four from row three in the above matrices we get $p \mid b_{13}$ and rescaling can ensure $b_{14} = 1$. Finally, subtracting a multiple of row two from row three gets $p \mid a_{33}$ and matrices of the form

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & a_{34} \\ 0 & 0 & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2b_{33} & b_{34} \\ 1 & 0 & b_{34} & 2b_{44} \end{pmatrix}.$$

This then gives equations for $(\overline{Q}_1, \overline{Q}_2)$ of the required form.

□

Lemma 92 *Let (Q_1, Q_2) be a QI with coefficients in $\mathbb{Z}_p$. Suppose $L \subset \overline{C}_4$ is a line defined over $\mathbb{F}_p$ and let $P \in \overline{C}_4(\mathbb{F}_p)$ be a non-regular point on L. Also, let $(Q_1', Q_2') = \Phi(Q_1, Q_2, L)$ and let $P' \in \overline{C}_4'(\mathbb{F}_p)$ be the image of P under the isomorphism ρ in Lemma 90. Then, by replacing (Q_1, Q_2) with a $\mathbb{Z}_p$-equivalent QI, we may assume that $L = \{x_3 = x_4 = 0\}$, $P = (1:0:0:0)$, $P' = (1:0:0:0)$ and $Q_i'(x_1, x_2, x_3, x_4) = \frac{1}{p} Q_i(x_1, x_2, px_3, px_4)$ for $i \in \{1, 2\}$. By further rearrangement, we may also assume*

$$(\overline{Q}_1, \overline{Q}_2) = (x_2x_3 + x_4l_1(x_3, x_4), x_1x_4 + f_1(x_3, x_4)),$$

[31] Henceforth, when we refer to a row operation, the corresponding column operation will be assumed.

for some quadratic form f_1 and linear form l_1 and

$$(\overline{Q}_1', \overline{Q}_2') = (x_2x_3 + x_4l_2(x_2, x_3, x_4), x_1x_4 + f_2(x_2, x_3, x_4)),$$

for some quadratic form f_2 and linear form l_2.

Proof : By Lemma 91, we may assume that the other singular point on L is at $(0\colon 1\colon 0\colon 0)$ and therefore that L and P are of the correct form. Also

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & a_{34} \\ 0 & 0 & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2b_{33} & b_{34} \\ 1 & 0 & b_{34} & 2b_{44} \end{pmatrix},$$

giving the correct form for $(\overline{Q}_1, \overline{Q}_2)$. Once L is given by $L = \{x_3 = x_4 = 0\}$, we have $Q_i'(x_1, x_2, x_3, x_4) = \frac{1}{p}Q_i(x_1, x_2, px_3, px_4)$ for $i \in \{1, 2\}$ by definition. Now recall that the quadratic form q is given by $q(s, t) = st$, so the expression for the isomorphism in Lemma 90 is given by

$$\begin{aligned} \rho\colon L &\to \Gamma' \\ (s\colon t\colon 0\colon 0) &\mapsto (s^2t\colon st^2\colon G_1(s,t)\colon G_2(s,t)). \end{aligned}$$

Recall also that the G_i are given by

$$\begin{pmatrix} G_1(s,t) \\ G_2(s,t) \end{pmatrix} = \mathrm{adj}\begin{pmatrix} a_{13}s + a_{23}t & a_{14}s + a_{24}t \\ b_{13}s + b_{23}t & b_{14}s + b_{24}t \end{pmatrix}\begin{pmatrix} F_1(s,t) \\ F_2(s,t) \end{pmatrix},$$

for $F_i(s, t) = -\frac{1}{p}Q_i(s, t, 0, 0)$, which reduce in our case to

$$G_1(s, t) = sF_1(s, t), \quad G_2(s, t) = tF_2(s, t).$$

The point P is non-regular, so $p^2 \mid a_{11}$ and therefore $t \mid F_1(s, t)$. This means that, after dividing through by t,

$$\rho\colon (1\colon 0\colon 0\colon 0) \mapsto (1\colon 0\colon a_{12}'\colon b_{11}').$$

By subtracting a multiple of p times row three from row one in the matrices $\overline{V}_1$ and $\overline{V}_2$, we can get $p^2 \mid a_{12}$ and by subtracting a multiple of p times row four from row one, we can get $p^2 \mid b_{11}$. This means we have $\rho(P) = (1\colon 0\colon 0\colon 0)$ as required. It

remains to check the structure of $(\overline{Q}_1', \overline{Q}_2')$. Currently we have

$$\overline{V}_1' = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2a_{22}' & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \qquad \overline{V}_2' = \begin{pmatrix} 0 & b_{12}' & 0 & 1 \\ b_{12}' & 2b_{22}' & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

We can see here that subtracting a multiple of row three from row two gets rid of the $2a_{22}'$ and subtracting a multiple of row four from row two gets rid of the b_{12}'. This amounts to subtracting multiples of p times rows three and four from row two in the matrices for $\overline{V}_1$ and $\overline{V}_2$. This gives the desired form for the transformed QI.

□

Now we will show what happens to the thickness of points under the operation Φ, which will allow us to prove (1) in Theorem 89.

Lemma 93 *(i) Let C_4 be a 4-covering given by (Q_1, Q_2). Suppose $\overline{C}_4$ contains a line L defined over $\mathbb{F}_p$ and a non-regular point $P \in \overline{C}_4(\mathbb{F}_p)$ on L. Also let the transformed QI be given by $C_4' = \Phi(Q_1, Q_2, L)$ with equations (Q_1', Q_2') and suppose $P' \in \overline{C}_4'(\mathbb{F}_p)$ is the singular point defined by $\rho(P)$ in Lemma 90. Then $\tau(P', Q_1', Q_2') = \tau(P, Q_1, Q_2) - 1$.*
(ii) Let C_4 and C_4' be as above, with $\overline{C}_4$ containing a line L defined over $\mathbb{F}_p$ and singular points $P, P_1 \in \overline{C}_4(\mathbb{F}_p)$ on L. Suppose first that the point $P \in \overline{C}_4(\mathbb{F}_p)$ is regular, but that P_1 is non-regular. Then the image of L under the map ρ in Lemma 90 is a component of degree 2. If instead both P and P_1 are regular, then the image is a component of degree 3.

Proof : (*i*) We have the ideal $I = (Q_1(1, x_2, x_3, x_4), Q_2(1, x_2, x_3, x_4))$ in $S = \mathbb{Z}_p[[x_2, x_3, x_4]]$ and we would like $\overline{I}$ to have the structure as in part (2) of Lemma 84.

Using Lemmas 91 and 92, we may assume P and P' are at $(1\colon 0\colon 0\colon 0)$ and $L = \{x_3 = x_4 = 0\}$. By setting $x_1 = 1$, we also have that the ideals generated by the equations for $\overline{C}_4$ and $\overline{C}_4'$ have the following structure

$$\begin{aligned} \overline{I} &= (x_2x_3 + x_4l_1(x_3, x_4), x_4 + f_1(x_3, x_4)), \\ \overline{I}' &= (x_2x_3 + x_4l_2(x_2, x_3, x_4), x_4 + f_2(x_2, x_3, x_4)), \end{aligned}$$

for some linear forms l_1 and l_2 and quadratic forms f_1 and f_2. Now, by a map ϕ that replaces x_i by x_i plus higher order terms for $i = 2, 3, 4$, we get an isomorphism

$$\phi\colon \frac{\mathbb{F}_p[[x_2, x_3, x_4]]}{(x_2x_3, x_4)} \longrightarrow \frac{\mathbb{F}_p[[x_2, x_3, x_4]]}{\overline{I}},$$

which is the desired hypothesis for Lemma 84 part (2). We get a similar isomorphism involving $\overline{I}'$. So choose $w, z \in S$ such that

$$w \equiv \phi(x_2) \text{ and } z \equiv \phi(x_3)$$

modulo p. We are assuming P has thickness $k > 1$, so there exist power series $u, v \in S$ congruent to w and z respectively (using the map ψ in Lemma 84) such that

$$u(x_2, x_3, x_4)v(x_2, x_3, x_4) \equiv p^k \quad (Q_1(1, x_2, x_3, x_4), Q_2(1, x_2, x_3, x_4)).$$

Multiplying the third and fourth coefficients by p and writing (Q_1, Q_2) in terms of (Q_1', Q_2') means

$$\begin{aligned} &u(x_2, px_3, px_4)v(x_2, px_3, px_4) \equiv p^k \quad (Q_1(1, x_2, px_3, px_4), Q_2(1, x_2, px_3, px_4)), \\ &u(x_2, px_3, px_4)v(x_2, px_3, px_4) \equiv p^k \quad (pQ_1'(1, x_2, x_3, x_4), pQ_2'(1, x_2, x_3, x_4)). \end{aligned}$$

The line above shows that $p \mid u(x_2, px_3, px_4)v(x_2, px_3, px_4)$, but $p \nmid u(x_2, px_3, px_4) = x_2 + ...$, so we must have $p \mid v(x_2, px_3, px_4)$. Then dividing through by p means

$$\frac{1}{p}u(x_2, px_3, px_4)v(x_2, px_3, px_4) \equiv p^{k-1} \quad (Q_1'(1, x_2, x_3, x_4), Q_2'(1, x_2, x_3, x_4)),$$

so we choose

$$u'(x_2, x_3, x_4) = u(x_2, px_3, px_4) \text{ and } v'(x_2, x_3, x_4) = \frac{1}{p}v(x_2, px_3, px_4).$$

Note that since $k > 1$, we still have $u'v' \equiv 0 \bmod (p, I')$ and (modulo p) we also have

$$\begin{aligned} u'(x_2, x_3, x_4) &\equiv x_2 + \text{ higher order terms}, \\ v'(x_2, x_3, x_4) &\equiv \lambda x_2 + x_3 + \text{ higher order terms}. \end{aligned}$$

Thus u' and v' generate the maximal ideal in $\mathbb{F}_p[[x_2, x_3, x_4]]/\overline{I}'$ and therefore together with p, they generate the maximal ideal in S/I'. This gives us the hypotheses of Lemma 84 and therefore we have the isomorphism in Corollary 85

$$\frac{S}{I'} \cong \frac{\mathbb{Z}_p[[u', v']]}{(u'v' - p^{k-1})},$$

showing that the thickness of P' is $k - 1$.

(ii) As above, we can use Lemma 91 to get $L = \{x_3 = x_4 = 0\}$, $P = (1\colon 0\colon 0\colon 0)$ and $P_1 = (0\colon 1\colon 0\colon 0)$. The map ρ is given by

$$\rho\colon (s\colon t\colon 0\colon 0) \mapsto (s^2t\colon st^2\colon sF_1(s,t)\colon tF_2(s,t)),$$

but now since P is regular, $p \nmid a'_{11}$ and therefore $t \nmid F_1$. If P_1 is non-regular, then $p \mid b'_{22}$, meaning $s \mid F_2$ and then the image is parametrised by

$$(st\colon t^2\colon F_1(s,t)\colon t(b_{11}s + b_{12}t)).$$

There are now no common factors, so this parametrises a component of degree 2. However, if P_1 is regular then $F_2(s,t)$ does have a t^2 term and then neither s or t is a common factor of $\rho((s\colon t\colon 0\colon 0))$. Therefore in this case L maps to a component of degree 3.

□

Now let us divert our attention to the map χ.

Lemma 94 *Let C_4 be a 4-covering given by (Q_1, Q_2) with coefficients in $\mathbb{Z}_p$. Let $P \in \overline{C}_4(\mathbb{F}_p)$ be a non-regular point lying on a smooth component $\Gamma \subset \overline{C}_4$ defined over $\mathbb{F}_p$ and let $P_1 \in \overline{C}_4(\mathbb{F}_p)$ be the other singular point on Γ (if another exists). Also let the transformed QI be given by $C'_4 = \chi(Q_1, Q_2, P)$ with equations (Q'_1, Q'_2).*

(*i*) *If the degree* $\mathrm{d}(\Gamma) > 1$ *then there exists an isomorphism*

$$\rho_\chi\colon \{R \in C_4(\mathbb{Q}_p)\colon \overline{R} \in \Gamma \setminus \{P, P_1\}\} \mapsto \{R' \in C'_4(\mathbb{Q}_p)\colon \overline{R'} \in \Gamma' \setminus \{P'_1, P'_2\}\},$$

for some component $\Gamma' \subset \overline{C}'_4$ defined over $\mathbb{F}_p$ and singular points $P'_1, P'_2 \in \overline{C}_4(\mathbb{F}_p)$. Moreover if $\mathrm{d}(\Gamma) = 4$ *then* $\mathrm{d}(\Gamma') = 2$ *and if* $1 < \mathrm{d}(\Gamma) < 4$ *then* $\mathrm{d}(\Gamma') = \mathrm{d}(\Gamma) - 1$.

(*ii*) *If* Γ *is a line, then all the smooth points on* Γ *map to a non-regular point* P_1'.

Proof : By an $\mathrm{SL}_4(\mathbb{Z}_p)$ transformation, we may assume $P = (1\colon 0\colon 0\colon 0)$. If we take a general smooth point $(x_1\colon x_2\colon x_3\colon x_4) \in \overline{C}_4(\mathbb{F}_p)$, lift it to a $\mathbb{Q}_p$ point, apply χ and reduce it modulo p, we get $(0\colon x_2\colon x_3\colon x_4)$ and this has coprime entries since we have ruled out $x_2 = x_3 = x_4 = 0$.

To prove (*i*), first suppose $\mathrm{d}(\Gamma) = 4$. Then we can parametrise Γ by four coprime expressions of degree 4; i.e. (since we have a node) without loss of generality we can write it as

$$(s^4 + t^4\colon s^3t\colon s^2t^2\colon st^3).$$

Note that the point P is represented by $(s,t) = (1,0)$ or $(0,1)$. Now, after applying χ, we get

$$(0\colon s^3t\colon s^2t^2\colon st^3) = (0\colon s^2\colon st\colon t^2),$$

which defines a component of degree 2. If $\mathrm{d}(\Gamma) = 3$, then we can parametrise it by

$$(s^3\colon s^2t\colon st^2\colon t^3)$$

and $(s,t) = (1,0)$ represents the point P. Applying χ maps the smooth points to

$$(0\colon s^2t\colon st^2\colon t^3) = (0\colon s^2\colon st\colon t^2),$$

which also defines a component of degree 2. If $\mathrm{d}(\Gamma) = 2$ and it contains P, then without loss of generality it is parametrised by

$$(s^2\colon st\colon t^2\colon 0).$$

Applying χ maps the smooth points to

$$(0\colon st\colon t^2\colon 0) = (0\colon s\colon t\colon 0),$$

which defines a line.

(*ii*) Similarly, if Γ is a line, then all the smooth points map to $(0\colon 1\colon 0\colon 0)$, which we will refer to as P_1'. Lemma 91 shows that we may assume the matrices

for the QI modulo p are given by

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & a_{34} \\ 0 & 0 & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2b_{33} & b_{34} \\ 1 & 0 & b_{34} & 2b_{44} \end{pmatrix}$$

and therefore the transformed QI looks like

$$\overline{V}'_1 = \begin{pmatrix} 2a''_{11} & a'_{12} & a'_{13} & a'_{14} \\ a'_{12} & 0 & 1 & 0 \\ a'_{13} & 1 & 0 & a_{34} \\ a'_{14}0 & 0 & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}'_2 = \begin{pmatrix} 2b'_{11} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Since p divides the second row and column of V'_2 and $p \mid a_{22}$, P'_1 has the form of a singular point. Note that since we had $p \mid b_{22}$ and this gets multiplied by p under χ, we must also have that P'_1 is a non-regular point, as required.

□

Lemma 95 *Let C_4 be a 4-covering given by (Q_1, Q_2) with coefficients in $\mathbb{Z}_p$. Let $P \in \overline{C}_4(\mathbb{F}_p)$ be a non-regular point* not *lying on a smooth component $\Gamma \subset \overline{C}_4$ defined over $\mathbb{F}_p$ and let $P_1, P_2 \in \overline{C}_4(\mathbb{F}_p)$ be the two singular points on Γ. Also let the transformed QI be given by $C'_4 = \chi(Q_1, Q_2, P)$ with equations (Q'_1, Q'_2). Then there exists an isomorphism*

$$\rho_\chi \colon \{R \in C_4(\mathbb{Q}_p) \colon \overline{R} \in \Gamma \setminus \{P_1, P_2\}\} \mapsto \{R' \in C'_4(\mathbb{Q}_p) \colon \overline{R'} \in \Gamma' \setminus \{P'_1, P'_2\}\},$$

for some component $\Gamma' \subset \overline{C}'_4$ defined over $\mathbb{F}_p$ of the same degree as Γ and singular points $P'_1, P'_2 \in \overline{C}_4(\mathbb{F}_p)$.

Proof : We may assume $P = (1 \colon 0 \colon 0 \colon 0)$ and then since $P \notin \Gamma$, we can parametrise Γ as

$$(0 \colon f_2(s,t) \colon f_3(s,t) \colon f_4(s,t)),$$

for some expressions f_i of degree at most 2. Now, if we lift a smooth point on Γ to a $\mathbb{Q}_p$ point, apply χ and reduce modulo p, this has the effect of multiplying the first co-ordinate by p, therefore the expression for Γ' is the same as above and the lemma holds.

□

The next lemma will ensure our co-ordinates are arranged nicely before we apply χ.

Lemma 96 *Let (Q_1, Q_2) be a QI with coefficients in $\mathbb{Z}_p$. Suppose $L \subset \overline{C}_4$ is a line defined over $\mathbb{F}_p$ and let $P \in \overline{C}_4(\mathbb{F}_p)$ be a non-regular point on L. Also, let $(Q_1', Q_2') = \chi(Q_1, Q_2, P)$. Then, by replacing (Q_1, Q_2) with a $\mathbb{Z}_p$-equivalent QI, we may assume that $L = \{x_3 = x_4 = 0\}$, $P = (1 : 0 : 0 : 0)$, and*

$$(Q_1'(x_1, x_2, x_3, x_4), Q_2'(x_1, x_2, x_3, x_4)) \\ = \left(\frac{1}{p^2} Q_1(x_1, px_2, px_3, px_4), \frac{1}{p} Q_2(x_1, px_2, px_3, px_4)\right).$$

Also, by further rearrangement,

$$(\overline{Q}_1, \overline{Q}_2) = (x_2x_3 + f_1(x_3, x_4), x_1x_4 + x_4l_1(x_3, x_4)),$$

for some quadratic form f_1 and linear form l_1 and

$$(\overline{Q}_1', \overline{Q}_2') = (x_2x_3 + f_2(x_1, x_3, x_4), x_1x_4),$$

for some quadratic form f_2.

Proof : By Lemma 91, we may assume that L and P are of the correct form and that

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & a_{34} \\ 0 & 0 & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2b_{33} & b_{34} \\ 1 & 0 & b_{34} & 2b_{44} \end{pmatrix},$$

giving the correct form for $(\overline{Q}_1, \overline{Q}_2)$. Once P is given by $(1 : 0 : 0 : 0)$, we have the equations for $Q_i'(x_1, x_2, x_3, x_4)$ for $i \in \{1, 2\}$ by definition. It remains to check the structure of $(\overline{Q}_1', \overline{Q}_2')$. Currently we have

$$\overline{V}_1' = \begin{pmatrix} 2a_{11}'' & a_{12}' & a_{13}' & a_{14}' \\ a_{12}' & 0 & 1 & 0 \\ a_{13}' & 1 & 2a_{33} & a_{34} \\ a_{14}' & 0 & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2' = \begin{pmatrix} 2b_{11}' & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

We can see here that subtracting a multiple of row four from row one gets rid of the $2b'_{11}$ and subtracting a multiple of row three from row one gets rid of the a'_{12}. This amounts to subtracting multiples of p times rows three and four from row one in the matrices for $\overline{V}_1$ and $\overline{V}_2$ and gives us the desired form for the transformed QI.

□

Having arranged the co-ordinates nicely, before we move into a power series argument, we have a few awkward cases to deal with.

Lemma 97 *Let C_4 be a 4-covering given by (Q_1, Q_2) with coefficients in $\mathbb{Z}_p$. Let $P \in \overline{C}_4(\mathbb{F}_p)$ be a non-regular point and let the transformed QI be given by $C'_4 = \chi(Q_1, Q_2, P)$ with equations (Q'_1, Q'_2).*

(i) Let P lie on a component $\Gamma \subset \overline{C}_4$ defined over $\mathbb{F}_p$ of degree 4 and let Γ' be the image of Γ under ρ_χ (in the sense of Lemma 94). Then Γ' contains a singular point that is regular (not necessarily defined over $\mathbb{F}_p$).

(ii) Let P lie on the intersection of two conics $\Gamma_1, \Gamma_2 \subset \overline{C}_4$ defined over $\mathbb{F}_p$ and let Γ'_1, Γ'_2 be their respective images under ρ_χ. Then the line Γ'_1 contains a singular point that is regular and does not lie on Γ'_2.

Proof : We may assume $P = (1 : 0 : 0 : 0)$. To prove (i), we know by an $\mathrm{SL}_2(\mathbb{Z}_p)$ transformation we may assume the matrices for the QI modulo p are given by

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2a_{22} & a_{23} & a_{24} \\ 0 & a_{23} & 2a_{33} & a_{34} \\ 0 & a_{24} & a_{34} & 2a_{44} \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & b_{12} & b_{13} & b_{14} \\ b_{12} & 2b_{22} & b_{23} & b_{24} \\ b_{13} & b_{23} & 2b_{33} & b_{34} \\ b_{14} & b_{24} & b_{34} & 2b_{44} \end{pmatrix}.$$

Now p does not divide all of b_{12}, b_{13} and b_{14}, so we may assume $b_{14} = 1$ and then by subtracting multiples of row four from rows two and three, we get $p \mid b_{12}$ and b_{13}. If we can ensure $p \mid a_{22}$, then after operating by χ we would have a singular point at $P'_1 = (0 : 1 : 0 : 0)$. It would also be regular, since $\overline{C}_4$ does not contain a line (and therefore $p \nmid b_{22}$).

We are allowed any transformation involving x_2, x_3 (since that will not affect b_{12} and b_{13}) to try to get $p \mid a_{22}$. It would suffice to find a solution to the conic

$$h(x_2, x_3) = a_{22}x_2^2 + a_{23}x_2x_3 + a_{33}x_3^2 = 0,$$

since we could move the solution to $(x_2, x_3) = (1, 0)$ and be done. To see that this conic does have a solution, let us consider it in affine space, where our QI has the form

$$f(x_2, x_3, x_4) = x_4 + g(x_2, x_3, x_4) = 0.$$

If we then take the tangent cone at the origin, we get $x_4 = f(x_2, x_3, x_4) = 0$, i.e $f(x_2, x_3, 0) = h(x_2, x_3) = 0$ and this conic must have a solution[32]. Hence $p \mid a_{22}$ and we may assume $b_{22} \equiv 1$, so $\overline{C}_4'$ contains the regular point P_1'. From the proof of Lemma 94, Γ' can be parametrised by

$$(0 \colon s^2 \colon st \colon t^2),$$

so $P_1' \in \Gamma'$ too.

(*ii*) The intersection of two conics containing P can be parametrised by

$$(s^2 \colon st \colon t^2 \colon 0) \text{ and } (t^2 \colon 0 \colon s^2 \colon st),$$

from which we can read off the equations for the QI as

$$x_2 x_4 = x_1 x_3 - x_2^2 - x_4^2 = 0.$$

The matrices for the QI modulo p have the form

$$\overline{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \qquad \overline{V}_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}.$$

After the operation of χ, the components Γ_1' and Γ_2' are given by

$$(0 \colon s \colon t \colon 0) \text{ and } (0 \colon 0 \colon s \colon t)$$

[32]Note that if we have split multiplicative reduction, then these tangents are defined over $\mathbb{F}_p$ and therefore so too is the regular point. This is not the case for non-split reduction.

and the matrices for $\overline{C}_4'$ modulo p look like

$$\overline{V}_1' = \begin{pmatrix} 2a_{11}'' & a_{12}' & a_{13}' & a_{14}' \\ a_{12}' & 0 & 0 & 1 \\ a_{13}' & 0 & 0 & 0 \\ a_{14} & 1 & 0 & 0 \end{pmatrix}, \qquad \overline{V}_2' = \begin{pmatrix} 2b_{11}' & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Therefore the point $(0\colon 1\colon 0\colon 0) \in \overline{C}_4'(\mathbb{F}_p)$ is singular and lies on Γ_1', but not Γ_2'. It is also regular, since $p \nmid b_{22}$.

□

Lemma 98 *Let C_4 be a 4-covering given by (Q_1, Q_2) with coefficients in $\mathbb{Z}_p$. Suppose $\overline{C}_4$ contains a line L defined over $\mathbb{F}_p$. Let $P \in \overline{C}_4(\mathbb{F}_p)$ be a non-regular point on L and $P_1 \in \overline{C}_4(\mathbb{F}_p)$ the other singular point on L. Also let the transformed QI be given by $C_4' = \chi(Q_1, Q_2, P)$ with equations (Q_1', Q_2') and let P_1' be the image of the smooth points on L under the operation ρ_χ (in the sense of Lemma 94). Then $\tau(P_1', Q_1', Q_2') = \tau(P_1, Q_1, Q_2) + 1$.*

Proof : Lemma 91 allows us to assume that L is given by $\{x_3 = x_4 = 0\}$, $P = (1\colon 0\colon 0\colon 0)$, $P_1 = (0\colon 1\colon 0\colon 0)$ and Lemma 94 shows that we may assume $P_1' = (0\colon 1\colon 0\colon 0)$. Lemma 96 shows that working in affine co-ordinates by setting $x_2 = 1$, the ideals generated by the equations for $\overline{C}_4(\mathbb{F}_p)$ and $\overline{C}_4'(\mathbb{F}_p)$ have the following structure:

$$\begin{aligned} \overline{I} &= (x_3 + f_1(x_3, x_4), x_1x_4 + x_3l(x_3, x_4)), \\ \overline{I}' &= (x_3 + f_2(x_1, x_3, x_4), x_1x_4), \end{aligned}$$

for some linear form l and quadratic forms f_1 and f_2. Now, by a map ϕ that replaces x_i by x_i plus higher order terms for $i = 1, 3, 4$, we get an isomorphism

$$\phi\colon \frac{\mathbb{F}_p[[x_1, x_3, x_4]]}{(x_1x_4, x_3)} \longrightarrow \frac{\mathbb{F}_p[[x_1, x_3, x_4]]}{\overline{I}'},$$

which is the desired hypothesis for Lemma 84 part (2). We get a similar isomorphism involving $\overline{I}$. So choose $w, z \in S = \mathbb{Z}_p[[x_1, x_3, x_4]]$ such that

$$w \equiv \phi(x_1), \quad z \equiv \phi(x_4)$$

modulo p. Then, if we assume P_1' has thickness $k > 1$, there exist power series $u', v' \in S$ congruent to w and z respectively such that

$$u'(x_1, x_3, x_4)v'(x_1, x_3, x_4) \equiv p^k \quad (Q_1'(x_1, 1, x_3, x_4), Q_2'(x_1, 1, x_3, x_4)).$$

Writing Q_1' and Q_2' in terms of Q_1 and Q_2 means

$$u'(x_1, x_3, x_4)v'(x_1, x_3, x_4) \equiv p^k \quad \left(Q_1\left(\frac{x_1}{p}, 1, x_3, x_4\right), pQ_2\left(\frac{x_1}{p}, 1, x_3, x_4\right)\right).$$

Therefore, over $\mathbb{F}_p[[x_1, x_3, x_4]]$, there exists a power series F such that

$$u'(px_1, x_3, x_4)v'(px_1, x_3, x_4) = F(px_1, x_3, x_4)Q_1(x_1, 1, x_3, x_4).$$

Now, $v'(px_1, x_3, x_4) = x_4+$ higher order terms and $Q_1(x_1, 1, x_3, x_4) = x_3+$ higher order terms, so they are both irreducible over $\mathbb{F}_p[[x_1, x_3, x_4]]$ (which is a unique factorisation domain). Therefore

$$u'(px_1, x_3, x_4) = f(px_1, x_3, x_4)Q_1(x_1, 1, x_3, x_4) + pu''(px_1, x_3, x_4),$$

for some $f, u'' \in S$. We have the freedom to adjust u' by multiples of Q_1, therefore we can ensure that $p \mid u'(px_1, x_3, x_4)$ using the above equation[33]. Thus we can write

$$u'(px_1, x_3, x_4)v'(px_1, x_3, x_4) - p^k = F_1Q_1(x_1, 1, x_3, x_4) + pF_2Q_2(x_1, 1, x_3, x_4),$$

for some power series F_1 and F_2 and p divides the left hand side, so we must have $p \mid F_1$. Dividing through by p then means we have

$$\frac{1}{p}u'(px_1, x_3, x_4)v'(px_1, x_3, x_4) \equiv p^{k-1} \quad (Q_1(x_1, 1, x_3, x_4), Q_2(x_1, 1, x_3, x_4)),$$

so let us choose

$$u(x_1, x_3, x_4) = \frac{1}{p}u'(px_1, x_3, x_4), \quad v(x_1, x_3, x_4) = v'(px_1, x_3, x_4).$$

[33] We replace u' by pu''.

Note $k > 1$, so we still have $uv \equiv 0 \bmod (p, I)$ and (modulo p) we also have

$$u(x_1, x_3, x_4) = x_1 + \lambda x_3 + \mu x_4 + \text{ higher order terms},$$
$$v(x_1, x_3, x_4) = x_4 + \text{ higher order terms}.$$

So u and v are linearly independent and span a space of dimension 2, therefore they generate the maximal ideal in $\mathbb{F}_p[[x_1, x_3, x_4]]/\bar{I}$. So, together with p, they generate the maximal ideal in S/I. This gives the hypothesis of Lemma 84 and therefore the required isomorphism in Corollary 85

$$\frac{S}{I} \cong \frac{\mathbb{Z}_p[[u, v]]}{(uv - p^{k-1})},$$

showing that the thickness of P_1 is $k - 1$.

□

Proof of Theorem 89:

1. Lemma 90 shows

   $$\Phi\colon [a, b, c, d] \mapsto [a, ?, ?, ?].$$

   Lemma 93 (*i*) shows that if $d \not\equiv a - 1$ then the thickness of the non-regular point between components d and a drops by one, i.e.

   $$\Phi\colon [a, b, c, d] \mapsto [a, ?, ?, d + 1]$$

   and similarly if $b \not\equiv a + 1$ then

   $$\Phi\colon [a, b, c, d] \mapsto [a, b - 1, ?, ?].$$

   Lemma 93 (*ii*) shows that if the point between components d and a is regular then we see the component a at least twice in the image, i.e.

   $$\Phi\colon [a, b, c, a - 1] \mapsto [a, ?, ?, a]$$

   and

   $$\Phi\colon [a, a + 1, c, d] \mapsto [a, a, ?, ?].$$

   Therefore we have

   $$\Phi\colon [a, b, c, d] \mapsto [a, b - 1, ?, d + 1]$$

in all cases and since the sum $s = a + b + c + d$ remains constant, we must have

$$\Phi\colon [a, b, c, d] \mapsto [a, b - 1, c, d + 1],$$

as required.

2. Lemma 95 shows that if $a \neq b$ and $c \neq d$ then

$$\chi\colon [a, b, c, d] \mapsto [?, b, c, ?].$$

It also shows that if $a \neq b$ and $b \neq c$ then

$$\chi\colon [a, b, c, c] \mapsto [?, b, ?, ?].$$

Then Lemma 94 shows the following:

$$\begin{aligned}\chi\colon [a, a, a, a] &\mapsto [?, a, a, ?],\\ [a, b, b, b] &\mapsto [?, b, b, ?],\\ [a, b, c, c] &\mapsto [?, ?, c, ?],\\ [a, a, b, b] &\mapsto [?, a, b, ?],\end{aligned}$$

for distinct entries a, b and c. Lemma 97 (i) shows that the image of a component of degree 4 always contains a regular point, so in fact we know

$$\chi\colon [a, a, a, a] \mapsto [a - 1, a, a, ?] \text{ or } [?, a, a, a + 1].$$

Similarly, Lemma 97 (ii) shows that for $a \neq b$,

$$\chi\colon [a, a, b, b] \mapsto [a - 1, a, b, ?] \text{ or } [?, a, b, b + 1].$$

Now, using Lemma 98, we know that if $a \neq b$, then the thickness of the point between a and b goes up by one under the operation of χ. Therefore, since we have established that in all cases if $a \neq b$ that

$$\chi\colon [a, b, c, d] \mapsto [?, b, c, ?],$$

we have Lemma 98 implies

$$\chi\colon [a, b, c, d] \mapsto [a - 1, b, c, ?].$$

We have now determined all but one entry of the bracket in all cases, so invoking the fact that the sum of the entries remains constant, we must have

$$\chi\colon [a,b,c,d] \mapsto [a-1,b,c,d+1],$$

as required.

3. This is a corollary of the previous part.

□

This gives us an algorithm for getting to a vertex where a can be seen at least 3 times, as described in the following lemma.

Lemma 99 *Given $P \in C_4(\mathbb{Q}_p)$, there exists a unique minimal QI which is $\mathbb{Q}_p$-equivalent to C_4 such that when mapped to this equivalence class, P reduces to a smooth point on a component of degree at least 3.*

Proof : Let P be on component a in the reduction of C_4 and let s be the sum of the components in the bracket $[a,?,?,?]$ modulo n. Then, we also have the equivalence class $[a,a,a,s-3a]$ in the graph of equivalence classes. This can be reached using the following method.

Applying Φ to the component a will never decrease the degree of that component and there is only a finite number of vertices with a occurring once. This process will not loop, so eventually a will occur with higher multiplicity. If this only gets us to a conic $[a,a,c,d]$, then 'flipping' the (possibly degenerate) conic cd will not decrease the degree of a and so we eventually see a three times.

□

Lemma 100 *Only $\mathbb{Z}_p$-equivalence classes of QIs where a component is seen at least three times need to be considered when computing ε_p from the graph of equivalence classes.*

Proof : If a point is singular or if it lies on a line or conic, then we must use one of the operations Φ, χ or χ^{-1} to compute its contribution.

□

These equivalence classes are in some sense analogous to the end quartics in section 2.6, since they have no contribution apart from on the component that would return us to a previous class.

Note that the above two results also hold for additive reduction, but we must adjust the definition of the sum.

4.1.2 Application to Reduction Type I_4

The theorem in the previous section gives us a toolkit for generating the whole graph from one starting vertex. Let us illustrate this with the graph for I_4 starting from the equivalence class represented by $[0,0,0,0]$. Note that since n is even, this is not the only graph for I_4 and there are separate ones for $s = 1$ and $s = 2$ (note the graph for $s = 3$ is identical to that for $s = 1$). To assist us, we can write down all the vertices with $s = 0$ straight away:

$$[0,0,0,0],[0,0,1,3],[0,0,2,2],[0,1,1,2],[0,2,3,3],$$
$$[1,1,1,1],[1,1,3,3],[1,2,2,3],[2,2,2,2],[3,3,3,3].$$

From the starting vertex, there is only one possible operation; that is applying χ to the singular point. Thus

$$\chi\colon [0,0,0,0] \mapsto [3,0,0,1] = [0,0,1,3].$$

At this new vertex, we have four possible transformations (apart from returning to the start), the brackets on the left represent the same QI:

$$[0,0,1,3] \overset{\chi^{-1}}{\longmapsto} [3,1,1,3] = [1,1,3,3],$$
$$[1,3,0,0] \overset{\Phi}{\longmapsto} [1,2,0,1] = [0,1,1,2],$$
$$[3,0,0,1] \overset{\Phi}{\longmapsto} [3,3,0,2] = [0,2,3,3],$$
$$[3,0,0,1] \overset{\chi}{\longmapsto} [2,0,0,2] = [0,0,2,2].$$

Then continuing with the new vertices until we have found all the possible edges:

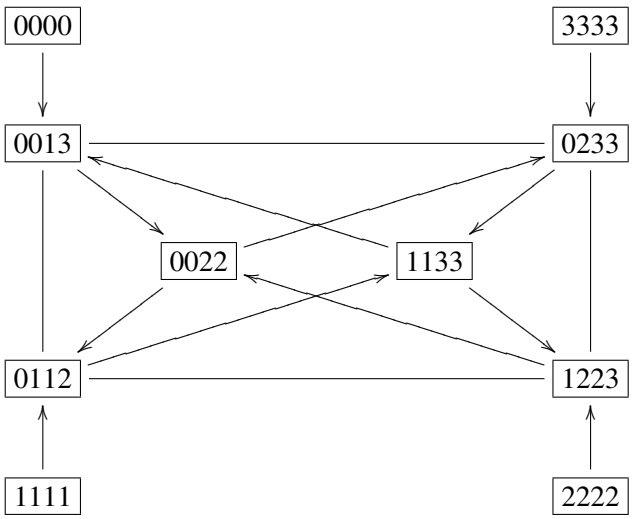
$$[1,1,2,0] \overset{\chi^{-1}}{\longmapsto} [0,2,2,0] = [0,0,2,2],$$
$$[2,0,1,1] \overset{\chi^{-1}}{\longmapsto} [1,1,1,1],$$
$$[2,0,1,1] \overset{\Phi}{\longmapsto} [2,3,1,2] = [1,2,2,3].$$

$$[1,1,3,3] \overset{\chi^{-1}}{\longmapsto} [0,2,3,3],$$
$$[3,3,1,1] \overset{\chi^{-1}}{\longmapsto} [2,0,1,1] = [0,1,1,2],$$
$$[3,3,1,1] \overset{\chi}{\longmapsto} [2,3,1,2] = [1,2,2,3].$$

$$[3,3,0,2] \overset{\chi^{-1}}{\longmapsto} [2,0,0,2] = [0,0,2,2],$$
$$[0,2,3,3] \overset{\chi^{-1}}{\longmapsto} [3,3,3,3],$$
$$[2,3,3,0] \overset{\Phi}{\longmapsto} [2,2,3,1] = [1,2,2,3].$$

$$[3,1,2,2] \overset{\chi^{-1}}{\longmapsto} [2,2,2,2],$$
$$[1,2,2,3] \overset{\chi}{\longmapsto} [0,2,2,0] = [0,0,2,2].$$

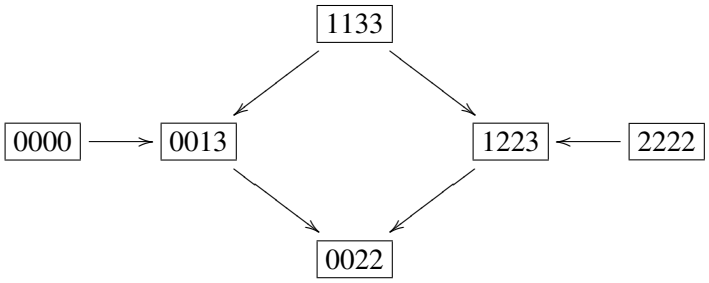
This gives us all the edges:



where lines represent the map Φ and arrows χ.

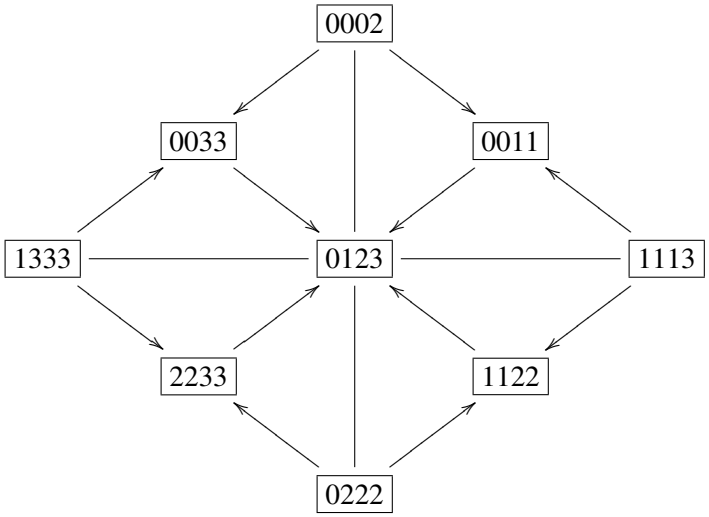
Now the furthest vertex from $[0,0,0,0]$ is $[2,2,2,2]$ and this means ε_p would be p^{-16} at $[0,0,0,0]$. However, if we were to search on the QI represented by $[0,0,2,2]$, then we would actually find ε_p to be p^{-8}.

It is also worth noting that we can easily derive the graph for $c_p = 1$ or 2 from this. Since n is even, we can have $c_p = 2$, meaning that the Galois action swaps components 1 and 3. So we have the subgraph of those nodes fixed by Galois, i.e.

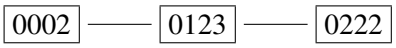


Here it is best to search on a QI represented by $[0,0,2,2]$, since then ε_p is only p^{-4}. In contrast to the graph above for split multiplicative reduction, here we have a unique vertex which gives the best bound.

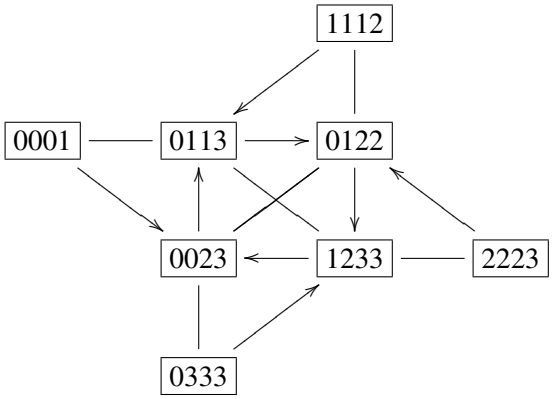
We will now include the graphs for $s = 2$ for split multiplicative reduction:



and for non-split multiplicative reduction:



Here the best bound we can get is p^{-4} at vertex $[0, 1, 2, 3]$ for both graphs. For $s = 1$ there is no non-split multiplicative case, but the graph for split multiplicative reduction is



Here the best bound is p^{-8} at one of the four central vertices.

4.2 Program Output

We have seen above how it is possible to construct a graph of equivalence classes for multiplicative reduction I_m. It is the sort of algorithmic construction that lends itself nicely to a computer, so we will show the following output from MAGMA.

For $m = 1$, there is one equivalence class where the component is seen four times, so the graph is a single vertex and $\varepsilon_p = 1$.

For $m = 2$, if the sum $s = 0$, then there are three equivalence classes and the graph is a line of three vertices: $[0, 0, 0, 0]$, $[0, 0, 1, 1]$ and $[1, 1, 1, 1]$. The contributions ε_p are given as p^{-8}, p^{-2} and p^{-8} respectively. If $s = 1$, then there are only two vertices in the graph, both giving $\varepsilon_p = p^{-4}$.

For $m = 3$, we get the same graph for each value of s (since m is coprime to 4). There are five equivalence classes, giving contributions of $\varepsilon_p = p^{-k}$ for $k = 4, 8, 8, 8$ and 10 respectively. This is the same as the graph from the naive example in section 4.1.

For $m = 4$, if $s = 0$, we get the graph in the previous section, so there are 10 vertices and the contributions are $\varepsilon_p = p^{-k}$ for $k = 8, 8, 10, 10, 10, 10, 16, 16, 16$ and 16. If $s = 1$ (or 3), we get a graph of 8 vertices with $k = 8, 8, 8, 8, 12, 12, 12$ and 12 and if $s = 2$, we get 9 vertices with $k = 4, 8, 8, 8, 8, 10, 10, 10$ and 10.

The remaining results up to $m = 20$ are shown in the table below. The value of ε_p is given as the k in p^{-k}. We give the best value of k and at how many vertices this is achieved, as well as the worst value of k. The number of vertices in the graph is given by N and we can check that summing the values of N for each value of s gives us the number of brackets $[a, b, c, d]$ for a given m, i.e. $m(m+1)(m+2)(m+3)/24$.

m	s	N	Best k	Worst k	m	s	N	Best k	Worst k
1	0	1	0(1)	0	12	0	116	20(2)	48
2	0	3	2(1)	8		1	112	20(4)	44
	1	2	4(2)	4		2	115	16(1)	42
3	0	5	4(1)	10	13	0	140	20(1)	50
4	0	12	8(2)	16	14	0	172	22(2)	56
	1	8	8(4)	12		1	168	22(2)	52
	2	9	4(1)	10	15	0	204	24(3)	58
5	0	14	8(1)	18	16	0	245	24(1)	64
6	0	22	10(2)	24		1	240	26(4)	60
	1	20	10(2)	20		2	244	24(2)	58
7	0	30	12(3)	26	17	0	285	26(2)	66
8	0	43	12(1)	32	18	0	335	26(1)	72
	1	40	14(4)	28		1	330	28(2)	68
	2	42	12(2)	26	19	0	385	28(1)	74
9	0	55	14(2)	34	20	0	434	32(2)	80
10	0	73	14(1)	40		1	428	32(4)	76
	1	70	16(2)	36		2	425	28(1)	74
11	0	91	16(1)	42					

The first thing to notice from this table is that there are strong similarities between m and $m + 8$ (starting at say $m = 4$), which suggests that the structure of the centre of the graph stays roughly the same. It seems to be the case that the best vertices see four components spaced as evenly as possible round the polygon.

The best k increases each time we increase m and the relationship seems to be $k \approx 3m/2$, but that is going only by the results above. The worst k never exceeds $4m$, because this is the maximum diameter of the graph; i.e. the distance from $[0,0,0,0]$ to $[m/2, m/2, m/2, m/2]$ if m is even and $s = 0^{34}$. The diameter is slightly less for other s or if m is odd.

Overall, this shows that we can make more than a factor of two difference if we choose our starting equivalence class to be at the centre of these graphs as opposed to the edge.

We can compare this with our findings at $n = 2$. We saw that for multiplicative reduction, if N is the number of vertices in the graph (all in a line), then the best bound we can get is $k = N - 1$ or $k = N$, depending on the parity of N. The worst k was $2N$, starting at either end of the graph. By consulting Sadek's table in [Sad10a], we see that for reduction type I_m, N is approximately $m/2$, so we are comparing m for binary quartics with $4m$ for QIs. Now recall that in the former case, the bound is divided by 4 and in the latter by 8. This means the bounds we work with are (approximately) only double the size on QIs compared to binary quartics. So we are definitely better to work with QIs, since there is still the extra factor of two dividing the height of the point on the elliptic curve. It also suggests that minimisation becomes even more important for 4-coverings than for 2-coverings.

4.2.1 An Application

Now let us consider a large example and see if any improvements can be made to point-searching using our knowledge of the structure of these graphs. Let us consider the elliptic curve (found by Dujella, see [Duj]) given by

$$E: y^2 + xy = x^3 - 38837881159624688541650399995251089392 0x + 29459909281655453303137155419740890801127814976005254277 12,$$

[34] This is $m/2$ applications of χ until we have $[0, m/2, m/2, 0]$ followed by $m/2$ applications of χ^{-1} applied to the conic representing the $m/2$ component to get $[m/2, m/2, m/2, m/2]$. Counting the weighted edges, this has distance $(6+2)m/2 = 4m$.

which has the following bad primes and reduction types:

2	3	5	7	11	31	47	53	97	193	317	407	601	1033
I_{16}	I_8	I_4	I_8	I_8	I_8	I_8	I_4	I_2	I_2	I_8	I_4	I_2	I_2

If we ignore torsion (this has full 2-torsion), then 4-descent yields a set $\{C_{4,i}\}$ of 28 curves[35]. On each one, we took the three largest bad primes (409, 601 and 1033) and constructed their graphs of equivalence classes. We took representatives from each equivalence class where a component could be seen with degree at least 3 (there are two of these for $p = 1033$ and 601 and four for 409). We then found reduced 4-coverings equivalent to each of the 16 combinations that this provides. This meant that if one of the $C_{4,i}$ contained a point, that point would be smooth at *all* of the three primes on at least one of these 16 possibilities.

Only one of the 28 curves produced a point in this manner when we searched up to $H(P) = 10^6$, namely the curve

$$\begin{aligned} C_{4,14}\colon\ & 121x_1^2 + 77696x_1x_2 + 8340x_1x_3 + 30221x_1x_4 + 7568x_2^2 + 12177x_2x_3 + \\ & 10490x_2x_4 + 9643x_3^2 - 20190x_3x_4 - 9814x_4^2 = 0, \\ & 107370x_1^2 + 46217x_1x_2 - 91866x_1x_3 - 10196x_1x_4 - 9822x_2^2 - 39019x_2x_3 \\ & + 105777x_2x_4 - 10375x_3^2 - 8198x_3x_4 - 5908x_4^2 = 0. \end{aligned}$$

A search up to $H(P) = 10^8$ was needed to find a point on this curve itself:

$$(-8556741\colon\ -110404787\colon 142301810\colon 34455771),$$

but a point of smaller height was found in one of the other 16 equivalence classes. We took that equivalence class and then repeated the process with the graphs for $p = 47, 53, 97, 193$ and 317, which gave the possibility of the following curve:

$$\begin{aligned} & 15459x_1x_2 + 10188x_1x_3 + 24625x_1x_4 + 1383x_2^2 + 470x_2x_3 + 97728x_2x_4 + \\ & 3143x_3^2 - 36202x_3x_4 - 43088x_4^2 = 0, \\ & 82188x_1x_2 + 57858x_1x_3 + 185618x_1x_4 + 26501x_2^2 + 26012x_2x_3 - 27041x_2x_4 \\ & + 1351x_3^2 + 67613x_3x_4 + 92512x_4^2 = 0. \end{aligned}$$

[35] I am very grateful to Tom Fisher for sending me the 28 curves. The 4-descent routine on the current version of MAGMA was not up to the task for such a large curve and we required a (preliminary) improved routine which is specific to curves with rational 2-torsion.

This is in a different $\mathbb{Z}_p$-equivalence class for the eight largest bad primes, but is equivalent over $\mathbb{Q}_p$ and it contains (by inspection!) the point $(1:0:0:0)$. Both this point and the one found on $C_{4,14}$ correspond to the same point on E.

This example demonstrates two things. Firstly that the height of a point can vary dramatically depending on our choice of 4-covering, so simply minimising and reducing is not enough to find the best curve to use. Secondly, it shows that 4-descent does not always find the best curve on which to search.

In running this sort of search to find new points, it is a bit impractical to find the graphs for all the bad primes and then find all the combinations where we see a component at least three times (for the above example, that would be 2^{32} curves), but by doing so at just the large primes, we certainly save ourselves a lot of time in actual point-searching.

5 Conclusion

As a summary, in this thesis we have shown how to compute explicitly a bound for the height difference between a point on an elliptic curve and its corresponding point on a 2- or 4-covering. The bounds turned out to be fairly small and in particular they were better than those achieved by previous methods.

We have shown that it is more important to optimise the bound at the finite places than at infinity, since these contributions make up the majority of the bound. For both $n = 2$ and $n = 4$, we showed how a graph of $\mathbb{Z}_p$-equivalence classes can be constructed and showed how to find the vertices that would give the best bounds at each finite place.

This was of particular interest when $n = 4$ and the elliptic curve had multiplicative reduction, since the graphs could become large. We gave the details of the graphs for reduction type I_m for $m \leq 20$ in section 4.2. We then used these ideas to exhibit an application, which improved a search for points on a 4-covering of large conductor.

5.1 Directions for Further Study

The first task would be to fully implement the calculation of ε_2 for QIs. This should not involve any further theoretical work, but the current routine would have to be completely overhauled so as to avoid viewing any QIs in matrix form. This would take some time, but should not be too hard.

Currently, our investigations into the graph of equivalence classes can give us a 'best' single vertex which we should use for a search or a set of c_p different vertices. It might be interesting to investigate the possibility of a compromise; i.e. if we were only willing to use N vertices to search, for $1 < N < c_p$, which would be the best ones? This would involve partitioning the graph and choosing a representative from each subset of vertices.

The next obvious step would be to attempt to calculate a height bound between E and 3-coverings. There are good methods for minimising and reducing ternary cubics, so that would not be a sticking point. We would have to understand the 3-covering map in detail, whose equations are a little more complicated than

either the 2-covering map or the 4-to-2-covering map, but not unworkable (indeed not as intimidating as the full 4-covering map). An analogue of ε_p would then be straightforward to define and Theorem 4.2 in [Sad10a] suggests that a graph of $\mathbb{Z}_p$-equivalence classes could be drawn and analysed in a similar way. The bounds obtained from ternary cubics would not be as powerful as those we have calculated from QIs, but there may be reasons why the situation would be simpler or easier to implement on a computer.

The methods we have used could also be applied to 8-coverings, but there is currently no theory of minimisation for these curves (although I am led to believe this is on the way), so investigations along these lines would be likely to run into difficulties at present. However if something were possible, we might expect the bounds to be not much greater than in the $n = 4$ case. We saw a contribution of at most $p^{-m/4}$ at the $n = 2$ level becoming at most $p^{-m/2}$ at the $n = 4$ level for multiplicative reduction of type I_m, so perhaps we could expect no worse than p^{-m} for $n = 8$ if we could minimise and define a graph of equivalence classes sensibly. Investigations into 3- and 8-coverings could also lead to a generalisation for higher values of n.

I believe that most of the theory could be generalised to a number field K, but since so much relies on the descent algorithms, it makes sense to continue over $\mathbb{Q}$. There is also no real theory of minimisation or reduction over a number field, which somewhat forces our hand.

References

[AKM+01] S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum, and A. R. Perlis. Jacobians of genus one curves. *J. Number Theory*, 90(2):304–315, 2001.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Cas62] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.

[Cas67] J. W. S. Cassels. Corrigenda: "Survey article—Diophantine equations with special reference to elliptic curves". *J. London Math. Soc.*, 42:183, 1967.

[Cas91] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[CFS09] J. E. Cremona, T. Fisher, and M. Stoll. Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves. *http://www.dpmms.cam.ac.uk/ taf1000/papers/minred-234.html*, 2009.

[CLO97] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[CLO05] D. A. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[CM00] J. E. Cremona and B. Mazur. Visualizing elements in the Shafarevich-Tate group. *Experiment. Math.*, 9(1):13–28, 2000.

[CPS06] J. E. Cremona, M. Prickett, and S. Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[Cre01] J. E. Cremona. Classical invariants and 2-descent on elliptic curves. *J. Symbolic Comput.*, 31(1-2):71–87, 2001. Computational algebra and number theory (Milwaukee, WI, 1996).

[Cre08] J. E. Cremona. Computing in component groups of elliptic curves. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 118–124. Springer, Berlin, 2008.

[DLLP08] L. Dupont, D. Lazard, S. Lazard, and S. Petitjean. Near-optimal parameterization of the intersection of quadrics. II. A classification of pencils. *J. Symbolic Comput.*, 43(3):192–215, 2008.

[Duj] A. Dujella. *Elliptic Curves Tables*. http://www.web.math.hr/ duje/.

[EH00] D. Eisenbud and J. Harris. *The geometry of schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Fis06] T. Fisher. Testing equivalence of ternary cubics. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 333–345. Springer, Berlin, 2006.

[Fis07] T. Fisher. A new approach to minimising binary quartics and ternary cubics. *Math. Res. Lett.*, 14(4):597–613, 2007.

[Fis08] T. Fisher. Finding rational points on elliptic curves using 6-descent and 12-descent. *J. Algebra*, 320(2):853–884, 2008.

[GKZ08] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants and multidimensional determinants*. Modern Birkhäuser Classics. Birkhäuser Boston Inc., Boston, MA, 2008. Reprint of the 1994 edition.

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[HP94] W. V. D. Hodge and D. Pedoe. *Methods of algebraic geometry. Vol. II*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1994. Book III: General theory of algebraic varieties in

projective space, Book IV: Quadrics and Grassmann varieties, Reprint of the 1952 original.

[HS00] M. Hindry and J. H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[Hul86] K. Hulek. Projective geometry of elliptic curves. *Astérisque*, (137):143, 1986.

[Liu94] Q. Liu. Modèles minimaux des courbes de genre deux. *J. Reine Angew. Math.*, 453:137–164, 1994.

[Liu02] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[MSS96] J. R. Merriman, S. Siksek, and N. P. Smart. Explicit 4-descents on an elliptic curve. *Acta Arith.*, 77(4):385–404, 1996.

[Sad10a] M. M. Sadek. Counting models of genus one curves. 2010.

[Sad10b] M. M. Sadek. Minimal genus one curves. 2010.

[SC02] M. Stoll and J. E. Cremona. Minimal models for 2-coverings of elliptic curves. *LMS J. Comput. Math.*, 5:220–243 (electronic), 2002.

[SC03] M. Stoll and J. E. Cremona. On the reduction theory of binary forms. *J. Reine Angew. Math.*, 565:79–99, 2003.

[Ser02] J-P. Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[Sik95] S. Siksek. Infinite descent on elliptic curves. *Rocky Mountain J. Math.*, 25(4):1501–1538, 1995.

[Sil88] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.

[Sil90] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sta05] S.K.M Stamminger. Explicit 8-descent on elliptic curves. 2005.

[Sto] M. Stoll. *Short Course Lecture Notes: Descent on Elliptic Curves*. http://www.faculty.jacobs-university.de/mstoll/schrift.html.

[SZ03] S. Schmitt and H. G. Zimmer. *Elliptic curves*, volume 31 of *de Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin, 2003. A computational approach, With an appendix by Attila Pethö.

[Tho08] T. Thongjunthug. Computing a lower bound for the canonical height on elliptic curves over totally real number fields. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 139–152. Springer, Berlin, 2008.

[Uch06] Y. Uchida. On the difference between the ordinary height and the canonical height on elliptic curves. *Proc. Japan Acad. Ser. A Math. Sci.*, 82(3):56–60, 2006.

[Wei54] A. Weil. Remarques sur un mémoire d'Hermite. *Arch. Math. (Basel)*, 5:197–202, 1954.

[Wei83] A. Weil. Euler and the Jacobians of elliptic curves. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 353–359. Birkhäuser Boston, Boston, MA, 1983.

[Wom03] T. Womack. Explicit descent on elliptic curves. 2003.

[Zim76] H. G. Zimmer. On the difference of the weil height and the néron-tate height. *Math. Z.*, 147(1):35–51, 1976.