POWER INTEGRAL POINTS ON ELLIPTIC CURVES

Daniel Buck

A thesis submitted for the degree of Doctor of Philosophy

University of East Anglia

School of Mathematics

September 2014

Abstract

This thesis looks at some of the modern approaches towards the solution of Diophantine equations, and utilizes them to display the nonexistence of perfect powers occurring in certain types of sequences. In particular we look at the denominator divisibility sequences (B_n) formed by Mordell elliptic curves $E_D\colon y^2 = x^3 + D$. For the curve-point pair (E_{-2}, P), where $E_{-2}\colon y^2 = x^3 - 2$, and $P = (3, 5)$ is a nontorsion point, we prove that no term B_n is a perfect 5^{th} power, and we give the explicit bound $p \leq 137$ for any term in the associated elliptic denominator sequence to be a perfect power $B_n = Z_n^p$ for $1 < n < 113762879$. We then look at obtaining upper bounds on p for the seventy-two rank 1 Mordell curves in the range $|D| < 200$ to possess a p^{th} perfect power. This is done by consideration of the finite number of rational and irrational newforms corresponding to an also finite number of levels of these newforms: in thirty cases we give a bound via examination of both the rational and irrational cases, and for the remaining forty-two cases our bound is merely for the rational case due to computational limitations.

Contents

List of Tables

Acknowledgements

This thesis was started under the supervision of Prof. Graham Everest, who sadly passed away in 2010. He showed me $1 + 2 + 3 + 4 + \cdots = -\frac{1}{12}$. I dedicate this thesis to his memory.

This thesis was supported by an EPSRC DTA studentship award for which I am most grateful.

My thanks to the UEA for allowing me to continue my interest in mathematics to research level. My good wishes to all my fellow researchers in all their undertakings. Many thanks to my advisor Prof. Shaun Stevens who took over the role from our friend Graham. Shaun's knowledge, attention to detail, generosity and clear mind has saved me from many a schoolboy error. I would also like to thank Prof. Simar Siksek for drawing my attention to an unresolved matter in the thesis.

I wish to thank my friends and family for their love and for all the help they have given me.

Chapter 1

Introduction

A divisibility sequence is a sequence $(W(n))_{n\in\mathbb{Z}}$ of integers with the property that $W(m) \mid W(n)$ if $m \mid n$. The most famous example of a divisibility sequence is the Fibonacci sequence. These linear recurrence sequences were studied extensively by Lucas. The modular approach of Sir Andrew Wiles [47, 41] in his celebrated proof of Fermat's Last Theorem was utilized by Bugeaud, Mignotte, and Siksek [8] to show that the only perfect powers in the Fibonacci sequence are 0, 1, 8, and 144.

There are also divisibility sequences satisfying a nonlinear recurrence relation. These are the elliptic divisibility sequences (EDSs) and the recurrence relation comes from the recursion formula for elliptic division polynomials associated with an elliptic curve.

In recent years, as a consequence of this intimate relation between EDSs and elliptic curves, this form of nonlinear recurrence sequence has been found to be more amenable to investigation and has had numerous application in fields such as logic and cryptography.

This thesis shall revisit the modular approach of Wiles for solving Diophantine equations related to EDSs using a technique inspired by that found in [8]. If we label a point on an elliptic curve $P = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3}\right)$, we find in many cases EDSs occur naturally as the denominator B_P, up to sign. This relationship was studied extensively in a remarkable monograph of Ward [45]: he showed that every non-singular EDS has an associated elliptic curve. Much of the theory of Lucas' linear recurrence sequences carries over to the EDSs, and we find if the EDS has an asso-

ciated singular cubic curve then the singular EDS is described by Lucas' functions. Just over fifty years later Shipsey [32] used properties of EDSs over finite fields to study the elliptic curve discrete logarithm problem (ECDLP). She produced an elegant repeated doubling style algorithm to calculate high order terms in logarithmic time. Swart [39] gave a comprehensive overview of congruences for EDSs, while expanding on Ward's equations defining the elliptic curve related to an EDS. One of the noticeable leaps forward in our understanding of EDSs is found in the work of Stange [37] in her construction of so called *elliptic net polynomials*. These are an extension of the rank 1 division polynomials and have an associated *elliptic net*. It is seen that EDSs are in fact rank 1 elliptic nets.

A brief breakdown of the thesis is as follows:

In Chapter 2 we introduce some necessary elliptic curve theory needed for our later work.

In Chapter 3 we discuss the polynomials related to multiples of points on an elliptic curve.

In Chapter 4 we discuss elliptic divisibility sequences which obey the same recurrence relation as the division polynomials, and show how these EDSs are related to elliptic curves as a consequence. We investigate them over finite fields $\mathbb{F}_p$, where p is a prime, and find the sequences are $\equiv 0 \pmod{p}$ at regular intervals which we call the rank of the sequence $r(p)$. The sequence is also periodic modulo p, with period some multiple of the rank.

In Chapter 5 the machinery of the modularity of elliptic curves is given in the form of a 'black box'. We list the important theorems used in later work, and introduce the concept of rational and irrational newforms and how they are linked to elliptic curves. The technique of Ribet's [30] of level lowering the conductor of elliptic Frey curves attached to Diophantine equations is shown, as well as how it can be used in eliminating newforms to show the nonexistence of any purported solution to a Diophantine equation. The correspondence between elliptic curves defined over $\mathbb{Q}$ and how they 'arise' from either rational or irrational newforms is shown and is central to the theory expanded on in the sequel as to the existence of p^{th} powers, where p is some (prime) exponent in the Diophantine equation.

In Chapter 6 we look at the structure of the elliptic denominator and ask when does the equation $B_P = Z^f$ have a solution, where $Z \in \mathbb{Z}_{>0}$ and $f \in \mathbb{Z}_{>1}$. It turns

out the question we end up asking using the 'modular method' is when are there solutions to the equation

$$B_P = Z^p \qquad \text{for } p = 11, \text{ or } p \geq 17, \text{ where } p \text{ is prime.}$$

For the Mordell elliptic curve $y^2 = x^3 - 2$ we resolve the case of fifth powers occurring in Theorem 6.3.1, with an application of elementary techniques alongside the advanced Chabauty's method. Our result is ultimately gained through use of the computer algebra system `magma` [42].

We then investigate the general Mordell curve $E_D\colon y^2 = x^3 + D$, where D is a nonzero integer, and the associated denominator divisibilty sequence $(B_{nP})_{n\in\mathbb{Z}}$, with the aim of finding which denominators occur as p^{th} powers for p a prime. To do so we assume the elliptic denominator of $[n]P$ is a p^{th} power for some prime p:

$$B_n = Z_n^p.$$

Then letting the n^{th} multiple of a nontorsion point $P \in E_D(\mathbb{Q})$ be written as

$$[n]P = \left(\frac{A_n}{Z_n^{2p}}, \frac{C_n}{Z_n^{3p}}\right), \quad A_n, C_n, Z_n \in \mathbb{Z},\ \gcd(A_n, Z_n) = \gcd(C_n, Z_n) = 1,$$

we obtain the Diophantine equation

$$C_n^2 - A_n^3 = DZ_n^{6p}, \tag{1.0.1}$$

which has associated to it the Frey curve

$$E_{B,n}\colon Y^2 = X^3 - 3A_nX + 2C_n. \tag{1.0.2}$$

In Chapter 7 we give an algorithm for bounding the exponent p in the case that the Frey curves (1.0.2) constructed in Chapter 6, Subsection 6.4.1 arise from rational newforms. This algorithm is based on the Chinese Remainder Theorem and uses a sieve process to gain contradictions through congruences, allowing for the elimination of newforms, and in so doing to any purported solution to the Diopantine equation (1.0.1).

In Chapter 8 we investigate rank 1 Mordell curves $E_D\colon y^2 = x^3 + D$, where $|D| < 200$, $D \neq 0$. We remove the problem of integral points $Q \in E_D(\mathbb{Q})$, where Q is a power integral point for all primes p, since $B_Q = 1^p$ for all p. This allows us to (hopefully) eliminate all newforms and gain a upper bound for p.

Finally, in Chapter 9, we end with a look to future work on the existence of power integral points on curves of rank greater than 1 by utilizing the methods in this thesis for higher dimension elliptic nets.

Chapter 2

Algebraic Curves

2.1 Affine Varieties

Let K be a field and $\bar{K}$ an algebraic closure of the ground field K.

2.1.1 Affine n-Space

Definition 2.1.1. *Affine n-space* (over K) is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{(a_1, \ldots, a_n) : a_i \in \bar{K}\}.$$

The *set of K-rational points of* $\mathbb{A}^n$ is the set

$$\mathbb{A}^n(K) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n : a_i \in K\}.$$

If K is a perfect field, then the set of K-rational points of $\mathbb{A}^n$ is precisely the set of points which are fixed by the Galois group $\mathrm{Gal}(\bar{K}/K)$

$$\mathbb{A}^n(K) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n : \sigma(a_i) = a_i \text{ for all } \sigma \in \mathrm{Gal}(\bar{K}/K)\}.$$

Assume $x_1, \ldots, x_n$ are independent variables over K then a polynomial

$$f \in K[x_1, \ldots, x_n]$$

can be viewed as a K-valued function $f\colon \mathbb{A}^n \to K$ on $\mathbb{A}^n$ by evaluating f at the points in $\mathbb{A}^n$

$$f\colon (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n) \in K.$$

Thus $K[x_1, \ldots, x_n]$ is the ring of K-valued functions on $\mathbb{A}^n$, denoted by $K[\mathbb{A}^n]$ and called the *coordinate ring of* $\mathbb{A}^n$.

Example 2.1.2. Let $K = \mathbb{R}$, $n = 3$. Then the coordinate ring of Euclidean 3-space $\mathbb{R}^3$ is denoted by $\mathbb{R}[\mathbb{A}^3]$ and is the ring of polynomials in three variables, $\mathbb{R}[x, y, z]$ with respect to x, y, z the coordinate functions on $\mathbb{R}^3$.

For each fixed subset S of functions in the coordinate ring $K[\mathbb{A}^n]$ there is a subset of affine space $Z(S)$ which is the set of points in $\mathbb{A}^n$ where all the functions in S are simultaneously zero:

$$Z(S) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}.$$

Definition 2.1.3. A subset V of $\mathbb{A}^n$ is an *affine algebraic set* if $V = Z(S)$ for some $S \subseteq K[\mathbb{A}^n]$. Then V is called the locus of S in $\mathbb{A}^n$.

Definition 2.1.4. A nonempty subset Y of a topological space that cannot be decomposed into two proper subsets Y_1 and Y_2 each of which is closed in Y is called *irreducible*.

Definition 2.1.5. An *affine algebraic variety* is an irreducible affine algebraic subset of $\mathbb{A}^n$. It is called a *curve* if $n = 2$ and the variety is defined by a single bivariate polynomial.

Definition 2.1.6. Let $C(K)$ be an affine algebraic curve with equation $f(x, y) = 0$. We note a polynomial $g(x, y)$ is the zero function on C if and only if it is a multiple of f. This leads us to define the ring of regular functions of C to be

$$K[C] = K[x, y]/\langle f(x, y)\rangle.$$

Its field of fractions $K(C)$ is called the field of rational functions of C.

Example 2.1.7. Consider the affine plane curve $C\colon y^2 = x^3 + ax + b$ defined over a field K. Its function field is the field $K(x, y)$, generated by the transcendental elements satisfying the algebraic relation.

Definition 2.1.8. *Projective n-space* $\mathbb{P}^n$ (over K) is the set of lines through the origin in $\mathbb{A}^{n+1}$

$$\mathbb{P}^n = \mathbb{P}^n(\bar{K}) = \{(a_0, \ldots, a_n) \in \mathbb{A}^{n+1} : \text{ some } a_i \neq 0\}/\sim,$$

where we define the equivalence relation $\sim$ by

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Longleftrightarrow (x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n) \text{ for some } \lambda \in \bar{K}^*.$$

A point $P = (x_0 : \ldots : x_n) \in \mathbb{P}^n$ thus represents the equivalence class of the $(n+1)$-tuple $(x_0, \ldots, x_n)$, and the x_i's are *homogeneous* or *projective* coordinates for P. The *set of K-rational points of* $\mathbb{P}^n$ is the set of lines through the origin in $\mathbb{A}^{n+1}$ defined over K

$$\mathbb{P}^n(K) = \{(a_0 : \ldots : a_n) : (a_0, \ldots, a_n) \in \mathbb{A}^{n+1}(K) \text{ is nonzero}\}.$$

Definition 2.1.9. A projective variety is an irreducible algebraic set in $\mathbb{P}^n$ with the induced topology, that is, the simultaneous solution set of a set of homogeneous polynomials in $K[x_0, \ldots, x_n]$.

Definition 2.1.10. An *algebraic curve* is a projective variety of dimension one.

Example 2.1.11. The affine plane curve of Example 2.1.7 has the defining polynomial $f(x, y) = y^2 - x^3 - ax - b$ in two variables. This can be completed into the projective algebraic curve of equation $F(x, y, z) = y^2z - x^3 - axz^2 - bz^3$. The zeros of this homogeneous polynomial in three variables describes the plane projective curve C': $y^2z = x^3 + axz^2 + bz^3$.

2.1.2 Genus

Curves are classified by a nonnegative integer known as the *genus* g. Every curve of genus 0 defined over $\mathbb{C}$ is birationally equivalent to the line. Curves of genus 0 defined over $\mathbb{Q}$ are birationally equivalent to the line or a conic. Hence the theory of curves of genus 0 is fully understood. The next Theorem gives the formula for the genus of a nonsingular curve C.

Theorem 2.1.12. *Let a curve C be given by the zero set of some homogeneous irreducible polynomial $f(X,Y,Z) \in \bar{K}[X,Y,Z]$, where the degeree of f is some integer $d \geq 1$. If C is nonsingular the genus is given by*

$$\frac{(d-2)(d-1)}{2}.$$

Proof. See [21, Ch. 8.3]. □

Example 2.1.13. Lines are curves of degree 1 having equations of the form

$$aX + bY + cZ = 0.$$

Conics are curves of degree 2 having equations of the form

$$aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0.$$

Cubics are curves of degree 3 having equations of the form

$$aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3 = 0.$$

By the genus formula lines and conics have genus 0, and smooth cubics have genus 1.

2.2 Divisors

We begin with some definitions, and fix some notation.

Definition 2.2.1. Let C be an algebraic curve and P a point on C. Let M_P be the ideal of $\bar{K}[C]$ given by

$$M_P = \{f \in \bar{K}[C] : f(P) = 0\}.$$

Note that M_P is a maximal ideal, since there is an isomorphism

$$\bar{K}[C]/M_P \longrightarrow \bar{K} \quad \text{given by} \quad f \longmapsto f(P).$$

Definition 2.2.2. Let C be an algebraic curve and P a point on C. Let the *local ring of* C at P, denoted $\bar{K}[C]_P$, be the localization of $\bar{K}[C]$ at M_P. We have,

$$\bar{K}[C]_P = \{F \in \bar{K}[C]_P : F = f/g \text{ for some } f, g \in \bar{K}[C] \text{ with } g(P) \neq 0\}.$$

Definition 2.2.3. Let C be a curve and $P \in C$ a nonsingular (or *smooth*) point. The (normalised) valuation on $\bar{K}[C]_P$ is given by

$$\begin{aligned} \mathrm{ord}_P \colon \bar{K}[C]_P &\longrightarrow \{0, 1, 2, \dots\} \cup \{\infty\}, \\ \mathrm{ord}_P(f) &= \sup\{d \in \mathbb{Z} : f \in M_P^d\}. \end{aligned}$$

Definition 2.2.4. The *divisor group of a curve* C, denoted $\mathrm{Div}(C)$, is the free abelian group generated by the points of C. Thus a divisor is a formal sum

$$D = \sum_{P \in C} n_P(P), \quad n_P \in \mathbb{Z}$$

and $n_P = 0$ for all but finitely many $P \in C$. The *degree of* D is

$$\deg(D) = \sum_{P \in C} n_P.$$

If we assume C is smooth, and let $f \in \bar{K}(C)^*$ then we can associate to f the divisor $\mathrm{div}(f)$ given by

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

2.3 Elliptic Curves

2.3.1 Weierstrass Cubic

An *elliptic curve* is a nonsingular projective algebraic curve of genus 1 with a specified basepoint. Elliptic curves can be written as the locus of cubic equations in the projective plane $\mathbb{P}^2$ having one point (the basepoint) on the line at infinity; after scaling X and Y we have the projective *Weierstrass equation* of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2.3.1}$$

where $a_1, \ldots, a_6 \in \bar{K}$. To find the point at infinity set $Z = 0$ in (2.3.1) to find $0 = X^3$ and so $X = 0$, with Y being any nonzero number in K. Hence $O = (0 : Y : 0) = (0 : 1 : 0)$ is the only $\bar{K}$-rational point on the line at infinity $Z = 0$. Moreover O is a nonsingular point of inflection, with the tangent line being the line at infinity.

Since the behavior at $(0 : 1 : 0)$ is well understood, for ease of notation we shall let $x = X/Z$ and $y = Y/Z$ to give the nonhomogeneous affine form of the Weierstrass equation for an elliptic curve

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.3.2}$$

although we must always remember the extra point at infinity. If the coefficients $a_1, \ldots, a_6 \in K$, then E is said to be *defined over* K, written E/K.

We now define some standard notation needed when simplifying (2.3.2).

If $\mathrm{char}(\bar{K}) \neq 2$ we can complete the square in (2.3.2) by setting

$$\eta = y + \frac{a_1}{2}x + \frac{a_3}{2} \tag{2.3.3}$$

to give

$$\eta^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}, \tag{2.3.4}$$

where the auxiliary quantities b_2, b_4, and b_6 are given by

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6. \end{aligned} \tag{2.3.5}$$

Moreover if the ground field has $\mathrm{char}(\bar{K}) \neq 2, 3$ we can complete the cube in (2.3.4) by setting

$$\xi = x + \frac{b_2}{12}, \tag{2.3.6}$$

then

$$\eta^2 = \xi^3 - \frac{c_4}{48}\xi - \frac{c_6}{864},$$

with the invariants c_4 and c_6 given by

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned} \tag{2.3.7}$$

If $\mathrm{char}(\bar{K}) \neq 2$ we now set $\eta = \frac{1}{2}y$ in (2.3.4) to obtain the Weierstrass equation

$$E\colon y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{2.3.8}$$

with b_2, b_4, b_6 as in (2.3.5).

Let us also define the quantities

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= c_4^3/\Delta, \end{aligned}$$

provided $\Delta \neq 0$. These satisfy the relations

$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad 1728\Delta = c_4^3 - c_6^2.$$

Definition 2.3.1. The quantity Δ is the *discriminant* of the Weierstrass equation, and j is the *j-invariant* of the elliptic curve.

If further $\mathrm{char}(\bar{K}) \neq 2,\ 3$, every elliptic curve over K can be written in the canonical form

$$E\colon y^2 = x^3 - 27c_4x - 54c_6, \tag{2.3.9}$$

on replacing (x, y) in (2.3.8) with $\left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$, thereby eliminating the x^2 term, with c_4, c_6 as in (2.3.7).

Now even when working with a field of characteristic 0 we should like to reduce our equation modulo p for various primes, including the primes 2 and 3 for which our equation is more complicated to deal with. However if we make the assumption that we are working in a field K of characteristic not equal to 2 or 3 then we may

assume our elliptic curve has a Weierstrass equation of the form

$$E : y^2 = x^3 + ax + b.$$

This is known as the *short Weierstrass form* and has the associated quantities

$$\Delta = -16(4a^3 + 27b^2), \quad j = -\frac{1728(4a)^3}{\Delta}.$$

Proposition 2.3.2. *A curve given by a Weierstrass equation is classified as follows:*

(a) *It is nonsingular if and only if* $\Delta \neq 0$.

(b) *It has a node if and only if* $\Delta = 0$ *and* $c_4 \neq 0$.

(c) *It has a cusp if and only if* $\Delta = c_4 = 0$.

Proof. See [35, Ch. III, Prop. 1.4]. □

We have defined the elliptic curve in terms of a Weierstrass equation, but what of the uniqueness of this expression? It will be seen in Proposition 2.3.9 that for a given elliptic curve E, assuming the line at infinity, i.e., the line $Z = 0$ in $\mathbb{P}^2$, intersects E only at $(0 : 1 : 0)$, then the only change of variables fixing $(0 : 1 : 0)$ and giving a Weierstrass form for the equation of E is

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + su^2x' + t, \end{aligned}$$

with u, r, s, $t \in \bar{K}$, $u \neq 0$. The coefficients a_i transform as

$$\begin{aligned} ua_1' &= a_1 + 2s, \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\ u^3a_3' &= a_3 + ra_1 + 2t, \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{aligned} \tag{2.3.10}$$

The auxiliary quantities b_i transform as

$$\begin{aligned} u^2 b_2' &= b_2 + 12r, \\ u^4 b_4' &= b_4 + r b_2 + 6r^2, \\ u^6 b_6' &= b_6 + 2r b_4 + r^2 b_2 + 4r^3, \\ u^8 b_8' &= b_8 + 3r b_6 + 3r^2 b_4 + 3r^4. \end{aligned} \tag{2.3.11}$$

The quantities c_4, c_6, Δ, and j transform as

$$u^4 c_4' = c_4, \quad u^6 c_6' = c_6, \quad u^{12}\Delta' = \Delta, \quad j' = j. \tag{2.3.12}$$

For the short Weierstrass form it follows the only permissable change of variables is

$$x = u^2 x', \quad y = u^3 y',$$

with $u \in \bar{K}^*$; and then

$$u^4 a' = a, \quad u^6 b' = b, \quad u^{12}\Delta' = \Delta.$$

In fact, after tedious calculation, the next Proposition holds.

Proposition 2.3.3. *Two elliptic curves are isomorphic (over $\bar{K}$) if and only if they have the same j-invariant.*

Proof. See [35, Ch. III, Prop. 1.4]. □

This explains (2.3.12): the j-invariant is an invariant of the isomorphism class of the curve, and does not depend on the particular Weierstrass equation chosen. It is also true that for every $j \in K$ there exists an E over $\bar{K}$ with $j_E = j$.

Remark 2.3.4. By Proposition 2.3.3 two elliptic curves E and E' are isomorphic over a fixed algebraic closure of K if and only if they have the same j-invariant. Two elliptic curves with the same j-invariant are called *twists*, and although isomorphic over $\bar{K}$ they may not necessarily be so over K.

The next Section shows that curves that are isomorphic are also isomorphic as abstract groups.

2.3.2 The Group Law

As discussed in [35, Ch. III, Prop. 2.2], there is a binary operation + on an elliptic curve E that makes E into an abelian group. We take the point at infinity to be the identity of the group. The set of points $E(K)$ forms a subgroup of E. We give the relevant propositions, equations, and algorithms describing this group law.

Proposition 2.3.5. *Let E be an elliptic curve given by a Weierstrass equation, and let P, $Q \in E$, and L be the line joining them (this will be a tangent line if $P = Q$) and R be the third point of intersection of L with E. Let L' be the vertical line joining R and O. Then $P + Q$ is the third point of intersection that L' makes with E. These compositions have the following properties:*

(a) *If a line L intersects E at three (not necessarily distinct) points P, Q, and R, then*

$$(P + Q) + R = O.$$

(b) *$P + O = P$ for all $P \in E$.*

(c) *$P + Q = Q + P$ for all P, $Q \in E$.*

(d) *For each $P \in E$ there exists a point $-P$ such that*

$$P + (-P) = O.$$

(e) *Let P, Q, $R \in E$. Then*

$$(P + Q) + R = P + (Q + R).$$

(f) *If E is defined over a field K the set of points*

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

forms a subgroup of E.

Proof. See [35, Ch. III, Prop. 2.2]. □

Remark 2.3.6. The only real difficulty in proving the set of points in E forms an abelian group is the property of associativity.

Definition 2.3.7. We define the multiplication-by-m map $[m]\colon E \to E$ by

$$[m]P = \begin{cases} \underbrace{P + \cdots + P}_{(m \text{ terms})} & \text{for } m > 0, \\ \underbrace{-P \cdots - P}_{(m \text{ terms})} & \text{for } m < 0, \\ O & \text{for } m = 0. \end{cases}$$

We sometimes denote $[m]P$ by just mP.

2.3.3 Group Law Algorithm

We now derive explicit formulas for the group operations on E. Let

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6.$$

If we let $P_0 = (x_0, y_0) \in E$, then to find $-P_0$ we look at the line through P_0 and O:

$$L\colon x - x_0 = 0.$$

Now consider the quadratic

$$F(x_0, y) = y^2 + (a_1x_0 + a_3)y - (x_0^3 + a_2x_0^2 + a_4x_0 + a_6),$$

which will have two roots y_0 and y_0' and factor as

$$F(x_0, y) = c(y - y_0)(y - y_0'),$$

and comparing coefficients of y^2 and y we see $c = 1$ and $y_0' = -y_0 - a_1x_0 - a_3$. Hence

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3). \tag{2.3.13}$$

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E. If $x_1 = x_2$ and $y_2 = -y_1 - a_1x_1 - a_3$ then we have just shown $P_1 + P_2 = O$. So assume otherwise. Then

if $P_1 \neq P_2$ there exists a chord through P_1 and P_2, or if $P_1 = P_2$ a tangent line, of the form

$$L\colon y = \lambda x + \nu.$$

Looking at the cubic equation $F(x, \lambda x + \nu) = 0$, which has three roots x_1, x_2, x_3, we have that $P_3 = (x_3, y_3)$ is the third point of intersection with L such that

$$P_1 + P_2 + P_3 = O;$$

now our cubic can be written

$$F(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3)$$

and comparing coefficients of x^3 and x^2 we see $c = 1$ and the sum of roots is

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2.$$

Therefore $P_3 = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \lambda x_3 + \nu)$. Now consider the negation of P_3: $P_1 + P_2 = -P_3$, which we label as $-P_3 = (x_3', y_3')$. We find after using (2.3.13) that

$$\begin{aligned} x_3' &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3' &= -(\lambda + a_1)x_3 - \nu - a_3, \end{aligned} \tag{2.3.14}$$

where λ and ν are given by

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2, \end{cases} \tag{2.3.15}$$

$$\nu = \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2. \end{cases} \tag{2.3.16}$$

From this we can deduce: The *addition formula* for points $P_1 = (x_1, y_1)$, $P_2 =$

(x_2, y_2), with $P_1 \neq \pm P_2$ is

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2. \tag{2.3.17}$$

The *duplication formula* for $P = (x, y)$ is

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}. \tag{2.3.18}$$

Example 2.3.8. Let E be the elliptic curve given by

$$E\colon y^2 = x^3 - 36.$$

Given $P = (-3, 9)$ on E what is $2P$? By (2.3.14) the gradient of the tangent to P is given by $\lambda = (3 \cdot (-3)^2 - 36)/2 \cdot 9 = -1/2$. Hence

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 = \left(-\frac{1}{2}\right)^2 - (-3) - (-3) = \frac{25}{4}, \\ y_3 &= -\frac{1}{2} \cdot \frac{25}{4} + 9 - \left(-\frac{1}{2}\right)(-3) = -\frac{35}{8}. \end{aligned}$$

So $2P = \left(\frac{25}{4}, -\frac{35}{8}\right)$.

The next Proposition shows that every elliptic curve can be written as a plane cubic, and conversely, every smooth Weierstrass plane cubic curve is an elliptic curve. It also shows how an elliptic curve E has essentially a unique Weierstrass equation, up to a change of variables.

Proposition 2.3.9. *Let E/K be an elliptic curve.*

(a) *There exist functions x, $y \in K(E)$ such that the map*

$$\phi\colon E \longrightarrow \mathbb{P}^2, \quad \phi = (x : y : 1),$$

gives an isomorphism from E/K onto a curve with Weierstrass equation

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with $a_1, \ldots, a_6 \in K$; and such that $\phi(O) = (0 : 1 : 0)$. (The functions x, y

are called Weierstrass coordinate functions *on* E.*)*

(b) *A Weierstrass equation for* E *is unique up to a linear change of variables* $T(r, s, t, u)$ *given by*

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t \tag{2.3.19}$$

with u, r, s, $t \in K$, $u \neq 0$.

(c) *Conversely, any smooth cubic curve given by a Weierstrass equation as in (a) is an elliptic curve defined over* K *with basepoint* $O = (0 : 1 : 0)$.

Proof. See [35, Ch. III, Prop. 3.1]. □

Corollary 2.3.10. *Let* E/K *be an elliptic curve with Weierstrass coordinate functions* x *and* y. *Then*

$$K(E) = K(x, y) \quad \textit{and} \quad [K(E) : K(x)] = 2.$$

Proof. See [35, Ch. III, Cor. 3.1.1]. □

Remark 2.3.11. We call such a transformation in Proposition 2.3.9 (b) an *admissable change of variables* as given in (2.3.19). An admissable change of variables is termed *unihomothetic* if $u = 1$.

2.4 Singular Weierstrass Equations

2.4.1 Singular Points

If a cubic curve $f(x, y)$ has discriminant $\Delta \neq 0$, then this curve is *nonsingular* and describes an elliptic curve. If however $f(x, y)$ has discriminant $\Delta = 0$ then it is *singular* and contains a *singular point* $Q = (x_S, y_S)$ where the partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ both vanish at Q. Hence for a point to be singular on a cubic curve given by $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ it must vanish at both its partial differentials with respect to x and y respectively:

$$\begin{aligned} \frac{\partial f}{\partial x}(x_S, y_S) &= a_1 y_S - 3x_S^2 - 2a_2 x_S - a_4 = 0, \\ \frac{\partial f}{\partial y}(x_S, y_S) &= 2y_S + a_1 x_S + a_3 = 0. \end{aligned} \tag{2.4.1}$$

In particular, if $f(x, y) = y^2 - g(x)$ then (x_S, y_S) is singular if and only if x_S is a double or triple root of g.

Since a cubic can only have one double or triple root, f may only have one singular point. Suppose that a given Weierstrass equation has discriminant $\Delta = 0$, then Proposition 2.3.2 tells us that it has a singular point. In fact if we discard the singular point the set of nonsingular points form an abelian group. We note a singular cubic curve will then have genus 0.

Definition 2.4.1. Let E be a (possibly singular) curve given by a Weierstrass equation. We denote the *nonsingular part of* E by E_{ns}, that is the nonsingular points of E. If E is defined over a field K we denote the set of nonsingular points of $E(K)$ by $E_{\text{ns}}(K)$.

Let E be a singular curve defined over a field K, i.e., E is given by a singular Weierstrass equation. Let the singular point be $Q = (x_S, y_S) \in E(K)$. After the change of variables $x \to x' + x_S$, $y \to y' + y_S$, we can assume that the Weierstrass equation for E is

$$E\colon y^2 + a_1 xy - a_2 x^2 - x^3 = 0; \qquad a_1, a_2 \in K, \tag{2.4.2}$$

with singular point $Q = (0, 0)$.

Let

$$y^2 + a_1 xy - a_2 x^2 = (y - \alpha_1 x)(y - \alpha_2 x),$$

where α_1, α_2 are in K or in a quadratic extension of K. Then Q is a *node* if $\alpha_1 \neq \alpha_2$, and a *cusp* if $\alpha_1 = \alpha_2$.

The next result states that $E_{\text{ns}}(K)$ form a group, and determines the structure of this group.

Theorem 2.4.2. *Let E/K be a singular cubic curve with singular point $Q = (0, 0)$.*

(a) *If Q is a cusp, then there is one tangent line at Q. Then the map $\gamma\colon E_{ns}(K) \to K^+$ defined by*

$$\gamma\colon O \mapsto 0, \qquad \gamma\colon (x,y) \mapsto x/(y-\alpha_1 x)$$

is a group isomorphism.

(b) *If Q is a node with $\alpha_1,\ \alpha_2 \in K$, then the map $\mu_1\colon E_{ns}(K) \to K^*$ defined by*

$$\mu_1\colon O \mapsto 1, \qquad \mu_1\colon (x,y) \mapsto (y-\alpha_2 x)/(y-\alpha_1 x)$$

is a group isomorphism. In this case the slopes of the tangent lines to the node are in K and we say E has split multiplicative reduction.

(c) *If Q is a node with $\alpha_1,\ \alpha_2 \notin K$, then $K_1 = K(\alpha_1,\alpha_2)$ is a quadratic extension of K. We have by part (b): $E_{ns}(K) \subset E_{ns}(K_1) \cong K_1^*$. Let $L = \{t \in K_1^* : N_{K_1/K}(t) = 1\}$ be the subgroup of K_1^* consisting of elements of norm 1. Then the map $\mu_2\colon E_{ns}(K) \to L$ defined by*

$$\mu_2\colon O \mapsto 1, \qquad \mu_2\colon (x,y) \mapsto (y-\alpha_2 x)/(y-\alpha_1 x)$$

is a group isomorphism. In this case the slopes of the tangent lines to the node are not in K, but in K_1, and we say E has nonsplit multiplicative reduction.

Proof. See [5, Thm. 8.1]. □

2.5 Torsion Points

Definition 2.5.1. Let E/K be an elliptic curve and let $P \neq O$ be a point in $E(K)$. The duplication formula (2.3.18) can then generate a sequence of points where $[k]P = (x_k, y_k)$ is the k^{th} multiple of P, for some $k \in \mathbb{Z}$. If $[n]P = O$ for some $n \in \mathbb{Z}$, then we say P is a *torsion point* of order n. If there is no such n then we say P has *infinite order* and is a *nontorsion point*.

If we include the point at infinity this then imbues the set of torsion points with a group structure, with O acting as the identity.

Definition 2.5.2. The m-torsion subgroup of E, denoted by $E[m]$, is the set of points of order dividing m in E,

$$E[m] = \{P \in E : [m]P = O\}.$$

The torsion subgroup of E, denoted by E_{tors}, is the set of points of finite order,

$$E_{\text{tors}} = \bigcup_{m \geq 1} E[m].$$

For E/K we have $E(K)_{\text{tors}}$ denotes the torsion points in $E(K)$.

Theorem 2.5.3 (Lutz–Nagell)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ given by the nonhomogeneous affine form of the Weierstrass equation*

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

where $a_1, \ldots, a_6 \in \mathbb{Z}$.

(a) *If $a_1 = 0$ and if $P = (x(P), y(P)) \in E(\mathbb{Q})_{\text{tors}}$, then $x(P)$, $y(P) \in \mathbb{Z}$.*

(b) *For any a_1, if $P = (x(P), y(P)) \in E(\mathbb{Q})_{\text{tors}}$, then $4x(P)$, $8y(P) \in \mathbb{Z}$.*

(c) *If $a_1 = a_3 = a_2 = 0$, so that E is given by*

$$y^2 = x^3 + ax + b, \tag{2.5.1}$$

and if $P = (x(P), y(P)) \in E(\mathbb{Q})_{\text{tors}}$, then either $y(P) = 0$ (and P has order 2) or else $y(P) \neq 0$ and $y(P)^2 \mid d$, where $d = -4a^3 - 27b^2$ is the discriminant of the cubic polynomial (2.5.1).

The Lutz–Nagell Theorem 2.5.3 can be used to explicitly compute the torsion subgroup of curves defined over $\mathbb{Q}$. To find it put the curve in the form of (2.5.1) with a, $b \in \mathbb{Z}$, and consider $y \in \mathbb{Z}$ such that $y^2 \mid \Delta$, then check if (x, y) is an integer solution of (2.5.1). Since there can only be finitely many such solutions

then we gain a bound on $|E(\mathbb{Q})_{\text{tors}}|$, say equal to n. Now for each integer solution (x, y), on raising it to powers up to the bound we may effectively check if it is a torsion point.

Example 2.5.4. Consider the point $P = (2, 3)$ on the elliptic curve $E\colon y^2 = x^3 + 1$. We have that $[2]P = (0, 1)$, $[3]P = (-1, 0)$, $[4]P = (0, -1)$, $[5]P = (2, -3)$, and $[6]P = O$. Hence P is a torsion point of order 6 on E. Thus P has order 6, $[2]P$ has order 3, $[3]P$ has order 2, $[4]P$ has order 3, $[5]P$ has order 6, and $[6]P$ has order 1. Geometrically we note $[5]P$ is the reflection of P in the x-axis, as is $[4]P$ of $[2]P$, and so these points are inverse to each other: $[5]P + P = O$ and $[4]P + [2]P = O$.

Example 2.5.5. Let E be the elliptic curve given by

$$\begin{aligned} E\colon y^2 &= x^3 - 36x \\ &= x(x + 6)(x - 6). \end{aligned}$$

By the factorisation and part (c) of Theorem 2.5.3 we immediately see the points of order 2 on E are given by $P_1 = (0, 0)$, $P_2 = (-6, 0)$, $P_3 = (6, 0)$. Using the addition formula we find $P_1 + P_2 = (6, 0)$, $P_1 + P_3 = (-6, 0)$, $P_2 + P_3 = (0, 0)$, and that $[2]P_i = O$ for $i = 1, 2, 3$. We have $\{O, P_1, P_2, P_3\}$ is the full 2-torsion group and is isomorphic to the Klein-4 group.

$$E(\mathbb{Q})[2] \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

In 1978 Mazur gave the following Theorem categorizing the type of possible torsion groups.

Theorem 2.5.6 (Mazur [26])**.** *The only possible torsion groups for elliptic curves over* $\mathbb{Q}$ *are the cyclic groups of order* 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 *and* $\mathbb{Z}/2 \times \mathbb{Z}/2n$ *for* $n = 1, 2, 3, 4$.

Example 2.5.7. The largest group $\mathbb{Z}/2 \times \mathbb{Z}/8$ occurs for the curve:

$$E\colon y^2 + xy = x^3 - 1070x + 7812,$$

a.k.a. $Y^2 = X(X - 64)(4X - 175)$.

2.6 Integral and Rational Points on Curves

Throughout this Section K will denote a number field. We are primarily concerned with the case when $K = \mathbb{Q}$, but it is best to highlight the results in their full generality with K a number field, although we shall avoid the technicalities involved and rely on references to cover the assured complexities of the results. An important result of Siegel's was his 1929 proof that for a smooth algebraic curve C/K of genus g at least one, there are only finitely many points $P \in C(K)$ that have their coordinates in the ring of integers R of the number field K.

In fact he proved more than this using the idea of S-integers. For our purposes we shall only need the concept of S-integers in the field $\mathbb{Q}$.

Definition 2.6.1. Let $K = \mathbb{Q}$, and let $S = \{p_1, \ldots, p_n\}$ be a finite set of rational primes. The rational integers a/b, a, $b \in \mathbb{Z}$, where $\gcd(a, b) = 1$ and the prime divisors of b (possibly empty) belong to the set S form the so called *S-integers* $\mathbb{Z}_S$. Clearly $\mathbb{Z}_S$ is a subring of $\mathbb{Q}$, and has $\mathbb{Z}_S^*$ as the group of multiplicatively invertible elements of $\mathbb{Z}_S$, the so called *S-units*. These S-units will be ± 1 and any rational numbers having a prime factorisation with all prime elements coming from S. We may specialise to one prime p, in which case a *p-integer* means $\{p\}$-integer.

Siegel proved his Theorem on the finiteness of S-integers in the more sophisticated setting of number fields K. Here we give a brief explanation: let S be a finite set of nonequivalent normalised valuations of K containing the set S_∞ of all Archimedean va1uations. A nonzero element $a \in K$ is called *S-integral*, respectively an *S-unit*, if for every valuation $v \notin S$ we have $v(a) \leq 1$, respectively $v(a) = 1$; for further details see [27, Chap. 3, Subsec. 3.3].

Theorem 2.6.2 (Siegel)**.** *Let $f(x) \in K[x]$ be a polynomial of degree $d \geq 3$ with distinct roots in $\bar{K}$. Let R be the ring of integers of K. Then the equation*

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

has only finitely many solutions in S-integers x, $y \in R_S$.

Proof. See [35, Ch. IX, Thm. 4.3]. □

Corollary 2.6.3. *Let C/K be a smooth curve of genus $g \geq 1$ and let f be a nonconstant function in the function field $K(C)$. Then there are only finitely many points $P \in C(K)$ such that $f(P) \in R_S$.*

Proof. See [35, Ch. IX, Cor. 4.3.1]. □

If we take the coordinate functions $x(P)$ and $y(P)$, Siegel's Theorem implies that a curve of genus ≥ 1 has only finitely many integral points.

Example 2.6.4. An elliptic curve defined over $\mathbb{Q}$ can have only finitely many integral points.

We now look at rational points on a curve, and how a finite set of these generate the whole set.

Theorem 2.6.5 (Mordell–Weil)**.** *Let E be an elliptic curve defined over a number field K. Then $E(K)$ is a finitely generated abelian group.*

Proof. See [35, Ch. VIII, Thm. 6.7]. □

Remark 2.6.6. Mordell proved this first for elliptic curves. Later Weil showed the same holds for higher dimensional abelian varieties.

The next Theorem superseded Siegel's, and was originally conjectured by Mordell in 1922 for the specific case of the field $\mathbb{Q}$. The eventual proof, extended to any number field K, by Faltings in 1983 was one of the triumphs of twentieth century mathematics.

Theorem 2.6.7 (Faltings [20])**.** *Let C be a curve defined over a number field K. If C has a genus $g > 1$, then there are only finitely many K-rational points.*

By the Mordell–Weil Theorem $E(\mathbb{Q})$ is a finitely generated abelian group, and as such it can be written as the direct sum of its torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ and a torsion free subgroup $\mathbb{Z}^r$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

where $E(\mathbb{Q})_{\text{tors}}$ is finite, and r is a nonnegative integer called the *rank*.

Remark 2.6.8. The group $E(K)$ is finite if and only if the rank is zero.

2.7 Isogenies

For an elliptic curve E/K we have seen that the group of points $E(K)$ form a finitely generated abelian group. The next definition concerns the maps between the group structures formed by elliptic curves.

Definition 2.7.1. An *isogeny* is a morphism of algebraic groups that is surjective and has a finite kernel.

Let E and E' be two elliptic curves defined over a field K. An isogeny ϕ between them is a surjective morphism $\phi\colon E \to E'$ which preserves basepoints (i.e., ϕ maps the identity point on E to that on E'). If the kernel is cyclic then the isogeny is termed cyclic, otherwise it is termed noncyclic.

Any nonsingular rational map between elliptic curves that maps the basepoint from one to the other is a homomorphism, and thus an isogeny.

Definition 2.7.2. We define the degree d of ϕ to be the degree of the extension $K(E)/\phi^*K(E')$,

$$\deg(\phi) := [K(E) : \phi^*K(E')],$$

where $\phi^*\colon K(E') \to K(E)$ is the associated injection of function fields. We say the isogeny is *separable (inseparable, purely inseparable)*, if the extension $K(E)/\phi^*K(E')$ is also.

If two curves have an isogeny ϕ of degree d between them, then we say ϕ is a d-isogeny, and the curves are d-isogenous. The degree is essentially the degree of the rational functions involved.

An equivalent definition of degree is that it is equal to the order, d say, of the finite kernel of an isogeny ϕ, which is then again termed a d-isogeny.

Definition 2.7.3. Given an isogeny $\phi\colon E \to E'$ of elliptic curves of degree d, the *dual isogeny* is an isogeny $\hat{\phi}\colon E' \to E$ of the same degree such that $\phi \circ \hat{\phi} = [d]$. Here $[d]$ denotes the multiplication-by-d isogeny $P \mapsto [d]P$ which has degree d^2.

We summarize the main properties of the dual isogeny:

(a) $\deg(\hat{\phi}) = \deg(\phi) = d$.

(b) $\hat{\phi} \circ \phi = [d]_E$, $\phi \circ \hat{\phi} = [d]_{E'}$.

(c) $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$.

(d) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.

(e) $\widehat{[d]} = [d]$.

(f) $\hat{\hat{\phi}} = \phi$.

Vélu [44] has shown how to find an isogeny $\phi\colon E \to E'$ via explicit fomulæ, given the kernel of the isogeny. In his formula he makes use of coordinates of a point $P = (x_1, y_1)$ of order d on the curve and its multiples $[k]P = (x_k, y_k)$, $1 < k < d$.

Theorem 2.7.4 (Vélu [44])**.** *Let E/K be an elliptic curve given by a Weierstrass equation*

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

Let F be a subgroup of $E(K)$ of finite order p, where p is a prime, which we want to be the kernel of the isogeny. Now since if $P \in F$ then $-P \in F$ also, we may partition the set of points in $F \backslash F_2 \cup \{O\}$ as two sets R, $-R$, say, where F_2 is the set of points of order 2 in F. Put $S = F_2 \cup R$ and for each $T = (x_T, y_T) \in S$ set

$$\begin{aligned}
g_T^x &= 3x_T^2 + 2a_2x_T + a_4 - a_1y_T, \\
g_T^y &= -2y_T - a_1x_T - a_3, \\
u_T &= 4x_T^3 + b_2x_T^2 + 2b_4x_T + b_6, \\
v_T &= \begin{cases} g_T^x & \text{if } T \in F_2, \\ 6x_T^2 + b_2x_T + b_4 & \text{if } T \notin F_2, \end{cases} \\
v &= \sum_{T \in S} v_T, \\
w &= \sum_{T \in S} (u_T + x_T v_T).
\end{aligned}$$

Given the above quantities there exists an elliptic curve

$$E'\colon y'^2 + a_1x'y' + a_3y' = x'^3 + a_2x'^2 + (a_4 - 5v)x' + (a_6 - b_2v - 7w)$$

with an isogeny $\phi\colon E \to E'$ *given by*

$$x' = x + \sum_{T\in S}\left(\frac{v_T}{x - x_T} + \frac{u_T}{(x - x_T)^2}\right),$$
$$y' = y - \sum_{T\in S}\left(u_T\frac{2y + a_1x + a_3}{(x - x_T)^3} + v_T\frac{a_1(x - x_T) + y - y_T}{(x - x_T)^2} + \frac{a_1x_T - g_T^xg_T^y}{(x - x_T)^2}\right)$$

which has kernel F*.*

Example 2.7.5. Consider the elliptic curves E' and E defined over $\mathbb{Q}$ given by

$$E'\colon y'^2 = x'^3 + 54,$$

and

$$E\colon y^2 = x^3 - 2.$$

We have the the nontorsion points $P' = (3, 9)$ on E', and $P = (3, 5)$ on E; hence the group of rational points for each curve is given by $E'(\mathbb{Q}) = \langle(3, 9)\rangle$, and $E(\mathbb{Q}) = \langle(3, 5)\rangle$ respectively.

The 3rd *division polynomials* (see Chapter 3) evaluated at P' and P factor as

$$\Psi_3(P') = \Psi_3(P) = 3x^4 + 648x = 3x(x + 6)(x^2 - 6x + 36),$$

which indicate there exists a 3-isogeny between E' and E, which we see from Cremona's tables [13]. For isogenies of prime degree p we can use Vélu's formulæ to explicitly find the points mapped under an isogeny.

By Vélu the rational map in the x'-coordinate is

$$x' \mapsto X = x' + \frac{216}{x'^2}.$$

Substituting $x' = 3$ into the map gives $3 \mapsto 3 + \frac{216}{3^2} = 3^3$, and this gives the curve

$y^2 = x^3 - 2 \cdot 3^6$. On making the change of variables $x = \frac{X}{3^2}$ and $y = \frac{Y}{3^3}$ we have

$$x' \mapsto x = \frac{x'}{3^2} + \frac{216}{3^2 x'^2} = \frac{x'}{9} + \frac{24}{x'^2}.$$

We do similar for the rational map for y' to give the rational map

$$(x', y') \mapsto \left(\frac{x^3 + 216}{x^2}, \frac{x^3 y - 432y}{x^3} \right)$$

which is the desired 3-isogeny mapping the generator P' to P.

2.8 Minimal Weierstrass Equations

In this Section we use the following notation:

K a local field, complete with respect to a discrete valuation v;

$R = \{x \in K : v(x) \geq 0\}$, the ring of integers of K.

Let E/K be an elliptic curve with Weierstrass equation

$$E\colon y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{2.8.1}$$

Since the map $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ takes each a_i to $u^i a_i$, for suitable choice of u we can find a Weierstrass equation with all coefficients $a_i \in R$. Then the discriminant Δ satisfies $v(\Delta) \geq 0$; and since v is discrete we can look for an equation with $v(\Delta)$ as small as possible.

Definition 2.8.1. Let E/K be an elliptic curve. If $v(\Delta)$ is minimized subject to the condition that all the $a_i \in R$ then the Weierstrass equation (2.8.1) is termed a *minimal Weierstrass equation for E at v*, and $v(\Delta)$ is termed the *valuation of the minimal discriminant of E at v*.

Let E be an elliptic curve defined over $\mathbb{Q}$. If all the $a_i \in \mathbb{Z}$ in (2.3.2) then E is said to be integral or defined over $\mathbb{Z}$. By applying the change of coordinates $T(0, 0, 0, u)$ from part (b) of Proposition 2.3.9 for some suitable u, any Weierstrass model can be transformed to an integral model; all invariants, except possibly j, are then integral. If $|\Delta|$ is minimal the model is called a *global minimal model*

for E. The discriminant $\Delta_{\min}$ for a global minimal model is termed the minimal discriminant and is uniquely determined by E. Every $E/\mathbb{Q}$ has a minimal model, which is not unique, with isomorphisms between minimal models having $u = \pm 1$, and r, s, $t \in \mathbb{Z}$.

To look at it another way any global minimal model for $E/\mathbb{Q}$ is a minimal Weierstrass equation for E at p, for any prime p (where we have the embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, $p \mapsto p$). Then for any finite place p of $\mathbb{Q}$ we can obtain a generalized Weierstrass equation, integral at p, with a discriminant of minimal p-adic valuation. Since $\mathbb{Q}$ has class number 1 we can glue together these local equations to obtain a global integral generalized Weierstrass equation with (unique) discriminant $\Delta_{\min}$ having minimal p-adic valuation at all primes p.

2.9 Reduction of the Weierstrass Equation Modulo p

In this Section our elliptic curves will be defined over $\mathbb{Q}$.

In order to understand the rational points on an elliptic curve $E/\mathbb{Q}$, we consider it reduced modulo a prime number p. At certain primes the reduced curve becomes singular and so fails to be an elliptic curve. This occurs exactly when the characteristic is a prime factor of the discriminant $\Delta_{\min}$ of a minimal model of E.

Fix a prime p. Let $\tilde{E}$ denote the reduction of the Weierstrass equation modulo p.

$$\tilde{E}\colon y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6.$$

Hence we obtain a reduction map

$$\begin{aligned} E(\mathbb{Q}) &\longrightarrow \tilde{E}(\mathbb{F}_p) \\ P &\mapsto \tilde{P} \end{aligned} \tag{2.9.1}$$

The nonsingular points of $\tilde{E}(\mathbb{F}_p)$ form a group, denoted $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$. We define two subsets of $E(\mathbb{Q})$:

$$\begin{aligned} E_0(\mathbb{Q}) &= \{P \in E(\mathbb{Q}) : \tilde{P} \in \tilde{E}_{\text{ns}}(\mathbb{F}_p)\}, \\ E_1(\mathbb{Q}) &= \{P \in E(\mathbb{Q}) : \tilde{P} = \tilde{O}\}. \end{aligned} \tag{2.9.2}$$

So $E_0(\mathbb{Q})$ is the set of points of *nonsingular reduction*, and $E_1(\mathbb{Q})$ is the *kernel of the reduction map*.

If we reduce an elliptic curve defined over $\mathbb{Q}$ modulo a prime p that doesn't divide the minimal discriminant we obtain an elliptic curve defined over a finite field $E/\mathbb{F}_p \cong \tilde{E}$. In this case E has *good reduction* at p with E remaining an elliptic curve for the *good primes* that do not divide the discriminant.

However if $p \mid \Delta_{\min}(E)$, then E has *bad reduction* at p. At these *bad primes*, $\tilde{E}$ is singular and so fails to be an elliptic curve. Removing the singular point again gives a set of nonsingular points which form an abelian group.

With the notation above we have

Theorem 2.9.1. *There is a short exact sequence of abelian groups*

$$0 \to E_1(\mathbb{Q}) \to E_0(\mathbb{Q}) \to \tilde{E}_{ns}(\mathbb{F}_p) \to 0. \tag{2.9.3}$$

Proof. See [35, Ch. VII, Prop. 2.1]. □

Thus the group $E_0(\mathbb{Q})/E_1(\mathbb{Q})$ is isomorphic to the finite group of nonsingular points modulo p.

2.9.1 The Group E/E_0

We see that the group $E_0(\mathbb{Q})$ consists of those points of $E(\mathbb{Q})$ which do not reduce to a singuar point of $\tilde{E}_{\text{ns}}(\mathbb{F}_p)$. In particular it is made of two pieces: the part $\tilde{E}_{\text{ns}}(\mathbb{F}_p)$, and the formal group $E_1(\mathbb{Q})$. Importantly the quotient $E(\mathbb{Q})/E_0(\mathbb{Q})$ is finite.

Theorem 2.9.2. *Let $E/\mathbb{Q}$ be an elliptic curve. If $\tilde{E}$ has split multiplicative reduction then $E(\mathbb{Q})/E_0(\mathbb{Q})$ is cyclic of order $v(\Delta) = -v(j)$. Otherwise the quotient group $E(\mathbb{Q})/E_0(\mathbb{Q})$ is finite, of order at most 4.*

Corollary 2.9.3. *The subgroup $E_0(\mathbb{Q})$ has finite index in $E(\mathbb{Q})$.*

2.9.2 The Conductor of an Elliptic Curve

Definition 2.9.4. The *conductor* N_E of $E/\mathbb{Q}$ is defined to be

$$N_E := \prod_p p^{f_p}$$

where the product is over all primes and the exponent f_p is defined below.

$$f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p, \\ 1 & \text{if } E \text{ has multiplicative reduction at } p, \\ 2+\delta_p & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

Here δ_p depends on wild ramification in the action of the inertia group at p of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the Tate module $T_p(E)$. It can be calculated by Tate's algorithm (Section 2.10). The conductor divides the minimal discriminant, and its prime divisors coincide with those of the minimal discriminant. The conductor encodes the type of reduction at p.

Remark 2.9.5. We call curves *stable* if E has good reduction, *semistable* if E has multiplicative reduction, and *unstable* if E has additive reduction at a prime p.

2.10 Tate's Algorithm

Let E/K be an elliptic curve given by the nonhomogeneous affine form of the Weierstrass equation

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

where $a_1, \ldots, a_6 \in R$, where R is the ring of integers of a number field K. Tate's algorithm is an eleven step process which on its completion, which might happen after a finite number of repetitions, we obtain the Weierstrass equation in minimal form. It allows us to compute the valuation of the minimal discriminant $v_p(\Delta_{\min})$, and $f_p(E/K)$ the exponent of the conductor of E/K for each prime p dividing $\Delta_{\min}$.

The algorithm can be found in [35, Ch. IV. Sec. 9], where it is presented close to Tate's original exposition in [40], and can be consulted for extra details.

2.11 Elliptic Curves over Finite Fields

In Section 2.9 we looked at the reduction of an elliptic curve modulo a prime p. With this in hand we can extend Theorem 2.5.3.

Theorem 2.11.1 (Lutz–Nagell)**.** *If p is an odd prime such that $p \nmid \Delta$, then the restriction to $E(\mathbb{Q})_{\text{tors}}$ of the reduction homomorphism $r_p\colon E(\mathbb{Q}) \to \tilde{E}(\mathbb{Z}/p\mathbb{Z})$ is one-one. This remains valid for $p = 2$ if $2 \nmid \Delta$ and $a_1 = 0$.*

2.11.1 Counting Points over a Finite Field

If $E/\mathbb{F}_q$ is an elliptic curve defined over a finite field, where q is a power of a prime p, then the set of rational points is

$$E(\mathbb{F}_q) = \{(x, y) \in E(\mathbb{F}_q) : x, y \in \mathbb{F}_q\} \cup \{O\}.$$

The number of points in $E(\mathbb{F}_q)$ is finite.

For the group of points $E(\mathbb{F}_q)$, q odd, a cubic $x^3 + ax^2 + bx + c$ is a square around half the time for $x \in \{0, 1, \ldots, q-1\}$ giving two values $\pm y$, and one if $y = 0$, adding the "point at infinity" we should expect to have around $q+1$ points on the curve over a finite field. The difference between these two values can be made exact.

Definition 2.11.2. The *trace of Frobenius*, $a_q(E)$, of an elliptic curve E is defined by

$$a_q(E) = q + 1 - |E(\mathbb{F}_q)|. \tag{2.11.1}$$

In fact $a_q(E)$ turns out to be the trace of the q-power Frobenius map considered as a linear transformation of the Tate module of E.

Theorem 2.11.3 (Hasse)**.** *If E is an elliptic curve defined over the finite field $\mathbb{F}_q$ then the number of rational points $|E(\mathbb{F}_q)|$ satisfies*

$$|E(\mathbb{F}_q)| = q + 1 - a_q(E), \quad \textit{with} \quad |a_q(E)| \leq 2\sqrt{q}.$$

Proof. See [35, Ch. V, Thm. 1.1]. □

The next result is mainly due to Deuring, and gives the possible values that $E(\mathbb{F}_q)$ can take.

Theorem 2.11.4. *Let $\mathbb{F}_q$ be a finite field with cardinality $q = p^n$, and let $t \in \mathbb{Z}$ be such that $|t| \leq 2q^{1/2}$. There exists an elliptic curve E defined over $\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = q + 1 - t$ if and only if one of the following conditions is satisfied:*

(a) *$p \nmid t$*

(b) *n is even and $t = \pm 2q^{1/2}$.*

(c) *n is even, $p \not\equiv 1 \pmod 3$, and $t = \pm q^{1/2}$.*

(d) *n is even, $p \not\equiv 1 \pmod 4$, and $t = 0$.*

(e) *n is odd, $p = 2$ or 3, and $t = \pm p^{(n+1)/2}$.*

(f) *n is odd and $t = 0$.*

Proof. See [12, Thm. 7.3.12]. □

Theorem 2.11.5. *Let $\mathbb{F}_q$ be a finite field with cardinality $q = p^n$. The group $E(\mathbb{F}_q)$ is the product of at most two cyclic groups, and if we write $E(\mathbb{F}_q) \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z})$ with $d_2 \mid d_1$, then $d_2 \mid q - 1$.*

Proof. See [5, Thm. 7.10]. □

Example 2.11.6. Consider the set of points of the elliptic curve $E\colon y^2 = x^3 - 2$ over the finite field $\mathbb{F}_5$. We can easily find all points (x, y) with $x, y \in \{0, \pm 1, \pm 2\}$ by solving

$$y^2 \equiv x^3 - 2 \pmod 5.$$

For this we need to find when $x^3 - 2$ is a quadratic residue modulo 5, these residues being 0, 1, and 4. We find the six points to be

$$\{(1, \pm 2),\ (2, \pm 1),\ (3, 0),\ O\}$$

where O is the "point at infinity". These points form a cyclic group of order 6.

$$E(\mathbb{F}_5) \cong \mathbb{Z}/6\mathbb{Z}.$$

2.11.2 The Singular Situation for Finite Fields

For finite fields we have the analogue of Theorem 2.4.2:

Theorem 2.11.7. *If an elliptic curve becomes singular over a finite field $\mathbb{F}_q$ with singular point Q then we have*

(a) If Q is a cusp, then $E_{ns}(\mathbb{F}_q) \cong \mathbb{F}_q^+$ of order q.

(b) If Q is a node with tangents whose slopes are rational over $\mathbb{F}_q$ (split multiplicative reduction), then $E_{ns}(\mathbb{F}_q) \cong \mathbb{F}_q^*$ of order $q-1$.

(c) If Q is a node with tangents whose slopes are quadratic over $\mathbb{F}_q$ (nonsplit multiplicative reduction), then $E_{ns}(\mathbb{F}_q)$ is isomorphic to the subgroup of order $q+1$ in $\mathbb{F}_{q^2}^*$ (a cyclic group of order q^2-1).

Corollary 2.11.8. *If an elliptic curve E has bad reduction at a prime p, so $p \mid \Delta(E)$, the trace at $q = p^m$ for $m \geq 1$ is given by*

(a) if the reduction is additive $a_q(E_{ns}) = 0$;

(b) if the reduction is split multiplicative $a_q(E_{ns}) = 1$;

(c) if the reduction is nonsplit multiplicative $a_q(E_{ns}) = -1$.

Proof. For primes of singular reduction the trace of Frobenius is given by $a_q(E_{\mathrm{ns}}) = q - |E_{\mathrm{ns}}(\mathbb{F}_q)|$, where we subtract 1 for the singular point in the trace formula (2.11.1), and so using this formula together with Theorem 2.11.7 the three cases are clear. □

2.12 Quadratic Twists

Definition 2.12.1. Let K be a field with $\mathrm{char}(K) \neq 2$. Let E/K be an elliptic curve of the form:

$$E\colon y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Given $d \in K^*$ the *quadratic twist* of E by d is the curve $E^{(d)}$, defined by:

$$E^{(d)} \colon dy^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{2.12.1}$$

To convert $E^{(d)}$ to an ordinary Weierstrass form, multiply (2.12.1) through by d^3 and set $Y = d^2y$, $X = xd$, then (2.12.1) becomes

$$E^{(d)} \colon d^4\left(\frac{Y}{d^2}\right)^2 = d^3\left(\frac{X}{d}\right)^3 + a_2d^3\left(\frac{X}{d}\right)^2 + a_4d^3\left(\frac{X}{d}\right) + a_6d^3,$$

or equivalently

$$E^{(d)} \colon Y^2 = X^3 + a_2dX^2 + a_4d^2X + a_6d^3.$$

These two elliptic curves E and $E^{(d)}$ are not isomorphic over K, but over the quadratic field extension $K(\sqrt{d})$.

If $\mathrm{char}(K) = 2$, then given $d \in K$ such that $x^2 + x + d$ is an irreducible polynomial over K, a curve E/K given in long Weierstrass form (2.3.2) has quadratic twist given by

$$E^{(d)} \colon y^2 + a_1xy + a_3y = x^3 + (a_2 + a_1^2d)x^2 + a_4x + a_6 + a_3^2d.$$

Now E is not isomorphic to $E^{(d)}$ over K, but over the field extension $K[x]/(x^2 + x + d)$.

2.12.1 Quadratic Twists over Finite Fields

If we take our field to be a finite field $\mathbb{F}_q$ with an odd number q of elements and d a nonsquare in $\mathbb{F}_q^*$, then for each $x \in \mathbb{F}_q$ there exists a $y \in \mathbb{F}_q$ such that the point $P = (x, y)$ belongs to one of E or $E^{(d)}$. There are always two such values y, so that

$$|E(\mathbb{F}_q)| + |E^{(d)}(\mathbb{F}_q)| = 2q + 2.$$

In particular we get $a_q(E) = -a_q(E^{(d)})$. Thus we get:

Theorem 2.12.2. *Let $E/\mathbb{F}_p$ with Weierstrass equation of the form $y^2 = f(x)$, for some cubic f, p an odd prime, $d \in \mathbb{F}_p^*$. Let $E^{(d)}$ be the quadratic twist of E by d.*

Then

$$a_p(E^{(d)}) = \left(\frac{d}{p}\right) a_p(E) \tag{2.12.2}$$

where $\left(\frac{d}{p}\right)$ *is the Legendre symbol.*

Proof. See [12, Prop. 7.3.16]. □

Example 2.12.3. In Subsection 7.2.1 we study the elliptic curve

$$E\colon Y^2 = X^3 - 3UX + 2V.$$

We find we have to consider the twist of E by $\sqrt{-1}$, which is

$$E^{(-1)}\colon Y^2 = X^3 - 3UX - 2V.$$

If (X_0, Y_0) is a point on E, then $(-X_0, iY_0)$ (where $i = \sqrt{-1}$) is seen to be a point on $E^{(-1)}$ since

$$(iY_0)^2 = -Y_0^2 = -(X_0^3 - 3U_nX_0 + 2V_n) = (-X_0)^3 - 3U_n(-X_0) - 2V_n.$$

This shows E and $E^{(-1)}$ are isomorphic over $\mathbb{Q}(\sqrt{-1})$, but not over $\mathbb{Q}$.

2.13 Elliptic Curves over $\mathbb{C}$

The aim of this Section will be to illustrate some of the elliptic functions utilized in the sequel. The Weierstrass $\wp$-function can be used in the parametric equations of elliptic curves. It can be thought of as the fundamental elliptic function having periods ω_1, ω_2 and a double pole at the origin with residue 0. The Weierstrass ζ-function and the Weierstrass σ-function are also introduced, with the latter function being shown later to be closely associated with some of the polynomial expressions concerned with evaluating points on elliptic curves.

Although we study all these functions under the label of elliptic functions it should be noted that only the Weierstrass $\wp(z;\Lambda)$-function and its derivative are elliptic functions, because only these functions are doubly periodic. The other

Weierstrass functions $\zeta(z;\Lambda)$ and $\sigma(z;\Lambda)$ are not elliptic functions because they are only quasi-periodic functions with respect to z.

2.13.1 Complex Tori

Definition 2.13.1. A *lattice in* $\mathbb{C}$ is a set

$$\Lambda = \langle \omega_1, \omega_2 \rangle = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2,$$

with $\{\omega_1, \omega_2\}$ a basis for $\mathbb{C}$ over $\mathbb{R}$. The lattice Λ can be equivalently expressed via a homothetic transformation as a normalised lattice Λ_τ,

$$\Lambda_\tau = \langle 1, \tau \rangle = \frac{1}{\omega_1}\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau \quad \text{where} \quad \tau = \frac{\omega_2}{\omega_1}, \quad \Im\left(\frac{\omega_2}{\omega_1}\right) > 0,$$

where the imaginary part of the ratio of periods may be taken to be positive by exchanging the roles of ω_1, ω_2 if necessary.

From henceforth we shall assume all our lattices are normalised by putting $\omega_1 = 1$ and $\omega_2 = \tau$.

Definition 2.13.2. Let $\Lambda_\tau = \{m\tau + n : m, n \in \mathbb{Z}\}$ be the lattice generated by 1 and τ. A *fundamental parallelogram* for the lattice Λ_τ is a set of the form

$$D = \{t_1 + t_2\tau : 0 \leq t_1, t_2 < 1\}.$$

Definition 2.13.3. A *complex torus* is a qoutient of the complex plane by a lattice Λ,

$$\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}.$$

2.13.2 Elliptic Functions

Definition 2.13.4. An *elliptic function* f, with respect to the lattice Λ, is a meromorphic function $f\colon \mathbb{C} \longrightarrow \mathbb{C}$, which is doubly periodic with respect to Λ:

$$f(z + \omega) = f(z) \quad \text{for all } z \in \mathbb{C},\ \omega \in \Lambda.$$

The set of all such functions is denoted by $\mathbb{C}(\Lambda)$. It is clear $\mathbb{C}(\Lambda)$ is a field.

Definition 2.13.5. The *Eisenstein series of weight* $2k$ associated to a lattice Λ is defined to be

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2k}}$$

and is absolutely convergent for all $k > 1$ [35, Ch. VI, Thm. 3.1(a)]. We also define

$$G_{2k}(\tau) = G_{2k}(\Lambda_\tau) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^{2k}}.$$

Definition 2.13.6. The Weierstrass $\wp$-function (relative to Λ) is defined by

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right), \quad z \in \mathbb{C},\ z \notin \Lambda. \tag{2.13.1}$$

We see $\wp(z;\Lambda)$ is a meromorphic doubly periodic function with a pole of order 2 at each period (with none other), and converges absolutely and uniformly in any bounded closed domain containing none of the lattice points [35, Ch. VI, Thm. 3.1(b)]. It is thus an (even) elliptic function [35, Ch. VI, Thm. 3.1(c)]. If the lattice has been fixed we shall write $\wp(z;\Lambda) = \wp(z)$ for concision. The derivative of the $\wp$-function is

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3} \tag{2.13.2}$$

and so $\wp'(z)$ has a pole of order 3 at each period.

Proposition 2.13.7. *For* $0 < |z| < \min_{0 \neq \omega \in \Lambda}(|\omega|)$ *the Laurent series expansion for* $\wp(z)$ *is*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}, \tag{2.13.3}$$

and the Laurent series expansion for $\wp'(z)$ *is*

$$\wp'(z) = -\frac{2}{z^3} + \sum_{k=1}^{\infty} 2k(2k+1) G_{2k+2} z^{2k-1}. \tag{2.13.4}$$

Proof. When $|z| < |\omega|$,

$$\begin{aligned}\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega^2}\left(\frac{1}{(1-(z/\omega))^2} - 1\right) \\ &= \frac{1}{\omega^2}\left(\sum_{k=1}^{\infty}(k+1)\frac{z^k}{\omega^k}\right).\end{aligned}$$

Therefore

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\neq 0}\sum_{k=1}^{\infty}\frac{z^k}{\omega^{k+2}},$$

where we sum over ω first, and then over k. The series expansion for $\wp'(z)$ follows similarly. □

Theorem 2.13.8. *The set of doubly periodic functions for Λ is an algebraic function field $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$.*

Proof. See [46, Thm. 9.3 (5)]. □

Theorem 2.13.8 shows every elliptic function is a rational combination of $\wp$ and $\wp'$.

2.13.3 Parametrizing Elliptic Curves

Theorem 2.13.9. *The $\wp$-function satisfies the nonlinear differential equation*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 \tag{2.13.5}$$

where g_2, g_3 are the elliptic invariants of the $\wp$-function, and are defined by the Eisenstein series

$$g_2(\Lambda) = 60G_4(\Lambda) \quad \textit{and} \quad g_3(\Lambda) = 140G_6(\Lambda).$$

Proof. By Proposition 2.13.7 if we cube the relations for $\wp(z)$, and square the Laurent series expansions for $\wp'(z)$, found in (2.13.3) and (2.13.4) respectively, we can show that

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6,$$

is identically zero. See [46, Thm. 9.8]. □

Theorem 2.13.9 shows that the points $(\wp(z), \wp'(z))$ lie on the curve $y^2 = 4x^3 - g_2x - g_3$. Hence the differential equation (2.13.5) can be used to show that $\mathbb{C}/\Lambda$ is always complex analytically isomorphic to an elliptic curve.

Proposition 2.13.10. *Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ be the quantities associated to a lattice $\Lambda \subset \mathbb{C}$. The polynomial $f(x) = 4x^2 - g_2x - g_3$ has distinct roots, so its discriminant $\Delta(\Lambda) = g_2^3 - 27g_3^2$ is nonzero.*

Proof. See [46, Prop. 9.9]. □

The nonvanishing of the discriminant in Proposition 2.13.10 implies the next Theorem that shows how the $\wp$-function can be used to parametrize elliptic curve equations.

Proposition 2.13.11. *Let Λ be a lattice and let $E/\mathbb{C}$ be the elliptic curve*

$$E\colon y^2 = 4x^3 - ax - b. \tag{2.13.6}$$

Then the map

$$\begin{aligned} \theta\colon \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}) \\ z &\longmapsto (\wp(z) : \wp'(z) : 1) \\ 0 &\longmapsto O \end{aligned}$$

is a complex analytic isomorphism of complex Lie groups.

Proof. See [35, Ch. VI, Prop. 3.6]. □

In fact we can show every elliptic curve over $\mathbb{C}$ corresponds to a torus.

Proposition 2.13.12. *Let $E/\mathbb{C}$ be the elliptic curve defined by $y^2 = 4x^3 - ax - b$. Then there exists a lattice Λ such that $g_2(\Lambda) = a$ and $g_3(\Lambda) = b$. Then there is an isomorphism of groups $\mathbb{C}/\Lambda \cong E(\mathbb{C})$.*

Proof. See [46, Ch. 9, Thm. 9.19]. □

By normalizing we have assumed $\Lambda = \Lambda_E = \mathbb{Z} + \mathbb{Z}\tau$ with $\Im(\tau) > 0$. The value of τ is determined modulo the action of $\mathrm{SL}_2(\mathbb{Z})$ on the complex upper half plane $\mathbb{H}$ and is the *period* of E.

Proposition 2.13.11 shows the map $z \mapsto (\wp(z) : \wp'(z) : 1)$ takes nonlattice points of $\mathbb{C}$ to points $(x, y) \in \mathbb{C}^2$ satisfying the nonsingular equation (2.13.6).

Remark 2.13.13. If we divide the coefficients of the Weierstrass form (2.13.6) by 4 and set y to $\frac{1}{2}y$, $A = -\frac{g_2}{4}$, and $B = -\frac{g_3}{4}$, we gain the form

$$E\colon y^2 = x^3 + Ax + B.$$

Hence we have the Weierstrass $\wp$-function and its derivative map $\mathbb{C}/\Lambda$ to E via $(x, y) = (\wp(z), \frac{1}{2}\wp'(z))$.

Definition 2.13.14. The Weierstrass ζ-function (relative to Λ) is defined

$$\zeta(z) = \zeta(z; \Lambda) = \frac{1}{z} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right), \quad z \in \mathbb{C},\ z \notin \Lambda. \tag{2.13.7}$$

Proposition 2.13.15. *The Weierstrass ζ-function relative to the lattice Λ satisfies:*

(a) *For all $z \in \mathbb{C}$, $\frac{d}{dz}\zeta(z) = -\wp(z)$.*

(b) $\zeta(-z) = -\zeta(z)$.

(c) *For all $\omega \in \Lambda$ and all $z \in \mathbb{C}$,*

$$\zeta(z + \omega) = \zeta(z) + \eta(\omega),$$

where the number $\eta(\omega)$ is independent of z. The map

$$\eta\colon \Lambda \longrightarrow \mathbb{C}$$

is called the quasi-period map associated to Λ.

Proof. For (a), the series (2.13.7) converges absolutely and uniformly, and so differentiating it term by term gives the series for $-\wp$ which is convergent. For (b),

we note replacing ω by $-\omega$ does not change $\zeta(z)$. Evaluating at $-z$ gives $-\zeta(z)$. For (c)

$$\frac{d}{dz}\zeta(z+\omega) = -\wp(z+\omega) = -\wp(z) = \frac{d}{dz}\zeta(z).$$

Integrating, we find the quantity

$$\eta(\omega) = \zeta(z+\omega) - \zeta(z)$$

is independent of z. □

Definition 2.13.16. The Weierstrass σ-function (relative to Λ) is obtained by integrating $\wp$ twice and exponentiating to give the product

$$\sigma(z) = \sigma(z;\Lambda) = z \prod_{\substack{w\in\Lambda \\ w\neq 0}} \left(1 - \frac{z}{w}\right) e^{(z/w)+\frac{1}{2}(z/w)^2}. \tag{2.13.8}$$

This function is holomorphic on $\mathbb{C}$. It has simple zeros at each $z \in \Lambda$ and no other zeros [35, Ch. VI, Thm. 3.3(a)].

The Weierstrass σ-function is not periodic with respect to Λ, but has a quasi-periodicity which we now describe: Let $\eta\colon \Lambda \to \mathbb{C}$ be the quasi-period map for Λ, and define $\lambda\colon \Lambda \to \{\pm 1\}$ by

$$\lambda(\omega) = \begin{cases} 1 & \text{if } \omega \in 2\Lambda, \\ -1 & \text{if } \omega \notin 2\Lambda. \end{cases}$$

The Weierstrass σ-function satisfies the following transformation formula:

$$\sigma(z+\omega;\Lambda) = \lambda(\omega)e^{\eta(\omega)(z+\frac{\omega}{2})}\sigma(z;\Lambda) \quad \text{for all } z \in \mathbb{C} \text{ and } \omega \in \Lambda. \tag{2.13.9}$$

Definition 2.13.17. Fix a lattice $\Lambda \subset \mathbb{C}$ corresponding to an elliptic curve E. For $\mathbf{v} = (v_1, \ldots, v_r) \in \mathbb{Z}^r$, define a function $\Psi_{\mathbf{v}}$ on $\mathbb{C}^r$ in variables $\mathbf{z} = (z_1, \ldots, z_r)$

as follows:

$$\Psi_{\mathbf{v}}(\mathbf{z};\Lambda) = (-1)^{\sum_{1\le i\le j\le r} v_i v_j+1} \frac{\sigma(v_1 z_1+\cdots+v_r z_r;\Lambda)}{\left(\prod_{i=1}^{r}\sigma(z_i;\Lambda)^{2v_i^2-\sum_{j=1}^{r} v_i v_j}\right)\left(\prod_{1\le i<j\le r}\sigma(z_i+z_j;\Lambda)^{v_i v_j}\right)}, \tag{2.13.10}$$

where for $\mathbf{v}=0$ we set $\Psi_{\mathbf{v}}\equiv 0$.

In particular we outline the first two cases of Definition 2.13.17 as these will be of particular interest to us in the sequel.

Example 2.13.18. For each $m\in\mathbb{Z}$ we have a function on $\mathbb{C}$ in the variable z:

$$\Psi_m(z;\Lambda) = (-1)^{m+1}\frac{\sigma(mz;\Lambda)}{\sigma(z;\Lambda)^{m^2}}. \tag{2.13.11}$$

For each $(m,n)\in\mathbb{Z}^2$ we have a function on $\mathbb{C}^2$ in the variables z and w:

$$\Psi_{m,n}(z,w;\Lambda) = (-1)^{(m+n)^2+1}\frac{\sigma(mz+nw;\Lambda)}{\sigma(z;\Lambda)^{m^2-mn}\sigma(z+w;\Lambda)^{mn}\sigma(w;\Lambda)^{n^2-mn}}. \tag{2.13.12}$$

Lemma 2.13.19. *Let u and v be complex variables. Then we have the relation*

$$\wp(u)-\wp(v) = -\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}. \tag{2.13.13}$$

Fix a lattice $\Lambda\subset\mathbb{C}$ corresponding to an elliptic curve E. Let vectors $\mathbf{u}=(u_1,\ldots,u_r)$, $\mathbf{v}=(v_1,\ldots,v_r)\in\mathbb{Z}^r$. Then for the vector $\mathbf{z}$ of r complex variables $\mathbf{z}=(z_1,\ldots,z_r)\in\mathbb{C}^r$ we have

$$\wp(\mathbf{u}\cdot\mathbf{z})-\wp(\mathbf{v}\cdot\mathbf{z}) = -\frac{\Psi_{\mathbf{u}+\mathbf{v}}(\mathbf{z})\Psi_{\mathbf{u}-\mathbf{v}}(\mathbf{z})}{\Psi_{\mathbf{u}}(\mathbf{z})^2\Psi_{\mathbf{v}}(\mathbf{z})^2}. \tag{2.13.14}$$

Proof. Equation (2.13.13) is a standard result; see [34, Cor. 5.6 (a)]. Equation (2.13.14) follows from (2.13.13) by calculation using (2.13.10) to give

$$\frac{\Psi_{\mathbf{u}+\mathbf{v}}(\mathbf{z})\Psi_{\mathbf{u}-\mathbf{v}}(\mathbf{z})}{\Psi_{\mathbf{u}}(\mathbf{z})^2\Psi_{\mathbf{v}}(\mathbf{z})^2} = \frac{\sigma((\mathbf{u}+\mathbf{v})\cdot\mathbf{z})\sigma((\mathbf{u}-\mathbf{v})\cdot\mathbf{z})}{\sigma(\mathbf{u}\cdot\mathbf{z})^2\sigma(\mathbf{v}\cdot\mathbf{z})^2}.$$

□

2.13.4 Torsion Points in $\mathbb{C}$

Which points in $E(\mathbb{C})$ have $[n]P = O$? Using the $\wp$-function we have $\wp(nz) = n\wp(z) = 0$ if and only if $nz \in \Lambda$. Hence we need $z \in \frac{1}{n}\Lambda$. Since $\frac{1}{n}\Lambda/\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^2$ we get: There is an isomorphism of abstract groups

$$E(\mathbb{C})[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Chapter 3

The Division Polynomials

Throughout we let K be a field of characteristic 0.

3.1 General Theory

Let K be a field and E/K an elliptic curve given by the Weierstrass equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.1.1}$$

Let $P = (x, y) \in E(K)$. Look at the sequence of points $[n]P = (x_n, y_n)$ for $n \in \mathbb{Z}$, $[n]P \neq O$. By the addition law on E/K, two points P_1, P_2 on E have $P_1 + P_2$ described by rational functions of the coordinates of P_1 and P_2. It follows $[n]P$ can be expressed in terms of rational functions in x, y and the coefficients of the Weierstrass equation (3.1.1).

One way we can investigate the group of n-torsion points $E[n]$, for nonzero n, is to introduce a function Ψ_n which has zeros exactly at the points in $E[n]\backslash\{O\}$ with one pole at O. Let $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ be the defining equation for E, and let $K(E)$ be the field of fractions of $K[E] = K[x, y]/\langle y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6\rangle$.

Proposition 3.1.1. *Consider an elliptic curve defined over a field K with Weierstrass model $f(x, y) = 0$, where*

$$f(x, y) := y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6; \quad a_i \in K. \tag{3.1.2}$$

The division polynomials *are the unique polynomials in the quotient field* $K[x,y]/\langle f(x,y)\rangle$ *which satisfy the following nonlinear recursion:*

$$\begin{aligned}
\Psi_0 &= 0,\\
\Psi_1 &= 1,\\
\Psi_2 &= 2y + a_1x + a_3,\\
\Psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
\Psi_4 &= \Psi_2\Big(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\Big),
\end{aligned}$$

where the b_i *are as usual,*

$$\Psi_{m+n}\Psi_{m-n}\Psi_r^2 = \Psi_{m+r}\Psi_{m-r}\Psi_n^2 - \Psi_{n+r}\Psi_{n-r}\Psi_m^2 \quad \textit{for all } m > n > r. \tag{3.1.3}$$

Furthermore they are given inductively by the duplication formulas

$$\Psi_{2n+1} = \Psi_{n+2}\Psi_n^3 - \Psi_{n-1}\Psi_{n+1}^3 \qquad \textit{for } n \geq 2, \tag{3.1.4a}$$

$$\Psi_2\Psi_{2n} = \Psi_n\Big(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2\Big) \qquad \textit{for } n \geq 3, \tag{3.1.4b}$$

Proof. For a proof of the general recursion (3.1.3) and the fact that this together with the fixed values Ψ_0, Ψ_1, Ψ_2, Ψ_3, Ψ_4, determines the division polynomials uniquely see [18, Prop. 3.52, 3.53], and also [1, Ch. 4.4.5.(a)], [35, Ch. III, Ex. 3.7]. For some of the classical elliptic function theory underpinning these results see [9, Ch. III.4, Ch. IV.3]. □

Proposition 3.1.2. *Let* E/K *be an elliptic curve given by Weierstrass equation*

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

For $n \in \mathbb{Z}_{\neq 0}$, the n^{th} division polynomial Ψ_n *is the unique rational function* $\Psi_n \in K(E)$ *having divisor*

$$\operatorname{div}(\Psi_n) = \sum_{P \in E[n]} (P) - n^2(O), \tag{3.1.5}$$

with leading coefficient n*. Set* $\Psi_0 = 0$ *by convention.*

Proof. See [18, Prop. 3.57]. □

With Proposition 3.1.2 in hand we have

Theorem 3.1.3. *The division polynomials satisfy*

$$\Psi_{-n} = -\Psi_n. \tag{3.1.6}$$

Proof. This is clear from Proposition 3.1.2 and the fact that if P is any torsion point then so is its inverse $-P$, i.e., $E[n] = E[-n]$. □

Remark 3.1.4. Let $P = (x, y)$ be a point on an elliptic curve. Concerning notation we shall write either of $\Psi_n(P)$ or $\Psi_n(x, y)$ for the n^{th} division polynomial evaluated at the point P.

Theorem 3.1.5. *Let $x(P)$ denote the x-coordinate of a point $P = (x(P), y(P))$ on an elliptic curve E/K. Then the division polynomials satisfy*

$$\Psi_n^2(x, y) = n^2 \prod_{P \in E(K)[n] \setminus \{O\}} \Big(x - x(P)\Big) = n^2 x^{n^2-1} + \cdots \quad \in \mathbb{Z}[x]$$

a primitive integral polynomial vanishing at the x-coordinates of torsion points on the curve of order dividing n.

Proof. We have that $\operatorname{div}(x - x(P)) = (P) + (-P) - 2(O)$ since the only zeros of $x - x(P)$ are P and $-P$. Then by (3.1.5)

$$\operatorname{div}(\Psi_n^2) = \sum_{P \in E[n]} 2(P) - 2n^2(O),$$

while

$$\begin{aligned} \operatorname{div}\left(n^2 \prod_{P \in E[n] \setminus \{O\}} (x - x(P))\right) &= \sum_{P \in E[n] \setminus \{O\}} \operatorname{div}(x - x(P)) \\ &= \sum_{P \in E[n] \setminus \{O\}} \Big((P) + (-P)\Big) + 2(O) \\ &= \sum_{P \in E[n]} 2(P) - 2n^2(O), \end{aligned} \tag{3.1.7}$$

where we can do the last step since $E[n] = -E[n]$. Hence the divisors of two rational functions agree. Moreover the leading coefficient is n^2 in both rational

functions so they must be the same. The power of x follows as there are $n^2 - 1$ torsion points in $E[n]\backslash\{O\}$. □

Proposition 3.1.6. *For n odd, $\Psi_n \in K[x]$ (where we identify $K[x]$ with its image in $K(E)$), while for n even, $\Psi_n \in (2y + a_1x + a_3)K[x]$.*

Proof. If n is odd $E[n]$ contains no point of order 2 and we can write $E[n] = S \cup -S \cup \{O\}$ for some set S where $-S = \{-P : P \in S\}$. Then $\Psi_n = n\sum_{P\in S}(x - x(P))$ by the same argument as in Theorem 3.1.5.

For the case n even, $E[2] \subseteq E[n]$. Decompose $E[n] = S \cup -S \cup E[2]$ such that, as $\mathrm{char}(K) \neq 2$, $\Psi_n = \frac{n}{2}\Psi_2 \sum_{P\in S}(x - x(P))$. Now there are three nonzero points of order 2 which sum to O since by (3.1.5) there is a rational function with divisor $(E[2]) - 4(O)$, namely the line $2y + a_1x + a_3$, since a point (x, y) is a 2-torsion point if and only if $2y + a_1x + a_3 = 0$. □

Corollary 3.1.7. *For m and n having the same parity then $\Psi_m\Psi_n \in K[x]$.*

Proof. If m and n are odd the result follows by Proposition 3.1.6. If they are even then we need merely note $\Psi_2^2 = (2y+a_1x+a_3)^2 = 4x^3+b_2x^2+2b_4x+b_6 \in K[x]$. □

The next Lemma proves the division polynomials in characteristic zero have coefficients in $\mathbb{Z}$.

Lemma 3.1.8. *The division polynomials Ψ_n satisfy*

$$\Psi_n \in \begin{cases} \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x] & \text{if } n \text{ is odd,} \\ \Psi_2\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x] & \text{if } n \text{ is even.} \end{cases} \tag{3.1.8}$$

Proof. Because of the antisymmetric property (3.1.6) we need only prove for the case $n \geq 0$. The Lemma is true for $0 \leq n \leq 4$ by Proposition 3.1.1. Assume by induction that the Lemma is true for $1 \leq k \leq n - 1$. We subdivide into two cases:

If n is odd, say $n = 2k + 1$ with $k \geq 2$, then by the formula (3.1.4a) we have

$$\Psi_{2k+1} = \Psi_{k+2}\Psi_k^3 - \Psi_{k-1}\Psi_{k+1}^3 \quad \text{for } k \geq 2. \tag{3.1.9}$$

We note that $2k + 1 > k + 2$ and so by examination of the suffixes on the RHS of (3.1.9) we have if k is even, then by induction Ψ_2^4 divides the $\Psi_{k+2}\Psi_k^3$

term, where $\Psi_2^2 = (4x^3 + b_2x^2 + 2b_4x + b_6)^2$, and so $\Psi_{k+2}\Psi_k^3$ is a polynomial in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$, for the $\Psi_{k-1}\Psi_{k+1}^3$ term we note both suffixes are odd, so, by induction, $\Psi_{k-1}\Psi_{k+1}^3$ is a polynomial in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$. Hence $\Psi_{2k+1} \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$ if k is even. If k is odd the same reasoning applies. Thus for n odd we have $\Psi_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$.

If $n = 2k$ with $k \geq 3$, then $2k > k + 2$. Equation (3.1.4b) gives

$$\Psi_{2k} = \frac{\Psi_k}{\Psi_2}(\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2) \quad \text{for } k \geq 3. \tag{3.1.10}$$

Now Ψ_{k-2}, Ψ_{k-1}, Ψ_k, Ψ_{k+1}, Ψ_{k+2} are polynomials satisfying the conditions of the inductive hypothesis since all suffixes are less than $2k$. If k is odd then Ψ_2^2 divides $(\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2)$, while if k is even Ψ_2 divides Ψ_k, Ψ_{k+2}, and Ψ_{k-2} and so Ψ_2^2 divides $\Psi_k(\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2)$. Hence Ψ_{2k} is a polynomial in $\Psi_2\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$ as required. □

Let $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ be the defining equation of an elliptic curve E. Since the division polynomials will be evaluated at points on an elliptic curve, we compute them modulo $f(x, y)$. Thus in particular the degree of y in Ψ_n never exceeds 1 (since we can replace y^2 by $x^3 + a_2x^2 + a_4x + a_6 - a_1xy - a_3y$ whenever it occurs).

By Lemma 3.1.8 the division polynomials in characteristic zero have integer coefficients, and we are thus allowed to reduce them modulo a prime p. Therefore all equations found in characteristic zero still hold in positive characteristic p, since by Lemma 3.1.8 they are equations in the quotient field of the integral domain $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]/\langle f(x, y)\rangle$ – providing no denominator is zero after reducing modulo p.

Lemma 3.1.9. *For the division polynomials defined in a field of arbitrary characteristic we have $\Psi_n \neq 0$ for $n \neq 0$.*

Proof. See [18, Lem. 3.56]. □

Proposition 3.1.10.

$$\Psi_n(x, y) = \begin{cases} nx^{(n^2-1)/2} + g(x) & \text{if } n \text{ is odd,} \\ (2y + a_1x + a_3)\left(\frac{n}{2}x^{(n^2-4)/2} + h(x)\right) & \text{if } n \text{ is even.} \end{cases} \tag{3.1.11}$$

where $g,\ h \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$ *and* $\deg(g) < (n^2-1)/2$, $\deg(h) < (n^2-4)/2$.

Proof. We prove by induction. The result (3.1.11) is true for $\Psi_1,\ \Psi_2,\ \Psi_3,\ \Psi_4$. Assume (3.1.11) holds for all integers m such that $0 \leq m \leq n-1$ with $n-1 \geq 4$. Let $n = 2k+1$ with k even, then the leading term of $\Psi_{k+2}\Psi_k^3$ is

$$(k+2)k^3\Big((2y + a_1x + a_3)/2\Big)^4 x^{\frac{(k+2)^2-4}{2}+\frac{3k^2-12}{2}}.$$

Now the leading coefficient of $(2y + a_1x + a_3)^4$ is $16x^6$ and so this becomes

$$(k+2)k^3 x^{\frac{(2k+1)^2-1}{2}}.$$

Similarly the leading term of $\Psi_{k-1}\Psi_{k+1}^3$ is

$$(k-1)(k+1)^3 x^{\frac{(2k+1)^2-1}{2}}.$$

Using the formula $\Psi_{2k+1} = \Psi_{k+2}\Psi_k^3 - \Psi_{k+1}^3\Psi_{k-1}$ we have on subtraction

$$(k+2)k^3 x^{\frac{(2k+1)^2-1}{2}} - (k-1)(k+1)^3 x^{\frac{(2k+1)^2-1}{2}}$$

the leading term for Ψ_{2k+1} to be $(2k+1)x^{((2k+1)^2-1)/2}$ as required. Hence the polynomials Ψ_n, with n odd, are of degree $(n^2-1)/2$ with leading coefficient n, and coefficients in the ring $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. The other cases are treated similarly. □

Theorem 3.1.11. *Let* E/K *be an elliptic curve with Weierstrass equation*

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0; \quad a_i \in K.$$

There exist polynomials Φ_n, *and* Ω_n *in the quotient field* $K[x, y]/\langle f(x, y)\rangle$ *defined*

by

$$\Phi_n = x\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}, \qquad \textit{for all } n \in \mathbb{Z}, \tag{3.1.12}$$

$$\Phi_{-n} = \Phi_n, \tag{3.1.13}$$

$$\Omega_n = \frac{1}{2\Psi_2}\left(\Psi_{n-1}^2\Psi_{n+2} - \Psi_{n-2}\Psi_{n+1}^2 - \Psi_2\Psi_n(a_1\Phi_n + a_3\Psi_n^2)\right), \tag{3.1.14}$$

$$\Omega_{-n} = \Omega_n + (a_1\Phi_n + a_3\Psi_n^2)\Psi_n \qquad \textit{for } n \neq 0, \tag{3.1.15}$$

such that, for all nonsingular points $P = (x, y) \in E(\bar{K})$

$$[n]P = \left(\frac{\Phi_n(x,y)}{\Psi_n^2(x,y)}, \frac{\Omega_n(x,y)}{\Psi_n^3(x,y)}\right) \quad \textit{if } [n]P \neq O. \tag{3.1.16}$$

Proof. See [31, Thm. 2.26] for the polynomial recursions, and [6, Lem. III.5] for the proof of (3.1.16). □

Proposition 3.1.12. *The division polynomials* Φ_n *and* Ω_n *satisfy*

$$\Phi_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x] \quad \textit{for all } n, \tag{3.1.17}$$

$$\Omega_n \in \begin{cases} \Psi_2\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x] & \textit{if } n \textit{ is odd}, \\ \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x] & \textit{if } n \textit{ is even}. \end{cases} \tag{3.1.18}$$

Proof. If n is odd, then Ψ_{n+1} and Ψ_{n-1} are in $\Psi_2\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$ so their product is in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$. Therefore $\Phi_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$. If n is even the proof is similar.

The results for Ω_n follow from Lemma 3.1.8. □

Proposition 3.1.13. *The polynomials* Φ_n *and* Ψ_n^2 *are polynomials in the variable* x *alone with coefficients in the ring* $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. *In particular they are of the form*

$$\Phi_n(x) = x^{n^2} + \textit{(lower degree terms)},$$
$$\Psi_n^2(x) = n^2x^{n^2-1} + \textit{(lower degree terms)}.$$

Proof. The result for Ψ_n^2 follows immediately from Theorem 3.1.5. For Φ_n we compare the degrees and leading terms in $\Phi_n = x\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}$ in similar manner to Proposition 3.1.10. □

3.1.1 The Representation of Division Polynomials by Elliptic Functions

The next Proposition is [35, Ch. VI, Ex. 6.15].

Proposition 3.1.14. *Let $E/\mathbb{C}$ be an elliptic curve and let Ψ_n be the division polynomial defined in Proposition 3.1.1. Let Λ be some fixed complex lattice such that $E \cong \mathbb{C}/\Lambda$ and z a complex variable. Considered as a function on $\mathbb{C}/\Lambda$, $\Psi_n(z)$ is given by*

$$\Psi_n(z;\Lambda) = (-1)^{n+1}\frac{\sigma(nz;\Lambda)}{\sigma(z;\Lambda)^{n^2}}. \tag{3.1.19}$$

Proof. By Proposition 2.13.11 we have the isomorphic mapping

$$\theta\colon \mathbb{C}/\Lambda \to E'(\mathbb{C}),\ z \mapsto (\wp(z) : \wp'(z) : 1)$$

where E' is of the form

$$E'\colon y^2 = 4x^3 - g_2x - g_3. \tag{3.1.20}$$

This isomorphism between points $z_P \in \mathbb{C}/\Lambda$ and the points $P \in E'(\mathbb{C})$, where $x(P) = \wp(z_P)$, $y(P) = \wp'(z_P)$ with respect to the elliptic curve (3.1.20), can be used to describe the division polynomials $\Psi_n(x(P), y(P)) = \Psi_n(\wp(z_P), \wp'(z_P))$ in the usual way. Hence, with respect to the lattice Λ, we may calculate the complex function $\Psi_n(z_P)$ as being identical to the division polynomial $\Psi_n(\wp(z_P), \wp'(z_P))$. This shows, after making the identification $\Psi_n(z_P) = \Psi_n(\wp(z_P), \wp'(z_P))$, that $\Psi_n(z_P)$ is in the field of elliptic functions, being a rational function in $\mathbb{C}(\wp, \wp')$.

Now let $E/\mathbb{C}$ be the curve given in long Weierstrass form

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1.21}$$

and define a change of variables, as described in (2.3.3) and (2.3.6), to give the

mapping

$$\begin{aligned} \xi\colon E'(\mathbb{C}) &\longrightarrow E(\mathbb{C}) \\ (\wp(z), \wp'(z)) &\longmapsto \left(\wp(z) - \frac{b_2}{12}, \frac{\wp'(z)}{2} - \frac{a_1}{2}\left(\wp(z) - \frac{b_2}{12}\right) - \frac{a_3}{2}\right). \end{aligned}$$

Therefore under the map $\xi \circ \theta$ we see $\mathbb{C}/\Lambda$ is isomorphic to $E(\mathbb{C})$, and so $E'(\mathbb{C}) \cong E(\mathbb{C})$. Due to this isomorphism we have the function $\Psi_n(z)$ given by

$$\Psi_n(z) = \Psi_n\left(\wp(z) - \frac{b_2}{12}, \frac{\wp'(z)}{2} - \frac{a_1}{2}\left(\wp(z) - \frac{b_2}{12}\right) - \frac{a_3}{2}\right).$$

Let Λ be some fixed lattice, and let us define

$$\Upsilon_n(z;\Lambda) := \frac{\sigma(nz;\Lambda)}{\sigma(z;\Lambda)^{n^2}},$$

then $\Upsilon_n(z)$ is an elliptic function, which we now prove by showing the function on the right hand side is meromorphic with period lattice Λ. Let $\omega \in \Lambda$. From (2.13.9) it follows that

$$\begin{aligned} \frac{\sigma(n(z+\omega))}{\sigma(z+\omega)^{n^2}} &= \frac{\lambda(n\omega)e^{\eta(n\omega)(nz+\frac{n\omega}{2})}\sigma(nz)}{\lambda(\omega)^{n^2}e^{\eta(\omega)(z+\frac{\omega}{2})^{n^2}}\sigma(z)^{n^2}} \\ &= \frac{\lambda(\omega)^n e^{\eta(\omega)(z+\frac{\omega}{2})^{n^2}}\sigma(nz)}{\lambda(\omega)^{n^2}e^{\eta(\omega)(z+\frac{\omega}{2})^{n^2}}\sigma(z)^{n^2}} \\ &= \frac{\sigma(nz)}{\sigma(z)^{n^2}}. \end{aligned}$$

By the isomorphic mapping described we have $(\mathbb{C}/\Lambda)[n] \cong E[n]$. Now Ψ_n vanishes exactly at each nonzero $u \in (\mathbb{C}/\Lambda)[n]$. There are n^2-1 nonzero torsion points of $E'(\mathbb{C})[n]$, and so n^2-1 such points u. Since $\Psi_n(z)$ has exactly one pole of order n^2-1 at $z=0$, the order of vanishing at each nonzero torsion point is one, reflecting the fact that each of the n^2-1 nonzero roots is distinct, and so all the zeros are simple.

It is clear from (2.13.8) that the function $\Upsilon_n(z)$ also has a pole of order n^2-1 at $z=0$ and simple zeros at $\frac{1}{n}\Lambda\backslash\Lambda$.

Hence $\Psi_n(z)$ and $\Upsilon_n(z)$ have the same divisor and so are proportional functions. Multiplying by z^{n^2-1} to take account of the poles at $z=0$ we can therefore write

$$z^{n^2-1}\Psi_n(z) = cz^{n^2-1}\Upsilon_n(z), \tag{3.1.22}$$

which is analytic at $z=0$.

Plugging the definition of the Weierstrass σ-function in Equation (2.13.8) into the RHS of (3.1.22) gives

$$\begin{aligned} z^{n^2-1}\Upsilon_n(z) = z^{n^2-1}\frac{\sigma(nz)}{\sigma(z)^{n^2}} &= z^{n^2-1}\cdot\frac{nz\prod_{\substack{w\in\Lambda\\ w\neq 0}}\left(1-\frac{nz}{w}\right)e^{(nz/w)+\frac{1}{2}(nz/w)^2}}{z^{n^2}\prod_{\substack{w\in\Lambda\\ w\neq 0}}\left(1-\frac{z}{w}\right)^{n^2}e^{(z/w)^{n^2}+\frac{1}{2}(z/w)^{2n^2}}} \\ &= n\prod_{\substack{w\in\Lambda\\ w\neq 0}}\frac{\left(1-\frac{nz}{w}\right)}{\left(1-\frac{z}{w}\right)^{n^2}}e^{\frac{nz}{w}(1-n)} \end{aligned}$$

which tends to n as $z\to 0$.

By letting $x=\wp(z)$, $y=\frac{1}{2}\wp'(z)$ in Lemma 3.1.10, we find for the LHS of (3.1.22) that

$$z^{n^2-1}\Psi_n(z) = \begin{cases} nz^{n^2-1}\wp(z)^{(n^2-1)/2}+\cdots & \text{if } n \text{ is odd,} \\ nz^{n^2-1}\frac{1}{2}\wp'(z)\wp(z)^{(n^2-4)/2}+\cdots & \text{if } n \text{ is even.} \end{cases}$$

By the Laurent expansions (2.13.3) and (2.13.3) we see $\wp(z)=\frac{1}{z^2}+\cdots$ has a pole of order 2 at 0 and $\wp'(z)=\frac{-2}{z^3}+\cdots$ has a pole of order 3 at 0. Plugging these in gives

$$z^{n^2-1}\Psi_n(z) = \begin{cases} n+\cdots & \text{if } n \text{ is odd,} \\ -n+\cdots & \text{if } n \text{ is even.} \end{cases}$$

Hence on taking the limit

$$\lim_{z\to 0} z^{n^2-1}\Psi_n(z) = (-1)^{n+1}n.$$

Hence the constant c in (3.1.22) is $(-1)^{n+1}$, and so substituting in for $\Upsilon_n(z)$ we

have

$$\Psi_n(z) = (-1)^{n+1}\frac{\sigma(nz)}{\sigma(z)^{n^2}}$$

as required. □

We also have the identities

Proposition 3.1.15.

$$\begin{aligned}\Psi_{mn}(z) &= \Psi_m(z)^{n^2}\Psi_n(mz),\\ \Phi_{mn}(z) &= \Psi_m(z)^{2n^2}\Phi_n(mz),\\ \Omega_{mn}(z) &= \Psi_m(z)^{3n^2}\Omega_n(mz),\end{aligned} \tag{3.1.23}$$

for all integers m, n.

Proof. Consider $\Psi_{mn}(z)$, where z is understood to be a complex variable. Using the properties of the Weierstrass σ-function we have

$$\begin{aligned}\Psi_{mn}(z) = \frac{\sigma(mnz)}{\sigma(z)^{m^2n^2}} &= \left(\frac{\sigma(mz)}{\sigma(z)^{m^2}}\right)^{n^2}\left(\frac{\sigma(mnz)}{\sigma(mz)^{n^2}}\right)\\ &= \Psi_m(z)^{n^2}\Psi_n(mz).\end{aligned}$$

The other two equations have similar proofs based upon the given proof for Ψ_{mn} and then on subsequent use of the polynomial expressions for Φ_n and Ω_n given in Theorem 3.1.11. □

Proposition 3.1.16. *Let E/K be an elliptic curve, and $\Delta(E) \neq 0$. We have $\Phi_n(x)$ and $\Psi_n^2(x)$ are relatively prime polynomials in $K[x]$.*

Proof. See [46, Cor. 3.7]. □

Proposition 3.1.17. *We have $\Psi_{n-1}(x,y)$ and $\Psi_n(x,y)$ are relatively prime polynomials in $K[x,y]$ for all $n \geq 1$.*

Proof. See [46]. □

Corollary 3.1.18. *We have* $\gcd(\Psi_{n-1}\Psi_{n+1}(x), \Psi_n^2(x)) = 1$.

We saw in Subsection 2.13.4 that $E(\mathbb{C})[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, and so $E(\mathbb{C})[n]$ has n^2 elements. The roots of Ψ_n are the nonzero points of order n on E. It follows from Theorem 3.1.11 that $P = (x, y) \neq O$ is an n-torsion point if and only if $\Psi_n(x, y) = 0$. For any given $x \in \mathbb{C}$ there are at most two points $(x, y) \in E(\mathbb{C})$. Now the point O is the identity and so is 1-torsion, and the distinct roots of the Weierstrass equation of an elliptic curve are 2-torsion, with $2(x_r, 0) = 0$ where x_r denotes each of the three distinct roots. For order $n > 2$ we have that if $n(x, y) = 0$, so will $n(x, -y) = 0$, so we have two torsion points for each respective x if $n > 2$. By Proposition 3.1.13 we know if n is odd then $\Psi_n(x)$ has at most $(n^2 - 1)/2$ distinct roots.

Similarly, if n is even, $\Psi_n(x, y)/(2y + a_1x + a_3)$ has at most $(n^2 - 4)/2$ distinct roots, and the polynomial $\left(\Psi_n(x, y)/(2y + a_1x + a_3)\right)^2$ corresponds to all points for which $[n]P = 0$ except the four in the 2-torsion subgroup $E(\mathbb{C})[2]$ of order 1 or 2. Hence the roots of $\Psi_n(x, y)$ are distinct. In other words each root of $\Psi_n(x, y)$ gives rise to exactly two n-torsion points having order greater than 2.

3.2 From Polynomial to Sequence

The division polynomials form a *divisibility sequence*, that is they satisfy the property $\Psi_m \mid \Psi_n$ whenever $m \mid n$. In fact more can be said in that they form a *strong divisibility sequence* with the property $\gcd(\Psi_m, \Psi_n) = \Psi_{\gcd(m,n)}$ [45, Thm. 6.4].

Theorem 3.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve and p be a prime such that the a_i are p-integers. Then for all $P = (x_P, y_P) \in E(\mathbb{Q})$ which are nonsingular modulo p we have*

$$\Psi_n(x_P, y_P) \equiv 0 \pmod{p} \quad \textit{if and only if} \quad [n]\tilde{P} = \tilde{O}$$

on the reduced curve; here $[n]\tilde{P}$ denotes the reduction of $[n]P$ modulo p.

Proof. See [39, Thm. 3.10.5]. □

For two birationally equivalent elliptic curves E/K and E'/K, the birational map is a group homomorphism. Hence for two points $P \in E(K)$, and $P' \in E'(K)$, we have $P \in E[n]$ if and only if $P' \in E'[n]$ for all $n \in \mathbb{Z}_{>0}$.

Theorem 3.2.2 (Swart [39, Thm. 3.10.7]). *Let E/K be an elliptic curve over a field K. Let E' be the elliptic curve obtained from E by an admissible change of variables* (2.3.19)

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t.$$

Then

$$\Psi'_n(x', y') = u^{n^2-1}\Psi_n(x, y) \qquad \text{for all } n \in \mathbb{Z}. \tag{3.2.1}$$

By the nice form of the Ψ_n given in Proposition 3.1.10 we can turn any rational division polynomial sequence into an integral one by choosing the right equivalence of forms given in (3.2.1), clearing the denominators.

Theorem 3.2.3 (Swart [39, Thm. 3.10.8]). *Let E/K be a singular cubic curve. The point $P = (x_0, y_0)$ is singular if and only if $\Psi_3(x_0, y_0) = \Psi_4(x_0, y_0) = 0$. Then $\Psi_n(x_0, y_0) = 0$ for all $|n| > 1$.*

Proof. Let E' be birationally equivalent to E with $P' = (0, 0)$ a point on E'. Then by (2.4.1) P' is singular if and only if $a'_3 = a'_4 = 0$. From the division polynomials evaluated at $P' = (0, 0)$ we have

$$\Psi'_2(0, 0) = a'_3, \quad \Psi'_3(0, 0) = b'_8, \quad \Psi'_4(0, 0) = (b'_4b'_8 - b'^2_6)\Psi'_2(0, 0),$$

where $b'_4 = a'_1a'_3+2a'_4$, $b'_6 = a'^2_3$ and $b'_8 = -a'_1a'_3a'_4+a'_2a'^2_3-a'^2_4$. So $a'_3 = a'_4 = 0$ if and only if $\Psi'_3(0, 0) = \Psi'_4(0, 0) = 0$, from which $\Psi'_2(0, 0) = 0$ also. A brief induction shows $\Psi'_n(0, 0) = 0$ for all $n \in \mathbb{Z}$. Since $\Psi_n(x_0, y_0) = \Psi'_n(0, 0)$ by Theorem 3.2.2 the result follows, with E being singular at $P = (x_0, y_0)$ if and only if $\Psi_n(x_0, y_0) = 0$. The singular point P is then the simultaneous root for all Ψ_n. □

3.2.1 Valuations of the Division Polynomials

Let $E/\mathbb{Q}$ be an elliptic curve given by Weierstrass equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.2.2}$$

By Theorem 3.1.11 the n^{th} multiple of a point on an elliptic curve may be given in terms of the division polynomials

$$[n]P = \left(\frac{\Phi_n(x,y)}{\Psi_n^2(x,y)}, \frac{\Omega_n(x,y)}{\Psi_n^3(x,y)}\right) \quad \text{if } [n]P \neq O. \tag{3.2.3}$$

Ayad has shown that any cancellation occurring between the numerator and the denominator of (3.2.3) happens exactly at the primes of singular reduction at P. Throughout we shall write $\Psi_n(P)$ for the n^{th} division polynomial evaluated at a point $P = (x_1, y_1)$.

Theorem 3.2.4 (Ayad [2, Thm. A]). *Let $E/\mathbb{Q}$ be an elliptic curve defined by (3.2.2) with all $a_i \in \mathbb{Z}$. Let $P \in E(\mathbb{Q})$ be a point in $E(\mathbb{Q})$ such that $P \not\equiv O \pmod{p}$, for p a prime. Then the following conditions are equivalent:*

(a) *$v_p(\Psi_2(P)) > 0$ and $v_p(\Psi_3(P)) > 0$.*

(b) *For all integers $n \geq 2$, $v_p(\Psi_n(P)) > 0$.*

(c) *There exists an integer $m_0 \geq 2$ such that $v_p(\Psi_{m_0}(P)) > 0$ and $v_p(\Psi_{m_0+1}(P)) > 0$.*

(d) *There exists an integer $n_0 \geq 2$ such that $v_p(\Psi_{n_0}(P)) > 0$ and $v_p(\Phi_{n_0}(P)) > 0$.*

(e) *Reduction of P modulo p is singular.*

Shipsey [32, Sec. 4.4] has shown that for the case $K = \mathbb{Q}$ no cancellation occurs if $P = (0,0)$, $a_6 = 0$, and $\gcd(a_3, a_4) = 1$. See Subsection 4.7.1 for details.

Cheon and Hahn in [10] estimate valuations of division polynomials and compute them explicitly at singular primes. The following result of theirs shows that the common factors of $\Phi_n(P)$ and $\Psi_n^2(P)$ have valuations at p asymptotic to cn^2 for some constant c, when P modulo p is singular, which is complementary to Ayad's result.

Theorem 3.2.5 (Cheon–Hahn [10, Thm. 4]). *Given a nontorsion point in $P \in E(\mathbb{Q}) \backslash E_0(\mathbb{Q})$ with order r in the finite group $E(\mathbb{Q})/E_0(\mathbb{Q})$, set $g_n = \gcd(\Phi_n, \Psi_n^2)$.*

Then for any integer m and k where $1 \leq k < r$, we have

$$v_p(g_n) = \begin{cases} v_p(g_r)m^2 & \text{if } n = mr, \\ v_p(g_r)(2m)^2 \pm 2m\left(2v_p\left(\frac{\Psi_k}{\Psi_{r-k}}\right) + v_p(g_r)\right) + 2v_p(\Psi_k) & \text{if } n = 2mr \pm k. \end{cases} \tag{3.2.4}$$

We now give a Lemma that will be useful when studying any cancellation that occurs between the division polynomials of multiples of points on an elliptic curve. In particular it can be used to give bounds for any cancellation.

Lemma 3.2.6. *Let P be a nontorsion point in $E_0(\mathbb{Q})$. If $v_p(x(P)) < 0$, then*

$$v_p(x([n]P)) = v_p(x(P)) + 2v_p(n)$$

for all $n \in \mathbb{Z}_{>0}$.

Proof. See [10, Lem. 1]. □

Remark 3.2.7. Saying $v_p(x(P)) < 0$ is equivalent to saying $P \equiv O \pmod{p}$.

Chapter 4

Elliptic Divisibility and Denominator Sequences

4.1 Elliptic Divisibility Sequences

Definition 4.1.1. Let K be a field. An *elliptic divisibility sequence* (EDS) over K is a sequence $(W_n)_{n\geq 1}$ defined by four initial terms W_1, W_2, W_3, $W_4 \in K$ and satisfying the quartic nonlinear recurrence

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 \quad \text{for all } m,\, n \in \mathbb{Z}. \tag{4.1.1}$$

An EDS is called *nondegenerate* if $W_1W_2W_3 \neq 0$.

We call $[W_1, W_2, W_3, W_4]$ the *seed* of the sequence (W_n).

The nonlinear recurrence (4.1.1) is better visualised by using the duplication formulas:

$$W_{2n+1}W_1^3 = W_{n+2}W_n^3 - W_{n-1}W_{n+1}^3 \qquad \text{for all } n \geq 2, \tag{4.1.2a}$$

$$W_{2n}W_2W_1^2 = W_{n+2}W_nW_{n-1}^2 - W_nW_{n-2}W_{n+1}^2 \qquad \text{for all } n \geq 3. \tag{4.1.2b}$$

Theorem 4.1.2. *A sequence $(W_n)_{n\geq 1}$ of elements of K with $W_1W_2W_3 \neq 0$ is an EDS if and only if both (4.1.2a) and (4.1.2b) hold.*

Proof. Equation (4.1.2a) follows from (4.1.1) by replacing m by $n+1$, and n by

n. Equation (4.1.2b) follows from (4.1.1) by replacing m by $n+1$, and n by $n-1$ in (4.1.1).

Conversely it is seen by induction on Equations (4.1.2a) and (4.1.2b), that every subsequent positive indexed term is determined by the initial terms W_1, W_2, W_3, W_4. Hence if two EDSs W and W' agree on W_1, W_2, W_3, W_4 they agree on all terms, and so must be equal. For (4.1.1) to follow from (4.1.2a) and (4.1.2b) we must apply an induction on m and n for each equation to show they are equivalent to (4.1.1). □

The next two theorems determine when an EDS arises from given initial values, with the second giving a criteria for an EDS to be integral.

Theorem 4.1.3 (Ward [45]). *Given three rational numbers W_2, W_3, and W_4, then there is an EDS with initial values $W_0 = 0$, $W_1 = 1$, W_2, W_3, and W_4, unless $W_2 = 0$ and $W_4 \neq 0$. Moreover the solution is unique if W_2 and W_3 are not both zero.*

Theorem 4.1.4 (Ward [45]). *Let (W_n) be an EDS with $W_0 = 0$, and the first four terms integers: $W_1 = 1$, W_2, and W_3 not both zero and having $W_2 \mid W_4$. Then (W_n) is an EDS, having all terms integers and the divisibility property of $W_m \mid W_n$ whenever $m \mid n$. Conversely given three integers W_2, W_3, and W_4 with $W_2 \mid W_4$, there exists an EDS (W_n) with initial terms $W_0 = 0$, $W_1 = 1$, W_2, W_3, and W_4.*

We explain what is meant by the uniqueness of an integer EDS satisfying the conditions of Theorem 4.1.4: by setting $n = 2$ in (4.1.1) we obtain

$$W_1^2 W_{m+2} W_{m-2} = W_{m+1} W_{m-1} W_2^2 - W_3 W_1 W_m^2. \tag{4.1.3}$$

Hence from given terms W_0, W_1, W_2, W_3, and W_4, we calculate W_5 by setting $m = 3$ in (4.1.3) to get

$$W_5 = \frac{W_4 W_2^3 - W_1 W_3^3}{W_1^3} \tag{4.1.4}$$

which since $W_1 = 1$ has W_5 an integer. In similar fashion we construct the entire sequence. Therefore any integer EDS is uniquely defined by its first five terms.

The solutions to the recurrence in (4.1.1) satisfy a more general recursion relation given by

Theorem 4.1.5.

$$W_{m+n}W_{m-n}W_t^2 = W_{m+t}W_{m-t}W_n^2 - W_{n+t}W_{n-t}W_m^2 \quad \textit{for all } m,\ n,\ t \in \mathbb{Z}. \tag{4.1.5}$$

Proof. Using recurrence (4.1.1), we work out expressions for $W_{m+t}W_{m-t}W_n^2W_1^2$ and $W_{n+t}W_{n-t}W_m^2W_1^2$.

$$W_{m+t}W_{m-t}W_n^2W_1^2 = W_n^2\Big(W_{m+1}W_{m-1}W_t^2 - W_{t+1}W_{t-1}W_m^2\Big) \tag{4.1.6}$$

for all m,$t \in \mathbb{Z}$.

$$W_{n+t}W_{n-t}W_m^2W_1^2 = W_m^2\Big(W_{n+1}W_{n-1}W_t^2 - W_{t+1}W_{t-1}W_n^2\Big) \tag{4.1.7}$$

for all n,$t \in \mathbb{Z}$. Now subtract (4.1.6) from (4.1.7) to give

$$\begin{aligned} W_1^2\Big(W_{m+t}W_{m-t}W_n^2 - W_{n+t}W_{n-t}W_m^2\Big) &= W_t^2\Big(W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2\Big) \\ &= W_{m+n}W_{m-n}W_t^2W_1^2 \qquad \text{for all } m,\ n,\ t \in \mathbb{Z}, \end{aligned}$$

where we have used (4.1.1) for the term in parentheses. □

Lemma 4.1.6 (Ward [45, Lem. 4.1])**.** *Let (W_n) be an EDS with $W_1 = 1$, $W_2W_3 \neq 0$; if two consecutive terms are zero in (W_n), then $W_n = 0$ for all $n \geq 4$.*

Theorem 4.1.7. *Let (W_n) be a nondegenerate EDS. Then, if $W_m \neq 0$, $(W_{mn}/W_m)_{n\geq 1}$ is an EDS. In particular (W_n/W_1) is an EDS.*

Definition 4.1.8. By Theorem 4.1.7 if (W_n) is an EDS then so is (W_n/W_1). We shall term (W_n/W_1) a *normalised* EDS.

The next Theorem shows the antisymmetric property of EDSs.

Theorem 4.1.9. *Nondegenerate, normalised elliptic divisibility sequences (W_n) have $W_0 = 0$, $W_1 = 1$, and $W_{-n} = -W_n$ for all $n \in \mathbb{Z}$.*

Proof. Set $m = n = 0$ in (4.1.1) to see that $W_0 = 0$. Normalised by definition has $W_1 = 1$. Now setting $n = 0$ in (4.1.1) gives $W_m^2W_1^2 = -W_1W_{-1}W_m^2$ for all $m \in \mathbb{Z}$, and so (unless all terms $W_m = 0$) $W_{-1} = -W_1$. Finally setting $m = 0$

in (4.1.1) gives $W_nW_{-n}W_1^2 = W_1W_{-1}W_n^2 = -W_n^2W_1^2$ for all $n \in \mathbb{Z}$, from which $W_n = -W_{-n}$. □

Example 4.1.10. (a) The sequence of integers $\mathbb{Z}$ is an EDS.
(b) The sequence

$$\left(\frac{n}{3}\right) = \begin{cases} 0 & \text{if } 3 \mid n, \\ 1 & \text{if } n \equiv 1 \pmod 3, \\ -1 & \text{if } n \equiv -1 \pmod 3. \end{cases}$$

is an EDS, where $(\frac{\cdot}{p})$ is the Legendre symbol. (This example is due to Ward [45].) Its first few terms are

$$1, -1, 0, 1, -1, 0, 1, -1, 0, 1, -1, 0, \ldots$$

(c) The sequence starting $W_1 = 1$, $W_2 = 3$, $W_3 = -112$, $W_4 = -49$,

$$1, 3, -112, -49, 1403605, -\tfrac{1414564928}{3}, -1971963612493,$$
$$\tfrac{1738288005631793}{9}, \tfrac{92912484855445437627 2}{3}, \tfrac{3145039597589171641266324 55}{27}, \ldots$$

is an noninteger EDS, even though its seed is made up of integers, because $W_2 \nmid W_4$.
(d) The sequence starting $W_1 = 1$, $W_2 = 10$, $W_3 = 171$, $W_4 = -7660$,

$$1, 10, 171, -7660, -12660211, -22652313570, -58809175344521,$$
$$1735132266687114280, 3571727821871440552622 01,$$
$$1154553432516829071988561920 50, \ldots$$

is an integer EDS, since the seed is made up of integers with $W_2 \mid W_4$.

We will come across Example 4.1.10 (d) again in Chapter 6, when we find its terms are intimately linked with the denominators of multiples of the point $(3, 5)$ on the elliptic curve $y^2 = x^3 - 2$.

Definition 4.1.11. Given two EDSs (W_n) and (W'_n), if there exists a rational contant $\theta \in K^*$ such that the sequence (W'_n) is defined by

$$W'_n = \theta^{n^2-1} W_n \quad \text{for all } n \in \mathbb{Z}, \tag{4.1.8}$$

then (W_n) and (W'_n) are said to be *equivalent* EDSs.

Theorem 4.1.12. *Let (W_n) be an EDS, and let $\theta \in K^*$. Then $(\theta^{n^2-1}W_n)$ is also an EDS.*

Proof. Let $V_n = \theta^{n^2-1}W_n$, then

$$\begin{aligned} V_{m+n}V_{m-n}V_1^2 &= \theta^{(m+n)^2-1}W_{m+n}\theta^{(m-n)^2-1}W_{m-n}W_1^2 \\ &= \theta^{2(m^2+n^2-1)}\left(W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2\right) \\ &= \theta^{(m+1)^2-1}W_{m+1}\theta^{(m-1)^2-1}W_{m-1}\theta^{2(n^2-1)}W_n^2 \\ &\quad - \theta^{(n+1)^2-1}W_{n+1}\theta^{(n-1)^2-1}W_{n-1}\theta^{2(m^2-1)}W_m^2 \\ &= V_{m+1}V_{m-1}V_n^2 - V_{n+1}V_{n-1}V_m^2 \end{aligned}$$

and so (V_n) is an equivalent EDS to (W_n) as required. □

4.2 Normalised EDSs and Elliptic Curves

The next Theorem due to Ward shows how EDSs arise from the values of division polynomials of an elliptic curve. We will write $\Psi_n(P)$ for Ψ_n evaluated at the point $P = (x_1, y_1)$.

Theorem 4.2.1 (Ward [45, Thm. 12.1])**.** *Let E/K be an elliptic curve given by*

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.2.1}$$

and let $P \in E(K)$ be a nonzero point. Then the sequence (W_n) defined by

$$W_n = \Psi_n(P) \qquad \text{for all } n \geq 1, \tag{4.2.2}$$

where Ψ_n is the n^{th} division polynomial for E, is a normalised EDS.

Proof. See Ward [45, Thm. 12.1]. □

We also have that given an integer EDS starting $W_1 = 1$, $W_2W_3 \neq 0$ and $W_2 \mid W_4$, then there exists an elliptic curve $E \cong \mathbb{C}/\Lambda$ (for some lattice Λ) and a

complex constant $z \in \Lambda$ such that

$$W_n = \Psi_n(z;\Lambda) = \frac{\sigma(nz;\Lambda)}{\sigma(z;\Lambda)^{n^2}},$$

where $\sigma(z;\Lambda)$ is the Weierstrass function associated to Λ.

Moreover, the modular invariants $g_2(\Lambda)$ and $g_3(\Lambda)$ associated to the lattice Λ, and the Weierstrass functions $\wp(z,\Lambda)$ and $\wp'(z,\Lambda)$ evaluated at the point z on the elliptic curve $\mathbb{C}/\Lambda$ are all in the field $\mathbb{Q}(W_2, W_3, W_4)$. This shows that $g_2(\Lambda)$, $g_3(\Lambda)$, $\wp(z,\Lambda)$, and $\wp'(z,\Lambda)$ are all defined over the same field as the terms of the sequence (W_n). The rational expressions for $g_2(\Lambda)$, $g_3(\Lambda)$, $\wp(z,\Lambda)$, $\wp'(z,\Lambda)$ in $\mathbb{Q}(W_2, W_3, W_4)$ may be found in [45, Eqn. 13.6, 13.7, 13.5, 13.1] respectively.

Now when an EDS W is associated to a specific curve-point pair (E, P) we shall write $W = W_{E,P}$ for clarity.

4.3 Curves from Nets of Rank 1

We have already seen in Proposition 2.3.9 how the Weierstrass equation for an elliptic curve E is unique up to an admissable change of variables as given in (2.3.19). A *unihomothetic* change of variables is of the form

$$x' = x + r, \quad y' = y + sx + t, \tag{4.3.1}$$

with r, s, $t \in \bar{K}$ and $u = 1$ in (2.3.19).

We can now give explicit formulæ to describe an elliptic curve arising from an EDS of rank 1. These were originally due to Ward [45, Thm. 12.1], but we give Swart's more succinct version here.

Theorem 4.3.1 (Swart [39, Thm. 4.5.3])**.** *Let $(W_n)_{n\geq 1}$ be a normalised nondegenerate EDS. Then there exists an elliptic curve with Weierstrass equation*

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

such that $W = W_{E,P}$ with point $P = (0,0)$. It is unique up to a unihomothetic

change of coordinates (4.3.1)*, with the* a_i *being given by*

$$a_1 = \frac{W_4 + W_2^5 - 2a_4W_2W_3}{W_2^2W_3},$$
$$a_2 = \frac{W_2W_3^2 + a_4(W_4 + W_2^5) - a_4^2W_2W_3}{W_2^3W_3},$$
$$a_3 = W_2, \qquad a_4 = 1, \qquad a_6 = 0.$$

Proof. We have the division polynomials Ψ_1, Ψ_2, Ψ_3, and Ψ_4 are invariant under the unihomethetic change of variables (4.3.1). Then a calculation checks $W_{E,P}$ agrees with W at the first four terms and so $W_{E,P} = W$. Conversely suppose $W = W_{E',P'}$. After applying a unihomethetic transformation (4.3.1) taking P' to $(0,0)$, and a_4 to 1, substitution of the division polynomials into the equations above verifies that $a_i' = a_i$ for all i. □

Example 4.3.2. The simplest, unbounded, nonsingular EDS is given by the seed $[1, 1, -1, 1]$. Its first few terms are

$$1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -23, 29, 59, 129, \ldots$$

It is associated to the point $P = (0, 0)$ on elliptic curve $E\colon y^2 + y = x^3 - x$. It is the 'simplest' EDS due to the fact that E has the smallest conductor, $N = 37$, for elliptic curves over $\mathbb{Q}$ of positive rank.

4.4 Integrality

If $E/\mathbb{Q}$ has defining Weierstrass equation with integer coefficients, and $P = (x_1, y_1)$ is an integer point on E, then the ring $R = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ is then just $\mathbb{Z}$, and $\Psi_n(x_1, y_1) \in \mathbb{Z}$ for all n.

Theorem 4.4.1. *Let* R *be an integral domain with field of fractions* K*. Let* W_1*,* W_2*,* W_3*, and* W_4 *in* R *be such that* W_1 *divides each of* W_2*,* W_3*, and* W_4*, and such that* $W_2 \mid W_4$*. Then there is a unique EDS* $(W_n)_{n\geq 1}$ *in* K *with* $W_i \in R$ *for all* i *having seed* $[W_1, W_2, W_3, W_4]$*. Moreover;*

(a) (W_n) *is a* divisibility sequence*, in the sense that*

$$m \mid n \Longrightarrow W_m \mid W_n.$$

(b) *If R is a principal ideal domain and* $\gcd(W_3, W_4) = 1$*, then (W_n) satisfies the stronger divisibility relation*

$$\gcd(W_m, W_n) = W_{\gcd(m,n)} \qquad \textit{for all } m,\ n \geq 1.$$

Proof. We know there is a unique EDS in K with this seed. That $W_i \in R$ for all i is proved by induction, by in fact proving $W_2 \mid W_{2k}$ and $W_1 \mid W_k$ simultaneously.

For (a) we proceed by induction. Assume that

$$W_s \mid W_t \quad \text{whenever} \quad s \mid t \quad \text{for} \quad s \leq t < n.$$

This is true for $n \leq 5$. Hence take $n > 5$, and let $n = uv$. Thus we need to show $W_u \mid W_{uv}$, where we can take $u \geq 2$, $v \geq 2$. If $v = 2k$ then $n = 2uk$ and (4.1.2b) gives

$$W_{2uk} W_2 W_1^2 = W_{uk}\Big(W_{uk+2} W_{uk-1}^2 - W_{uk-2} W_{uk+1}^2\Big)$$

Then W_2 divides the term in the parenthesis. Also by hypothesis $W_u \mid W_{uk}$ as $u < uk < n$, so we have $W_u W_2 W_1^2 \mid W_{2uk} W_2 W_1^2$ from which $W_u \mid W_{uv}$.

If v is odd then u and uv are of the same parity. Setting $m + n = uv$ and $m - n = u$ in (4.1.1), where $m = \frac{1}{2}u(v+1)$, $n = \frac{1}{2}u(v-1)$

$$W_{uv} W_u W_1^2 = W_{\frac{u(v+1)}{2}+1} W_{\frac{u(v+1)}{2}-1} W_{\frac{u(v-1)}{2}}^2 - W_{\frac{u(v-1)}{2}+1} W_{\frac{u(v-1)}{2}-1} W_{\frac{u(v+1)}{2}}^2 .$$

By hypothesis $W_u^2 \mid W_{u(v+1)/2}^2$ and $W_u^2 \mid W_{u(v-1)/2}^2$. Hence $W_u^2 W_1^2$ divides the RHS, and so $W_u^2 W_1^2 \mid W_{uv} W_u W_1^2$ from which $W_u \mid W_{uv}$ as required.

For (b) we need the following result:

Theorem 4.4.2. *Suppose R is a PID, (W_n) is an EDS in R and p in R is a prime divisor of W_n. Then*

$$v_p(W_{mn}) = v_p(W_n) + v_p(m), \tag{4.4.1}$$

where $v_p(a)$ is the maximal integer t such that p^t divides a, for a in R nonzero.

Proof. See [10, Lem. 1]. □

Proof of (b) Let $d = \gcd(m, n)$, and write $m = ad$, $n = bd$ for some a, $b \in \mathbb{Z}$. By (4.4.1), for any prime $p \mid W_d$ we have

$$v_p(W_{da}) = v_p(W_d) + v_p(a) \quad \text{and} \quad v_p(W_{db}) = v_p(W_d) + v_p(b).$$

Since $\gcd(a, b) = 1$, at least one of $v_p(a)$ or $v_p(b)$ is zero. Hence

$$\begin{aligned} v_p(\gcd(W_m, W_n)) &= \min\{v_p(W_{da}), v_p(W_{db})\} \\ &= \min\{v_p(W_d) + v_p(a), v_p(W_d) + v_p(b)\} \\ &= v_p(W_d) \\ &= v_p(W_{\gcd(m,n)}). \end{aligned}$$

Therefore if $p \mid W_d$ then $p \mid \gcd(W_m, W_n)$ to the same order. On the other hand, if a prime p divides both W_m and W_n then reducing modulo p the m^{th} and n^{th} multiple of the point P, writing $W = W_{E,P}$ for some point P on the elliptic curve E, gives $[m]P \equiv [n]P \equiv O \pmod{p}$. But $d = \gcd(m, n)$, therefore $[d]P \equiv O \pmod{p}$ and so $p \mid W_d$. □

Remark 4.4.3. We have defined an EDS (W_n) given by $[W_1, W_2, W_3, W_4]$, to be a sequence of terms in a field K which satisfy (4.1.1). Ward [45] defined things slightly differently. Firstly Ward confined himself to the rationals $\mathbb{Q}$, and the finite fields $\mathbb{F}_p$. If a sequence obeyed (4.1.1) but contained any nonintegral terms it was termed an *elliptic sequence*. The only sequences of any arithmetical interest to him were termed *proper sequences*, these being solutions to (4.1.1) with the following conditions: $W_0 = 0$, $W_1 = 1$, $W_2 W_3 \neq 0$. For Ward an EDS was defined as follows: Let (W_n) be a proper solution of (4.1.1). Then (W_n) is an *elliptic divisibility sequence* if and only if W_2, W_3, W_4 are integers and $W_2 \mid W_4$. Moreover he proves that (W_n) is then uniquely determined by W_2, W_3, and W_4.

So for Ward, and various authors after, the term EDS is reserved for proper integral sequences with seed $[1, W_2, W_3, cW_2]$ with $c \in \mathbb{Z}$. We do not make this

distinction, and for us Ward's elliptic sequences are now EDSs.

Corollary 4.4.4 (Swart [39, Corollary 4.5.4])**.** *The EDS* (W_n) *having associated elliptic curve* E *is an integer valued EDS if and only if* E *has integer values of* a_3*,* b_8*, and* b_4b_8*.*

Proof. (W_n) is an integer EDS if and only if W_2, W_3, and $\frac{W_4}{W_2}$ are integers. Since

$$W_2 = a_3, \quad W_3 = b_8, \quad \text{and} \quad \tfrac{W_4}{W_2} = (b_4b_8 - a_3^4),$$

we thus require a_3, b_8, and b_4b_8 to be integers. □

4.5 Periodicity of EDSs

This Chapter shall look at the periodicity of integer EDSs modulo primes. Ward showed every prime occurs as a *primitive divisor* at some point in an integer EDS (a prime p is a *primitive divisor* of W_n if $p \mid W_n$ and $p \nmid W_1W_2 \cdots W_{n-1}$).

4.5.1 Rank of Apparition

Definition 4.5.1. Let m be an integer. The *rank of apparition* (or *rank*) $r(m)$ of m in an integer EDS (W_n) is the smallest integer $r(m)$ such that $W_{r(m)} \equiv 0 \pmod{m}$.

When no confusion can arise we shall sometimes drop the parenthetic m and refer to the rank of m simply as r.

The idea of the rank of an integer results in periodic behaviour which is of use in studying properties of EDSs. The next result illustrates a degenerate condition whereby an EDS does not have a rank.

Theorem 4.5.2 (Ward [45, Thm. 6.2])**.** *Let* (W_n) *be an integer EDS. A necessary and sufficient condition that a prime* p *has a rank of apparition* $r(p)$elliptic divisibility sequence!rank of apparition *is that* $p \nmid \gcd(W_3, W_4)$*.*

The next result shows the periodic behaviour of the rank.

Theorem 4.5.3 (Ward [45, Thm. 5.2]). *Let (W_n) be an integer EDS and let $r(p)$ be its rank of apparition for prime p. Then*

$$W_n \equiv 0 \pmod{p} \quad \text{if and only if} \quad n \equiv 0 \pmod{r(p)}.$$

Using the Hasse bound from Theorem 2.11.3 on the number of points on an elliptic curve over a finite field the next Theorem was independently proved by Ayad and then Shipsey.

Theorem 4.5.4 (Ayad [3], Shipsey [32]). *An integer EDS admits every prime p as a divisor, with the rank $r(p)$ obeying the following bound*

$$r(p) \leq p + 1 + 2\sqrt{p}.$$

This means any integer EDS has 2 appearing as a factor by at least the fifth term, 3 appearing as a factor by at least the seventh term, 5 appearing as a factor by at least the tenth term, and so on. The periodicity inherent in EDSs is a consequence of the periodicity of the Weierstrass σ-function.

Let us now consider the rank of primes p raised to integer powers $s \geq 1$ and label these ranks as $r(p^s)$.

Theorem 4.5.5 (Swart [39, Thm. 4.7.5]). *Let p be a prime with $r(p) \geq 4$ in an nondegenerate integer EDS (W_n). Let $p^w \parallel W_r$.*

If p is odd, or $p = 2$ and $w \geq 2$, then for $s \in \mathbb{Z}_{\geq 1}$, p^s has rank given by

$$r(p^s) = \begin{cases} r(p) & \text{if } s \leq w, \\ pr(p^{s-1}) & \text{if } s > w. \end{cases}$$

If $p = 2$ and $w = 1$ then for some $v \geq 2$,

$$r(p^s) = \begin{cases} r(p) & \text{if } s = 1, \\ 2r(p) & \text{if } 2 \leq s \leq v, \\ 2r(p^{s-1}) & \text{if } s > v. \end{cases}$$

For odd p and $s \geq k \geq w$, this means $r(p^s) = p^{s-k} r(p^k)$.

4.5.2 Periodicity

We now investigate the periodic properties of integer EDSs modulo primes p. Ward showed that an integer EDS (W_n) with rank of apparition $r(p) \geq 4$ is periodic with period $\pi_p(W_n) = r\tau$, where τ is an arithmetical function of p and (W_n) which can be calculated (see Corollary 4.5.7), with $\tau \mid p-1$.

4.5.3 Ward's Partial Periodicity

We have just encountered the rank of apparition of an integer EDS (W_n). Now with this rank of apparition, $r(p)$, we may propose the idea that $W_{r(p)+k} \equiv W_k \pmod{p}$, but this would be wrong. In fact the right expression is $W_{r(p)\tau+k} \equiv W_k \pmod{p}$, where τ is an arithmetical function discovered by Ward to work out the correct period of an EDS which turns out to be $r\tau$, (see Corollary 4.5.7). Ward did however find a fascinating symmetry formula describing the general case, which gave the exact congruence relating $W_{lr(p)+k}$ and W_k, which he termed the 'partial periodicity' pattern with respect to the rank.

Theorem 4.5.6 (Ward [45, Thm. 9.2]). *Let (W_n) be an integer EDS and let $p > 3$ be a prime, with rank of apparition $r(p) > 3$. Then there exist integers a, b that satisfy the periodicity congruence*

$$W_{lr+k} \equiv a^{lk} b^{l^2} W_k \pmod{p} \quad \text{for all } l,\ k \in \mathbb{Z}_{\geq 0}. \tag{4.5.1}$$

Moreover the integers a and b may be explicitly computed via the congruences

$$a \equiv \frac{W_{r-2}}{W_2 W_{r-1}} \pmod{p}, \quad b \equiv \frac{W_2 W_{r-1}^2}{W_{r-2}} \pmod{p}. \tag{4.5.2}$$

The following Corollary gives a method for computing τ and thus makes explicit the relation between the rank of apparition, if greater than 3, of an odd prime and the period of the sequence.

Corollary 4.5.7 (Ward [45, Thm. 11.1]). *Let (W_n) be an integer EDS and p an odd prime with rank of apparition $r(p)$ greater than 3. Let ε and κ be the orders of W_2/W_{r-2} and W_{r-1} respectively modulo p. Then (W_n) is periodic modulo p with*

period $\pi_p(W_n) = r\tau$ *where*

$$\tau = 2^\alpha \operatorname{lcm}(\varepsilon, \kappa), \tag{4.5.3}$$

and

$$\alpha = \begin{cases} 1 & \text{if } \varepsilon \text{ and } \kappa \text{ are both odd,} \\ -1 & \text{if } \varepsilon \text{ and } \kappa \text{ are both even and divisible by the same power of } 2, \\ 0 & \text{otherwise.} \end{cases} \tag{4.5.4}$$

In his derivation of Corollary 4.5.7, Ward uses the invariants g_2 and g_3 of the elliptic function representation of the EDS. To this end he derives polynomials for g_2 and g_3 in terms of W_2, W_3, and W_4 with integral coefficients divided by powers of 2, 3, W_2, and W_3 (see [45, Eq. 13.6, 13.7]). Hence, with respect to Corollary 4.5.7, the rank has to be greater than 3, and the primes 2 and 3 have to be considered separately.

Ward checks all the eight *a priori* sequences modulo 2, distinguishing between them by the posible residues of W_2, W_3, W_4 modulo 2, and finds only six are possible. He finds two of these sequences have $r > 3$ and $\tau = 1$. However on using (4.5.3) we arrive at an erroneous value of $\tau = 2$. Hence the restriction to odd primes is necessary.

Ward then checks the twenty-one possible sequences modulo 3 and explicitly works out by hand the values of the rank and period by using the duplication formulas (4.1.2a) and (4.1.2b) modulo 3; in the twelve cases where the rank is greater than 3, Ward also lists ε, κ, and τ. His table in [45, Ch. III] shows Corollary 4.5.7 to be true for $p = 3$.

The next result of Ward's completely characterises integer EDSs modulo primes with ranks of apparition 2 or 3.

Theorem 4.5.8 (Ward [45, Thm. 7.1])**.** *If a prime p has rank of apparition 2 in an integer EDS (W_n), and $p \nmid \gcd(W_3, W_4)$ then*

$$W_n \equiv \begin{cases} 0 \pmod{p} & \text{if } n = 2k, \\ (-1)^{\frac{1}{2}k(k-1)} W_3^{\frac{1}{2}k(k+1)} \pmod{p} & \text{if } n = 2k+1. \end{cases}$$

If a prime p has rank of apparition 3 in an integer EDS (W_n), and $p \nmid \gcd(W_3, W_4)$ then

$$W_n \equiv \begin{cases} 0 \pmod{p} & \text{if } n = 3k, \\ (-W_2)^{\frac{1}{2}k(k-1)} W_4^{\frac{1}{2}k(k+1)} \pmod{p} & \text{if } n = 3k+1, \\ -(-W_2)^{\frac{1}{2}k(k+1)(k+2)} W_4^{\frac{1}{2}k(k+1)} \pmod{p} & \text{if } n = 3k+2. \end{cases}$$

Corollary 4.5.9. *Let $E/\mathbb{Q}$ be an elliptic curve and $P \in E(\mathbb{Q})$ be a nonzero point. The period of $(\Psi_n(P), \Phi_n(P), \Omega_n(P))$ modulo a prime p is $r\tau$.*

Proof. By Theorem 4.2.1 we have the fact that the division polynomials for an elliptic curve $E/\mathbb{Q}$ evaluated at a nonzero point $P \in E(\mathbb{Q})$ form a normalised EDS (W_n) defined by $W_n = \Psi_n(P)$ for $n \geq 1$. Since the period of the sequence (W_n) is $r\tau$, so is the period for $(\Psi_n(P))$. Now by Theorem 3.1.11 we recall the formulas $\Phi_n = x\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}$, and $\Omega_n = (4y)^{-1}(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)$, and so $\Phi_n(P) = x(P)W_n^2 - W_{n-1}W_{n+1}$, and $\Omega_n(P) = (4y(P))^{-1}(W_{n+2}W_{n-1}^2 - W_{n-2}W_{n+1}^2)$. Hence $\Phi_n(P)$, and $\Omega_n(P)$ are also periodic with period $r\tau$. □

Example 4.5.10. Take the the rank 1 elliptic curve $E_{357\text{d}1}\colon y^2 + y = x^3 + x^2 - 42x + 110$ with generator point $P = (0, 10)$, where 357d1 is its Cremona reference. It has an associated EDS $(W(357\text{d}1)_n) = [1, 21, -1323, -1750329]$.

Over $\mathbb{F}_2$ the sequence has $r(2) = 5$, with period $\pi_2(W(357\text{d}1)_n) = 5$:

$$(W(357\text{d}1)_n) \equiv [1, 1, 1, 1, 0] \pmod{2}.$$

Over $\mathbb{F}_3$ the sequence has $r(3) = 2$ since $W_2 = 21 = 3 \cdot 7$. Therefore we cannot use Corollary 4.5.7 to work out τ since the rank has to be greater than 3. Also since 3 divides $W_3 = -3^3 7^2$ as well as W_2, when looking modulo 3 these two consecutive terms are zero, and so by Lemma 4.1.6 this means the sequence modulo 7 looks like

$$(W(357\text{d}1)_n) \equiv [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, \dots] \pmod{3}$$

with every term bar W_1 equal to zero.

Over $\mathbb{F}_5$ the sequence has $r(5) = 9$, with period $\pi_5(W(357\text{d}1)_n) = 18$:

$$(W(357\text{d}1)_n) \equiv [1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0] \pmod{5}.$$

Over $\mathbb{F}_7$ the sequence has $r(7) = 2$, since $W_2 = 21 = 3 \cdot 7$. Therefore by the exact reasoning for $p = 3$ above we have the sequence over $\mathbb{F}_7$ look like

$$(W(357\text{d}1)_n) \equiv [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, \dots] \pmod 7$$

with every term bar W_1 equal to zero.

Over $\mathbb{F}_{11}$ the sequence has $r(11) = 15$, with period $\pi_{11}(W(357\text{d}1)_n) = 150$:

$$(W(357\text{d}1)_n) \equiv [1, 10, 8, 2, 3, 8, 4, 3, 2, 3, 8, 7, 2, 3, 0, 7, 5, 5, 5, 8, 1, 2, 6, 5, 8, 1, 9,$$
$$4, 2, 0, 5, 8, 10, 7, 3, 7, 1, 1, 7, 3, 7, 10, 8, 5, 0, 2, 4, 9, 1, 8, 5, 6, 2, 1, 8, 5, 5, 5, 7, 0, 3,$$
$$2, 7, 8, 3, 2, 3, 4, 8, 3, 2, 8, 10, 1, 0, 10, 1, 3, 9, 8, 3, 7, 8, 9, 8, 3, 4, 9, 8, 0, 4, 6, 6, 6, 3,$$
$$10, 9, 5, 6, 3, 10, 2, 7, 9, 0, 6, 3, 1, 4, 8, 4, 10, 10, 4, 8, 4, 1, 3, 6, 0, 9, 7, 2, 10, 3, 6, 5,$$
$$9, 10, 3, 6, 6, 6, 4, 0, 8, 9, 4, 3, 8, 9, 8, 7, 3, 8, 9, 3, 1, 10, 0] \pmod{11}.$$

Over $\mathbb{F}_{13}$ the sequence has $r(13) = 13$, with period $\pi_{13}(W(357\text{d}1)_n) = 26$:

$$(W(357\text{d}1)_n) \equiv$$
$$[1, 8, 3, 4, 6, 8, 1, 9, 7, 11, 1, 8, 0, 5, 12, 2, 6, 4, 12, 5, 7, 9, 10, 5, 12, 0] \pmod{13}.$$

4.6 The Sign of an EDS

Definition 4.6.1. If (W_n) is an integer EDS, then so is $((-1)^{n-1}W_n)$, termed the *inverse* of the EDS (W_n).

Theorem 4.6.2 (Silverman & Stephens [36, Thm. 1])**.** *Let (W_n) be an integer EDS. Then after replacing (W_n) by $((-1)^{n-1}W_n)$ if necessary, there exists an irrational number $\beta \in \mathbb{R}$ such that*

$$\operatorname{sign}(W_n) = (-1)^{\lfloor n\beta \rfloor} \text{ for all } n. \tag{4.6.1}$$

$$\operatorname{sign}(W_n) = \begin{cases} (-1)^{\lfloor n\beta \rfloor + \frac{n}{2}} & \text{if } n \text{ is even,} \\ (-1)^{\frac{n-1}{2}} & \text{if } n \text{ is odd.} \end{cases} \tag{4.6.2}$$

(Here $\lfloor t \rfloor$ denotes the greatest integer less than or equal to t.)

4.7 Denominator Divisibility Sequences

Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass model

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.7.1}$$

Let $P \in E(\mathbb{Q})$ be a point on the elliptic curve that is not the identity, then P can be expressed as

$$P = (x(P), y(P)) = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3}\right) \tag{4.7.2}$$

with A_P, B_P, $C_P \in \mathbb{Z}$, $\gcd(A_P, B_P) = \gcd(C_P, B_P) = 1$, and $B_P \geq 1$. (Note that by the extended Euclidean algorithm if a, b, $c \in \mathbb{Z}$ with $\gcd(a, b) = \gcd(c, b) = 1$, there exist integers s, t, u, $v \in \mathbb{Z}$ such that $as + bt = cu + bv = 1$. Hence

$$\begin{aligned} 1 &= (as + bt)(cu + bv) = ac(su) + b(ctu + btv + asv) \\ &= acU + bV \end{aligned}$$

where $U = su$ and $V = ctu + btv + asv$. Hence the conditions $\gcd(A_P, B_P) = \gcd(C_P, B_P) = 1$ are equivalent to the more concise $\gcd(A_PC_P, B_P) = 1$.)

Definition 4.7.1. Taking the multiples of a nontorsion point $P \in E(\mathbb{Q})$, where E is given by (4.7.1) and P is given by (4.7.2). The n^{th} multiple of P is given by

$$[n]P = \left(\frac{A_{nP}}{B_{nP}^2}, \frac{C_{nP}}{B_{nP}^3}\right) \tag{4.7.3}$$

with A_{nP}, B_{nP}, $C_{nP} \in \mathbb{Z}$, $\gcd(A_{nP}, B_{nP}) = \gcd(C_{nP}, B_{nP}) = 1$, and $B_{nP} \geq 1$. The denominators of these points form a *divisibility sequence* (B_{nP}). We shall term this a *denominator divisibility sequence* (DDS).

This thesis will be interested in the sequences (B_{nP}) that the elliptic denominators of multiples of points on elliptic curves make.

For brevity we shall tend to drop the subscript P from the definition given in (4.7.3) and write our DDSs as just (B_n). As well, in a lot of cases, the (B_{nP}) form an integer EDS if each member of the sequence is given the correct sign in accordance with that occuring in the recurrence (4.1.1).

Therefore geometric construction via rational points on elliptic curves yields a divisibility sequence (B_{nP}) of positive integers, whereas algebraic construction via recursion (4.1.1) yields an elliptic divisibility sequence (W_n) of signed rationals.

We have seen that the n^{th} multiple of a point can be described in terms of the so called division polynomials

$$[n]P = \left(\frac{\Phi_n(x,y)}{\Psi_n^2(x,y)}, \frac{\Omega_n(x,y)}{\Psi_n^3(x,y)}\right) \quad \text{if } [n]P \neq O. \tag{4.7.4}$$

Recall that Ayad in Theorem 3.2.4 has shown that any cancellation occurring between the numerator and the denominator of (4.7.4) happens exactly at the primes of singular reduction at P.

To investigate the relationship between the B_{nP} and the $\Psi_n(P)$, we find on comparing equations (4.7.3) and (4.7.4) that

$$v_p(x([n]P)) = v_p(A_{nP}) - 2v_p(B_{nP}) = v_p(\Phi_n(P)) - 2v_p(\Psi_n(P)). \tag{4.7.5}$$

Now if $p \nmid B_P$ then $v_p(\Phi_n(P))$, and $v_p(\Psi_n(P)) \geq 0$. By Ayad's Theorem 3.2.4 we see that if P reduces to a nonsingular point, and if $P \not\equiv O \pmod{p}$, which is equivalent to $p \nmid B_P$, then $v_p(\Phi_n(P))v_p(\Psi_n(P)) = 0$. In which case by (4.7.5) if $v_p(x([n]P)) \geq 0$, then since $\gcd(A_{nP}, B_{nP}) = 1$, we have $v_p(B_{nP}) = v_p(\Psi_n(P)) = 0$. Similarly if $v_p(x([n]P)) < 0$, then we have $v_p(B_{nP}) = v_p(\Psi_n(P)) = -\frac{1}{2}v_p(x([n]P))$. This implies the following proposition.

Proposition 4.7.2. *Let $E/\mathbb{Q}$ be an elliptic curve such that all $a_i \in \mathbb{Z}$. Let $P \in E(\mathbb{Q})$ be a nontorsion point such that $P \not\equiv O \pmod{p}$ for some prime p, and let (B_{nP}) be the DDS associated to E and P. Then if P modulo p is nonsingular, we have*

$$v_p(B_{nP}) = v_p(\Psi_n(P)).$$

Note that, in general, we do not have $B_{nP} = |\Psi_n(x,y)|$ since the rational number A_n/B_n^2 has A_n and B_n coprime, but we cannot be sure

$$\gcd(\Phi_n(P), \Psi_n^2(P)) = 1$$

as there may be some bounded cancellation when evaluated at a point P. If

we drop the condition that $P \not\equiv O \pmod{p}$ from Proposition 4.7.2 we have the stronger result for a scaled version of $\Psi_n(P)$

$$\widehat{\Psi}_n(P) = B_P^{n^2}\Psi_n(P).$$

Then if P modulo p is nonsingular for all primes p we have

$$B_{nP} = |\widehat{\Psi}_n(P)|.$$

Referring to (4.7.4) we find the scaled versions for $\Phi_n(P)$, and $\Omega_n(P)$ to be

$$\widehat{\Phi}_n(P) = B_P^{2n^2}\Phi_n(P), \quad \widehat{\Omega}_n(P) = B_P^{3n^2}\Omega_n(P).$$

Then if P modulo p is nonsingular for all primes p we have

$$A_{nP} = \widehat{\Phi}_n(P), \quad C_{nP} = \widehat{\Omega}_n(P).$$

(See [2]).

Ingram [23] has given a quantitative bound showing the extent of the cancellation of this fraction. For the Lemma we shall fix some notation: Let $r(P,p)$ be the order of P in the finite group $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$. Now set

$$M(P) = \operatorname{lcm} r(P,p),$$

as p varies over all primes.

Lemma 4.7.3 (Ingram [23, Lem. 3])**.** *Let $E/\mathbb{Q}$ be an elliptic curve, let $P \in E(\mathbb{Q})$ be a nontorsion point, and have B_n, Ψ_n, and M be as defined above. Then for $n \geq 1$,*

$$\log B_n \leq \log|\Psi_n| \leq \log B_n + n^2 M^2 \log|\Delta(E)|.$$

4.7.1 The Singular Situation

We now explain why a DDS is not necessarily an integer EDS by merely adding in the right signs. The following example illustrates the singular example given by Shipsey in [32], and how this fails to give us an integer EDS.

After moving $P \to (0,0)$ we have a Weierstrass equation of the form

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x. \tag{4.7.6}$$

Let

$$f(x,y) = x^3 + a_2x^2 + a_4x - y^2 - a_1xy - a_3y$$

with partial derivatives $\frac{\partial f}{\partial x} = 3x^2 + 2a_2x - a_1y + a_4$ and $\frac{\partial f}{\partial y} = -2y - a_1x - a_3$, where at $P = (0,0)$

$$\frac{\partial f}{\partial x}(0,0) = a_4, \quad \text{and} \quad \frac{\partial f}{\partial y}(0,0) = -a_3.$$

Hence both derivatives vanish at the origin when reduced at those primes dividing both a_3 and a_4. Hence it follows that if $\gcd(a_3, a_4) = 1$ then $P = (0,0)$ has everywhere nonsingular reduction, while if $\gcd(a_3, a_4) > 1$ then $P = (0,0)$ is singular modulo primes dividing $\gcd(a_3, a_4)$.

Example 4.7.4. In her thesis Shipsey shows $P = (0,0)$ on

$$E\colon y^2 + 27y = x^3 + 28x^2 + 27x$$

is not associated to an integer EDS. We see P is singular modulo 3, since on letting

$$f(x,y) = x^3 + 28x^2 + 27x - y^2 - 27y,$$

we have

$$\frac{\partial f}{\partial x}(0,0) = a_4 = 3^3 \quad \text{and} \quad \frac{\partial f}{\partial y}(0,0) = -a_3 = 3^3.$$

However we note $3P = (-1,-27)$ is nonsingular modulo every prime since

$$\frac{\partial f}{\partial x}(-1,-27) = -2 \cdot 13 \quad \text{and} \quad \frac{\partial f}{\partial y}(-1,-27) = -3^3.$$

Hence $3P$ does have an associated integer EDS since the partial derivatives there are coprime.

Example 4.7.5. The integer EDS U with seed $[1, 10, 171, -7660]$ from Example 4.1.10 (d) has an associated elliptic curve-point pair: $E\colon y^2 = x^3 - 2$, $P = (3,5)$.

See Table 4.7.1 to see that $B_{kP} = |U_k|$ for $1 \leq k \leq 4$, and so the EDSs (U_n) and the DDS (B_{nP}) are the same if we give the DDS the correct sign.

$$\begin{aligned} P &= \left(\frac{3}{1}, \frac{5}{1}\right) && B_P = 1 \\ [2]P &= \left(\frac{129}{100}, \frac{-383}{1000}\right) && B_{2P} = 10 \\ [3]P &= \left(\frac{164323}{29241}, \frac{-66234835}{5000211}\right) && B_{3P} = 171 \\ [4]P &= \left(\frac{2340922881}{58675600}, \frac{113259286337279}{449455096000}\right) && B_{4P} = 7660 \end{aligned}$$

Table 4.7.1: DDS associated to Elliptic Curve $E\colon y^2 = x^3 - 2$ and Point $P = (3, 5)$

If we had used $[2](3,5) = \left(\frac{129}{100}, \frac{-383}{1000}\right)$ to generate the EDS instead, we would have a noninteger EDS, V say, having seed

$$\left[1, \tfrac{-383}{500}, \tfrac{-2265231357}{100000000}, \tfrac{43378306667177857}{250000000000000}\right],$$

with the DDS seed $[10, 7660, 22652313570, 1735132266687114280]$, i.e., the DDS containg all the elliptic denominators of the even multiples of P.

We note V is equivalent to an integer EDS V' by $V'_n = 20^{n^2-1}V_n$ to give the seed for V' being $[1, -6128, -579899227392, 5685681411480336072704]$.

Example 4.7.6. Recall the EDS $(W(357\text{d}1)_n)$ from Example 4.5.10 having the seed $[1, 21, -1323, -1750329]$. It has the associated rank 1 elliptic curve $E_{357\text{d}1}\colon y^2+y = x^3 + x^2 - 42x + 110$ with generator point $P = (0, 10)$. We note that since P is an integral point then $P \not\equiv O \pmod{p}$ for all primes p. However since $W_2 = 3 \cdot 7$, and $W_3 = -3^3 \cdot 7^2$ we have by Theorem 3.2.4 that P reduces to a singular point modulo primes 3 and 7. In Table 4.7.2 we see the valuations for the EDS and the DDS are the same for all primes except $p = 3$, and $p = 7$. Hence $r(3) = r(7) = 2$, for the EDS, but for the DDS we find these primes occur first at $r_s(3) = 14$ and $r_s(7) = 12$, the s subscript indicating 'singular'.

EDS :	0	1	$3 \cdot 7$	$-3^3 \cdot 7^2$	$-3^6 \cdot 7^4$
DDS :	1	1	1	1	1
EDS :	$-2 \cdot 3^{10} \cdot 7^6$	$3^{15} \cdot 7^9$	$3^{21} \cdot 7^{12}$	$3^{27} \cdot 7^{16}$	$-3^{34} \cdot 5 \cdot 7^{20}$
DDS :	2	1	1	1	5
EDS :	$-2^2 \cdot 3^{42} \cdot 7^{25}$	$-3^{51} \cdot 7^{30}$	$3^{61} \cdot 7^{37}$	$3^{72} \cdot 7^{42} \cdot 13$	$-3^{85} \cdot 7^{49}$
DDS :	2^2	1	7	13	3
EDS :	$-2 \cdot 3^{96} \cdot 7^{56} \cdot 11$	$-3^{109} \cdot 7^{64} \cdot 37$	$3^{123} \cdot 7^{72} \cdot 97$	$3^{138} \cdot 5 \cdot 7^{81} \cdot 17$	$3^{154} \cdot 7^{90} \cdot 191$
DDS :	$2 \cdot 11$	37	97	$5 \cdot 7$	191
EDS :	$-2^3 \cdot 3^{171} \cdot 7^{100} \cdot 29$	$-3^{189} \cdot 7^{110} \cdot 349$	$-3^{207} \cdot 7^{121} \cdot 151$	$3^{226} \cdot 7^{132} \cdot 23 \cdot 139$	$3^{246} \cdot 7^{145} \cdot 673$
DDS :	$2^3 \cdot 29$	349	151	$23 \cdot 139$	$7 \cdot 673$

Table 4.7.2: EDS $(W(357\text{d}1)_n)$ and associated DDS coming from Elliptic Curve $E_{357\text{d}1}\colon y^2 + y = x^3 + x^2 - 42x + 110$ and Point $P = (0, 10)$

Chapter 5

Modularity of Elliptic Curves

5.1 Modular Machinery

The following treatment of the modular machinery needed is heavily borrowed from Siksek [11, Ch. 15]. We now recall definitions and properties of modular forms.

Definition 5.1.1. By a newform of level N we mean a cusp form of weight 2 without character on $\Gamma_0(N)$, which belongs to the newspace and is normalised so that $c_1 = 1$ in the Fourier expansions around ∞, and is a simultaneous eigenfunction for all the Hecke operators. Newforms have q-expansions given by

$$f(\tau) = q + \sum_{n=2}^{\infty} c_n q^n, \qquad q = e^{2\pi i \tau}. \tag{5.1.1}$$

We summarize some crucial facts about newforms:

- For each positive integer N, there are finitely many newforms of level N, as determined by the modular symbols algorithm.
- If f is a newform with coefficients c_n as in (5.1.1) and $K = \mathbb{Q}(c_2, c_3, \dots)$ then K is a *finite and totally real* extension of $\mathbb{Q}$, that is it is a totally real number field.
- The c_n are algebraic integers belonging to the ring of integers $\mathbb{Z}_K$ of the number field K. If $K = \mathbb{Q}$ then $c_n \in \mathbb{Z}$ and the newforms are termed

rational and correspond to elliptic curves. Otherwise they are *irrational* and are associated to higher dimensional modular abelian varieties.

- Let L be the Galois closure of K, then if σ is an element of $\mathrm{Gal}(L/K)$ and f any newform then $\sigma(f)$ is also a newform termed a conjugate of f. We will usually identify a newform up to Galois conjugacy.

- If ℓ is a prime then $|c_\ell| \leq 2\ell^{1/2}$, and in fact this is true for the conjugates of f and so $|\sigma(c_\ell)| \leq 2\ell^{1/2}$. This is the Ramanujan conjecture, proven in generality by Deligne.

It turns out it is much easier to deal with irrational newforms. The next Proposition gives a recursive formula for the number of newforms of level N (no closed form for the number of newforms up to conjugacy is known). The formula follows from the dimension formula for the space of cuspidal modular forms on $\Gamma_0(N)$ of weight k ($k \geq 2$ even). The formula itself may be found in [25].

Proposition 5.1.2. *We define five arithmetic functions $A_i(N)$ for $1 \leq i \leq 5$ by asking that they be multiplicative, and that their values on prime powers p^k be given as follows:*

(a) $A_1(p) = -1$, $A_1(p^k) = 0$ *for* $k \geq 2$.

(b) $A_2(p) = p - 1$, $A_2(p^2) = p^2 - p - 1$, $A_2(p^k) = (p-1)(p^{k-1} - p^{k-3})$ *for* $k \geq 3$.

(c) *For p odd,* $A_3(p) = \left(\frac{-4}{p}\right) - 1$, $A_3(p^2) = -\left(\frac{-4}{p}\right)$, $A_3(p^k) = 0$ *when* $k \geq 3$, *while* $A_3(2) = A_3(2^2) = -1$, $A_3(2^3) = 1$, *and* $A_3(2^k) = 0$ *for* $k \geq 4$.

(d) *For* $p \neq 3$, $A_4(p) = \left(\frac{-3}{p}\right) - 1$, $A_4(p^2) = -\left(\frac{-3}{p}\right)$, $A_4(p^k) = 0$ *when* $k \geq 3$, *while* $A_4(3) = A_4(3^2) = -1$, $A_4(3^3) = 1$, *and* $A_4(3^k) = 0$ *for* $k \geq 4$.

(e) $A_5(p^2) = p - 2$, $A_5(p^{2k}) = p^{k-2}(p-1)^2$, *for* $k \geq 2$, *while* $A_5(p^{2k-1}) = 0$ *for* $k \geq 1$.

The number of newforms of level N (counting conjugate ones as distinct) is equal to

$$A_1(N) + \frac{A_2(N)}{12} - \frac{A_3(N)}{4} - \frac{A_4(N)}{3} - \frac{A_5(N)}{2}.$$

Corollary 5.1.3. *There are no newforms at levels*

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 12,\ 13,\ 16,\ 18,\ 22,\ 25,\ 28,\ 60.$$

Moreover, for all other levels there are newforms.

Proof. Follows from an immediate (computer-aided) computation from the proposition. □

Example 5.1.4. If $N = 198 = 2 \cdot 3^2 \cdot 11$ we compute $A_1(198) = 0$; $A_2(198) = 50$; $A_3(198) = 2$; $A_4(198) = -4$; $A_5(198) = 0$: the formula gives the number of newforms as

$$0 + \frac{50}{12} - \frac{2}{4} - \frac{-4}{3} - \frac{0}{2} = 5.$$

Using `Sage` [38] we find all five newforms are rational, for which $K = \mathbb{Q}$.

$$\begin{aligned}
f_1 &= q - q^2 + q^4 - 2q^5 - 4q^7 - q^8 + 2q^{10} + q^{11} - 6q^{13} + \cdots, \\
f_2 &= q + q^2 + q^4 + 2q^7 + q^8 + q^{11} - 4q^{13} + 2q^{14} + \cdots, \\
f_3 &= q + q^2 + q^4 + 2q^7 + q^8 - q^{11} + 2q^{13} + 2q^{14} + \cdots, \\
f_4 &= q - q^2 + q^4 + 2q^7 - q^8 + q^{11} + 2q^{13} - 2q^{14} + \cdots, \\
f_5 &= q - q^2 + q^4 + 4q^5 - 2q^7 - q^8 - 4q^{10} - q^{11} + 4q^{13} + \cdots.
\end{aligned}$$

If $N = 594 = 2 \cdot 3^3 \cdot 11$ we compute $A_1(594) = 0$; $A_2(594) = 160$; $A_3(594) = 0$; $A_4(594) = 4$; $A_5(594) = 0$: the formula gives the number of newforms as

$$0 + \frac{160}{12} - \frac{0}{4} - \frac{4}{3} - \frac{0}{2} = 12.$$

Using `Sage` we find there are eight newforms in the conjugacy class for which $K =$

$\mathbb{Q}$, while there are four newforms in the conjugacy class for which $K = \mathbb{Q}(\sqrt{10})$.

$$
\begin{aligned}
f_1 &= q - q^2 + q^4 - 2q^5 + q^7 - q^8 + 2q^{10} - q^{11} - \cdots, \\
f_2 &= q - q^2 + q^4 + q^5 + 4q^7 - q^8 - q^{10} - q^{11} + \cdots, \\
f_3 &= q - q^2 + q^4 - 3q^5 - 4q^7 - q^8 + 3q^{10} - q^{11} + \cdots, \\
f_4 &= q - q^2 + q^4 - 2q^5 - q^7 - q^8 + 2q^{10} + q^{11} + \cdots, \\
f_5 &= q + q^2 + q^4 + 2q^5 - q^7 + q^8 + 2q^{10} - q^{11} + \cdots, \\
f_6 &= q + q^2 + q^4 - q^5 + 4q^7 + q^8 - q^{10} + q^{11} + \cdots, \\
f_7 &= q + q^2 + q^4 + 2q^5 + q^7 + q^8 + 2q^{10} - q^{11} - \cdots, \\
f_8 &= q + q^2 + q^4 + 3q^5 - 4q^7 + q^8 + 3q^{10} + q^{11} + \cdots, \\
f_9 &= q - q^2 + q^4 + \tfrac{1}{2}(1+\alpha)\,q^5 + 2q^7 - q^8 - \tfrac{1}{2}(1+\alpha)\,q^{10} + q^{11} + \cdots, \\
f_{10} &= \sigma(f_9), \\
f_{11} &= q + q^2 + q^4 + (\beta - 1)q^5 + 2q^7 + q^8 + (\beta - 1)q^{10} - q^{11} + \cdots, \\
f_{12} &= \sigma(f_{11}),
\end{aligned}
$$

where $\alpha = -3 + 2\sqrt{10}$, $\beta = 2 + \sqrt{10}$, and σ is the nontrivial automorphism of $\mathbb{Q}(\sqrt{10})$. We note that up to Galois conjugacy we only have ten newforms to deal with.

Definition 5.1.5. Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. If there exists a newform f of level N such that $c_\ell(f) = a_\ell(E)$ for all primes ℓ, we say that E is *modular*.

For rational newforms the map $f \mapsto E_f$, where E_f is an elliptic curve defined over $\mathbb{Q}$, is due to Eichler and Shimura.

Theorem 5.1.6 (Eichler–Shimura)**.** *Given a cuspidal newform f of weight 2 and level N it is possible to construct an elliptic curve E of conductor N such that*

$$c_\ell(f) = \ell + 1 - |E(\mathbb{F}_\ell)|, \qquad \ell \nmid N.$$

Proof. See [16, Ch. 8]. □

The famed Taniyama–Shimura–Weil Conjecture, or the Modularity Conjecture, was whether the map $f \mapsto E_f$ was surjective, that is to say that associated to any

elliptic curve defined over $\mathbb{Q}$ is a newform. This was famously proved by Wiles and Taylor–Wiles in [47, 41] for the semistable elliptic curve case and proven in full generality by Breuil, Conrad, Diamond and Taylor in [7].

Theorem 5.1.7 (Modularity Theorem for Elliptic Curves)**.** *Let $N \geq 1$ be an integer. Every rational newform f of level N has an associated rational elliptic curve $E_f/\mathbb{Q}$ with conductor equal to N such that for all primes $\ell \nmid N$ we have $c_\ell(f) = a_\ell(E_f)$, where $c_\ell(f)$ is the ℓ^{th} Fourier coefficient in the q-expansion of f and $a_\ell(E_f) = \ell + 1 - |E_f(\mathbb{F}_\ell)|$. For any given integer $N \geq 1$, the association $f \mapsto E_f$ is a bijection between rational newforms of level N and isogeny classes of elliptic curves of conductor N.*

Proof. See [7]. □

Looking back to Example 5.1.4 we find for the level $N = 198$, the rational newforms f_1 to f_5 correspond to the five isogeny classes of elliptic curves of conductor 198, and have been arranged so they correspond to elliptic curves in the respective order 198a1, 198b1, 198c1, 198d1, and 198e1 in the tables of Cremona [13]. Similarly for the eight rational newforms of level $N = 594$, they correspond to the eight isogeny classes of elliptic curves of conductor 594. These eight rational newforms have been arranged so they correspond to the elliptic curves in the respective order 594a1, 594b1, 594c1, 594d1, 594e1, 594f1, 594g1, and 594h1 in the tables of Cremona [13].

5.2 Ribet's Level Lowering Theorem

Definition 5.2.1. Let E be a rational elliptic curve with $\Delta_{\min}$ the discriminant for a minimal model of E, and N be the conductor of E. Suppose p is a prime, and let

$$N_p = N \Big/ \prod_{\substack{q \| N \\ p | v_q(\Delta_{\min})}} q. \tag{5.2.1}$$

5.2.1 Definition of "Arises From"

Definition 5.2.2. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Now suppose there is a newform of level N' not necessarily equal to N, with the Fourier coefficients c_i of its q-expansion generating the number field $K = \mathbb{Q}(c_2, c_3, \dots)$. We say the curve E arises *modulo* p from the newform f, and write $E \sim_p f$, if there is some prime ideal $\mathfrak{p}$ of K above p such that for almost all primes ℓ, we have $a_\ell(E) \equiv c_\ell(f) \pmod{\mathfrak{p}}$.

Proposition 5.2.3. *Suppose $E \sim_p f$. Then there is some prime ideal $\mathfrak{p}$ in the ring of integers $\mathbb{Z}_K$ above p such that for all prime numbers ℓ we have:*

$$c_\ell(f) \equiv \begin{cases} a_\ell(E) \pmod{\mathfrak{p}} & \text{if } \ell \nmid pNN', \\ \pm(\ell+1) \pmod{\mathfrak{p}} & \text{if } \ell \nmid pN' \text{ and } \ell \parallel N. \end{cases} \tag{5.2.2}$$

Furthermore, if $\mathbb{Z}_K = \mathbb{Z}$ then

$$c_\ell(f) \equiv \begin{cases} a_\ell(E) \pmod{p} & \text{if } \ell \nmid NN', \\ \pm(\ell+1) \pmod{p} & \text{if } \ell \nmid N' \text{ and } \ell \parallel N. \end{cases} \tag{5.2.3}$$

Proof. This comes from modularity. The strengthening in the case $\mathbb{Z}_K = \mathbb{Z}$ is due to Kraus and Oesterlé [24]. For further details see [14], Chapter 2. □

If f is a rational newform, then we know that f corresponds to some elliptic curve $F = E_f$ by the Modularity Theorem. Hence if E arises modulo p from f then we shall also say that E arises modulo p from F, and write $E \sim_p F$.

The strengthening of Proposition 5.2.3 in removing the dependency on the prime p is beneficial in the sense that p shall later become the exponent in some equation, and so to have conditions imposed on it would complicate matters. As such the Proposition of Kraus and Oesterlé is the one we shall need.

Remark 5.2.4. The condition that $\ell \nmid NN'$ says E and F both have good reduction at ℓ.

The condition that $\ell \nmid N'$ and $\ell \parallel N$ says E has multiplicative reduction at ℓ, whilst F has good reduction at ℓ.

We now give a simplified form of Ribet's Theorem which will be sufficient for our needs.

Theorem 5.2.5 (Ribet's Level Lowering Theorem [30]). *Suppose E is a rational elliptic curve in global minimal form and $p \geq 5$ is a prime number. Assume there does not exist a p-isogeny defined over $\mathbb{Q}$ from E to some other elliptic curve. Let N_p be defined as above. Then there exists a newform f of level N_p such that $E \sim_p f$.*

Let $E/\mathbb{Q}$ have $\Delta_{\min} = \prod_{q|\Delta_{\min}} q^{\delta_q}$ and $N = \prod_{q|\Delta_{\min}} q^{f_q}$. Suppose E is a Weil curve having a modular parametrization of level N given via a normalised newform $f(\tau) = q + \sum_{n=2}^{\infty} c_n q^n$. Ribet's Theorem then states that we can perform a level descent modulo primes p dividing one of the exponents δ_q, as long as we have $f_q = 1$. Then let N_p be as in (5.2.1). Then there exists a newform g of level N_p such that $g(\tau) = q + \sum_{n=2}^{\infty} d_n q^n$ with integral coefficients having $c_n \equiv d_n \pmod{p}$ for $1 \leq n < \infty$. Equivalently by the Modularity Theorem there exists an elliptic curve E' with conductor N_p, with the coefficients of the L-series of E and E' congruent modulo p.

To apply Ribet's Theorem we require the absence of any p-isogenies for the elliptic curve E as explained in Theorem 5.2.5, that is there must be no subgroup of E of order p that is stable under conjugation. We could do this by testing the p^{th} division polynomial for irreducibility, but this can be tricky. Mazur has shown there are no p-isogenies with $p > 163$ and j-invariant nonintegral. We list some useful theorems for determining the lack of isogenies.

Theorem 5.2.6 (Mazur [26], Diamond & Kramer [17], Dahmen [14]). *Let $E/\mathbb{Q}$ be an elliptic curve with j-invariant j and conductor N. Let p be a prime. Then E does not have any p-isogeny if at least one of the following conditions holds.*

(a) *$p \geq 17$ and $j(E) \notin \mathbb{Z}[1/2]$.*

(b) *$p \geq 11$ and N is squarefree.*

(c) *$p \geq 5$, N is squarefree, and $|E(\mathbb{Q})[2]| = 4$, meaning $E(\mathbb{Q})$ has full 2-torsion.*

(d) *$p \geq 3$ and $v_2(N) = 3$, 5, or 7.*

(e) $p = 11$ *or* $p \geq 17$ *and the pair* (p, j) *has no corresponding entry in Table 5.2.1.*

(f) E *has a rational* 2*-torsion point,* $p \geq 7$ *and*

$$(p, j) \neq (7, -3^3 \cdot 5^3),\ (7, 3^3 \cdot 5^3 \cdot 17^3).$$

p	j
11	$-2^{15},\ -11^2,\ -11 \cdot 131^3$
17	$-17 \cdot 373^3/2^{17},\ -17^2 \cdot 101^3/2$
19	$-2^{15} \cdot 3^3$
37	$-7 \cdot 11^3,\ -7 \cdot 137^3 \cdot 2083^3$
43	$-2^{18} \cdot 3^3 \cdot 5^3$
67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

Table 5.2.1: Pairs (p, j) corresponding to rational isogenies

Proof. For (a), (b), (c) see [26]; for (d) see [17]; for (e), (f) see [14, Ch. 2, Thm. 22]. □

Remark 5.2.7. If E has no p-isogenies then Ribet's theorem implies that $E \sim_p f$ for some newform of level N_p. Here we note that, as well as any rational newforms of level N_p, there may be irrational newforms at that level defined over number fields of arbitrary degree, and these will also have to be taken into consideration when considering the existence of solutions of Diophantine equtions in the sequel. This is made precise in the following proposition.

Proposition 5.2.8. *An elliptic curve defined over* $\mathbb{Q}$ *can arise from a newform whose defining field* K *has arbitrarily large degree.*

Proof. See [11, Prop. 15.2.9]. □

5.2.2 A Bound for p

The next Proposition, taken from Cohen [11], will be of help when it comes to bounding the prime exponent occurring in a Diophantine equation.

Proposition 5.2.9. *Let $E/\mathbb{Q}$ be an elliptic curve defined over the rationals of conductor N, and let $t \in \mathbb{Z}$ be a divisor of the order of the torsion group $E_{\text{tors}}(\mathbb{Q})$. Let f be a newform of level N' with Fourier coefficients c_n, which generate a totally real field K, and let ℓ be a prime such that $\ell^2 \nmid N$ and $\ell \nmid N'$. Define*

$$S_\ell = \{a \in \mathbb{Z} : -2\sqrt{\ell} \leq a \leq 2\sqrt{\ell} \text{ and } a \equiv \ell + 1 \pmod{t}\},$$
$$B'_\ell(f) = \mathcal{N}_{K/\mathbb{Q}}\left((\ell+1)^2 - c_\ell^2\right) \prod_{a \in S_\ell} \mathcal{N}_{K/\mathbb{Q}}(a - c_\ell), \text{ and}$$
$$B_\ell(f) = \begin{cases} \ell B'_\ell(f) & \text{if } f \text{ is irrational } (K \neq \mathbb{Q}), \\ B'_\ell(f) & \text{if } f \text{ is rational } (K = \mathbb{Q}). \end{cases}$$

Then if $E \sim_p f$ we have $p \mid B_\ell(f)$.

Proof. See [11, Prop. 15.4.1]. □

This proposition allows us to bound p if we can find an ℓ such that $B_\ell(f) \neq 0$. This is not always possible but is certain in the following cases:

Proposition 5.2.10. *In each of the following cases there are infinitely many ℓ for which $B_\ell(f) \neq 0$:*

(a) When f is irrational.

(b) When f is rational and t is a prime number or 4, for every elliptic curve F isogenous to the elliptic curve corresponding to f we have $t \nmid |F(\mathbb{Q})|$.

(c) If f is rational and $t = 4$, and if for every elliptic curve F isogenous to the elliptic curve corresponding to f then $F(\mathbb{Q})$ does not have full 2-torsion.

Proof. See [11, Prop. 15.4.2]. □

We note for (a) if f is irrational there exist infinitely many ℓ such that $c_\ell \notin \mathbb{Q}$, which implies $B_\ell(f) \neq 0$, at least for all those ℓ such that $(\ell+1)^2 - c_\ell^2 \neq 0$. Hence

if p is a prime not dividing $B'_\ell(f)$ then $E \not\sim_p f$. In particular, if q is the largest prime dividing $B'_\ell(f)$ then, for any $p > q$, $E \not\sim_p f$.

Our strategy for bounding the exponent p for irrational newforms is then:

(1) Find all irrational newforms of (lowered) level N'.

(2) For each such f, find ℓ such that $c_\ell \notin \mathbb{Q}$ (smallest such ℓ).

(3) Compute $B_\ell(f)$ and find its largest prime divisor q.

Proposition 5.2.10 lends some justification to our work in the sequel; for it is seen that for rational newforms we may end up in the situation that $B_\ell(f) = 0$ for all ℓ, and so a bound will be impossible to procure in such a case using Proposition 5.2.9. Our method however shall always enable one to find a bound, at least in theory, i.e., if computationally feasible.

5.3 The Modular Approach

One of the twentieth centuries defining mathematical moments was the proof of Fermat's Last Theorem (FLT) by Sir Andrew Wiles, with a little help from Richard Taylor (see [47, 41]). Using Galois representations on the p-torsion of the Frey elliptic curve associated with FLT, Ribet's Level Lowering Theorem shows that the Galois representation is of a level 2 newform of which there are none.

This contradiction forms the basis of the *modular method*. To a putative solution of a Diophantine equation we associate an elliptic curve E, called a Frey curve. The Frey curve E must satisfy the following conditions:

- The coefficients of (the Weierstrass equation for) E are dependent on the solution of the Diophantine equation.
- The minimal discriminant $\Delta_{\min}$ of E has the form $\Delta_{\min} = C \cdot D^p$ where C is some constant independent of the solution of the equation but intrinsic to the equation itself, D is some value dependent on the solution of the equation, and p is a fixed prime (independent of the solution).
- Primes dividing D have multiplicative reduction for E.

Now apply Ribet's theorem, for which we need to know E has no p-isogeny.

Example 5.3.1. Let $p \geq 5$ be an odd prime, and a, b, c be coprime positive integers, $abc \neq 0$, such that

$$a^p + b^p + c^p = 0 \tag{5.3.1}$$

is a nontrivial solution to FLT. The trick here is to associate to this purported solution the elliptic Frey curve $E_{\alpha,\beta,\gamma}$ given by

$$E_{\alpha,\beta,\gamma}\colon y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

and proceed to show it cannot exist.

To this end let

$$\begin{aligned} a^p &= \alpha - \beta, \\ b^p &= \beta - \gamma, \\ c^p &= \gamma - \alpha. \end{aligned} \tag{5.3.2}$$

From the group of equations (5.3.2), we find on addition to derive the Fermat Equation (5.3.1).

Now by a change of coordinates we can move one of the roots of the elliptic curve equation to the origin. Do this for γ: then $E_{\alpha,\beta,\gamma}$ is the nonsingular algebraic curve of genus 1 over $\mathbb{Q}$, whose projective completion is a semistable elliptic Frey curve over $\mathbb{Q}$ given by

$$E_{a,b,c}\colon y^2 = x(x+c^p)(x-b^p).$$

The elliptic discriminant for the Frey curve is

$$\Delta = (abc)^{2p}.$$

which is nonzero since the solution (5.3.1) is nontrivial. The minimal discriminant for the Frey curve is

$$\Delta_{\min} = \frac{1}{2^8}(abc)^{2p},$$

which is an integer since one of a, b, c is even.

The conductor N is the radical of abc.

$$\begin{aligned} N &= \prod_{\ell \text{ prime},\, \ell \mid abc} \ell \\ &= \operatorname{rad}(abc). \end{aligned}$$

By Theorem 5.2.6 (c), since $E(\mathbb{Q})[2] = \{O,\ (0,0),\ (0,b^p),\ (0,-c^p)\}$ and $p \geq 5$, the curve E has no p-isogenies and we can apply Ribet's Level Lowering Theorem.

5.3.1 The Tables of Papadopoulos

Let E be an elliptic curve over $\mathbb{Q}$. In his paper Papadopoulos [28] provides tables which give the exponent of the prime factors of the conductor of an elliptic curve dealing with the cases for q a prime, $q = 2$, $q = 3$, and $q \geq 5$, see Tables 5.3.1, 5.3.2, and 5.3.3 respectively.

Often the 3-tuple $(v_q(c_4), v_q(c_6), v_q(\Delta))$ is enough to determine the powers of q dividing the conductor. However we might end up in a situation where the same 3-tuple of valuations have different values of f_q owing to the case of Tate we end up in after applying Tate's algorithm which is used to find a minimal model with the outcome one of 11 cases. In his paper Papadopoulos distinguishes each possible case to derive the correct value for f_q dependent on which case of Tate we end up in. Moreover the Kodaira symbol, which encodes the type of reduction of an elliptic curve at q, is included in the tables.

For the prime 3 Papadopoulos uses the terminology: a curve satisfies the property P_i, for $i = 2$ or 5, if there exists $u \in \mathbb{Z}$ such that $u^3 - 3c_4u - 2c_6 \equiv 0 \pmod{3^{3+i}}$. This is satisfied if and only if there exists $v \in \mathbb{Z}$ such that $v^3 + b_2v^2 + 8b_4v + 16b_6 \equiv 0 \pmod{3^i}$.

He gives the conditions: if $v_3(c_4) \geq 2$, $v_3(c_6) = 3$ the condition P_2 is:

$$c_{6,3}^2 + 2 \equiv 3c_{4,2} \pmod 9, \quad \text{where } c_{4,2} = c_4/3^2 \text{ and } c_{6,3} = c_6/3^3; \tag{5.3.3}$$

whereas if $v_3(c_4) \geq 4$, $v_3(c_6) = 6$ the condition P_5 is:

$$c_{6,6}^2 + 2 \equiv 3c_{4,4} \pmod 9, \quad \text{where } c_{4,4} = c_4/3^4 \text{ and } c_{6,6} = c_6/3^6. \tag{5.3.4}$$

For the prime $q = 2$ the situation is more complicated and we have the following Proposition which classifies the different cases of Tate's algorithm.

Proposition 5.3.2 (Papadopoulos [28]). *Let E be an elliptic curve in global Weierstrass form. With reference to Table 5.3.1 corresponding to a case ≥ 3 in Tate's algorithm, there exists r, $t \in \mathbb{Z}$ such that*

$$2 \mid a_4 + r^2, \ 2 \mid t^2 + a_4 a_2 - a_6.$$

(a) *If $a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv 0 \pmod{2^2}$ then we are in a case of Tate's algorithm ≥ 4; otherwise we are in case 3.*

(b) *If $b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \equiv 0 \pmod{2^3}$ then we are in a case of Tate's algorithm ≥ 5; otherwise we are in case 4.*

(c) *If $b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \not\equiv 0 \pmod{2^5}$ then we are in case 6 of Tate's algorithm.*

(d) *If $b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \equiv 0 \pmod{2^5}$, then there exists $t \in \mathbb{Z}$ such that $a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv 0 \pmod{2^3}$. Choose one t. We are in case 6 if we have $v_2(a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1) = 3$; otherwise we are in a case of Tate's algorithm ≥ 7.*

(e) *If $b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \equiv 0 \pmod{2^5}$ and there exists $s \in \mathbb{Z}$ such that $a_2 + 3r - sa_1 - s^2 \equiv 0 \pmod{2^2}$, then we are in a case of Tate's algorithm ≥ 8.*

(f) *If $v_2(b_8 + 3rb_6 + 3r^2 b_4 + r3b_2 + 3r^4) \geq 7$ we are in a case of Tate's algorithm ≥ 10.*

(g) *If $v_2(c_4) \geq 8$ and $v_2(\Delta) \leq 12$, then there exists $r \in \mathbb{Z}$ such that $v_2(b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4) \geq 8$. E is a nonminimal equation if there exists $u \in \mathbb{Z}$ such that $v_2(b_6 + 2rb_4 + r^2 b_2 + 4r^3 - u^2) \geq 8$; otherwise we are in case 10 of Tate's algorithm.*

(h) *If $v_2(c_4) \leq 4$, then there exists $r \in \mathbb{Z}$ such that $v_2(b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4) \geq 8$ and a $t \in \mathbb{Z}$ such that $v_2(a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1) \geq 5$. If $v_2(a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1) \geq 6$, then E is nonminimal.*

5.3.2 The Diophantine Equation $Ay^p + Bx^q = Cz^r$

Let A, B, C be nonzero and p, q, $r \in \mathbb{Z}_{\geq 2}$. Consider the ternary Diophantine equation

$$Ay^p + Bx^q = Cz^r, \quad \gcd(x, y, z) = 1 \tag{5.3.5}$$

We term the triple (p, q, r) the signature of the equation (5.3.5). Now let the characteristic of the equation (5.3.5) be defined as

$$\chi(p, q, r) := \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1.$$

- For $\chi < 0$, Darmon and Granville [15] have shown there are only finitely many integer solutions.
- For $\chi = 0$, the only possible sets for $\{p, q, r\}$ are $\{3, 3, 3\}$, $\{2, 4, 4\}$, and $\{2, 3, 6\}$.
- For $\chi > 0$, $\{p, q, r\}$ are $\{2, 2, k\}$ with $k \geq 2$, or $\{2, 3, m\}$ with $m = 3$, 4, or 5.

These three cases are termed the hyperbolic case, the Euclidean case, and the spherical case for $\chi < 0$, $\chi = 0$, and $\chi > 0$ respectively.

5.3.3 The Diophantine Equation $Ay^2 + Bx^3 = Cz^p$ and the Frey Curve of Barros

In this Section we look at the particular form of the ternary Diophantine equation from Subsection 5.3.2 with signature $(2, 3, p)$. To be able to study this Diophantine equation using the modular method we shall need a corresponding Frey curve which is found in a result of Barros [4] which we shall require later for examining the Diophantine equation $y^2 - x^3 = Dz^{6p}$.

Theorem 5.3.3 (Barros [4, Thm. 5.1])**.** *Let A, B, C, x, y, z be integers, such that $\gcd(Ay, Bx, Cz) = 1$. Let p be a prime number. Suppose also that*

(a) *A is squarefree;*

(b) *B is cubefree;*

Table 5.3.1: Papadopoulos' Table for $q = 2$

Kodaira Symbol	I_0	$\mathrm{I}_{n,\,(n>0)}$	II	III	IV	I_0^*
Tate's Case	1	2	3	4	5	6
$v_2(c_4)$	0	0	≥ 4	≥ 5	≥ 6	≥ 6
$v_2(c_6)$	0	n	5	≥ 6	5	≥ 8
$v_2(\Delta)$	0	n	4	6	6	10
Extra Conditions			*	*	*	*
$v_2(N)$	0	1	4	3	2	4

Kodaira Symbol	I_1^*	I_2^*	I_3^*	$\mathrm{I}_{n,\,(n\geq 4)}^*$	IV^*	III^*	II^*	Non minimal equation
Tate's Case	7	7	7	7	8	9	10	
$v_2(c_4)$	4	6	4	6	≥ 7	7	≥ 8	≥ 8
$v_2(c_6)$	6	≥ 9	6	≥ 9	6	9	10	≥ 11
$v_2(\Delta)$	8	12	11	$8+n$	8	12	14	≥ 15
Extra Conditions	*	*	*	*	*	*	*	*
$v_2(N)$	3	6	4	4	2	3	4	6

Table 5.3.2: Papadopoulos' Table for $q = 3$

Kodaira Symbol	I_0	$\mathrm{I}_{n,\,(n\geq 0)}$	II	III	IV	I_0^*	$\mathrm{I}_{n,\,(n>0)}^*$	IV^*	III^*	II^*	Non minimal equation
Tate's Case	1	2	3	4	5	6	7	8	9	10	
$v_3(c_4)$	0	0	≥ 2	≥ 3	≥ 4	2	3	≥ 4	≥ 4	5	≥ 6
$v_3(c_6)$	0	≥ 3	3	4	≥ 5	5	≥ 6	6	≥ 8	8	≥ 9
$v_3(\Delta)$	0	n	3	5	6	6	$6+n$	9	9	11	≥ 12
Extra Conditions			not P_2	P_2				not P_5	P_5		
$v_3(N)$	0	1	3	2	2	2	2	3	2	3	5

Table 5.3.3: Papadopoulos' Table for $q \geq 5$

Kodaira Symbol	I_0	$\mathrm{I}_{n,\,(n>0)}$	II	III	IV	I_0^*	$\mathrm{I}_{n,\,(n>0)}^*$	IV^*	III^*	II^*	Non minimal equation
Tate's Case	1	2	3	4	5	6	7	8	9	10	
$v_q(c_4)$	0	0	≥ 1	1	≥ 2	2	≥ 2	≥ 3	3	≥ 4	≥ 4
$v_q(c_6)$	≥ 0	0	1	≥ 2	2	≥ 3	3	4	≥ 5	5	≥ 6
$v_q(\Delta)$	0	n	2	3	4	6	$6+n$	8	9	10	≥ 12
$v_q(N)$	0	0	1	2	2	2	2	2	2	2	

(c) *C is p^{th} powerfree.*

Finally we consider the equation

$$Ay^2 + Bx^3 = Cz^p. \tag{5.3.6}$$

The Frey curve associated to (5.3.6) is

$$E\colon Y^2 = X^3 + 3ABxX + 2A^2By. \tag{5.3.7}$$

(1) The minimal discriminant of E is

$$\Delta_{\min} = \begin{cases} -2^6 3^3 A^3 B^2 C z^p & \text{if } v_2(Cz^p) < 6, \\ -2^{-6} 3^3 A^3 B^2 C z^p & \text{if } v_2(Cz^p) \geq 6. \end{cases}$$

(2) The conductor N of the curve E is given by

$$N = 2^{f_2} 3^{f_3} \operatorname{rad}_{2,3}(AB)^2 \operatorname{rad}_{2,3}(Cz),$$

where f_2 is given in Table 5.3.4 and f_3 is given in Table 5.3.5.

(3) Suppose that $p = 11$ or $p \geq 17$ and the curve E does not correspond to one of the equations:

$$11 \cdot (\pm 7)^2 - 1 \cdot 8^3 = 3^3 \cdot 1^{11},\ (\pm 43)^2 - 11^2 \cdot 1^3 = 2^6 \cdot 3^3 \cdot 1^{11},$$
$$(\pm 4973)^2 - 11 \cdot 131^3 = 2 \cdot 3^3 \cdot 1^{11},\ 5 \cdot (\pm 14891)^2 - 17 \cdot 373^3 = 2^6 \cdot 3^3 \cdot 2^{17},$$
$$5 \cdot 7717^2 - 17^2 \cdot 101^3 = 2^7 \cdot 3^3 \cdot 1^{17},\ 19 \cdot 3 \cdot (\pm 3)^2 - 1 \cdot 8^3 \cdot 3^3 = 1 \cdot 1^{19},$$
$$5 \cdot (\pm 11 \cdot 1433 \cdot 11443)^2 - 7(137 \cdot 2083)^3 = 2^6 \cdot 3^3 \cdot 1^{37},$$
$$5 \cdot (\pm 47)^2 - 7 \cdot 11^3 = 2^6 \cdot 3^3 \cdot 1^{37},\ 3 \cdot 43 \cdot (\pm 3^2 \cdot 7) - 1 \cdot (2^4 \cdot 5)^3 = 1^{43},$$
$$3 \cdot 67 \cdot (\pm 3 \cdot 7 \cdot 31)^2 - 1 \cdot 2^3 \cdot 5 \cdot 11 = 1^{67},$$
$$3 \cdot 163 \cdot (\pm 3 \cdot 7 \cdot 11 \cdot 19 \cdot 127)^2 - 1 \cdot (2^4 \cdot 5 \cdot 23 \cdot 29)^3 = 1^{163},$$

Then $E \sim_p f$ for some newform f of level

$$N_p = 2^{f_2} 3^{f_3} \operatorname{rad}_{2,3}(AB)^2 \operatorname{rad}_{2,3}(C),$$

where f_2 is given in Table 5.3.4 and f_3 is given in Table 5.3.5.

The characteristic of equation (5.3.6) is given by

$$\chi(2,3,p) = \frac{1}{2} + \frac{1}{3} + \frac{1}{p} - 1 = \frac{1}{p} - \frac{1}{6} < 0.$$

Hence by Darmon and Granville (see Subsection 5.3.2) this shows there are only finitely many integer solutions possible for equation (5.3.6) when $p \geq 7$.

The associated quantities with (5.3.7) are

$$a_1 = a_2 = a_3 = 0, \quad a_4 = 3ABx, \quad a_6 = 2A^2By,$$

$$b_2 = 0, \quad b_4 = 2 \cdot 3ABx, \quad b_6 = 2^3A^2By, \quad b_8 = -3^2A^2B^2x^2,$$

$$c_4 = -2^4 3^2 ABx, \quad c_6 = -2^6 3^3 A^2 By,$$

$$\Delta = -2^6 3^3 A^3 B^2 (Ay^2 + Bx^3) = -2^6 3^3 A^3 B^2 C z^p, \quad j = \frac{2^6 3^3 Bx^3}{Ay^2 + Bx^3} = \frac{2^6 3^3 Bx^3}{Cz^p}.$$

With these quantities we can work out the valuations for the 3-tuple

$$(v_q(c_4), v_q(c_6), v_q(\Delta))$$

for primes 2 and 3 specifically, and for $q \geq 5$ in general, and check these against Tables 5.3.1, 5.3.2, and 5.3.3, to give Tables 5.3.4, 5.3.5, and 5.3.6 for the exponents f_q for the conductor N of E as given by

$$N = \prod_{q \text{ prime}} q^{f_q}.$$

Table 5.3.4: The Exponent f_2 for the Conductor of the Frey Curve (5.3.7)

$v_2(A)$	$v_2(y)$	$v_2(B)$	$v_2(x)$	$v_2(Cz^p)$	Conditions	$(v_2(c_4), v_2(c_6), v_2(\Delta))$	f_2	Tate's case
1	≥ 0	0	0	0		$(5, \geq 8, 9)$	8	4
0	≥ 1	0	0	0	$ABx \equiv 1 \pmod 4$	$(4, \geq 7, 6)$	5	4^*
0	≥ 1	0	0	0	$ABx \equiv 3 \pmod 4$	$(4, \geq 7, 6)$	6	3^*
0	0	1	0	0		$(5, 7, 8)$	7	4
0	0	1	1	0	$By \equiv 2 \pmod 8$	$(6, 7, 8)$	3	7^*
0	0	1	1	0	$By \equiv 6 \pmod 8$	$(6, 7, 8)$	4	6^*
0	0	1	≥ 2	0	$By \equiv 2 \pmod 8$	$(\geq 7, 7, 8)$	2	8^*
0	0	1	≥ 2	0	$By \equiv 6 \pmod 8$	$(\geq 7, 7, 8)$	4	6^*
0	0	2	≥ 0	0		$(\geq 6, 8, 10)$	6	6
0	0	0	≥ 1	0		$(\geq 5, 6, 6)$	6	3
0	0	0	0	1		$(4, 6, 7)$	7	3
0	0	0	0	2	$AB(x - 2Ay) \equiv 5 \pmod{16}$	$(4, 6, \geq 11)$	2	8^*
0	0	0	0	2	$AB(x - 2Ay) \equiv 9 \pmod{16}$	$(4, 6, 8)$	3	7^*
0	0	0	0	2	$AB(x - 2Ay) \equiv 1, 13 \pmod{16}$	$(4, 6, 8)$	4	6^*
0	0	0	0	3		$(4, 6, 9)$	5	6
0	0	0	0	4	$By \equiv 3 \pmod 4$	$(4, 6, 10)$	3	9^*
0	0	0	0	4	$By \equiv 1 \pmod 4$	$(4, 6, 10)$	4	7^*
0	0	0	0	5	$By \equiv 3 \pmod 4$	$(4, 6, 11)$	3	10^*
0	0	0	0	≥ 5	$By \equiv 1 \pmod 4$	$(4, 6, \geq 11)$	4	7^*
0	0	0	0	6	$By \equiv 3 \pmod 4$	$(4, 6, 12)$	0	1
0	0	0	0	≥ 7	$By \equiv 3 \pmod 4$	$(4, 6, \geq 13)$	1	2

Table 5.3.5: The Exponent f_3 for the Conductor of the Frey Curve (5.3.7)

$v_3(A)$	$v_3(y)$	$v_3(B)$	$v_3(x)$	$v_3(Cz^p)$	Conditions	$(v_3(c_4), v_3(c_6), v_3(\Delta))$	f_3	Tate's case
0	0	0	0	0	$A^2By \equiv \pm 2 \pmod 9$	$(2,3,3)$	2	$4P_2$
0	0	0	0	0	$A^2By \not\equiv \pm 2 \pmod 9$	$(2,3,3)$	3	3 not P_2
1	0	0	0	0		$(3,5,6)$	4	5
1	≥ 1	0	0	0		$(3,\geq 6,6)$	2	6
0	1	0	0	0		$(2,\geq 5,3)$	2	4
0	1	0	0	0		$(2,4,3)$	3	3
0	0	1	≥ 0	0		$(\geq 3,4,5)$	5	3
0	0	2	≥ 0	0		$(\geq 4,5,7)$	5	5
0	0	0	≥ 1	0	$A^2By \equiv \pm 4 \pmod 9$	$(\geq 3,3,3)$	2	$4P_2$
0	0	0	≥ 1	0	$A^2By \not\equiv \pm 4 \pmod 9$	$(\geq 3,3,3)$	3	3 not P_2
0	0	0	0	1		$(2,3,4)$	4	3
0	0	0	0	2		$(2,3,5)$	3	5
0	0	0	0	3		$(2,3,6)$	2	6
0	0	0	0	≥ 4		$(2,3,\geq 7)$	2	4

Table 5.3.6: The Exponent f_q, for $q \geq 5$, for the Conductor of the Frey Curve (5.3.7)

$v_q(A)$	$v_q(y)$	$v_q(B)$	$v_q(x)$	$v_q(Cz^p)$	$(v_q(c_4), v_q(c_6), v_q(\Delta))$	f_q	Tate's case
1	≥ 0	0	0	0	$(1,\geq 2,3)$	2	4
0	≥ 1	0	0	0	$(0,\geq 1,0)$	0	1
0	0	1	≥ 0	0	$(\geq 1,1,2)$	2	3
0	0	2	≥ 0	0	$(\geq 2,2,4)$	2	5
0	0	0	≥ 1	0	$(\geq 1,0,0)$	0	1
0	0	0	0	≥ 1	$(0,0,\geq 1)$	1	2

Chapter 6

Power Integral Points

6.1 Perfect Powers and DDSs

In this Chapter we consider an elliptic curve $E/\mathbb{Q}$ in Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{6.1.1}$$

and let a point $P \in E(\mathbb{Q})$ be represented as

$$P = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3}\right) \tag{6.1.2}$$

where A_P, B_P, and C_P are integers with $\gcd(A_PC_P, B_P) = 1$.

We can ask the following questions about B_P:

Question 1. Are there finitely many rational points $P \in E(\mathbb{Q})$ with B_P equal to a perfect power?

Question 2. Are there finitely many rational points $P \in E(\mathbb{Q})$ with B_P equal to a prime?

We shall be interested in solutions of the following equation.

$$B_P = Z^f \quad Z \in \mathbb{Z}_{>1},\ f \in \mathbb{Z}_{>1}. \tag{6.1.3}$$

Definition 6.1.1. Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass model (6.1.1). If $P \in E(\mathbb{Q})$ has its B_P term equal to a perfect power then we shall call that point a *power integral point* (PIP).

The next Theorem goes part way to settling the first question.

Theorem 6.1.2 (Everest, Reynolds, & Stevens [19])**.** *Let E be an elliptic curve in Weierstrass form over $\mathbb{Q}$ as in (4.7.1), and fix an integer $f > 1$. Then there exist only finitely many points P as in (6.1.2) such that B_P is an f^{th} power.*

Proof. See [19, Thm. 1]. □

The result of Theorem 6.1.2 is achieved by extending Theorem 2.6.2 of Siegel's on the finiteness of S-integer solutions for equations of the form $y^2 = f(x)$ of degree $d \geq 3$. As such it is a generalization of Theorem 2.6.2 for the field $\mathbb{Q}$ which states that there are only finitely many integral points on an elliptic curve $E/\mathbb{Q}$, which is the case $Z = 1$ with f arbitrary in (6.1.2).

Siegel [33] proved there are only finitely many (nonzero) points on an elliptic curve with $B_P = 1$. By the result of Theorem 6.1.2 for fixed $f > 1$, there are only finitely many (nonzero) $P \in E(\mathbb{Q})$ with $B_P = Z^f$ for some $Z \in \mathbb{Z}_{>1}$. Since 1 is a perfect power we can imagine PIPs as a generalization of integral points.

However Question 1 above is far from resolved by Theorem 6.1.2, for since f is arbitrary this leaves open the question of whether there are finitely many power integral points on an elliptic curve.

If the answer to Question 1 was affirmative it would be natural to ask:

Question 3. Is there an effective procedure for determining all power integral points?

Much work has been done to make Siegel's Theorem effective and there are many techniques which can find all of the integral points for large classes of elliptic curves [22].

For our purposes it is enough to investigate whether the B_P occur as a perfect power Z^p, for p some prime.

Reynolds has shown the following Theorem:

Theorem 6.1.3 (Reynolds [29, Thm. 1.2]). *Let (B_n) be a DDS generated by a nontorsion point $P \in E(\mathbb{Q})$. If 2 or 3 divide the first term of the DDS then there can be at most a finite number of perfect powers in the sequence. Morever any such power integral point having $B_n = Z^p$ for some integer Z and prime p has p explicitly bounded by E and P.*

Theorem 6.1.3 gives an answer to Question 1 when E has rank 1, no torsion and 2 or 3 divides B_P, for P a generator of $E(\mathbb{Q})$.

6.2 PIPs on Mordell Curves

We now consider the case of B_P occurring as p^{th} power integral points on Mordell curves, which are elliptic curves of the form

$$E_D \colon y^2 = x^3 + D. \tag{6.2.1}$$

We start with a finiteness Theorem of Reynolds.

Theorem 6.2.1 (Reynolds [29, Thm. 1.4]). *Let $E_D \colon y^2 = x^3 + D$, $D \in \mathbb{Z}_{\neq 0}$, be a Mordell curve possessing no integral points. Then in the associated DDS (B_n) there exist at most finitely many perfect powers, with an explicit bound dependent on E_D and P.*

Example 6.2.2. The rank 1 Mordell curve

$$E_{-2} \colon y^2 = x^3 - 2 \tag{6.2.2}$$

has $E_{-2}(\mathbb{Q}) \cong \mathbb{Z}$ with generator $P = (3, 5)$ (alternatively the generator $(3, -5)$). We note that the points $(3, 5)$ and $(3, -5)$ are power integral points as $B_P = 1$, and so cannot invoke the results of Reynolds in Theorem 6.2.1 on finiteness of power integral points.

There is much conjecture as to whether these two points yield the only perfect power values ($B_P = 1$) in the DDS (B_{nP}).

6.3 Fifth Powers on $E_{-2}\colon y^2 = x^3 - 2$

In this Section we give a result of the nonexistence of 5^{th} power integral points on the Mordell curve $E_{-2}\colon y^2 = x^3 - 2$ using the method of Chabauty.

By Example 6.2.2 we have $E_{-2}(\mathbb{Q}) = \langle (3,5) \rangle$, and remarked that $(3, \pm 5)$ are possibly the only PIPs on $E_{-2}\colon y^2 = x^3 - 2$. We have seen in Example 2.7.5 that there exists an explicit 3-isogeny $\sigma\colon E_{54} \to E_{-2}$ between the elliptic curves

$$E_{54}\colon y'^2 = x'^3 + 54 \tag{6.3.1}$$

and

$$E_{-2}\colon y^2 = x^3 - 2, \tag{6.3.2}$$

with $E_{54}(\mathbb{Q}) = \langle (3,9) \rangle$. Now, if $P' \in E_{54}(\mathbb{Q})$ maps to $P \in E_{-2}(\mathbb{Q})$ under this 3-isogeny, and $x'(P') = \frac{A_{P'}}{B_{P'}^2}$, then

$$x(P) = \frac{A_P}{B_P^2} = \frac{A_{P'}^3 + (2 \cdot 3B_{P'}^2)^3}{(3A_{P'}B_{P'})^2}. \tag{6.3.3}$$

We shall use this 3-isogeny to examine the existence of 5^{th} power integral points occurring in the denominator of the image point. In Theorem 6.3.1 we employ Chabauty's method to find the set of rational points on a hyperelliptic curve, which is then utilized in proving $(3, \pm 5)$ are the only 5^{th} power integral points on E_{-2}.

We now examine case by case the possibilities for cancellation in (6.3.3).

Case 1. $p \neq 2, 3$

If $p \neq 2$ or 3 it is trivial to see that if $p \mid A_{P'}B_{P'}$ and $p \mid A_{P'}^3 + (2 \cdot 3B_{P'}^2)^3$ then $p \mid A_{P'}$ and $p \mid B_{P'}$, which is absurd as $\gcd(A_{P'}, B_{P'}) = 1$. So we limit ourselves to the two cases $p = 2$ or $p = 3$.

Case 2. $p = 2$

If $2 \mid A_{P'}^3 + (2 \cdot 3B_{P'}^2)^3$ we must have $2 \mid A_{P'}$ so $2 \nmid B_{P'}$. But then $C_{P'}^2 \equiv 54 \equiv 6 \pmod 8$ which has no solution, and so there can be no cancellation by 2.

Case 3. $p = 3$

If $3 \mid 3A_{P'}B_{P'}$ and $3 \mid A_{P'}^3 + (2 \cdot 3B_{P'}^2)^3$ then $3 \mid A_{P'}$. Conversely if $3 \mid A_{P'}$, then $3^2 \mid 3A_{P'}B_{P'}$, and $3^3 \mid A_{P'}^3$. Now as $3^3 \mid (2 \cdot 3B_{P'}^2)^3$ it follows $3^3 \mid A_{P'}^3 + (2 \cdot 3B_{P'}^2)^3$. Hence cancellation occurs if and only if $3 \mid A_{P'}$.

We now consider the equation of the curve E_{54} to see if any higher power of 3 can divide $A_{P'}$. If $v_3(x') > 1$ then $v_3(x'^3) > 3$ and, since $v_3(54) = 3$, the ultrametric inequality implies $v_3(y'^2) = 3$, which is absurd. So any point on $E_{54}(\mathbb{Q})$ with $v_3(x') > 0$ must have $v_3(x') = 1$.

Hence we only need consider the two cases when either $3 \nmid A_{P'}$ or $3 \parallel A_{P'}$; in the former case there is no cancellation in (6.3.3), and in the latter case there is cancellation by 3^4.

We now consider the case for B_P occurring as a 5^{th} power.

Theorem 6.3.1 (Buck–Everest)**.** *The only points of the elliptic curve*

$$E_{-2}\colon y^2 = x^3 - 2,$$

for which the denominator B_P is a 5^{th} power are $(3, 5)$ and $(3, -5)$.

Proof. By observation there are at least two points in $E_{-2}(\mathbb{Q})$ whose denominator is a 5^{th} power, the points $(3, 5)$ and $(3, -5)$. Let $P \in E_{-2}(\mathbb{Q})$ and let $P' \in E_{54}(\mathbb{Q})$ be such that P' maps to P under the 3-isogeny σ. This is possible since $\sigma(3, 9) = (3, 5)$ so that $\sigma\colon E_{54}(\mathbb{Q}) \to E_{-2}(\mathbb{Q})$ is surjective. There are two cases to consider depending on the divisibility of $A_{P'}$ by 3.

Case (i) If $3 \nmid A_{P'}$ then no cancellation occurs in (6.3.3) and so $A_{P'} = 5^{\text{th}}$ power and $3B_{P'} = 5^{\text{th}}$ power, say $A_{P'} = s^5$, $B_{P'}^2 = \frac{1}{3}t^5$.

Looking at the x-coordinate

$$x(P') = \frac{A_{P'}}{B_{P'}^2} = 9\left(\frac{s}{t}\right)^5.$$

This yields on substituting $x = 9X^5$, $y = Y$ in (6.3.1)

$$Y^2 = 3^6(X^5)^3 + 54,$$

which becomes on letting $3X^3 = x$, $Y = y$, the hyperelliptic curve

$$C_3\colon y^2 = 3x^5 + 54. \tag{6.3.4}$$

The hyperelliptic curve C_3 doesn't have any useful additional structure itself, but we can embed it into the *Jacobian variety of the curve*, which we now explain.

Every nonsingular algebraic curve C of genus $g \geq 1$ has an associated abelian variety J of dimension g into which we can embed C by means of analytic maps. The abelian variety J is known as the *Jacobian variety* of the curve. Moreover it has an abelian group structure, and so we can think of the set $J(\mathbb{Q})$ of rational points on J as an abelian group via some (geometric) group law of composition. If we can find the points on the Jacobian of a curve, this will tell us about the curve that is the preimage of the points. Faltings' Theorem states for a curve C of genus $g \geq 2$, the set of rational points, $C(\mathbb{Q})$, on C is finite. Faltings' proof is ineffective as it provides no algorithm for determining these rational points. However if the rank r of the Mordell–Weil group of J is less than the genus of C, we can use Chabauty's method to try finding the rational points. Chabauty is an effective method for explicitly computing $C(\mathbb{Q})$ provided $r \leq g - 1$, it involves doing local calculations at some prime where C has good reduction.

The Mordell–Weil Theorem tells us that $J(\mathbb{Q})$ is finitely generated. When we compute $J(\mathbb{Q})$ it is actually the generators and relations we compute. So we try to compute $J(\mathbb{Q})$, then determine which points in $J(\mathbb{Q})$ lie on C. Points on J are represented as divisors on C. In `magma` at least one rational point on C must be known, as this plays a role in the algorithm.

Hyperelliptic curves have genus 2 and degree $n > 4$ with n distinct roots. For these curves `magma` requires a generator of the Mordell–Weil group of the Jacobian, which must have rank 1 in this case.

Now for C_3, `magma` computes the full set of rational points on the curve as consisting solely of the point at infinity, and so we have no need of Chabauty in this case, as this proves that no B_P is a 5^{th} power in this case. See Section 6.3.1 for the code.

Case (ii) If $3 \parallel A_{P'}$ then $A_{P'} = 3A'_{P'}$ and

$$\frac{A_{P'}^3 + (2 \cdot 3B_{P'}^2)^3}{(3A_{P'}B_{P'})^2} = \frac{3^3 A_{P'}'^3 + (2 \cdot 3B_{P'}^2)^3}{(3^2 A'_{P'}B_{P'})^2} = \frac{A_{P'}'^3 + 2^3 B_{P'}^6}{3(A'_{P'}B_{P'})^2} = \frac{A_P}{B_P^2}.$$

Since $3(A'_{P'}B_{P'})^2 \neq 5^{\text{th}}$ power there must be further cancellation in the numerator. Therefore $3 \mid {A'_{P'}}^3 + 8B_{P'}^6$.

This implies $A'_{P'} = 5^{\text{th}}$ power and $B_P = 5^{\text{th}}$ power with $A'_{P'} = s^5$ and $B_{P'}^2 = t^5$, say.

Looking at the x-coordinate

$$x(P') = \frac{A_{P'}}{B_{P'}^2} = \frac{3A'_{P'}}{B_{P'}^2} = 3\left(\frac{s}{t}\right)^5.$$

This yields on substituting $x' = 3X^5$, $y' = Y$ in (6.3.1),

$$Y^2 = 27X^{15} + 54,$$

which becomes on letting $X^3 = x$, $Y = y$, the hyperelliptic curve

$$C_4 \colon y^2 = 27x^5 + 54. \tag{6.3.5}$$

Now for C_4 `magma` tells us that $J_4(\mathbb{Q})$ has rank at most 1, so has genus strictly less than the genus of C_4 and we may use Chabauty's method.

By `magma` the full set of rational points consists of $(1 : -9 : 1)$, $(1 : 9 : 1)$, $(1 : 0 : 0)$, and so the only points for which $B_{P'}$ is a 5^{th} power are $(3, 5)$ and $(3, -5)$. □

The `magma` code needed for Theorem 6.3.1 is given in the next Subsection along with relevant explanation.

6.3.1 Magma Code for Theorem 6.3.1

For the computations required in Theorem 6.3.1 we shall need the Chabauty function from `magma`:

```
Chabauty(P : ptC)
```

For a curve C of genus 2 over $\mathbb{Q}$, this returns the full set of rational points. The algorithm involves Chabauty's method combined with a Mordell–Weil sieve. The argument P must be a rational point on the Jacobian of C, which is a generator of the Mordell–Weil group.

The algorithm requires knowledge of one rational point on the curve. (In particular, it cannot be used to show that a curve has no rational points!) Such a point may be supplied as the optional argument `ptC`; otherwise, one is found by searching.

We now give the code used in proving the Theorem 6.3.1.

`magma` code for obtaining the full set of rational points on the hyperelliptic curve $C_3\colon y^2 = 3x^5 + 54$.

```
> R<x> := PolynomialRing(Rationals());
> C3 := HyperellipticCurve(3 * x^5 + 54);
> C3;
Hyperelliptic Curve defined by y^2 = 3*x^5 + 54 over Rational Field
> ptsC3 := Points(C3 : Bound := 1000);
> ptsC3;
{@ (1 : 0 : 0) @}
```

showing the only rational point on $C_3(\mathbb{Q})$ as $(1 : 0 : 0)$, the point at infinity.

`magma` code for obtaining the full set of rational points on the hyperelliptic curve $C_4\colon y^2 = 27x^5 + 54$.

We start by verifying the rank bound of $J_4(\mathbb{Q})$ is 1:

```
> R<x> := PolynomialRing(Rationals());
> C4 := HyperellipticCurve(27 * x^5 + 54);
> C4;
Hyperelliptic Curve defined by y^2 = 27*x^5 + 54 over Rational
    Field
> J4 := Jacobian(C4);
> RankBound(J4);
1
```

Next we find some small points on C_4 and map them to J_4 (using the first point to define the map $C_4 \to J_4$):

```
> ptsC4 := Points(C4 : Bound := 1000);
```

```
> ptsC4;
{@ (1 : 0 : 0), (1 : -9 : 1), (1 : 9 : 1) @}
> ptsJ4 := [ ptsC4[i] - ptsC4[1] : i in [2, 3] ];
> ptsJ4;
[ (x - 1, -9, 1), (x - 1, 9, 1) ]
```

Now we pick a point, say $[x-1, 9, 1]$ on the Jacobian:

```
> PJ1 := J4 ! [ ptsC4[3], ptsC4[1] ];
> PJ1;
(x - 1, 9, 1)
```

Now call the Chabauty function with that point to list all points on C_4:

```
> all_pts := Chabauty(PJ1);
> all_pts;
{ (1 : -9 : 1), (1 : 9 : 1), (1 : 0 : 0) }
```

So by the Chabauty's method these are the full set of points on $C_4(\mathbb{Q})$.

6.4 The Modular Method for Mordell Curves

The method of Chabauty that proved successful in resolving the issue of 5^{th} powers on the Mordell curve $E_{-2}\colon y^2 = x^3 - 2$ in Section 6.3 failed to deliver on square powers. It is here we decided to implement the modular machinery of Chapter 5 to help in determining the existence of PIPs on Mordell curves. To start with we shall need the right Frey curve to work with.

6.4.1 Constructing The Frey Curve

The aim of this Section is to construct the Frey curve corresponding to the equation of the Mordell elliptic curve

$$E_D\colon y^2 = x^3 + D, \qquad D \in \mathbb{Z},\ D \neq 0. \tag{6.4.1}$$

This will allow us to use the modular method to tackle the existence of PIPs on the curve.

So let us assume the n^{th} multiple of a nontorsion point $P \in E_D(\mathbb{Q})$ is a p^{th} power integral point for some prime p, where we write the n^{th} multiple as

$$[n]P = \left(\frac{A_n}{Z_n^{2p}}, \frac{C_n}{Z_n^{3p}}\right), \quad A_n, C_n, Z_n \in \mathbb{Z},\ \gcd(A_n, Z_n) = \gcd(C_n, Z_n) = 1,$$

and the elliptic denominator of $[n]P$ as

$$B_n = Z_n^p.$$

To use the modular method we must apply Barros's Theorem 5.3.3 which considered the equation

$$Ay^2 + Bx^3 = Cz^p,$$

where now the integer coefficients become $A = 1$, $B = -1$, and $C = D$ in the Mordell equation (6.4.1).

We now investigate the Mordell curve by rewriting equation (6.4.1) as the rational equation

$$\left(\frac{C_n}{Z_n^{3p}}\right)^2 = \left(\frac{A_n}{Z_n^{2p}}\right)^3 + D,$$

and then changing it to an equation over the integers

$$C_n^2 - A_n^3 = DZ_n^{6p}, \tag{6.4.2}$$

by multiplying the equation for E_D by Z_n^{6p}, where $\gcd(A_n, C_n, DZ_n) = 1$, for which we require D be 6^{th} powerfree to be certain we have the last gcd condition. Here we note that (6.4.2) does not correspond to any of the equations listed in condition (3) of Theorem 5.3.3, and so we are free to use the Theorem when looking for Frey curves arising modulo p from newforms, but note the inherent limitation for p prime, that $p = 11$ or $p \geq 17$. We also assume that for a prime $p = 11$ or $p \geq 17$, D is p^{th} powerfree in accord with condition (c) of Theorem 5.3.3, since it is 6^{th} powerfree.

The signature of (6.4.2) is $(2, 3, 6p)$, with the characteristic of the equation given by

$$\chi(2, 3, 6p) = \frac{1}{2} + \frac{1}{3} + \frac{1}{6p} - 1 = \frac{1-p}{6p} < 0. \tag{6.4.3}$$

By Darmon and Granville (see Subsection 5.3.2) this shows there are only finitely many integer solutions possible for equation (6.4.2). Hence given any prime $p \geq 2$ there are only finitely many p^{th} power integral points (i.e., another proof of Theorem 6.1.2 for the specific case of Mordell curves).

The Frey curve associated to (6.4.2) is then

$$E_{B,n}\colon Y^2 = X^3 - 3A_nX + 2C_n. \tag{6.4.4}$$

The associated quantities with (6.4.4) are

$$\begin{gathered} a_1 = a_2 = a_3 = 0, \quad a_4 = -3A_n, \quad a_6 = 2C_n, \\ b_2 = 0, \quad b_4 = -2 \cdot 3A_n, \quad b_6 = -2^3C_n, \quad b_8 = -3^2A_n^2, \\ c_4 = 2^4 3^2 A_n, \quad c_6 = 2^6 3^3 C_n, \\ \Delta_{\min} = 2^6 3^3 (A_n^3 - C_n^2) = -2^6 3^3 D Z_n^{6p}, \quad j = -\frac{2^6 3^3 A_n^3}{D Z_n^{6p}}. \end{gathered} \tag{6.4.5}$$

Now by Theorem 5.3.3 we have:

(1) The minimal discriminant of $E_{B,n}$ is

$$\Delta_{\min} = \begin{cases} -2^6 3^3 D Z_n^{6p} & \text{if } Z_n \text{ is odd,} \\ -2^{-6} 3^3 D Z_n^{6p} & \text{if } Z_n \text{ is even.} \end{cases}$$

(2) The conductor N of the curve $E_{B,n}$ is given by

$$N = 2^{f_2} 3^{f_3} \operatorname{rad}_{2,3}(DZ_n),$$

where f_2 and f_3 are given in Tables 5.3.4 and 5.3.5 respectively.

(3) Suppose that $p = 11$ or $p \geq 17$, then $E_{B,n} \sim_p f$ for some newform f of level

$$N_p = 2^{f_2} 3^{f_3} \operatorname{rad}_{2,3}(D),$$

where f_2 and f_3 are given in Tables 5.3.4 and 5.3.5 respectively.

To investigate the existence of power integral points on E_D we must show, using the Modularity Theorem and our Frey curve, that none of the rational newforms of level N_p are associated with any $E_{B,n}$ for $n \geq 1$, with any necessary bound on p. Any irrational newforms will have to be dealt with using Proposition 5.2.9.

We now look case by case at (6.4.2) in search of any nontrivial solutions, by which we mean $A_n C_n Z_n \neq 0$.

6.4.2 Mordell Tables for the Exponents f_2, and f_3

This thesis is concerned with Mordell elliptic curves, and as such it will be beneficial to construct tables exclusively for such curves, for the exponents f_2, and f_3.

To do so we first derive the following valuations for c_2 and c_3 for the primes 2 and 3 from the quantities (6.4.5) and the same for the valuations at 2 and 3 of $\Delta_{\min}$, where for brevity we write simply Δ for $\Delta_{\min}$ from now on unless otherwise stated.

$$
\begin{aligned}
v_2(c_4) &= 4 + v_2(A_n), \\
v_2(c_6) &= 6 + v_2(C_n), \\
v_2(\Delta) &= \begin{cases} 6 + v_2(D) & \text{if } Z_n \text{ is odd}, \\ -6 + v_2(D) + 6p v_2(Z_n) & \text{if } Z_n \text{ is even}, \end{cases} \\
v_3(c_4) &= 2 + v_3(A_n), \\
v_3(c_6) &= 3 + v_3(C_n), \\
v_3(\Delta) &= 3 + v_3(D) + 6p v_3(Z_n).
\end{aligned}
$$

With this done we now refer to the tables of Papadopolous (see Tables 5.3.1, and 5.3.2), to compute values for f_2 and f_3.

Since we wish to use Theorem 5.3.3, throughout we assume that the prime exponent of Z_n has $p = 11$ or $p \geq 17$.

Exponent f_2

We split up the case for f_2 into whether Z_n is even or odd.

Case 1. Z_n is even

Since we assume A_n, C_n, and Z_n are pairwise coprime the equation $DZ_n^{6p} = C_n^2 - A_n^3$ has A_n and C_n both odd, as both cannot be even.

The congruences for the variables C_n and Z_n are

$$C_n^2 \equiv 1 \pmod 8, \quad Z_n^{6p} \equiv 0 \pmod 8.$$

On looking at the equation $C_n^2 - DZ_n^{6p} = A_n^3$ modulo 8 we have the congruence

$$A_n \equiv A_n^3 = C_n^2 \equiv 1 \pmod 8.$$

We have $v_2(A_n) = 0$, $v_2(C_n) = 0$, $v_2(DZ_n^{6p}) = v_2(D) + 6pv_2(Z_n) \geq 6p$, and so $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, \geq 13)$. This gives two possible values for f_2 according to Table 5.3.4: $f_2 = 1$ with $C_n \equiv 1 \pmod 4$, or $f_2 = 4$ with $C_n \equiv 3 \pmod 4$.

Now by Table 5.3.4 we observe that when $v_2(DZ_n^p) > 1$ with condition $C_n \equiv 1 \pmod 4$, then f_2 is less than when $C_n \equiv 3 \pmod 4$. We note a consequence of working with Mordell curves is that the negative of a nonzero point $(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3})$ is just $(\frac{A_n}{B_n^2}, -\frac{C_n}{B_n^3})$. Hence the condition $C_n \equiv 3 \pmod 4$ is equivalent to that of $-C_n \equiv 1 \pmod 4$, in the sense that the negative of the point is also on the curve. As it is in our interests to seek to limit the number of newforms in later work, we exploit this symmetry and take $C_n \equiv 1 \pmod 4$ in working out f_2 from henceforth. As such, the case of $C_n \equiv 3 \pmod 4$ shall not be further considered.

Hence if Z_n is even it is of no matter whether D is odd or even when working out f_2. If Z_n is odd however we must split the cases into those of D being even or odd.

Case 2.(i). Z_n is odd, and D is even

If Z_n is odd with D even then we have the congruences

$$C_n^2 \equiv 1 \pmod 8, \quad A_n \equiv 1 - D \pmod 8, \quad Z_n^{6p} \equiv 1 \pmod 8.$$

We also have $v_2(A_n) = 0$, $v_2(C_n) = 0$, $v_2(DZ_n^{6p}) = v_2(D)$, and so

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, 6 + v_2(D)) = (4, 6, \geq 7).$$

This gives the possible values for f_2 dependent ultimately on $v_2(D)$. This subdivides into five cases, with the case of $v_2(D) \geq 6$ absent since we assume D is 6^{th} powerfree.

Case I. $v_2(D) = 1$**,** $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, 7)$

This gives $f_2 = 7$.

Case II. $v_2(D) = 2$**,** $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, 8)$

For $v_2(D) = 2$, Table 5.3.4 cites three cases having $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, 8)$, each having a congruence condition $AB(x - 2Ay) \pmod{16}$, where for our case $A = 1$, $B = -1$, $x = A_n$, $y = C_n$ giving the conditions:

(a) $2C_n - A_n \equiv 5 \pmod{16}$ giving $f_2 = 2$.

(b) $2C_n - A_n \equiv 9 \pmod{16}$ giving $f_2 = 3$.

(c) $2C_n - A_n \equiv 1, 13 \pmod{16}$ giving $f_2 = 4$.

Moreover since $v_2(C_n) = 0$, and $A_n \equiv 1 - D \pmod 8$ we have the congruence conditions:

(d) $2C_n - A_n \equiv D + 1$ or $D + 5 \pmod 8$.

For each of the congruences, in (a), (b), (c), and (d) we express $2C_n - A_n$ as a value rather than a congruence. By doing this we obtain an expression for D, where we note the situation $D \equiv 0 \pmod 8$ cannot occur since it implies $v_2(D) > 2$. The eight cases for $2C_n - A_n$ can be expressed, with $k, j \in \mathbb{Z}$, as:

(i) $D + 1 + 8k = 5 + 16j \Rightarrow D = 8(2j - k) + 4$ giving $f_2 = 2$.

(ii) $D + 5 + 8k = 5 + 16j \Rightarrow D = 8(2j - k)$ which cannot occur.

(ii) $D + 1 + 8k = 9 + 16j \Rightarrow D = 8(2j - k + 1)$ which cannot occur.

(iv) $D + 5 + 8k = 9 + 16j \Rightarrow D = 8(2j - k) + 4$ giving $f_2 = 3$.

(v) $D + 1 + 8k = 1 + 16j \Rightarrow D = 8(2j - k)$ which cannot occur.

(vi) $D + 5 + 8k = 1 + 16j \Rightarrow D = 8(2j - k) - 4$ giving $f_2 = 4$.

(vii) $D + 1 + 8k = 13 + 16j \Rightarrow D = 8(2j - k) + 12$ giving $f_2 = 4$.

(viii) $D + 5 + 8k = 13 + 16j \Rightarrow D = 8(2j - k + 1)$ which cannot occur.

Case III. $v_2(D) = 3$**,** $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, 9)$

This gives $f_2 = 5$.

Case IV. $v_2(D) = 4$**,** $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, 10)$

This gives $f_2 = 3$.

Case V. $v_2(D) = 5$**,** $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, 11)$

This gives $f_2 = 3$.

Case 2.(ii). Z_n **is odd, and** D **is odd**

If Z_n is odd with D odd then we have the congruence $Z_n^{6p} \equiv 1 \pmod 8$ with A_n and C_n of different parities. The two cases are:

Case I. C_n **is odd, and** A_n **is even**

If C_n is odd and A_n is even we have

$$C_n^2 \equiv 1 \pmod 8, \quad A_n^3 = C_n^2 - DZ_n^{6p} \equiv 1 - D \pmod 8.$$

Now $A_n^3 \equiv 0 \pmod 8$, so $D \equiv 1 \pmod 8$. We have $v_2(C_n) = 0$, $v_2(A_n) \geq 1$, $v_2(DZ_n^{6p}) = 0$, and so $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4 + v_2(A_n), 6, 6) = (\geq 5, 6, 6)$, from which the tables give $f_2 = 6$.

Case II. C_n **is even, and** A_n **is odd**

If C_n is even we have the two cases $C_n^2 \equiv 0$ or $4 \pmod 8$. Now A_n is odd so we subdivide the two cases:

$$\text{(i)} \quad C_n \equiv 0 \pmod 4 \;\Rightarrow\; A_n \equiv A_n^3 = C_n^2 - DZ_n^{6p} \equiv -D \pmod 8,$$

or

$$\text{(ii)} \quad C_n \equiv 2 \pmod 4 \;\Rightarrow\; A_n \equiv A_n^3 = C_n^2 - DZ_n^{6p} \equiv 4 - D \pmod 8.$$

For the case $C_n \equiv 0 \pmod 4$ we have $v_2(C_n) = t \geq 2$, $v_2(A_n) = 0$, $v_2(DZ_n^{6p}) = 0$, and so $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6+t, 6)$. For the case $C_n \equiv 2 \pmod 4$ we have $v_2(C_n) = 1$, $v_2(A_n) = 0$, $v_2(DZ_n^{6p}) = 0$, and so $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 7, 6)$.

Both of these cases are then subdivided into the two cases:

Case II.(i). $C_n \equiv 0 \pmod 4$

If $C_n \equiv 0 \pmod 4$ then we have the two cases:

(1) If $A_n \equiv 1 \pmod 4$, then $D \equiv 3 \pmod 4$, and we have $f_2 = 6$.

(2) If $A_n \equiv 3 \pmod 4$, then $D \equiv 1 \pmod 4$, and we have $f_2 = 5$.

Case II.(ii). $C_n \equiv 2 \pmod 4$

If $C_n \equiv 2 \pmod 4$ then we have the two cases:

(1) If $A_n \equiv 1 \pmod 4$, then $D \equiv 1 \pmod 4$, and we have $f_2 = 5$.

(2) If $A_n \equiv 3 \pmod 4$, then $D \equiv 3 \pmod 4$, and we have $f_2 = 6$.

So, in summary, if $D \equiv 1 \pmod 4$ then $f_2 = 5$, and if $D \equiv 3 \pmod 4$ then $f_2 = 6$.

Exponent f_3

Since we assume A_n, C_n, and Z_n are pairwise coprime we look case by case at 3 dividing either of the variables A_n, C_n, Z_n, or D.

Case 1. $3 \mid A_n$

If $3 \mid A_n$, with $v_3(A_n) \geq 1$, we must have $v_3(C_n) = 0$, and $v_3(DZ_n^{6p}) = 0$. We then have

$$(v_3(c_4), v_3(c_6), v_3(\Delta)) = (\geq 3, 3, 3).$$

This gives $f_3 = 2$ with $C_n \equiv \pm 4 \pmod 9$, or $f_3 = 3$ with $C_n \not\equiv \pm 4 \pmod 9$. For the congruence on D we have $C_n^2 \equiv DZ_n^{6p} \pmod 9$, where $Z_n^{6p} \equiv 1 \pmod 9$ and so D has to be a square modulo 9, these being $1, 4, 7 \pmod 9$; hence $D \equiv 1 \pmod 3$.

Case 2. $3 \mid C_n$

If $3 \parallel C_n$, we have $v_3(C_n) = 1$, $v_3(A_n) = 0$, $v_3(DZ^{6p}) = 0$, and so

$$(v_3(c_4), v_3(c_6), v_3(\Delta)) = (2, 4, 3).$$

This gives $f_3 = 3$. If $3 \mid C_n$, with $v_3(C_n) \geq 2$, then $v_3(A_n) = 0$, $v_3(DZ_n^{6p}) = 0$, and so

$$(v_3(c_4), v_3(c_6), v_3(\Delta)) = (2, \geq 5, 3),$$

which gives $f_3 = 2$. We note if $3 \mid C_n$ then the congruences $Z_n^{6p} \equiv 1 \pmod 9$, and $A_n^3 \equiv \pm 1 \pmod 9$ imply that $D \equiv \pm 1 \pmod 9$.

Case 3. $3 \mid Z_n$

If $3 \mid Z_n$, we have $v_3(A_n) = 0$, $v_3(C_n) = 0$, $v_3(DZ_n^{6p}) = v_3(D) + 6pv_3(Z_n) \geq 6p$, and so

$$(v_3(c_4), v_3(c_6), v_3(\Delta)) = (2, 3, \geq 3 + 6p).$$

This gives $f_3 = 2$. We note possible congruences are $C_n^2 \equiv 1, 4, 7 \pmod 9$ and $A_n^3 \equiv \pm 1 \pmod 9$, but since $C_n^2 \equiv A_n^3 \pmod 9$ we must have $C_n^2 \equiv A_n^3 \equiv 1 \pmod 3$, hence $A_n \equiv 1 \pmod 3$.

Case 4. $3 \nmid A_n C_n Z_n$

If 3 does not divide either of A_n, C_n, or Z_n we have to take account of $3 \mid D$ or not. In such a case $v_3(A_n) = 0$, $v_3(C_n) = 0$, $v_3(DZ_n^{6p}) = v_3(D)$, and so

$$(v_3(c_4), v_3(c_6), v_3(\Delta)) = (2, 3, 3 + v_3(D)).$$

This gives a possible subdivision into five cases according to $v_3(D)$. We note as soon as $v_3(D) \geq 1$ we have $A_n \equiv 1 \pmod 3$ since $C_n^2 \equiv 1 \pmod 3$.

Case I. $v_3(D) = 0$, $(v_3(c_4), v_3(c_6), v_3(\Delta)) = (2, 3, 3)$

This gives $f_3 = 2$ or 3 dependent on whether we end at case 4 or 3 of Tate's algorithm respectively. If $A_n^3 \equiv 1 \pmod 9$ we have $D \equiv C_n^2 - A_n^3 \equiv 0 \pmod 3$, which cannot occur, and so $A_n^3 \equiv -1 \pmod 9$ with $D \equiv C_n^2 - A_n^3 \equiv 2 \pmod 3$.

Case II. $v_3(D) = 1$, $(v_3(c_4), v_3(c_6), v_3(\Delta)) = (2, 3, 4)$

This gives $f_3 = 4$.

Case III. $v_3(D) = 2$, $(v_3(c_4), v_3(c_6), v_3(\Delta)) = (2, 3, 5)$

This gives $f_3 = 3$.

Case IV. $3 \leq v_3(D) \leq 5$, $(v_3(c_4), v_3(c_6), v_3(\Delta)) = (2, 3, \geq 6)$

This gives $f_3 = 2$.

These results for f_2 and f_3 are collated in Tables 6.4.1 and 6.4.2 respectively. We have omitted from the table the cases when Z_n is even, in which case $f_2 = 1$, and when $3 \mid Z_n$, in which case $f_3 = 2$. The tables also indicate, in general, a decrease in f_2 and f_3 with higher valuations $v_2(D)$ and $v_3(D)$.

We note $c_4 = 2^4 3^2 A_n$, $c_6 = 2^6 3^3 C_n$, so in checking for condition P_2 we have $v_3(c_4) \geq 2$ always, and $v_3(c_6) = 3$ whenever $3 \nmid C_n$. The condition P_2 is:

$$c_{6,3}^2 + 2 \equiv 3c_{4,2} \pmod 9, \quad \text{where } c_{4,2} = c_4/3^2, \text{ and } c_{6,3} = c_6/3^3. \tag{6.4.6}$$

Table 6.4.1: Value of the Exponent f_2, for $C_n \not\equiv 3 \pmod 4$ and Z_n odd, for Mordell Curves

$v_2(A_n)$	$v_2(C_n)$	Conditions on D	$(v_2(c_4), v_2(c_6), v_2(\Delta_{\min}))$	f_2	Tate's case
≥ 1	0	$D \equiv 1 \pmod 8$	$(\geq 5, 6, 6)$	6	3
0	≥ 1	$D \equiv 1 \pmod 4$	$(4, \geq 7, 6)$	5	4^*
0	≥ 1	$D \equiv -1 \pmod 4$	$(4, \geq 7, 6)$	6	3^*
0	0	$v_2(D) = 1$	$(4, 6, 7)$	7	3
0	0	$v_2(D) = 2$	$(4, 6, \geq 11)$	2	8^*
0	0	$v_2(D) = 2$	$(4, 6, 8)$	3	7^*
0	0	$v_2(D) = 2$	$(4, 6, 8)$	4	6^*
0	0	$v_2(D) = 3$	$(4, 6, 9)$	5	6
0	0	$v_2(D) = 4$	$(4, 6, 10)$	3	9^*
0	0	$v_2(D) = 5$	$(4, 6, 11)$	3	10^*

Table 6.4.2: Value of the Exponent f_3, for $3 \nmid Z_n$, for Mordell Curves

$v_3(A_n)$	$v_3(C_n)$	Conditions on D	$(v_3(c_4), v_3(c_6), v_3(\Delta_{\min}))$	f_3	Tate's case
≥ 1	0	$D \equiv 1 \pmod 3$	$(\geq 3, 3, 3)$	2	$4P_2$
≥ 1	0	$D \equiv 1 \pmod 3$	$(\geq 3, 3, 3)$	3	3 not P_2
0	1	$D \equiv \pm 1 \pmod 9$	$(2, \geq 5, 3)$	2	4
0	1	$D \equiv \pm 1 \pmod 9$	$(2, 4, 3)$	3	3
0	0	$D \equiv 2 \pmod 3$	$(2, 3, 3)$	2	$4P_2$
0	0	$D \equiv 2 \pmod 3$	$(2, 3, 3)$	3	3 not P_2
0	0	$v_3(D) = 1$	$(2, 3, 4)$	4	3
0	0	$v_3(D) = 2$	$(2, 3, 5)$	3	5
0	0	$v_3(D) = 3$	$(2, 3, 6)$	2	6
0	0	$4 \leq v_3(D) \leq 5$	$(2, 3, 7)$	2	4

Proposition 6.4.1. *Let the Diophantine equation associated to the Mordell curve* $E_D\colon y^2 = x^3 + D$ *and point* $P = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right)$

$$C_n^2 = A_n^3 + DB_n^6. \tag{6.4.7}$$

Then if $D \not\equiv 0, 1, 3, 6, 8 \pmod 9$ *we have* $3 \nmid C_n$. *Moreover, if* $D \not\equiv \pm 1 \pmod 9$ *then*

$$A_n^3 \equiv -D \pmod 9 \iff 3 \nmid C_n.$$

Proof. By analysing (6.4.7) we find if $9 \nmid D$ then at most one of A_n, B_n, C_n is divisible by 3. If $3 \nmid A_nB_n$ then $A_n^3 \equiv \pm 1 \pmod 9$, and $B_n^6 \equiv 1 \pmod 9$; so $C_n^2 \equiv D \pm 1 \pmod 9$. Thus if $D \not\equiv \pm 1 \pmod 9$, then $3 \nmid C_n$. Now if $D \equiv \pm 1 \pmod 9$ then $3 \nmid A_nB_n$.

For the case $3 \mid C_n$, we see from the previous argument that if $D \equiv \pm 1 \pmod 9$ then $3 \nmid A_nB_n$. So $A_n^3 + DB_n^6 \equiv A_n^3 \pm 1 \equiv 0 \pmod 9$, then

$$A_n^3 \equiv -D \pmod 9 \iff 3 \nmid C_n.$$

□

Chapter 7

The Rational Newform Case

We have seen in Chapter 5 that an elliptic curve E defined over $\mathbb{Q}$ can arise from an irrational newform or a rational newform. Hence a PIP on the curve $E/\mathbb{Q}$ may correspond to a rational or irrational newform, dependent on the Frey curve it arises from. In light of this the following definition seems desirable.

Definition 7.0.2. If a power integral point corresponds to a rational newform we shall call this a *rational PIP*, and if it corresponds to a irrational newform we shall call this an *irrational PIP*.

In this Chapter we give an algorithm for bounding the exponent p in the case that the Frey curves constructed in Subsection 6.4.1 arise from rational newforms.

7.0.3 Periodicity

We want to follow the same kind of reasoning as was done with the resolution of which are the perfect powers occurring in the Fibonacci and the Lucas sequences by Bugeaud, Mignotte, and Siksek (see [8]). In the case of these sequences a successful employment of classical and modular approaches was achieved by looking at the periodicity of perfect powers modulo the number in question occurring in the sequence. The inherent equations associated to the sequences had congruence conditions put on the index n in the sequence. These equations were then associated to Frey curves, followed by techniques of level lowering and elimination of newforms. Finally the necessary bounds were put on the possible values for the

prime exponents of the powers by using linear forms in logarithms, and generating small sets of congruences modulo a large modulus. We wish to do the same with the equation $B_n = Z_n^p$.

7.0.4 The Frey Curve Modulo Primes

We have seen in (6.4.4) that the correct Frey curve for our problem is given by

$$E_{B,n}\colon Y^2 = X^3 - 3A_nX + 2C_n.$$

Now if the 3-tuple (A_n, C_n, B_n) were periodic modulo a prime ℓ we would have the Frey curves $E_{B,n}$ periodic as well. However the (B_n) sequences are not periodic modulo a prime ℓ, but we do know by Corollary 4.5.9 that for a point $P \in E_D(\mathbb{Q})$ the division polynomials 3-tuple $(\Phi_n(P), \Omega_n(P), \Psi_n(P))$ modulo a prime ℓ is periodic with period $r\tau$, where r is the rank of the prime ℓ, and τ is the multiplier of r which gives the period as given by Corollary 4.5.9.

So if we allow the n^{th} multiple of a point to be written instead as

$$[n]P = \left(\frac{U_n}{W_n^2}, \frac{V_n}{W_n^2}\right), \quad U_n,\ V_n,\ W_n \in \mathbb{Z},$$

where $W_n = \widehat{\Psi}_n(P)$, $U_n = \widehat{\Phi}_n(P)$, $V_n = \widehat{\Omega}_n(P)$ are the scaled versions of the division polynomials (see Proposition 4.7.2), then we can look instead at the associated curve

$$E_{W,n}\colon Y^2 = X^3 - 3U_nX + 2V_n, \tag{7.0.1}$$

which has $E_{W,n}$ periodic modulo ℓ, but is a twist of the Frey curve $E_{B,n}$.

7.0.5 Mordell DDSs and Twists of the Frey Curve

The Mordell curves $E_D\colon y^2 = x^3 + D$ with nontorsion point $P \in E_D(\mathbb{Q})$ have the associated EDSs (W_n) which gives us a curve $E_{W,n}$ defined over $\mathbb{Q}$, for each $n \in \mathbb{Z}_{n\neq 0}$, given by (7.0.1).

An immediate question is what happens if the EDS value equals some integral

multiple value of the denominator sequence, i.e., $W_n = d_n B_n$, for some $d_n \in \mathbb{Z}$. Explicity how does this situation affect the trace at a prime ℓ. The answer lies in the fact that the curves $E_{W,n}$ are quadratic twists of the $E_{B,n}$. Now if $d_n \neq \pm 1$, then d_n is divisible only by primes of bad reduction of P.

Now we can compute the trace of Frobenius Frob_ℓ on $E_{W,n}$ (which are periodic modulo ℓ) and compare back to the trace Frob_ℓ on $E_{B,n}$, which differ at most by a sign because $E_{W,n}$ is a quadratic twist of $E_{B,n}$. This is made precise for ℓ an odd prime, if $\ell \nmid d_n$, by Theorem 2.12.2; we have

$$a_\ell(E_{W,n}) = \left(\frac{d_n}{\ell}\right) a_\ell(E_{B,n}). \tag{7.0.2}$$

If all primes of bad reduction of P are quadratic residues modulo ℓ, and $\ell \equiv 1 \pmod 4$ then we always get the positive sign and the traces are equal. Henceforth we stick with the notation $E_{B,n}$ with the tacit understanding that we are in fact using its quadratic twist $E_{W,n}$.

7.1 Bounding the Exponent p

For the case of Mordell curves $E_D \colon y^2 = x^3 + D$, the associated Frey curve $E_{B,n}$ from (6.4.4) has a conductor given by $N_{E_{B,n}} = 2^{f_2} 3^{f_3} \operatorname{rad}_{2,3}(DB_n)$. If $E_{B,n}$ arises modulo p from some newform f then we write $E_{B,n} \sim_p f$. After level lowering we find the newform f has level $N_p = 2^{f_2} 3^{f_3} \operatorname{rad}_{2,3}(D)$, where we associate to each newform f of level N_p the corresponding elliptic curve E_f of conductor N_p by modularity.

If we assume the Mordell curve contains a power integral point, which we denote by $B_n = Z_n^p$, then by Kraus and Oesterlé (5.2.3) we subdivide into two cases dependent on whether a prime $\ell \geq 5$ has $\ell \nmid \operatorname{rad}_{2,3}(DZ_n)$, corresponding to good reduction on $E_{B,n}$ and on E_f at ℓ, or $\ell \geq 5$ has $\ell \mid \operatorname{rad}_{2,3}(Z_n)$, $\ell \nmid \operatorname{rad}_{2,3}(D)$, corresponding to multiplicative reduction on $E_{B,n}$ and good reduction on E_f at ℓ. Our choice of $\ell \geq 5$ is due to the fact that both 2 and 3 always divide $N_{E_{B,n}}$ and N_p, since we always have $f_2 \geq 1$ and $f_3 \geq 2$ by Tables 6.4.1, and 6.4.2.

Our method of attack will be to compare traces $a_\ell(E_{B,n})$ with coefficients $c_\ell(f)$ until we have ruled out the possibility, if we can, of any rational newform f cor-

responding modulo p to some Frey curve $E_{B,n}$. However there is a price to pay in doing this: if we use primes up to $\ell \leq \ell_r$ in comparing $a_\ell(E_{B,n})$ with $c_\ell(f)$ in order to conclude that f does not correspond to $E_{B,n}$, then we are assuming $p \geq \ell_r + 1 + 2\sqrt{\ell_r} = (\sqrt{\ell_r}+1)^2$, and so we cannot immediately rule out any p^{th} powers having p less than $(\sqrt{\ell_r}+1)^2$ in the rational newform case. The following Proposition 7.1.1, Lemma 7.1.2, 7.1.3 codifies these statements.

Proposition 7.1.1. *Let $E_{B,n}$ be the Frey curve*

$$E_{B,n}\colon Y^2 = X^3 - 3A_nX + 2C_n. \tag{7.1.1}$$

Let ℓ_0 be a prime of good reduction for $E_{B,n}$, and suppose f is a rational newform having a level which equals the right conductor N_p for prime p and index n. If $p \geq 4\sqrt{\ell_0}$ then for the correspondence $E_{B,n} \sim_p f$ we must have the equality $a_{\ell_0}(E_{B,n}) = c_{\ell_0}(f)$, and if $a_{\ell_0}(E_{B,n}) \neq c_{\ell_0}(f)$ then $E_{B,n} \not\sim_p f$. Moreover any primes $p < 4\sqrt{\ell_0}$ and dividing $\Big(a_{\ell_0}(E_{B,n}) - c_{\ell_0}(f)\Big) > 0$ have the correspondence $E_{B,n} \sim_p f$.

Let ℓ_1 be a prime of multiplicative reduction for $E_{B,n}$, and suppose g is a rational newform having a level which equals the right conductor N_q for prime q and index n. If $q \geq (\sqrt{\ell_1}+1)^2$ then $E_{B,n} \not\sim_q g$. Moreover any primes $q < (\sqrt{\ell_1}+1)^2$ and dividing $\Big(a_{\ell_1}(E_{B,n})(\ell_1+1) - c_{\ell_1}(g)\Big) > 0$ have the correspondence $E_{B,n} \sim_q g$.

Proof. Let ℓ be a prime of good reduction for $E_{B,n}$, so that by Proposition 5.2.3

$$a_\ell(E_{B,n}) \equiv c_\ell(f) \pmod{p}, \quad \ell \nmid N_{E_{B,n}}, \ell \nmid N_p. \tag{7.1.2}$$

The lower and upper bounds derived from Theorem 2.11.3 for the trace $a_\ell(E_{B,n})$ are given by

$$-2\sqrt{\ell} \leq a_\ell(E_{B,n}) \leq 2\sqrt{\ell}. \tag{7.1.3}$$

Since the same bounds hold for the newform coefficient: $|c_\ell(f)| \leq 2\sqrt{\ell}$, we find the difference between $a_\ell(E_{B,n})$ and $c_\ell(f)$ is bounded by

$$-4\sqrt{\ell} \leq a_\ell(E_{B,n}) - c_\ell(f) \leq 4\sqrt{\ell}. \tag{7.1.4}$$

Therefore if we take $p \geq 4\sqrt{\ell}$ then the congruence in (7.1.2) taken modulo p is

forced to become an equality. To see why let us assume $p \mid \left(a_\ell(E_n) - c_\ell(f)\right) \neq 0$, then by (7.1.4) this implies p divides an integer less than $4\sqrt{\ell}$: a contradiction, and so for (7.1.2) to hold with $p \geq 4\sqrt{\ell}$ we must have $a_\ell(E_{B,n}) = c_\ell(f)$ for f to arise modulo p from $E_{B,n}$. Moreover if $p < 4\sqrt{\ell}$, and $p \mid \left(a_\ell(E_{B,n}) - c_\ell(f)\right) > 0$, for some n, f, then $E_{B,n} \sim_p f$.

Now let ℓ be a prime of multiplicative reduction for $E_{B,n}$, so that by Proposition 5.2.3

$$c_\ell(f) \equiv a_\ell(E_{B,n})(\ell+1) \pmod{p}, \quad \ell \parallel N_{E_{B,n}}, \ell \nmid N_p. \tag{7.1.5}$$

where $a_\ell(E_{B,n}) = 1$ or -1 in the case of split or nonsplit multiplicative reduction respectively by Corollary 2.11.8. In similar fashion to the good reduction case we find the difference between $a_\ell(E_{B,n})(\ell+1)$ and $c_\ell(f)$ is bounded by

$$-2\sqrt{\ell} - (\ell+1) \leq c_\ell(f) - a_\ell(E_{B,n})(\ell+1) \leq 2\sqrt{\ell} + (\ell+1). \tag{7.1.6}$$

We note that unlike the good reduction case we can never force the congruence (7.1.5) to become the equality $c_\ell(f) = a_\ell(E_{B,n})(\ell+1)$ because $|c_\ell(f)| \leq 2\sqrt{\ell} < \ell + 1$ for all primes ℓ.

Hence by the inequality (7.1.6), if we take $p \geq \ell + 1 + 2\sqrt{\ell}$ then we can be sure $E_{B,n} \not\sim_p f$. Moreover if $p < \ell + 1 + 2\sqrt{\ell}$, and $p \mid \left(a_\ell(E_{B,n})(\ell+1) - c_\ell(f)\right) > 0$ for some n, f, then $E_{B,n} \sim_p f$. □

Finally we note in Proposition 7.1.1 the case of additive reduction, which has $a_\ell(E_{B,n}) = 0$ by Corollary 2.11.8, can not occur if we wish to invoke Proposition 5.2.3.

Lemma's 7.1.2, 7.1.3 explain how we use the bounds from Proposition 7.1.1.

Lemma 7.1.2. *Let a prime $\ell \geq 5$ divide a term B_n. Then the reduction of the Frey curve (7.1.1) modulo ℓ has a node, and we get multiplicative reduction (and $a_\ell(E_{B,n}) = \pm 1$).*

Proof. If a prime $\ell \geq 5$ divides B_n, then since A_n, B_n, and C_n are pairwise coprime, by (6.4.5) we have $\Delta = 2^6 3^3 (A_n^3 - C_n^2) = -2^6 3^3 D B_n^6 \equiv 0 \pmod{\ell}$, and $c_4 = 2^4 3^2 A_n \not\equiv 0 \pmod{\ell}$. By Proposition 2.3.2 (b) we then have that $\tilde{E}_{B,n}$

(mod ℓ) has a node, so we always get multiplicative reduction (and $a_\ell(E_{B,n}) = \pm 1$ by Corollary 2.11.8) at primes $\ell \mid B_n$. □

Note that we must have $\ell \geq 5$ in Lemma 7.1.2, since if $\ell = 2$ or 3 then $\Delta \equiv c_4 \equiv 0 \pmod{\ell}$ with $\tilde{E}_{B,n} \pmod{\ell}$ then having a cusp (and $a_\ell(E_{B,n}) = 0$ by Corollary 2.11.8), which cannot occur if we wish to invoke Proposition 5.2.3.

Lemma 7.1.3. *Let $P = \left(\frac{A_1}{B_1^2}, \frac{C_1}{B_1^3}\right)$ be a nontorsion point on the Mordell curve $E_D\colon y^2 = x^3 + D$. Let $\ell \geq 5$ not divide B_1 and not be a prime of singular reduction. Let $r(\ell) \geq 5$ be the rank of apparition of a prime ℓ, with $r(\ell)$ dividing the index n of a term in the sequence (B_n); then the Frey curve (7.1.1) has multiplicative reduction at ℓ.*

Proof. Let $(\Psi_n(P))$ be the (fractional) EDS associated to the curve-point pair (E_D, P), formed by the division polynomials evaluated at P. Now if $(\Psi_n(P))$ is not an integer sequence, it is equivalent to a normalised one, say (W_n) having $W_n = \theta^{n^2-1}\Psi_n(P)$ for some rational constant θ.

Then we can use Theorems 4.5.3 and 4.5.2 which say for an integer EDS (W_n), if $\ell \nmid \gcd(W_2, W_3)$ then

$$W_n \equiv 0 \pmod{\ell} \quad \text{if and only if} \quad n \equiv 0 \pmod{r(\ell)},$$

where $r(\ell)$ is the rank of apparition for the prime ℓ in (W_n). Now (W_n) will differ from the integer DDS in general, where for $\ell \mid B_1$ we have the point $P \equiv O \pmod{\ell}$, and any singular reduction coming from primes having $v_\ell(\Psi_2(P)) > 0$ and $v_\ell(\Psi_3(P)) > 0$ by 3.2.4. Away from these primes we have $v_\ell(B_n) = v_\ell(\Psi_n(P))$ by Proposition 4.7.2.

Now suppose we are checking at a prime ℓ with rank of apparition $r(\ell)$, and that $n \equiv 0 \pmod{r(\ell)}$. Then we have $\ell \mid B_n$ and Lemma 7.1.2 implies

$$a_\ell(E_{B,n}) = \pm 1 \quad \text{whenever} \quad n \equiv 0 \pmod{r(\ell)},$$

as required. □

When comparing traces of the Frey curve (7.1.1) and the newform coefficient for a particular newform f at a prime ℓ we now turn our attention to the bound

on p we can obtain with respect to the Diophantine equation

$$C_n^2 - A_n^3 = DZ_n^{6p}. \tag{7.1.7}$$

If we assume we are in the same situation as Lemma 7.1.3 and are checking at a prime ℓ, with rank of apparition $r(\ell)$, it was seen the condition $n \equiv 0 \pmod{r(\ell)}$ implied multiplicative reduction:

$$a_\ell(E_{B,n}) = \pm 1 \quad \text{whenever} \quad n \equiv 0 \pmod{r(\ell)},$$

so by Proposition 5.2.3 we need to rule out the possibility that

$$c_\ell(f) \equiv \pm(\ell + 1) \pmod{p}.$$

We certainly will not have the equality $c_\ell(f) = \pm(\ell+1)$ because $|c_\ell(f)| \leq 2\sqrt{\ell} < \ell + 1$.

Now when we compare the traces and coefficients when ruling out possibilities, we actually look at the twist of $E_{B,n}$

$$E_{W,n} \colon Y^2 = X^3 - 3U_n X + 2V_n, \tag{7.1.8}$$

which has $E_{W,n}$ periodic modulo ℓ. Now due to the periodicity as outlined in Corollary 4.5.9, we test all Frey curves $E_{W,n}$ up to $n = r(\ell)\tau$. This means in the multiplicative case we need to rule out any $n \equiv 0 \pmod{r(\ell)}$.

We have seen in Proposition 7.1.1 that in the case of good reduction, we cannot rule out any primes $p < 4\sqrt{\ell}$, and in the multiplicative case we cannot rule out $p < 2\sqrt{\ell} + \ell + 1$. Now in order to rule out any n divisible by $r(\ell)$ we are assuming $p \geq 2\sqrt{\ell} + \ell + 1 > |c_\ell(f)| + \ell + 1$. We must therefore take this greater bound since we always have multiplicative reduction occur for some Frey curve $E_{W,n}$, whenever $r(\ell) \mid n$ for some prime $\ell \mid B_n$.

Hence since we know we will get multiplicative reduction when the rank of apparition divides the index n, this shows that the bound in this case is $p > \ell + 1 + |c_\ell(f)|$, and we need to rule these out.

Lemma 7.1.4. *Suppose q is a prime dividing B_1, and $\ell > 3$ is a prime number*

not dividing D and with rank of apparition q in the sequence (B_n). Then no term B_n is a perfect p^{th} power, for $p > \max\{\ell + 1 + 2\sqrt{\ell},\ v_q(B_1) + 1,\ 17\}$.

Now assume ℓ is a prime with rank of apparition q with conditions: $\ell \nmid N_p$, and $p_0 > 2\sqrt{\ell} + \ell + 1$. Then for all $p \geq p_0$, B_n is not a p^{th} power, and equivalently B_1 is not.

Proof. Suppose $p > \max\{v_q(B_1) + 1,\ 17\}$ and B_n is a perfect p^{th} power. Then $v_q(B_n) = v_q(B_1) + v_q(n)$ is a multiple of p, and so is greater than $v_q(B_1)$. Hence $v_q(n) \geq 1$ and so q divides n, and ℓ divides B_n (since $r(\ell) = q$ and $n \equiv 0 \pmod{q}$). But then $E_{B,n}$ has multiplicative reduction at ℓ, while ℓ does not divide N_p (since it does not divide $6D$). Thus, by Proposition 7.1.1, we must have $p < \ell + 1 + 2\sqrt{\ell}$, as required. □

Example 7.1.5. Take the rank 1 Mordell curve $E_{130}\colon y^2 = x^3 + 130$, having nontorsion point $P = (\frac{399}{169}, \frac{26287}{2197})$. Hence $B_1 = 13$; this means we cannot work explicitly with the prime 13 in eliminating newforms since $[13]P$ and all its multiples reduce to the point at infinity. Now if we compute $[13]P$, B_{13} comes out as

$$\begin{aligned} B_{13} =& 13^2 \cdot 2963 \cdot 36979 \cdot 19711537 \cdot 164729839 \cdot 115431264469 \\ & \cdot 53214681173383 \cdot 16925364265342683968138230977139198275280129 3 \\ & 5374102716223157571438401900761006694823040968142664719743035 6 \\ & 4811547504962059975662019034531633425157695980294562259410148 0 \\ & 5038428787424863600482987427511835044892060442 7 \end{aligned}$$

where the last prime has 216 digits. We note $v_{13}(B_{13}) = v_{13}(B_1) + v_{13}(13) = 1 + 1 = 2$. We also find the rank of apparition of the prime 2963 is 13, and that $2963 \nmid 6 \cdot 130$ and so we can invoke Lemma 7.1.4. Hence $E_{B,13}$ has multiplicative reduction at 2963, and so B_n is not a p^{th} power for any prime $p > (\sqrt{2963} + 1)^2$, which has $p_0 = 3079$. Then for all $p \geq p_0$, B_n is not a p^{th} power.

The bound of $p_0 = 3079$ from Example 7.1.5 is rather large, and in the next Section we show an algorithm using a sieve based on the Chinese Remainder Theorem to lower the bound found using this manner (we end up getting $p_0 = 113$ in the rational PIP case).

7.2 The Chinese Remainder Sieve

In this Section we implement what we call the *Chinese Remainder Sieve* (CRS) which is an algorithm we have designed to work in `Pari/GP` [43] which makes use of the Chinese Remainder Theorem (CRT) to compare the traces of the Frey curves with the integral coefficients of newforms. Hence our algorithm can only be of use in testing rational newforms, and for any irrational newforms we must use the bound given in Proposition 5.2.9. The algorithm consists of various `Pari/GP` routines which will be explained in Subsection 7.2.2. On implementing these `Pari/GP` routines we can (hopefully) eliminate all rational newforms from occurring and show no power integral points occur, but this comes with an inherent bound due to the size of the final prime number used in eliminating the newforms, call this final prime number ℓ_r. Then we always have our results with the restriction: no perfect p^{th} powers for $p \geq p_0$, where by Lemma 7.1.4 p_0 is the next prime greater than $(\sqrt{\ell_r}+1)^2$. By Proposition 7.1.1 we see we can do slightly better than this bound by noticing the only primes less than this bound p_0 which need to be ruled out are those primes p dividing some $c_\ell(f) - a_\ell(E_{B,n})$ for primes ℓ of good reduction, and those primes p dividing some $c_\ell(f) - a_\ell(E_{B,n})(\ell+1)$, in the multiplicative case where $a_\ell(E_{B,n}) = 1$ or -1, and we test each n in range in both cases. In each of these cases we can compute these primes explicitly.

Set out r primes $\ell_1 < \ell_2 < \cdots < \ell_r$, then work out the lcm of the periods: $M = \text{lcm}(M(\ell_1), M(\ell_2), \ldots, M(\ell_r))$ and use the Chinese Remainder Theorem on the r sets of congruences associated to the sets $\mathcal{S}_{f,\ell_i}$, for $1 \leq i \leq r$, to get congruence conditions modulo M, where M is large, say $M > 10^9$. Then the hope is to show the possibilities for B_n being a p^{th} power integral point for such a large bound on n are impossible, allowing for any controlled bound, whereby if we stop at ℓ_r we have no p^{th} PIPs for $p \geq (\sqrt{\ell_r}+1)^2$, which is necessary by Proposition 7.1.1.

Let P be a nontorsion point on the Mordell curve $E_D\colon y^2 = x^3 + D$, with its n^{th} multiple given by $[n]P = (\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3})$. The pair (E_D, P) gives a finite set of newforms of levels N_p, which we shall denote by $\mathfrak{F}_{E_D,P}$, along with congruence conditions on n.

For $f \in \mathfrak{F}_{E_D,P}$ we should like to compute

$$\{n : a_\ell(E_{B,n}) = c_\ell(f)\}.$$

If we know $\left(\frac{d_n}{\ell}\right) = 1$, i.e., $\ell \equiv 1 \pmod 4$ and all primes of bad reduction are quadratic residues modulo ℓ, then this is

$$\mathcal{S}_{f,\ell} = \{n : a_\ell(E_{W,n}) = c_\ell(f)\};$$

otherwise it is contained in

$$\mathcal{S}_{f,\ell} = \{n : |a_\ell(E_{W,n})| = |c_\ell(f)|\}.$$

The $\mathcal{S}_{f,\ell}$ are given by congruence conditions (i.e., unions of arithmetic progressions) because the curve $E_{W,n}$ from (7.0.1) are periodic modulo ℓ, so the trace will also occur periodically modulo $M(\ell)$, where $M(\ell)$ is the period of the EDS (W_n) at ℓ. If we fix a newform $f \in \mathfrak{F}_{E_D,P}$ and compute the trace at ℓ for each curve $E_{W,n}$ for $n = 1$ to $M(\ell)$, this will give a finite list $\mathcal{T}_\ell$ of possible traces. Now after comparison with the newform's coefficient $c_\ell(f)$, if it is in $\mathcal{T}_\ell$, note the index n of the corresponding curve $E_{W,n}$ with the matching trace to obtain a set of congruences:

$$\mathcal{S}_{f,\ell} = \{n : n \equiv n_1, n_2, \dots \pmod{M(\ell)}\}. \tag{7.2.1}$$

It may be that $\mathcal{S}_{f,\ell}$ is empty, in which case we can discard f as a possibile newform corresponding to a PIP.

Let $\mathcal{L}$ be a set of primes. Fix a newfrom f; for each prime ℓ in $\mathcal{L}$ we obtain a set $\mathcal{S}_{f,\ell}$ as in (7.2.1), and write $\mathcal{S}_{f,\mathcal{L}}$ for the intersection of all such sets, so

$$\mathcal{S}_{f,\mathcal{L}} = \bigcap_{i=1}^{r} \mathcal{S}_{f,\ell_i} = \{n : n \text{ satisfies some simultaneous congruences}\}.$$

If ever $\mathcal{S}_{f,\mathcal{L}} = \varnothing$ then we can rule out f; if not then we get congruence conditions on n instead. If there is an $\mathcal{L}$ such that $\mathcal{S}_{f,\mathcal{L}}$ is empty for all f in $\mathfrak{F}_{E_D,P}$ then we are done, if not we still get strong congruence conditions on n.

It is in this manner that we shall proceed to build sets of congruences based on matching traces with coefficients, and then compare these sets using the Chinese Remainder Theorem.

7.2.1 The Modular Method Applied to $E_{-2}\colon y^2 = x^3 - 2$

We give here a worked example on the Mordell curve $E_{-2}\colon y^2 = x^3 - 2$ to illustrate how to implement the results. This is a good curve to use as after level lowering we end up with a level for which there are only rational newforms.

Our problem is to find where, in the DDS formed by the sequence of B_n coming from E_{-2}, we have B_n occurring as a p^{th} power. Specifically, we want to solve the equation

$$B_n = Z_n^p \qquad \text{for } p \text{ prime } p = 11, \text{ or } p \geq 17. \tag{7.2.2}$$

It was essentially a Theorem of Fermat that the only B_n coming from E_{-2} and equal to the perfect power 1 are B_1 and B_{-1}, since he showed the only integral points on E_{-2} were $(3, \pm 5)$. (For a proof of this fact see [35, Ch. IX.7 Prop. 7.1(b)].)

So let us assume that on E_{-2} the n^{th} multiple of the nontorsion point $P = (3, 5)$, given by $[n]P = (\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3})$, with $\gcd(A_n C_n, B_n) = 1$, is a power integral point with B_n a p^{th} power, say $B_n = Z^p$, where p is a prime $p = 11$, or $p \geq 17$.

The defining equation for E_{-2} has the associated Diophantine equation for this PIP as

$$C_n^2 - A_n^3 = -2Z_n^{6p}. \tag{7.2.3}$$

Firstly as we have already noted, the point $P = (3, 5)$ is a PIP itself as it has $B_P = 1$ (as does the other integral point on E_{-2}, $(3, -5)$), which is a perfect power raised to any integral exponent, so this already tells us some newforms can never be ruled out using this method since they are associated to the PIPs (3 ± 5). Hence the best we can do is rule out all other newforms of the level in question and get some lower bound on p^{th} powers associated to Frey curves arising modulo p from the newforms we know have to exist. Secondly there are no primes of bad reduction for P on E_{-2}, which tells us the only quadratic twists of the ensuing Frey curve come from $\mathbb{Q}(\sqrt{-1})$.

Consider the Frey curve derived from Theorem 5.3.3,

$$E_{B,n}\colon Y^2 = X^3 - 3A_nX + 2C_n. \tag{7.2.4}$$

Now in accord with our discussion on periodicity in Section 7.0.3, we change our nonperiodic Frey curve (7.2.4) to one that is:

$$E_{W,n}\colon Y^2 = X^3 - 3U_nX + 2V_n. \tag{7.2.5}$$

The conductor pertaining to the curve (7.2.5) is

$$N = 2^{f_2}3^{f_3}\operatorname{rad}_{2,3}(-2Z_n^{6p}) = 2^{f_2}3^{f_3}\operatorname{rad}_{2,3}(Z_n).$$

The values for f_2 and f_3 can be read off from Tables 6.4.1, 6.4.2, where we note in the case of f_3 we have the condition of Papadopoulos, P_2 satisfied from (5.3.3) since $c_4 = 2^4 3^2 A_n$, $c_6 = 2^6 3^3 C_n$, whence $v_3(c_4) \geq 2$, $v_3(c_6) = 3$, and so $f_3 = 2$ in all cases. We summarize the results for the conductor:

$$N = \begin{cases} 2 \cdot 3^2 \operatorname{rad}_{2,3}(Z_n) & \text{if } Z_n \text{ is even and } C_n \equiv 1 \pmod 4, \\ 2^7 \cdot 3^2 \operatorname{rad}_{2,3}(Z_n) & \text{if } Z_n \text{ is odd.} \end{cases} \tag{7.2.6}$$

We know there are only finitely many integer solutions possible for Equation (7.2.3) as its charcteristic is less than zero by Subsection 5.3.2. To start with we know that the point $P = (3, 5)$ is on $E_{-2}\colon y^2 = x^3 - 2$. Hence $(A_1, C_1, B_1) = (3, 5, 1)$ is a solution to (7.2.3) (as is $(3, -5, 1)$), so (7.2.5) gives us the curves

$$E_{W,+1}\colon Y^2 = X^3 - 9X + 10, \tag{7.2.7}$$

$$E_{W,-1}\colon Y^2 = X^3 - 9X - 10. \tag{7.2.8}$$

The curves (7.2.7) and (7.2.8) are the curves 1152a1 and 1152m1 in Cremona's tables respectively: as is seen the curves are twists coming from $\mathbb{Q}(\sqrt{-1})$. The

newform corresponding to $E_{W,-1}$ is

$$f_{-1} = q + 2q^5 - 2q^7 - 4q^{11} - 2q^{13} - 4q^{17} - 4q^{19} - 8q^{23} - q^{25} + 6q^{29} + \cdots,$$

while the newform corresponding to $E_{W,+1}$ is

$$f_{+1} = q + 2q^5 + 2q^7 + 4q^{11} - 2q^{13} - 4q^{17} + 4q^{19} + 8q^{23} - q^{25} + 6q^{29} - \cdots.$$

On inspection these are: $f_{-1} = f_1$ and $f_{+1} = f_{11}$ from Table 7.2.1. As explained in Subsection 7.0.5 these two curves have the same number of points modulo 5, 13, 17, 29, etc., but not modulo 7, 11, 19, 23, etc. This explains the sign changes for the coefficients in the q-expansions for the newforms f_{+1} and f_{-1} at prime exponents $\not\equiv 1 \pmod 4$.

Level lowering of the conductor given by (7.2.6) gives us

$$N_p = \begin{cases} 18 & \text{if } n \text{ is even, and } C_n \equiv 1 \pmod 4, \\ 1152 & \text{if } n \text{ is odd.} \end{cases} \tag{7.2.9}$$

Using the recursive formula given in Proposition 5.1.2 to compute the number of newforms of a level N_p we find

- No newforms of level 18.
- Twenty newforms of level 1152.

Remark 7.2.1. In fact the recursive formula gives forty newforms of level 1152, but we find using `Pari/GP` that each newform in this conjugacy class has a corresponding conjugate newform, and so up to conjugacy there are only twenty newforms. This also shows us that there are no irrational newforms at level 1152 (or indeed at level 18).

The twenty newforms of level 1152 are given in Table 7.2.1. In fact we only need be concerned with newforms f_1 to f_{10} as newforms f_{11} to f_{20} are just quadratic twists of the first ten by $\sqrt{-1}$ (Table 7.2.1 is ordered so f_i is a quadratic twist of f_{i+10} for $1 \leq i \leq 10$).

Hence to investigate the existence of power integral points on E_{-2}, other than $(3, \pm 5)$, we look to rule out, using the Modularity Theorem and our Frey curve,

$$
\begin{aligned}
f_1 &= q + 2q^5 - 2q^7 - 4q^{11} - 2q^{13} - 4q^{17} - 4q^{19} - 8q^{23} - q^{25} + 6q^{29} + \cdots \\
f_2 &= q - 2q^5 + 2q^7 - 4q^{11} + 2q^{13} - 4q^{17} - 4q^{19} + 8q^{23} - q^{25} - 6q^{29} - \cdots \\
f_3 &= q - 2q^5 + 2q^7 - 4q^{11} - 2q^{13} + 4q^{17} + 4q^{19} - 8q^{23} - q^{25} - 6q^{29} - \cdots \\
f_4 &= q + 2q^7 + 4q^{11} + 6q^{13} - 6q^{17} - 4q^{23} - 5q^{25} - 4q^{29} + 10q^{31} + 2q^{37} + \cdots \\
f_5 &= q + 2q^5 + 4q^7 + 2q^{11} - 2q^{13} + 2q^{17} + 2q^{19} + 4q^{23} - q^{25} - 6q^{29} + \cdots \\
f_6 &= q - 2q^5 + 4q^7 - 2q^{11} + 2q^{13} + 2q^{17} - 2q^{19} + 4q^{23} - q^{25} + 6q^{29} - \cdots \\
f_7 &= q + 4q^5 + 2q^7 - 4q^{11} + 2q^{13} + 2q^{17} + 8q^{19} - 4q^{23} + 11q^{25} - 6q^{31} + \cdots \\
f_8 &= q - 4q^5 - 2q^7 - 4q^{11} - 2q^{13} + 2q^{17} + 8q^{19} + 4q^{23} + 11q^{25} + 6q^{31} - \cdots \\
f_9 &= q + 2q^5 + 2q^7 + 4q^{11} + 2q^{13} + 4q^{17} - 4q^{19} - 8q^{23} - q^{25} + 6q^{29} - \cdots \\
f_{10} &= q + 2q^7 - 4q^{11} - 6q^{13} - 6q^{17} - 4q^{23} - 5q^{25} + 4q^{29} + 10q^{31} - 2q^{37} + \cdots \\
f_{11} &= q + 2q^5 + 2q^7 + 4q^{11} - 2q^{13} - 4q^{17} + 4q^{19} + 8q^{23} - q^{25} + 6q^{29} - \cdots \\
f_{12} &= q - 2q^5 - 2q^7 + 4q^{11} + 2q^{13} - 4q^{17} + 4q^{19} - 8q^{23} - q^{25} - 6q^{29} + \cdots \\
f_{13} &= q - 2q^5 - 2q^7 + 4q^{11} - 2q^{13} + 4q^{17} - 4q^{19} + 8q^{23} - q^{25} - 6q^{29} + \cdots \\
f_{14} &= q - 2q^7 - 4q^{11} + 6q^{13} - 6q^{17} + 4q^{23} - 5q^{25} - 4q^{29} - 10q^{31} + 2q^{37} + \cdots \\
f_{15} &= q + 2q^5 - 4q^7 - 2q^{11} - 2q^{13} + 2q^{17} - 2q^{19} - 4q^{23} - q^{25} - 6q^{29} + \cdots \\
f_{16} &= q - 2q^5 - 4q^7 + 2q^{11} + 2q^{13} + 2q^{17} + 2q^{19} - 4q^{23} - q^{25} + 6q^{29} + \cdots \\
f_{17} &= q + 4q^5 - 2q^7 + 4q^{11} + 2q^{13} + 2q^{17} - 8q^{19} + 4q^{23} + 11q^{25} + 6q^{31} + \cdots \\
f_{18} &= q - 4q^5 + 2q^7 + 4q^{11} - 2q^{13} + 2q^{17} - 8q^{19} - 4q^{23} + 11q^{25} - 6q^{31} - \cdots \\
f_{19} &= q + 2q^5 - 2q^7 - 4q^{11} + 2q^{13} + 4q^{17} + 4q^{19} + 8q^{23} - q^{25} + 6q^{29} + \cdots \\
f_{20} &= q - 2q^7 + 4q^{11} - 6q^{13} - 6q^{17} + 4q^{23} - 5q^{25} + 4q^{29} - 10q^{31} - 2q^{37} + \cdots
\end{aligned}
$$

Table 7.2.1: Newforms (up to Conjugacy) on $\Gamma_0(1152)$ of Weight 2 over $\mathbb{Z}$

any of the nine newforms f_2 to f_{10} of level 1152 attached to putative solutions of our equation using periodicity, and thereby obtain congruence conditions imposed on n as explained in Section 7.2. So we need to show these newforms are not associated with any $E_{W,n}$ with $n > 1$, where we are free to take positive n. We already have our first congruence condition on n, namely $n \equiv 1 \pmod 2$ since we ruled out the possibility of W_n being even, which is the same as the condition that the index n be even. Hereafter we need only take the odd multiples of the point $(3, 5)$, that is we are only now concerned with $E_{W,n}$ having n odd.

The smallest prime we can start with is $\ell = 5$, so now we take multiples of $(3, 5)$ and reduce the 3-tuple (U_n, V_n, W_n) modulo 5; we find the period modulo 5

to be $M(5) = 8$. The reduced Frey curves of odd index are all congruent modulo 8, and we have

$$\tilde{E}_{W,1} \cong \tilde{E}_{W,3} \cong \tilde{E}_{W,5} \cong \tilde{E}_{W,7} \colon Y^2 \equiv X^3 + X \pmod 8.$$

Hence the traces at 5 will all be the same: $a_5(E_{W,1}) = a_5(E_{W,3}) = a_5(E_{W,5}) = a_5(E_{W,7}) = 2$. This rules out any newforms that do not have 2 as a coefficient for q^5 in their Fourier expansions, leaving f_1, f_5, and f_9 (and their twists f_{11}, f_{15}, and f_{19}) in Table 7.2.1 as possibilities. Hence from our initial set of ten newforms only three remain with just our first value for the prime ℓ. The congruence we have is $n \equiv \pm 1, \pm 3 \pmod 8$ which is equivalent to n being odd as before. We present this result as a set:

$$\mathcal{S}_{f_r,\{5\}} = \begin{cases} \varnothing & \text{if } r \neq 1, 5, 9, \\ \{n : n \equiv 1 \pmod 2\} & \text{if } r = 1, 5, 9. \end{cases}$$

The newform f_1 cannot be discarded but we can continue in the same manner using periodicity to try to rule out the other two newforms f_5, and f_9.

For $\ell = 7$ we find, using `Pari/GP`, that $M(7) = 42$, with the possible traces at $\ell = 7$: $a_7(E_{W,n}) \in \{-2, -1\}$, which is equivalent to $a_7(E_{B,n}) \in \{\pm 1, \pm 2\}$ due to $7 \equiv 3 \pmod 4$. Now since f_5 has 4, and f_9 has 2 for the coefficient of q^7 in their respective expansions, we find we can rule out f_5, but not f_9 as it may be associated to some Frey curve $E_{B,n}$ having 2 as its coefficient for q^7 in its associated newform expansion. Hence $\mathcal{S}_{f_5,7} = \varnothing$, but $\mathcal{S}_{f_9,7} \neq \varnothing$. After cutting all equivalent congruences modulo 42 to get a congruence modulo 7, this gives the sets

$$\mathcal{S}_{f_1,7} = \mathcal{S}_{f_9,7} = \{n : n \equiv 1, 2, 3, 4, 5, 6 \pmod 7\}.$$

Solving the sets of congruences in $\mathcal{S}_{f_r,\{5\}}$, and $\mathcal{S}_{f_1,7}$ simultaneously gives

$$\mathcal{S}_{f_r,\{5,7\}} = \begin{cases} \varnothing & \text{if } r \neq 1,\ 9, \\ \{n : n \equiv \pm 1, \pm 3, \pm 5 \pmod{14}\} & \text{if } r = 1,\ 9. \end{cases}$$

For $\ell = 11$ we find, using `Pari/GP`, that $M(11) = 24$, and the possible traces at $\ell = 11$: $a_{11}(E_{W,n}) \in \{-6, -2, 0, 1, 4\}$, which is equivalent to $a_{11}(E_{B,n}) \in$

$\{0, \pm 1, \pm 2, \pm 4, \pm 6\}$. The coefficient of q^{11} for f_9 is 4 and so we cannot rule out f_9 as a possibility. We now check the set of twenty-four traces of the reduced Frey curve $E_{W,n}$ modulo 11 with respect to the order in which they appear to see where ± 4 appears to get a congruence for n. We do not find -4, but we do find 4 at index $n = 1$, 11, 13, and 23 to give the sets

$$\mathcal{S}_{f_1,11} = \mathcal{S}_{f_9,11} = \{n : n \equiv \pm 1 \pmod{12}\}.$$

Solving the sets of congruences in $\mathcal{S}_{f_r,\{5,7\}}$, and $\mathcal{S}_{f_1,11}$ simultaneously gives

$$\mathcal{S}_{f_r,\{5,7,11\}} = \begin{cases} \varnothing & \text{if } r \neq 1,\ 9, \\ \{n : n \equiv \pm 1, \pm 11, \pm 13, \pm 23, \pm 25, \pm 37 \pmod{84}\} & \text{if } r = 1,\ 9. \end{cases}$$

For $\ell = 13$ we find $M(13) = 114$. Since $13 \equiv 1 \pmod 4$ the coefficients of q^{13} for the newform twists are the same. We find $c_{13}(f_1) = -2$, and $c_{13}(f_9) = 2$, and so now check the set of 114 traces of the reduced Frey curve modulo 13 with respect to the order in which they appear to find where ± 2 appears. This gives the two sets:

$$\mathcal{S}_{f_1,13} = \{n : n \equiv 1, 7, 9, 11, 13, 15, 23, 25, 27, 29, 31, 37 \pmod{38}\};$$
$$\mathcal{S}_{f_9,13} = \{n : n \equiv 4, 6, 8, 10, 12, 18, 20, 26, 28, 30, 32, 34 \pmod{38}\}.$$

Solving the sets of congruences in $\mathcal{S}_{f_1,\{5,7,11\}}$, and $\mathcal{S}_{f_1,13}$ simultaneously gives

$$\mathcal{S}_{f_r,\{5,7,11,13\}} = \begin{cases} \varnothing & \text{if } r \neq 1, \\ \{n : n \equiv \pm 1, \pm 11, \pm 13, \pm 23, \ldots \pmod{1596}\} & \text{if } r = 1, \end{cases}$$

where n is congruent to 144 values.

So any p^{th} power integral point $[n]P$ with $p \geq (\sqrt{13} + 1)^2$, i.e., $p \geq 23$, by Proposition 7.1.1, must come from the newforms f_1 or f_{11}.

For $\ell = 17$ we find $M(17) = 288$. Since $17 \equiv 1 \pmod 4$ the coefficients of q^{17} for newforms and their twists are of the same sign; we have for the newform f_1

the set:

$$\mathcal{S}_{f_1,17} = \{n : n \equiv \pm 1, \pm 5 \pmod{18}\}.$$

Solving the sets of congruences in $\mathcal{S}_{f_1,\{5,7,11,13\}}$, and $\mathcal{S}_{f_1,17}$ simultaneously gives

$$\begin{aligned}\mathcal{S}_{f_1,\{5,7,11,13,17\}} = \{n : n \equiv 1, 13, 23, 37, 85, 107, 121, 143, 145, 167, 179,\\ 181, 215, 229, 239, 251, \ldots, 4703, 4751, 4765, 4775, 4787 \pmod{4788}\},\end{aligned}$$

where n is congruent to a total of 288 values.

When checking for the absence of perfect p^{th} powers in the DDS associated to the elliptic curve $E_{-2}\colon y^2 = x^3 - 2$ in the manner above, if we check up to the prime $\ell = 113$ we find the smallest congruence with $n > 1$ to be

$$n_0 \equiv 113762879 \pmod{1314822960360},$$

where 13148229603602 factorsises as $2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 19 \cdot 61 \cdot 97$. (This computation took 3h, 46min on a 2.5 GHz Intel Core i5 processor with 16 GB 1600 MHz DDR3 of RAM; for the timings of the other computations preceding this one, which were significantly lower see Table 7.2.2.) This means if we look at our Frey curve, with the exception of $n = 1$, no Frey curves $E_{W,n}$ are associated to any p^{th} PIP for $1 < n < 113762879$; the first possible candidate being $E_{113762879}$:

$$E_{W,113762879}\colon Y^2 = X^3 - 3A_{113762879}X + 2C_{113762879}.$$

In general the best we can hope for is a congruence condition on the index n and a bound on the exponent p. For the case above we have that there can be no p^{th} power integral point for any n such that $1 < n < 113762879$ for $p \geq (\sqrt{113}+1)^2$, i.e., $p \geq 137$.

Continuing in the manner above using `Pari/GP` we arrive at the following Theorem:

Theorem 7.2.2 (Buck)**.** *Let $\mathcal{B}_{E_{-2},P} = (B_n)$ be the DDS associated to the elliptic curve $E_{-2}\colon y^2 = x^3 - 2$ and point $P = (3, 5)$, and let (ℓ_{end}, p_0, n_0) be as in any row of the Table 7.2.2 below. Then there does not exist an n with $1 < n < n_0$, such that B_n is a perfect p^{th} power, with $p \geq p_0$ with p_0 the next prime $\geq (\sqrt{\ell_{end}}+1)^2$.*

The meaning of the Q_{opt} column of Table 7.2.2 will be explained in Subsection 7.2.2. Theorem 7.2.2 just gives a bound on the nonexistence of p^{th} perfect powers for B_n in the range $1 < n < n_0$, for $p \geq p_0$ and so this process can be carried on indefinitely getting higher bounds for n_0, and p_0 thus disqualifying more possibilities for n and p. In Theorem 7.2.2 the values obtained in Table 7.2.2 indicate the prime ℓ_{end} at which the value of the next smallest congruence increases.

ℓ_{end}	p_0	n_0	Q_{opt}	Time
5	11	1	2	4 ms
7	17	3	$2 \cdot 7$	10 ms
11	19	11	$2 \cdot 3 \cdot 7$	11 ms
17	29	13	$2 \cdot 3 \cdot 7 \cdot 19$	47 ms
23	37	23	$2 \cdot 3 \cdot 7 \cdot 19$	74 ms
29	41	121	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 19$	131 ms
37	53	1079	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 19$	299 ms
41	59	2519	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 19$	318 ms
61	79	16631	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 61$	666 ms
79	101	49391	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 61 \cdot 97$	26,323 ms
89	109	244441	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 61 \cdot 97$	32,701 ms
97	127	388079	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 61 \cdot 97$	9min, 45,177 ms
113	137	113762879	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 61 \cdot 97$	3h, 36min, 20,655 ms

Table 7.2.2: PIPs on Elliptic Curve E_{-2}: $y^2 = x^3 - 2$, and Point $P = (3, 5)$ for $N_p = 1152$, with Optimal Q_{opt}, and Timing for Q_{opt}

7.2.2 `Pari/GP` Implementation

The process outlined in the example in Subsection 7.2.1 was automated by the computer algebra system `Pari/GP`. For a rank 1 Mordell curve E_D, having generator P, we start by initialising the curve

```
e = ellinit([0, 0, 0, 0, D], 1)
```

ℓ :	2	3	5	7	11	13
$M(\ell)$:	2	3	2	$2 \cdot 3 \cdot 7$	$2^3 \cdot 3$	$2 \cdot 3 \cdot 19$
ℓ :	17	19	23	29	31	37
$M(\ell)$:	$2^5 \cdot 3^2$	3	$2^4 \cdot 11$	$2 \cdot 5 \cdot 7$	$2^2 \cdot 3 \cdot 5 \cdot 7$	$3^2 \cdot 7^2$
ℓ :	41	43	47	53	59	61
$M(\ell)$:	$2 \cdot 3 \cdot 5 \cdot 7$	$2^2 \cdot 3 \cdot 7$	$2^5 \cdot 23$	$2 \cdot 3^2 \cdot 13$	$2^3 \cdot 3 \cdot 29$	$2 \cdot 5 \cdot 61$
ℓ :	67	71	73	79	83	89
$M(\ell)$:	$2 \cdot 3 \cdot 7 \cdot 11$	$2^2 \cdot 3 \cdot 5 \cdot 7$	3^3	$3 \cdot 13 \cdot 97$	$2^2 \cdot 7 \cdot 41$	$2^4 \cdot 3 \cdot 5 \cdot 11$
ℓ :	97	101	103	107	109	113
$M(\ell)$:	$2^4 \cdot 3 \cdot 13$	$2 \cdot 5^2 \cdot 17$	$2 \cdot 7 \cdot 13 \cdot 17$	$2^3 \cdot 3^3 \cdot 53$	$2^4 \cdot 3^3 \cdot 7$	$2^5 \cdot 7 \cdot 19$

Table 7.2.3: Periods $M(\ell)$ for EDS Modulo ℓ, coming from Elliptic Curve E_{-2}: $y^2 = x^3 - 2$ and Point $P = (3, 5)$

and generator point

```
p = [a/b^2, c/b^3]
```

Then the `Pari/GP` routine `ellinput` generates a set of elliptic curves

```
Y = ellinput(Np)
```

of the right level N_p; the set `Y` is a set of 3-vectors: for i in the range of the length of `Y`, `Y[i][1]` is the initialised curve; `Y[i][2]` the set of congruence conditions; and `Y[i][3]` the value of the modulus. For each of these curves we then compute their traces at a prime ℓ, and our `Pari/GP` routine `ellapfreyn` generates a set of traces

```
X = ellapfreyn(e, p, l)
```

at that same prime ℓ for the Frey curves $E_{W,n}$. For reasons explained in Section 7.1 we start at $\ell = 5$ since 2 and 3 always divide both $N_{E_{W,n}}$ and N_p; as well we skip any primes dividing the elliptic denominator `b`, since these cannot be used with `edsrankofapp(e, p, l)`. When we work out the rank of apparition of a prime for a noninteger EDS derived from an elliptic curve-point pair, we need only be concerned with avoiding primes dividing the elliptic denominator `b`. This follows since we can normalise the fractional EDS $(w(n))$ to an equivalent integer EDS

$(w'(n))$ by multiplying the first four terms thus to get an integer seed:

$$w'(i) = w(i)b^{(i^2-1)} \quad \text{for } i = 1, \ldots, 4.$$

The ranks of any primes not dividing b staying the same.

The distinction between when the traces at a prime ℓ of $E_{B,n}$ are equal in sign or not to those of the twist $E_{W,n}$ is implemented in the code by the routine goodl which performs the following check: If -1 is a square modulo ℓ and all primes of bad reduction for the point P are squares modulo ℓ then we can check the actual values of the trace; otherwise we only check their absolute values at the possible loss of some efficiency. This gives us a set

```
U = goodl(e, p)
```

The values for a[n] are computed via the normalised recurrence for Φ_n in (3.1.12), and the c[n] computed from the a[n] and the defining Mordell curve equation; both are initially intmods. Finally when we compute the Frey trace we note the discriminant of the Frey curve is $\Delta = 2^6 3^3 (A_n^3 - C_n^2)$; in the function ellapfreyn we take the lifts, al[n], cl[n] of the intmods a[n], c[n] respectively, to give the trace as

```
ellap(ellinit([0, 0, 0, -3*(al[n] - l), 2*cl[n]]), l)
```

where we take (al[n] − l) to preclude the case of the lifts having

```
al[n]^3 - cl[n]^2 = 0
```

We now use the Pari/GP routine clnewform to compare these traces at a prime ℓ of the curves $E_{W,n}$ with the traces of the actual elliptic curves of conductor equal to the level N_p, thereby generating a set of congruence conditions modulo some divisor of the period $M(\ell)$ for each curve of level N_p. All the aforementioned conditions are handled by the algorithm recursively calling the routine clnewform. This is acheived by the routine

```
clnewformall(e, p, Y, Q, L, M, bd)
```

where L and M give lower and upper limits respectively for the range of primes to use in clnewform. clnewformall sets up the computation by disregarding any primes ℓ with period $M(\ell)$ greater than the bound parameter bd. The value Q is used by the

program as another bound, this time in the size of the modulus the congruences are allowed to have. First it checks if $\gcd(Q, M(\ell)) = 1$, and if so returns Y.

For each form there is in Y there is initially one defining congruence. To start with clnewform is run at the first prime ℓ in range, and for each prime tested checks it is not a factor of the denominator b, if so it skips that prime, if not it goes on to compare the traces of sets of Frey curve traces in set X with those traces of the elliptic curves attached to set Y by using the compare routine, which compares the traces of the elliptic curves one-by-one with those of the Frey curves, and if it finds a match at the j^{th} Frey curve, say X[j] = ellap(Y[i][1], l), where ellap is the `Pari/GP` routine for computing the trace of an elliptic curve; it then stores this result as Mod(j, m) in a `Pari/GP` vector, where m is the given modulus. Now, dependent on whether -1 is a square modulo ℓ and all primes of bad reduction are squares modulo ℓ we check the actual values of the traces to give the set of intmods

```
W = compare([X, M], ellap(Y[i][1], l));
```

otherwise we only check their absolute values to give the set of intmods

```
W = compare([abs(X), M], abs(ellap(Y[i][1], l)).
```

These congruence conditions in W are then compared using the CRT with those attached to the intmods Y[i][2] in ellinput by the routine chinchin leading to the form being either discarded, or having a solution set. This outputs a set of curves containing hopefully fewer curves than we initially started with, and strengthened conditions on the congruences. The output of clnewform will then act as input for future comparison by the routine for a different prime. If after completion any newforms remain they make up the output, along with any extra congruences generated to the new modulus.

For example take the first two primes we test with in the example of Subsection 7.2.1: $\ell_1 = 5$ and $\ell_2 = 7$. This involved solving the two sets of congruences $\mathcal{S}_{f_1,\{5\}} = \{n : n \equiv 1 \pmod 2\}$, and $\mathcal{S}_{f_1,7} = \{n : n \equiv 1, 2, 3, 4, 5, 6 \pmod 7\}$ simultaneously using a brute force approach in `Pari/GP` by writing out the congruences as sets modulo the product $2 \cdot 7 = 14$ to give possible values for n as:

$$n \in \{\mathbf{1}, \mathbf{3}, \mathbf{5}, 7, \mathbf{9}, \mathbf{11}, \mathbf{13}\};$$

$$n \in \{\mathbf{1}, 2, \mathbf{3}, 4, \mathbf{5}, 6, 8, \mathbf{9}, 10, \mathbf{11}, 12, \mathbf{13}\}.$$

The values for n in the intersection of these sets are shown in bold, and these elements hence satisfy both congruences giving:

$$n \in \{1, 3, 5, 9, 11, 13\}$$

which can be expressed as the congruence in the example

$$\mathcal{S}_{f_1,\{5,7\}} = \{n : n \equiv \pm 1, \pm 3, \pm 5 \pmod{14}\}.$$

In this way forms are discarded until at some prime ℓ_{end}, if possible, all forms are discarded, which will then show no p^{th} PIP is possible with $p \geq (\sqrt{\ell_{\text{end}}}+1)^2$. To do this by hand for each prime would be cumbersome, so clnewformall is an automated version which takes a start and end point for our range of tested primes.

For large ℓ the algorithm will generate lots of congruences, which we seek to limit by various utility sorting functions. As well we add in some extra parameters to speed up computation at the compromise of losing data: when working out the traces to compare, if the period is greater than some predefined bound then this set of traces is skipped and we move on to the next prime. If we fail to lose all newforms, then we can always refine our search later.

Another way we can control the process is to control the congruences, specifically the modulus of the systems we output by a parameter we call the *Q-part*. Because the traces at ℓ are modulo the period $M(\ell)$, we can use knowledge of the prime factors of the period by specifying which primes we wish to have contained in our modulus; any period which does not contain these has that prime skipped by clnewform. This has the benefit of not letting the modulus get too big, as we can keep large factors out, and also means we can use just a few small primes to quickly generate congruence sets we can do CRT with.

The Q-part acts as a control for setting which prime factors of the period $M(\ell)$ in clnewform we choose to have as a factor of the modulus. Since we check up to $\ell = 113$ in Theorem 7.2.2, we also check the prime factors of $M(\ell)$ for each ℓ in

the range $\ell = 2$ to 113; these form the set

$$\mathcal{S}_{M(\ell)} = \{2, 3, 5, 7, 11, 13, 19, 23, 29, 41, 53, 61, 97\}.$$

Hence for our optimum value of Q we choose the product of these primes as they will form the basis for the factors of the moduli when we run our program. This is the Q-part used in Theorem 7.2.2 whose values are exhibited in Table 7.2.2. However once the computation is run we see, with reference to Table 7.2.2, that no Q_{opt} uses primes 11, 23, 29, 41, and 53, which appear as prime factors for the periods $M(\ell)$ in Table 7.2.3 for $\ell = 23$, 67, 89 for 11; for $\ell = 47$ for 23; for $\ell = 59$ for 29; for $\ell = 83$ for 41; for $\ell = 107$ for 53.

For example, if we changed the optimal value of Q in Theorem 7.2.2 to one of primorial 19, i.e., $Q = 2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19$, we obtain the values in Table 7.2.4, where the table indicates the prime ℓ_{end} at which the value of the next smallest congruence increases in

```
clnewformall(e, p,[y[1]], 2*3*5*7*11*13*17*19, 5, l_end, 500000)
```

A quick examination of the differences between Table 7.2.2 and 7.2.4 shows the separation between the ℓ_{end} primes are the same up to $\ell_{\text{end}} = 41$ with the nonoptimal Q skipping $\ell_{\text{end}} = 61$, 79, 89, 97 since the Q_{opt} factors of 61 and 97 are no longer present. We find the next jump at $\ell_{\text{end}} = 101$ with $n_0 \equiv 52919 \pmod{74070360}$ where the modulo factorizes as $2^3\cdot3^2\cdot5\cdot7^2\cdot13\cdot17\cdot19$; we also find $\ell_{\text{end}} = 113$ giving $n_0 \equiv 2010959 \pmod{222211080}$ where the modulo factorizes as $2^3\cdot3^3\cdot5\cdot7^2\cdot13\cdot17\cdot19$ and takes just 1,525 ms compared to our best value of $n_0 = 113762879$ taking considerably longer at 3h, 36min when the Q-part is optimal.

Example 7.2.3. Consider the rank 1 Mordell curve $E_{66}\colon y^2 = x^3 + 66$, with nontorsion point $P = (\frac{1}{4}, \frac{65}{8}) \in E_{66}(\mathbb{Q})$. The conductor of E_{66} is $N = 114048$ and after level lowering this becomes $N_p = 198$, which has associated to it five rational newforms and no irrational ones. The Mordell curve E_{66} is also special in the sense that it contains no integral points, and so we may keep discarding the rational newforms until all are discarded, hypothetically, assuming there are no PIPs on the curve. This will give a bound which depends on how we set up the computation. We compute the first few periods which we give in Table 7.2.5, noting that

ℓ_{end}	p_0	n_0
5	11	1
7	17	3
11	19	11
17	29	13
23	37	23
29	41	121
37	53	1079
41	59	2519
101	127	52919
113	137	2010959

Table 7.2.4: PIPs on Elliptic Curve $E_{-2}\colon y^2 = x^3 - 2$, and Point $P = (3, 5)$ for $N_p = 1152$, with $Q = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

2 divides the numerator of the point and so we give this singular prime no period.

ℓ:	2	3	5	7	11	13
$M(\ell)$:	$\times$	3	2^3	$3 \cdot 13$	$2 \cdot 11$	2^2

ℓ:	17	19	23	29	31	37
$M(\ell)$:	$2^5 \cdot 3^2$	$2 \cdot 3^3 \cdot 7$	$2^4 \cdot 3 \cdot 11$	$2 \cdot 5 \cdot 7$	$2^2 \cdot 3^2 \cdot 5$	$2^2 \cdot 3^2 \cdot 7$

Table 7.2.5: Periods $M(\ell)$ for EDS Modulo ℓ, coming from Elliptic Curve $E_{66}\colon y^2 = x^3 + 66$ and Point $P = (\frac{1}{4}, \frac{65}{8})$

We now set the range to run from $\ell_1 = 5$ to ℓ_{end}, where ℓ_{end} is the finishing prime in clnewformall after all five newforms get discarded, with various single prime values of Q and note the time taken on a 2.5 GHz Intel Core i5 processor with 16 GB 1600 MHz DDR3 of RAM. We can then be sure there exist no p^{th} powers for the next prime $p \geq (\sqrt{\ell_{\text{end}}} + 1)^2$: call this bound p_0. The differences in the times show how long it takes for the congruences to gain a contradiction with each single Q prime being used for the modulus. Hence, as would be expected, the larger prime modulii take longer to give a contradiction, with a larger prime bound. We

shall return to this issue in Chapter 8 where we shall investigate Mordell curves containing no integral points and proceed to give the best bound possible for a range of curves, and in particular find E_{66} has $p_0 = 23$, as predicted by our test prime 2 in Table 7.2.6.

Q	ℓ_{end}	p_0	Time
2	13	23	5 ms
3	37	53	46 ms
5	59	79	38 ms
7	37	53	22 ms
11	263	307	12,404 ms
13	97	127	566 ms
17	509	557	4min, 3,914 ms
19	367	409	42,099 ms
23	277	313	15,233 ms
29	349	389	1min, 5,415 ms
31	929	991	54min, 51,093 ms
37	443	487	2min, 10,671 ms

Table 7.2.6: Q-part and the Time to Finishing Prime ℓ_{end} on $E_{66}\colon y^2 = x^3 + 66$

We saw in the case of the Mordell curve E_{-2} that we quickly halved the number of Frey curves we had to investigate by noting that n had to be odd. The function

```
ellinput(Np, Mod(0, 1))
```

is set by default to 0 (mod 1), but if we knew that n had to be odd, i.e., $n \equiv 1$ (mod 2), then we could initialise our set of forms as

```
ellinput(Np, Mod(1, 2))
```

Having some knowledge of the factorisation of the nontorsion point on the Mordell curve can also be made use of. We note that, for some prime q, if $q \mid B_1$ then $v_q(B_n) = v_q(B_1) + v_q(n)$. In particular if we have a perfect power $B_n = Z_n^p$, with $p \geq 11$, $p \neq 13$, we get

$$v_q(Z_n^p) = v_q(B_1) + v_q(n) \geq p,$$

so $v_q(n) \geq p - v_q(B_1)$. Thus we start with a congruence of $[\mathrm{Mod}(0, q^{p-v_q(B_1)})]$.

Chapter 8

Mordell Curves with No Integral Points

In this Chapter we look to implement our method in cases where we can prove there are no p^{th} power points for p large enough. For this we need our Mordell curves to contain no integral points.[1]

8.1 Mordell Curves

One of the drawbacks of our method is the problem of integral points, which have $B_1 = 1$, and so are power integral points for all primes p. Thus to test our approach we need Mordell curves with no integral points. Since Mordell curves have Weierstrass coefficient $a_1 = 0$, we have by Theorem 2.5.3 (a) that any torsion point $P = (x(P), y(P))$, must have $x(P),\ y(P) \in \mathbb{Z}$. Therefore Mordell curves possessing no integral points are torsion free.

We note that we can not use Propositon 5.2.9 to obtain a bound for the rational newform case. To see why, assume we have a prime ℓ such that $\ell^2 \nmid N$ and $\ell \nmid N_p$, where N is the conductor of the Mordell curve, and N_p is the lowered level of the newforms. Now consider the set

$$S_\ell = \{a \in \mathbb{Z} : -2\sqrt{\ell} \leq a \leq 2\sqrt{\ell} \text{ and } a \equiv \ell + 1 \pmod{t}\}$$

[1] Extensive data for Mordell curves with $|D| \leq 10000$ was communicated to the author by Attila Pëtho, for which he is extremely grateful.

of Propositon 5.2.9. Since a and c_ℓ both obey the Hasse bound: $|a| \leq 2\sqrt{\ell}$, and $|c_\ell| \leq 2\sqrt{\ell}$; when we form the product

$$\prod_{a \in S_\ell} \mathcal{N}_{K/\mathbb{Q}}(a - c_\ell)$$

this will always be zero, since one of the values of a in S_ℓ will necessarily equal c_ℓ, and so $B'_\ell(f)$ of the Proposition will always equal zero in this case, and so can not be used to calculate a bound for p. This also means for the irrational newform case we have to take $t = 1$ in the congruence $a \equiv \ell + 1 \pmod{t}$ since t divides the order of the torsion group $E_{\text{tors}}(\mathbb{Q})$ which in this case is trivial.

We have seen in Theorem 6.2.1 that this restriction on Mordell curves having no integral points assures that there exist at most finitely many perfect powers in the associated DDS (B_n).

Example 8.1.1. The Mordell curve of smallest conductor ($N = 52272 = 2^4 \cdot 3^3 \cdot 11^2$) and nonzero rank with no PIPs is

$$E_{11} \colon y^2 = x^3 + 11$$

as shown in [29, Prop. 1.5]. We shall use this example to show the implementation of the method applied to Mordell curves possessing no integral points, as we are at the advantage of also knowing it contains no PIPs. This curve has rank 1, trivial torsion, and generator $P = (\frac{-7}{4}, \frac{19}{8})$. The curve has DDS (B_n):

$$[2, 76, -103866, -1318861288].$$

The associated EDS is:

$$\left[1, \frac{19}{4}, \frac{-51933}{256}, \frac{-164857661}{8192}\right].$$

For each n^{th} multiple of P we have as before the associated Diophantine equation

$$C_n^2 - A_n^3 = 11B_n^6, \tag{8.1.1}$$

where we may assume the n^{th} multiple of P is a PIP, having $B_n = Z_n^p$, and so

(8.1.1) becomes

$$C_n^2 - A_n^3 = 11Z_n^{6p}. \tag{8.1.2}$$

To (8.1.2) we associate the Frey curve

$$E_{B,n}\colon Y^2 = X^3 - 3A_nX + 2C_n.$$

We note $B_n = Z_n^p$ is always even since it is divisible by $B_1 = 2$; this narrows our search for newforms. For each $n \in \mathbb{Z}$ we have the following quantities for the Frey curve:

(1) The minimal discriminant of $E_{B,n}$ is

$$\Delta_{\min} = -2^{-6} \cdot 3^3 \cdot 11 \cdot Z_n^{6p} \quad \text{as } Z_n \text{ is even.}$$

(2) The conductor N of the curve $E_{B,n}$ is given by

$$N = 2^{f_2} \cdot 3^{f_3} \cdot \mathrm{rad}_{2,3}(11Z_n),$$

where f_2 and f_3 can be looked up in Tables 6.4.1 and 6.4.2 respectively.

(3) Suppose that $p = 11$ or $p \geq 17$, then $E_{B,n} \sim_p f$ for some newform f of level

$$N_p = 2^{f_2} \cdot 3^{f_3} \cdot 11, \tag{8.1.3}$$

where f_2 and f_3 can be looked up in Tables 6.4.1 and 6.4.2 respectively.

For f_2, as Z_n is always even Table 6.4.1 gives $f_2 = 1$. For f_3 if we have $3 \mid Z_n$ then $f_3 = 2$. If not, then since $11 \equiv 2 \pmod 9$, Table 6.4.2 gives $f_3 = 2$ or 3 dependent on whether we end at Tate's case 4 or 3 respectively; in the terminology of Papadopolous we have Tate's case 4 occurring if P_2 is satisfied, and Tate's case 3 occurring if P_2 is not satisfied, where P_2 is the condition

$$\frac{c_6^2}{3^6} + 2 \equiv 3 \cdot \frac{c_4}{3^2} \pmod 9.$$

We find P_2 is not satisfied and we end up with $f_3 = 3$ if $3 \nmid Z_n$.

To summarise our results:

$$N_p = \begin{cases} 2 \cdot 3^2 \cdot 11 = 198 & \text{if } 3 \mid Z_n \text{ and } C_n \equiv 1 \pmod 4, \\ 2 \cdot 3^3 \cdot 11 = 594 & \text{if } 3 \nmid Z_n,\ C_n \equiv 1 \pmod 4 \text{ and end at Tate's case 3.} \end{cases} \tag{8.1.4}$$

Using $Q = 6$ as our test product of primes we eliminate newforms of each level N_p using a `Pari/GP` program thus:

Case 1. By Example 5.1.4 there exist five rational newforms and no irrational newforms of level $N_p = 198$. With respect to Example 5.1.4 we lose newforms f_1 and f_5 at $\ell = 5$, and lose the remaining three newforms at $\ell = 7$: we conclude $\mathcal{S}_{f,\{5,7\}} = \varnothing$.

Case 2. By Example 5.1.4 we know there exist, up to conjugacy, ten newforms of level $N_p = 594$; eight are rational and two are irrational. With respect to Example 5.1.4 we lose the rational newforms f_1, f_3, f_4, and f_8 at $\ell = 5$, and lose the remaining four newforms at $\ell = 7$: we conclude $\mathcal{S}_{f,\{5,7\}} = \varnothing$.

For the two irrational forms f_9 and f_{11}, since the conductor N of $E_{B,n}$ is $N = 2 \cdot 3^3 \cdot 11 \operatorname{rad}_{2,3}(Z_n)$, and the level of the newform is $N_p = 2 \cdot 3^3 \cdot 11$, if we choose $\ell \neq 2$, 3 or 11 then $\ell^2 \nmid N$ and $\ell \nmid N_p$ so we can use Proposition 5.2.9 (with $t = 1$) which states that if $E \sim_p f$ we have $p \mid B_\ell(f)$ for all such ℓ. For f_9 (and its Galois conjugate $\sigma(f_9) = f_{10}$) the Fourier coefficients generate a number field in $\alpha = -3 + 2\sqrt{10}$ (respectively $\sigma(\alpha) = -3 - 2\sqrt{10}$) with defining polynomial $x^2 + 6x - 31$. We find $c_5(f_9) = -1 + \sqrt{10} \notin \mathbb{Q}$; so with $S_5 = \{0, \pm 1, \pm 2, \pm 3, \pm 4\}$ we proceed to find $B_5(f_9)$.

$$\begin{aligned} B_5(f_9) &= 5\mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}\left((5+1)^2 - c_5(f_9)^2\right) \prod_{a \in S_5} \mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(a - c_5(f_9)) \\ &= 5\mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}\left(25 + 2\sqrt{10}\right)\ \mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(-c_5)\ \mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(c_5^2 - 1^2) \\ &\qquad \times \mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(c_5^2 - 2^2)\ \mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(c_5^2 - 3^2)\ \mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(c_5^2 - 4^2) \\ &= -511758000 \\ &= -2^4 \cdot 3^9 \cdot 5^3 \cdot 13. \end{aligned}$$

We can not do the same for $B_7(f_9)$ since $c_7(f_9) = 2 \in \mathbb{Q}$, but we can For $\ell = 13$:

$$\begin{aligned} B_{13}(f_9) &= -212161890683510065078782764929920000000 \\ &= -2^{12} \cdot 3^{25} \cdot 5^6 \cdot 13^5 \cdot 37^2 \cdot 43 \cdot 53 \cdot 67 \cdot 71^2 \end{aligned}$$

Hence, since 2, 3, 5, and 13 divide $B_5(f_9)$ and $B_{13}(f_9)$, but 37, 43, 53, 67 and 71 divide $B_{13}(f_9)$ and not $B_5(f_9)$, we deduce that $E \sim_p f_9$ is not possible for $p \geq 17$.

For f_{11} (and its Galois conjugate $\sigma(f_{11}) = f_{12}$) the Fourier coefficients generate a number field in $\beta = 2 + \sqrt{10}$ (respectively $\sigma(\beta) = 2 - \sqrt{10}$) with defining polynomial $x^2 - 4x - 6$. We find $c_5(f_{11}) = 1 + \sqrt{10} \notin \mathbb{Q}$ and so as with f_9 we compute $B_5(f_{11})$:

$$\begin{aligned} B_5(f_{11}) &= 5\mathcal{N}_{\mathbb{Q}(\beta)/\mathbb{Q}}\left((5+1)^2 - c_5(f_{11})^2\right) \prod_{a \in S_5} \mathcal{N}_{\mathbb{Q}(\beta)/\mathbb{Q}}(a - c_5(f_{11})) \\ &= 7676370000 \\ &= 2^4 \cdot 3^{10} \cdot 5^4 \cdot 13. \end{aligned}$$

For $\ell = 13$:

$$\begin{aligned} B_{13}(f_{11}) &= -303907573141244147275013149764480000000 \\ &= -2^{12} \cdot 3^{25} \cdot 5^6 \cdot 13^5 \cdot 37 \cdot 43 \cdot 53^2 \cdot 67 \cdot 71^2 \end{aligned}$$

We see we are in analogous situation as for f_9, and thus deduce that $E \sim_p f_{11}$ is not possible for $p \geq 17$.

We note $B_5(f_{11})$ and $B_5(f_9)$ both have the same prime factors, with the largest prime factor dividing them being 13. So for the irrational newforms we have, by Proposition 5.2.9, that for any $p > 13$, $E_{B,n} \not\sim_p f_k$ for $k = 9$, 11.

Hence, in accord with Reynolds, we find there can be no PIPs on E_{11} as no rational newforms correlate to any elliptic curves pertaining to a solution, with the caveat that any prime exponent $p \geq 7 + 1 + 2\sqrt{7}$, which is $p \geq 17$, or for the case of irrational newforms we (also) have the bound $p \geq 17$, and so we take $p_0 = 17$. Hence any possible prime exponents for a p^{th} perfect power remaining by this method are $p = 2$, 3, 5, 7, 11, or 13.

8.1.1 Sage Code for Case 2 of Example 8.1.1

We give here the Sage code for working out the prime bound for the irrational newforms of level 594 in Case 2 of Example 8.1.1.

To start with we need to know the q-expansions of the two irrational newforms and where the first irrational coefficients occur:

```
N=[Newforms(594,2,names='a')[k] for k in range(8,10)]
```

```
q - q^2 + q^4 + (a8 + 1)*q^5 + O(q^6)
q + q^2 + q^4 + (a9 - 1)*q^5 + O(q^6)
```

We know that there are, up to isogeny, ten newforms in total, and this is why we choose our range as range(8,10) since we only need the two irrational newforms (the irrational newforms come after the rational ones in Sage, and Sage sorts its lists starting with index 0, with range(i, j) returning [i, i+1, i+2, ..., j−1]: this explains the ranges chosen in the program). By observation of the q-expnsions we find the first irrational coefficients occur for $c_5(f_9)$, and $c_5(f_{11})$.

Now that we know we need to work with the coefficients c_5, we have to compute $B_5(f)$ from Proposition 5.2.9 to get a bound for p in the irrational case. The following code computes the prime factorisation of $B_5(f)$ for each irrational newform in turn and outputs the next greatest prime p_0 for which $E \not\sim_{p_0} f$.

```
l=5
N=[Newforms(594,2,names='a')[k] for k in range(8,10)]
c=[N[j].q_expansion(6)[5] for j in range(0,2)]

for j in range(0,2):
    A=[i-c[j] for i in range(1-l,l-1)]
    B=list(factor(norm(((l+1)^2-c[j]^2)*prod(A))))
    p=B[len(B)-1][0]
    next_prime(p)
```

Working step by step: we first set l=5, and then initialise the two irrational newforms, up to isogeny, of level 594, after which the coefficients c_5 for each newform are computed:

```
c=[N[j].q_expansion(6)[5] for j in range(0,2)]
```

```
[a8 + 1, a9 - 1]
```

Now each of the $(a - c_\ell)$ factors in the product $\prod_{a \in S_\ell} \mathcal{N}_{K/\mathbb{Q}}(a - c_\ell)$ are computed:

```
A=[i-c[j] for i in range(1-l,l-1)]
```

```
[-a8 - 5, -a8 - 4, -a8 - 3, -a8 - 2, -a8 - 1, -a8, -a8 + 1, -a8 +
    2]
[-a9 - 3, -a9 - 2, -a9 - 1, -a9, -a9 + 1, -a9 + 2, -a9 + 3, -a9 +
    4]
```

The next command forms the product $\prod_{a \in S_\ell} \mathcal{N}_{K/\mathbb{Q}}(a - c_\ell)$ of these factors as `prod(A)` and then computes the norm, `norm(((l+1)^2-c[j]^2)*prod(A))`, which is the norm of $B_5'(f)$ from Proposition 5.2.9, which it outputs as a list of factors:

```
B=list(factor(norm(((l+1)^2-c[j]^2)*prod(A))))
```

```
[(2, 4), (3, 9), (5, 2), (13, 1)]
[(2, 4), (3, 10), (5, 3), (13, 1)]
```

The last two lines of code pick out the last prime in the factor list, which is 13 in both cases, and outputs the next prime:

```
p=B[len(B)-1][0]
next_prime(p)
```

```
17, 17
```

Thus giving the bound of $p_0 = 17$.

This code can now easily be adapted for working with irrational newforms of other levels.

Example 8.1.2. For the rank 1 curve $E_{39}\colon y^2 = x^3 + 39$, having trivial torsion, and generator $P = (\frac{217}{4}, \frac{3197}{8})$, we find $f_2 = 1$ since $2 \mid B_1$, and so B_n is always even, and $v_3(39) = 1$ hence $f_3 = 4$ if $3 \nmid B_n$:

$$N_p = \begin{cases} 2 \cdot 3^2 \cdot 13 = 234 & \text{if } 3 \mid Z_n \text{ and } C_n \equiv 1 \pmod 4, \\ 2 \cdot 3^4 \cdot 13 = 2106 & \text{if } 3 \nmid Z_n,\ C_n \equiv 1 \pmod 4 \text{ and end at Tate's case 3.} \end{cases} \tag{8.1.5}$$

Case 1. There exist five rational newforms, and no irrational newforms, of level $N_p = 234$ (see Table 8.1.1). We lose two newforms f_2 and f_5 at $\ell = 5$; lose two newforms f_3 and f_4 at $\ell = 7$; lose the last newform f_1 at $\ell = 11$: $\mathcal{S}_{f,\{5,7,11\}} = \varnothing$.

$$\begin{aligned}
f_1 &= q - q^2 + q^4 - 2q^5 - 2q^7 - q^8 + 2q^{10} - \cdots, \\
f_2 &= q - q^2 + q^4 + q^5 + q^7 - q^8 - q^{10} + \cdots, \\
f_3 &= q + q^2 + q^4 - 2q^5 + 4q^7 + q^8 - 2q^{10} + \cdots, \\
f_4 &= q + q^2 + q^4 + 2q^5 - 2q^7 + q^8 + 2q^{10} + \cdots, \\
f_5 &= q + q^2 + q^4 + 3q^5 - q^7 + q^8 + 3q^{10} - \cdots.
\end{aligned}$$

Table 8.1.1: Newforms (up to Conjugacy) on $\Gamma_0(234)$ of Weight 2

Case 2. There exist twenty-two newforms of level $N_p = 2106$; six are rational, and sixteen irrational (see Table 8.1.2). For the rational case we lose the two newforms f_2 and f_3 at $\ell = 5$; we lose the remaining six newforms at $\ell = 7$: we conclude $\mathcal{S}_{f,\{5,7\}} = \varnothing$.

For $k = 7$ to 22 the Fourier coefficients of f_k generate a number field in α_k with defining polynomial as given in Table 8.1.3. We find we only need the q-expansion up to $O(q^6)$, since $5 \nmid N$ or N_p, and in all cases we find $c_5 \notin \mathbb{Q}$, and so can be sure $B_5(f) \neq 0$ for all newforms: thus we can use Proposition 5.2.9 (with $t = 1$) to find a bound for p such that if $p \geq p_0$ then $E_{B,n} \not\sim_p f$; see Table 8.1.3 for the p_0 for each irrational newform as given by the Proposition 5.2.9.

Now to find our general bound we note that for the rational newform case for level $N_p = 234$ we have $\mathcal{S}_{f,\{5,7\}} = \varnothing$, and for level $N_p = 2106$, $\mathcal{S}_{f,\{5,7,11\}} = \varnothing$. Hence for the rational case we take the largest prime occurring in these sets and use the bound from Proposition 7.1.1 to give $p \geq 11 + 1 + 2\sqrt{11}$, i.e., $p \geq 19$ in the rational case. We now compare this with the prime bounds p_0 calculated for the irrational newforms, as tabulated in Table 8.1.3, and find the (much) larger prime $p_0 = 239$ for irrational newforms f_{20} and f_{22}. We therefore choose this larger prime as our bound and conclude there can be no PIPs on E_{39} with $p \geq 239$, with possible prime exponents for a p^{th} perfect power having p necessarily less than 239.

Continuing in the manner above using `Pari/GP` we arrive at the following:

$$
\begin{aligned}
f_1 &= q - q^2 + q^4 + O(q^6),\\
f_2 &= q - q^2 + q^4 + 2q^5 + O(q^6),\\
f_3 &= q - q^2 + q^4 + 2q^5 + O(q^6),\\
f_4 &= q + q^2 + q^4 - 2q^5 + O(q^6),\\
f_5 &= q + q^2 + q^4 - 2q^5 + O(q^6),\\
f_6 &= q + q^2 + q^4 + O(q^6),\\
f_7 &= q - q^2 + q^4 + (\alpha_7 + 1)q^5 + O(q^6),\\
f_8 &= q - q^2 + q^4 + (\alpha_8 + 1)q^5 + O(q^6),\\
f_9 &= q - q^2 + q^4 - (\alpha_9 + 1)q^5 + O(q^6),\\
f_{10} &= q - q^2 + q^4 - \tfrac{1}{2}(\alpha_{10} + 1)q^5 + O(q^6),\\
f_{11} &= q - q^2 + q^4 + \tfrac{1}{2}(\alpha_{11} + 1)q^5 + O(q^6),\\
f_{12} &= q + q^2 + q^4 + \tfrac{1}{2}(\alpha_{12} - 1)q^5 + O(q^6),\\
f_{13} &= q + q^2 + q^4 - \tfrac{1}{2}(\alpha_{13} - 1)q^5 + O(q^6),\\
f_{14} &= q + q^2 + q^4 - \tfrac{1}{2}(\alpha_{14} - 1)q^5 + O(q^6),\\
f_{15} &= q + q^2 + q^4 + (\alpha_{15} - 1)q^5 + O(q^6),\\
f_{16} &= q + q^2 + q^4 - (\alpha_{16} - 1)q^5 + O(q^6),\\
f_{17} &= q - q^2 + q^4 + (\alpha_{17} + 1)q^5 + O(q^6),\\
f_{18} &= q + q^2 + q^4 + (\alpha_{18} - 1)q^5 + O(q^6),\\
f_{19} &= q - q^2 + q^4 - (\alpha_{19} + 1)q^5 + O(q^6),\\
f_{20} &= q - q^2 + q^4 - \tfrac{1}{2}(\alpha_{20} + 1)q^5 + O(q^6),\\
f_{21} &= q + q^2 + q^4 + \tfrac{1}{2}(\alpha_{21} - 1)q^5 + O(q^6),\\
f_{22} &= q + q^2 + q^4 - (\alpha_{22} - 1)q^5 + O(q^6).
\end{aligned}
$$

Table 8.1.2: Newforms (up to Conjugacy) on $\Gamma_0(2106)$ of Weight 2

Theorem 8.1.3 (Buck)**.** *Let $E_D\colon y^2 = x^3 + D$ be a Mordell curve. Take*

$$(D; P; \mathcal{S}, N_p; \#\ \textit{Rational}; \#\ \textit{Irrational}; p_0)$$

as in Table 8.1.4 and Table 8.1.5: P is a nontorsion point on E_D; $\mathcal{S}$ is the set of primes of bad reduction for the point; N_p is the conductor of the Frey curves after level lowering; # Rational is the number of rational newforms of level N_p; # Irrational is the number of irrational newforms of level N_p. Then there does not

Irrational Newform	Defining polynomial of Number Field	p_0
f_7	x^2+6x+3	31
f_8	x^2+2x-5	7
f_9	x^2+4x+1	29
f_{10}	x^2+6x-3	29
f_{11}	$x^2-2x-11$	29
f_{12}	$x^2+2x-11$	29
f_{13}	x^2-6x-3	29
f_{14}	x^2-6x-3	29
f_{15}	x^2-2x-5	7
f_{16}	x^2+2x-5	31
f_{17}	$x^3+5x^2-4x-29$	71
f_{18}	$x^3-5x^2-4x+29$	71
f_{19}	$x^4+2x^3-14x^2+6x+9$	89
f_{20}	$x^4-66x^2+72x+9$	239
f_{21}	$x^4-62x^2-168x+37$	89
f_{22}	$x^4-2x^3-15x^2+7x+1$	239

Table 8.1.3: Irrational Newforms of Level 2106 and their Number Fields

exist a B_{nP} which is a perfect p^{th} power with $p \geq p_0$, where we note for the best possible bound of $p \geq 11$, we exclude $p = 13$.

Since our program starts testing primes at $\ell = 5$, for reasons explained in Section 7.1, then if we get rid of all newforms at $\ell = 5$, we have by Proposition 7.1.1 that our bound for the rational newform case is $p \geq (\sqrt{5}+1)^2 \approx 10.47$, which has $p \geq 11$, which is then best possible (assuming any irrational newform bound had $p \geq 11$). With this understood we can invoke Theorem 5.3.3 which has $p = 11$ or $p \geq 17$ as conditions on p. Hence Theorem 8.1.3 can say nothing of p^{th} powers for $p = 2$, 3, 5, 7, or 13, for reasons wrapped up in Theorem 5.3.3, which in turn inherits from Theorem 5.2.6 on the absence of p-isogenies whose condition (e) disallows $p = 2$, 3, 5, 7, or 13.

In the case where we were unable to compute the irrational newforms due to constraints of time, we were still able to give the bound for any rational PIPs independently from any irrational case.

Theorem 8.1.4 (Buck)**.** *Let* $E_D\colon y^2 = x^3 + D$ *be a Mordell curve. Take*

$$(D; P; \mathcal{S}; N_p; \#\ \textit{Rational}; p_0)$$

as in Table 8.1.6 and Table 8.1.7: P *is a nontorsion point on* E_D*;* $\mathcal{S}$ *is the set of primes of bad reduction for the point;* N_p *is the conductor of the Frey curves after level lowering;* # *Rational is the number of rational newforms of level* N_p*. Then there does not exist a* B_{nP} *which is a perfect* p^{th} *power with* $p \geq p_0$ *corresponding to a rational newform, where we note for the best possible bound of* $p \geq 11$*, we exclude* $p = 13$*.*

Table 8.1.4: Rank 1 Mordell Curves $E\colon y^2 = x^3 + D$ with no PIPs $\geq p_0$

D	$P \in E_0$	$\mathcal{S}$	$\{N_p;$ # Rational; # Irrational$\}$	p_0
11	$(-\frac{7}{4}, \frac{19}{8})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 11;\ 2;\ 0\}; \{2 \cdot 3^3 \cdot 11;\ 8;\ 2\}$	17
39	$(\frac{217}{4}, \frac{3197}{8})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 13;\ 5;\ 0\}; \{2 \cdot 3^4 \cdot 13;\ 6;\ 16\}$	239
46	$(-\frac{7}{4}, \frac{51}{8})$	$\{3\}$	$\{2 \cdot 3^2 \cdot 23;\ 4;\ 3\}; \{2 \cdot 3^3 \cdot 23;\ 16;\ 4\}$	71
47	$(\frac{17}{4}, \frac{89}{8})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 47;\ 7;\ 4\}; \{2 \cdot 3^3 \cdot 47;\ 6;\ 8\}$	293
58	$(\frac{241}{36}, \frac{4087}{216})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 29;\ 13;\ 0\}$	11
61	$(-\frac{15}{4}, \frac{23}{8})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 61;\ 12;\ 5\}; \{2 \cdot 3^3 \cdot 61;\ 12;\ 18\}$	3701
62	$(\frac{1}{4}, \frac{63}{8})$	$\{3\}$	$\{2 \cdot 3^2 \cdot 31;\ 8;\ 2\}; \{2 \cdot 3^3 \cdot 31;\ 10;\ 10\}$	193
66	$(\frac{1}{4}, \frac{65}{8})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 11;\ 5;\ 0\}$	23
67	$(\frac{49}{36}, \frac{1801}{216})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 67;\ 6;\ 9\}$	107
83	$(\frac{2641}{36}, \frac{135737}{216})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 83;\ 5;\ 9\}$	421
118	$(\frac{9}{4}, \frac{91}{8})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 59;\ 12;\ 4\}; \{2 \cdot 3^3 \cdot 59;\ 22;\ 16\}$	4201
139	$(-\frac{1223}{324}, \frac{53837}{5832})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 139;\ 11;\ 15\}$	14563
147	$(\frac{1}{4}, \frac{97}{8})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 7;\ 2;\ 0\}$	11
166	$(-\frac{3207}{1444}, \frac{683251}{54872})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 83;\ 5;\ 9\}; \{2 \cdot 3^3 \cdot 83;\ 0;\ 20\}$	51437

Continued on next page

Table 8.1.4 – *Continued from previous page*

D	$P \in E_0$	$\mathcal{S}$	$\{N_p;$ # Rational; # Irrational$\}$	p_0
183	$(-\frac{47}{9}, \frac{172}{27})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 61;\ 12;\ 5\}; \{2 \cdot 3^3 \cdot 61;\ 12;\ 18\}$	3701

Table 8.1.5: Rank 1 Mordell Curves $E\colon y^2 = x^3 - D$ with no PIPs $\geq p_0$

D	$P \in E_0$	$\mathcal{S}$	$\{N_p;$ # Rational; # Irrational$\}$	p_0
43	$(\frac{1177}{36}, \frac{40355}{216})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 43;\ 9;\ 4\}$	31
57	$(\frac{4873}{36}, \frac{340165}{216})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 19;\ 7;\ 0\}$	11
58	$(\frac{5393}{484}, \frac{387655}{10648})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 29;\ 13;\ 0\}; \{2 \cdot 3^3 \cdot 29;\ 18;\ 6\}$	43
65	$(\frac{32049}{7396}, \frac{2573303}{636056})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 5 \cdot 13;\ 14;\ 3\}; \{2 \cdot 3^3 \cdot 5 \cdot 13;\ 23;\ 19\}$	331
66	$(\frac{357361}{7056}, \frac{213574985}{592704})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 11;\ 5;\ 0\}$	11
75	$(\frac{91}{9}, \frac{836}{27})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 5;\ 3;\ 0\}; \{2^5 \cdot 3^2 \cdot 5;\ 4;\ 0\}$	23
85	$(\frac{1552601}{27889}, \frac{1934117206}{4657463})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 7;\ 2;\ 0\}; \{2^2 \cdot 3^2 \cdot 7;\ 2;\ 0\}; \{2^3 \cdot 3^2 \cdot 7;\ 8;\ 0\}; \{2^4 \cdot 3^2 \cdot 7;\ 13;\ 1\}$	17
91	$(\frac{25}{4}, \frac{99}{8})$	$\{3\}$	$\{2 \cdot 3^2 \cdot 7 \cdot 13;\ 20;\ 5\}; \{2 \cdot 3^3 \cdot 7 \cdot 13;\ 28;\ 5\}$	19
101	$(\frac{6342921}{1073296}, \frac{11415613595}{1111934656})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 101;\ 13;\ 11\}; \{2 \cdot 3^3 \cdot 101;\ 16;\ 16\}$	3935389
120	$(\frac{169}{9}, \frac{2177}{27})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 5;\ 3;\ 0\}; \{2^5 \cdot 3^2 \cdot 5;\ 4;\ 0\}$	23
123	$(\frac{3193}{144}, \frac{179405}{1728})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 41;\ 10;\ 3\}$	19
129	$(\frac{55380313}{2039184}, \frac{410799717341}{2911954752})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 43;\ 9;\ 4\}$	31
131	$(\frac{3409}{144}, \frac{198055}{1728})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 131;\ 25;\ 9\}$	2549
166	$(\frac{13433}{676}, \frac{1540339}{17576})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 83;\ 5;\ 9\}; \{2 \cdot 3^3 \cdot 83;\ 0;\ 20\}$	51437

Continued on next page

Table 8.1.5 – *Continued from previous page*

D	$P \in E_0$	$\mathcal{S}$	$\{N_p;$ # Rational; # Irrational$\}$	p_0
171	$(\frac{10105}{1764}, \frac{305299}{74088})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 19;\ 7;\ 0\}$	11
195	$(\frac{5281}{36}, \frac{383761}{216})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 5 \cdot 13;\ 14;\ 3\}$	29

Table 8.1.6: Rank 1 Mordell Curves $E\colon y^2 = x^3 + D$ with no Rational PIPs $\geq p_0$

D	$P \in E_0$	$\mathcal{S}$	$\{N_p;\ \#\text{ Rational}\}$	p_0
69	$(-\frac{5}{9}, \frac{224}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 23;\ 4\};\ \{2^5\cdot 3^2\cdot 23;\ 10\}$	17
74	$(\frac{7}{9}, \frac{233}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 37;\ 7\};\ \{2^7\cdot 3^2\cdot 37;\ 20\}$	17
77	$(-\frac{61}{25}, \frac{988}{125})$	$\varnothing$	$\{2\cdot 3^2\cdot 7\cdot 11;\ 12\};\ \{2\cdot 3^3\cdot 7\cdot 11;\ 28\};\ \{2^5\cdot 3^2\cdot 7\cdot 11;\ 26\};\ \{2^5\cdot 3^3\cdot 7\cdot 11;\ 32\}$	29
102	$(\frac{763}{529}, \frac{124675}{12167})$	$\varnothing$	$\{2\cdot 3^2\cdot 17;\ 4\};\ \{2^7\cdot 3^2\cdot 17;\ 16\}$	17
103	$(\frac{13}{9}, \frac{278}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 103;\ 10\};\ \{2^6\cdot 3^2\cdot 103;\ 44\};\ \{2\cdot 3^3\cdot 103;\ 4\};\ \{2^6\cdot 3^3\cdot 103;\ 23\}$	19
110	$(\frac{59}{121}, \frac{13967}{1331})$	$\varnothing$	$\{2\cdot 3^2\cdot 5\cdot 11;\ 12\};\ \{2\cdot 3^3\cdot 5\cdot 11;\ 29\};\ \{2^7\cdot 3^2\cdot 5\cdot 11;\ 96\};\ \{2^7\cdot 3^3\cdot 5\cdot 11;\ 102\}$	2521
111	$(-\frac{215}{121}, \frac{13664}{1331})$	$\varnothing$	$\{2\cdot 3^2\cdot 37;\ 7\};\ \{2^6\cdot 3^2\cdot 37;\ 66\}$	29
130	$(\frac{399}{169}, \frac{26287}{2197})$	$\varnothing$	$\{2\cdot 3^2\cdot 5\cdot 13;\ 14\};\ \{2\cdot 3^3\cdot 5\cdot 13;\ 23\};\ \{2^7\cdot 3^2\cdot 5\cdot 13;\ 96\};\ \{2^7\cdot 3^3\cdot 5\cdot 13;\ 72\}$	113
133	$(\frac{39}{25}, \frac{1462}{125})$	$\varnothing$	$\{2\cdot 3^2\cdot 7\cdot 19;\ 15\};\ \{2\cdot 3^3\cdot 7\cdot 19;\ 19\};\ \{2^5\cdot 3^2\cdot 7\cdot 19;\ 44\};\ \{2^5\cdot 3^3\cdot 7\cdot 19;\ 32\}$	29
146	$(\frac{3215}{361}, \frac{200249}{6859})$	$\varnothing$	$\{2\cdot 3^2\cdot 73;\ 7\};\ \{2\cdot 3^3\cdot 73;\ 6\};\ \{2^7\cdot 3^2\cdot 73;\ 20\};\ \{2^7\cdot 3^3\cdot 73;\ 0\}$	11
149	$(-\frac{7}{16}, \frac{781}{64})$	$\varnothing$	$\{2\cdot 3^2\cdot 149;\ 17\};\ \{2\cdot 3^3\cdot 149;\ 2\}$	19
155	$(-\frac{271}{64}, \frac{4553}{512})$	$\varnothing$	$\{2\cdot 3^2\cdot 5\cdot 31;\ 29\};\ \{2\cdot 3^3\cdot 5\cdot 31;\ 20\}$	29
179	$(-\frac{35}{9}, \frac{296}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 179;\ 9\};\ \{2^6\cdot 3^2\cdot 179;\ 76\}$	17
182	$(\frac{7219}{81}, \frac{613439}{729})$	$\varnothing$	$\{2\cdot 3^2\cdot 7\cdot 13;\ 20\};\ \{2^7\cdot 3^2\cdot 7\cdot 13;\ 84\}$	29

Continued on next page

Table 8.1.6 – *Continued from previous page*

D	$P \in E_0$	$\mathcal{S}$	$\{N_p;$ # Rational; # Irrational$\}$	p_0
191	$(\frac{399}{4}, \frac{26287}{8})$	$\varnothing$	$\{2 \cdot 3^2 \cdot 191;\ 2\}; \{2 \cdot 3^3 \cdot 191;\ 0\}$	11

Table 8.1.7: Rank 1 Mordell Curves $E\colon y^2 = x^3 - D$ with no Rational PIPs $\geq p_0$

D	$P \in E_0$	$\mathcal{S}$	$\{N_p;\ \#\text{ Rational}\}$	p_0
21	$(\frac{37}{9}, \frac{118}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 7;\ 2\}$; $\{2^6\cdot 3^2\cdot 7;\ 40\}$	29
22	$(\frac{71}{25}, \frac{119}{125})$	$\varnothing$	$\{2\cdot 3^2\cdot 11;\ 5\}$; $\{2\cdot 3^3\cdot 11;\ 10\}$; $\{2^7\cdot 3^2\cdot 11;\ 32\}$; $\{2^7\cdot 3^3\cdot 11;\ 32\}$	29
29	$(\frac{3133}{9}, \frac{175364}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 29;\ 13\}$; $\{2^6\cdot 3^2\cdot 29;\ 84\}$	19
30	$(\frac{31}{9}, \frac{89}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 5;\ 3\}$; $\{2^7\cdot 3^2\cdot 5;\ 48\}$	29
38	$(\frac{4447}{441}, \frac{291005}{9261})$	$\varnothing$	$\{2\cdot 3^2\cdot 19;\ 7\}$; $\{2^7\cdot 3^2\cdot 19;\ 32\}$	29
50	$(\frac{211}{9}, \frac{3059}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 5;\ 3\}$; $\{2^7\cdot 3^2\cdot 5;\ 48\}$	29
51	$(\frac{13175}{9}, \frac{50986}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 17;\ 4\}$; $\{2^5\cdot 3^2\cdot 17;\ 18\}$	23
59	$(\frac{6715}{441}, \frac{545644}{9261})$	$\varnothing$	$\{2\cdot 3^2\cdot 59;\ 12\}$; $\{2^5\cdot 3^2\cdot 59;\ 8\}$	19
84	$(\frac{46}{9}, \frac{190}{27})$	$\{2\}$	$\{2^2\cdot 3^4\cdot 7;\ 4\}$; $\{2^4\cdot 3^4\cdot 7;\ 24\}$	19
93	$(\frac{1249}{225}, \frac{29818}{3375})$	$\varnothing$	$\{2\cdot 3^2\cdot 31;\ 6\}$; $\{2^6\cdot 3^2\cdot 31;\ 62\}$	29
94	$(\frac{11614031}{2181529}, \frac{24303384785}{3222118333})$	$\varnothing$	$\{2\cdot 3^2\cdot 47;\ 8\}$; $\{2\cdot 3^3\cdot 47;\ 6\}$; $\{2^7\cdot 3^2\cdot 47;\ 12\}$; $\{2^7\cdot 3^3\cdot 47;\ 22\}$	29
102	$(\frac{127}{9}, \frac{1405}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 17;\ 4\}$; $\{2^7\cdot 3^2\cdot 17;\ 16\}$	53
110	$(\frac{41671}{8649}, \frac{1091611}{804357})$	$\varnothing$	$\{2^7\cdot 3^2\cdot 5\cdot 11;\ 70\}$	17
115	$(\frac{2419}{441}, \frac{65512}{9261})$	$\varnothing$	$\{2\cdot 3^2\cdot 5\cdot 23;\ 19\}$; $\{2^5\cdot 3^2\cdot 5\cdot 23;\ 38\}$	29

Continued on next page

Table 8.1.7 – *Continued from previous page*

D	$P \in E_0$	$\mathcal{S}$	$\{N_p;\ \#\text{ Rational}\}$	p_0
130	$(\frac{1811}{289}, \frac{52931}{4913})$	$\varnothing$	$\{2\cdot 3^2\cdot 5\cdot 13;\ 48\}$; $\{2\cdot 3^3\cdot 5\cdot 13;\ 24\}$; $\{2^7\cdot 3^2\cdot 5\cdot 13;\ 96\}$; $\{2^7\cdot 3^3\cdot 5\cdot 13;\ 72\}$	47
137	$(\frac{141}{25}, \frac{814}{125})$	$\varnothing$	$\{2\cdot 3^2\cdot 137;\ 11\}$; $\{2\cdot 3^3\cdot 137;\ 8\}$; $\{2^6\cdot 3^2\cdot 137;\ 68\}$; $\{2^6\cdot 3^3\cdot 137;\ 56\}$	29
138	$(\frac{427}{81}, \frac{2125}{729})$	$\varnothing$	$\{2\cdot 3^4\cdot 23;\ 7\}$; $\{2^7\cdot 3^2\cdot 23;\ 12\}$	17
140	$(\frac{949}{9}, \frac{29233}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 5\cdot 7;\ 10\}$; $\{2^2\cdot 3^2\cdot 5\cdot 7;\ 10\}$; $\{2^3\cdot 3^2\cdot 5\cdot 7;\ 20\}$; $\{2^4\cdot 3^2\cdot 5\cdot 7;\ 42\}$	23
157	$(\frac{374822317}{4678569}, \frac{7255575252640}{10119744747})$	$\varnothing$	$\{2\cdot 3^2\cdot 157;\ 10\}$; $\{2^6\cdot 3^2\cdot 157;\ 50\}$	23
163	$(\frac{97}{16}, \frac{495}{64})$	$\{3\}$	$\{2\cdot 3^2\cdot 163;\ 15\}$; $\{2\cdot 3^3\cdot 163;\ 16\}$	19
164	$(\frac{333}{49}, \frac{4199}{343})$	$\varnothing$	$\{2\cdot 3^2\cdot 41;\ 9\}$; $\{2^2\cdot 3^2\cdot 41;\ 2\}$; $\{2\cdot 3^3\cdot 41;\ 4\}$; $\{2^3\cdot 3^2\cdot 41;\ 8\}$; $\{2^2\cdot 3^3\cdot 41;\ 6\}$; $\{2^4\cdot 3^2\cdot 41;\ 24\}$; $\{2^3\cdot 3^3\cdot 41;\ 11\}$; $\{2^4\cdot 3^3\cdot 41;\ 24\}$	29
165	$(\frac{229}{9}, \frac{3448}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 5\cdot 11;\ 12\}$; $\{2^6\cdot 3^2\cdot 5\cdot 11;\ 112\}$	47
166	$(\frac{13433}{676}, \frac{1540339}{17576})$	$\varnothing$	$\{2\cdot 3^2\cdot 83;\ 5\}$; $\{2\cdot 3^3\cdot 83;\ 0\}$	17
173	$(\frac{189}{25}, \frac{2012}{125})$	$\varnothing$	$\{2\cdot 3^2\cdot 173;\ 7\}$; $\{2\cdot 3^3\cdot 173;\ 6\}$; $\{2^6\cdot 3^2\cdot 173;\ 42\}$; $\{2^6\cdot 3^3\cdot 173;\ 20\}$	23
179	$(\frac{65}{4}, \frac{513}{8})$	$\{3\}$	$\{2\cdot 3^2\cdot 179;\ 10\}$; $\{2\cdot 3^3\cdot 179;\ 10\}$	19
182	$(\frac{14743}{2601}, \frac{44225}{132651})$	$\varnothing$	$\{2\cdot 3^2\cdot 7\cdot 13;\ 20\}$; $\{2^7\cdot 3^2\cdot 7\cdot 13;\ 84\}$	29
187	$(\frac{5047}{9}, \frac{358550}{27})$	$\varnothing$	$\{2\cdot 3^2\cdot 11\cdot 17;\ 17\}$; $\{2^5\cdot 3^2\cdot 11\cdot 17;\ 32\}$	23

Chapter 9

Final Remarks and a Look to Further Work

To extend on the case of curves containing integral points, as for $y^2 = x^3 - 2$, maybe it would be possible to use similar methods as contained in the work of [8] to get an upper bound on n such that B_n is a perfect power, by the use of elliptic logarithms, which is small enough to meet the lower bound we get. Despite other attempts it is always possibile to continue looking at more cases modulo ℓ to get stronger congruence conditions on n.

The method described in this thesis can only deal with prime exponents $p = 11$, or $p \geq 17$ in the rational newform case, along with any irrational newform case. Maybe we could find some other complementary *ad-hoc* techniques to help in eliminating cases of p^{th} perfect powers, as we did with the method of Chabauty in Section 6.3.

So far we only treat EDSs (or equivalently rank 1 curves with no torsion). It would be interesting to try to adapt those methods to look at power integral points on curves of higher rank. For this the idea would be to use a similar method as in the rank 1 case outlined in the thesis, but this time initially for a 2-dimensional array. The idea is similar to the rank 1 case: we associate a Frey curve to a rank 2 Mordell curve and compute the traces at a prime ℓ using a rank 2 version of our `Pari/GP` program `clnewform`. This forms a matrix of traces of dimension $r_P(\ell) \times r_Q(\ell)$, where $r_P(\ell)$, and $r_Q(\ell)$ are the rank of apparition at ℓ for the EDSs

associated to the points P and Q respectively. For each prime we do this for we obtain a rectangular array of `Pari/GP` 'intmods' for which we can use the Chinese Remainder Theorem on, using a rank 2 matrix version of our vectorial CRT program `chinchin`. Then after using the CRT on the arrays we should disprove the existence of any PIPs from occurring after some prime bound $p \geq p_0$.

Partial work has been done on this problem for Mordell curves of rank 2 possessing no integral points, and we hope to see the first substantial results of these endeavours soon.

Appendix A

Pari/GP Programs

Listing A.1: Introduction

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ Throughout an elliptic divisibility sequence shall be denoted as an
\\ eds and given in the form of the first four terms as a vector.
\\ By an eds being nondegerate we shall mean the first, second, and
\\ third terms are nonzero.
\\ Where formulae are referenced by name they are from the following
\\ sources - added here to avoid repetition:
\\ Morgan Ward:
\\ Memoir on Elliptic Divisibility Sequences, 1948.
\\ Rachel Shipsey:
\\ Elliptic Divisibility Sequences, University of London, 2000.
\\ Christine Swart:
\\ Elliptic  Curves and Related Sequences, University of London, 2003.
\\ Katherine Stange:
\\ Elliptic Nets and Elliptic Curves, Brown University, 2008.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
```

Listing A.2: Elliptic Curve Functions

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ The primes of bad reduction for an integral elliptic curve over Q
\\ e is an ellinit; returns a vector of primes dividing the
\\ discriminant (so these are bad reduction for this model but may not be
\\ bad for the underlying elliptic curve if this is not a minimal model)
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
ellbadprimes(e) = return(factor(abs(e[12]))[ ,1]~);
}
```

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ pntbadprimes(e, p)
\\ e is an elliptic curve and p = [a/b^2, c/b^3] is a point on that
\\ curve. pntbadprimes(e, p) returns the primes of singular reduction
\\ that divide both wh2 = w2 * b^3 and wh3 = w3 * b^8.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
pntbadprimes(e, p) = local(b, w, whn, wh, wh2, wh3, v, S);
  if(ellisoncurve(e, p) == 0, print("Point p is not on curve."); return(0));
  b = round(sqrt(abs(denominator(p[1]))));
  whn = vector(4);
  wh = vector(4);
  v = vector(2);
  S = vector(0);
  w = elltoeds(e, p);

  for(i = 1, 4, wh[i] = w[i] * b^(i^2 - 1));
    if(debug, print("Normalised Psihat Division Polynomials: " wh));
  wh2 = factor(abs(wh[2]))~[1, ];
  wh3 = factor(abs(wh[3]))~[1, ];
  v = [wh2, wh3];
  if(debug, print("Primes dividing wh2, wh3: " v));
  for(i = 1, length(v[1]),
    for(j = 1, length(v[2]),
      if(v[1][i] == v[2][j], S = concat(S, v[1][i]))));
  return(S);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ goodl(e, p)
\\ Takes as input an ellinit, e, and a point p on e.
\\ Program sets BP = 4 * product of primes of bad reduction P, for p on e.
\\ Then checks at index i from 1 through to
\\ (4 * product of bad primes P) - 1, whether i = 1 (mod 4), and if so
\\ tests if it is a square modulo P. Returns a 2-vector of squares modulo
\\ each bad prime P,  and value of n.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
goodl(e, p) = local(P, y, n, m);
  P = pntbadprimes(e, p);
  y = [];
  n = 4;
  for(i = 1, length(P), n = n * P[i];
  if(debug, print("mod " n)); );
    for(i = 1, n - 1, m = 1;
      if(Mod(i, 4) != Mod(1, 4), m = 0,
        for(j = 1, length(P), if(kronecker(i, P[j]) != 1, m = 0)));
          if(m == 1, y = concat(y, i)));
```

```
  return([y, n]);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ ellinput(N, mod)
\\ Returns a vector G of length(ellsearch(N)) of initialised elliptic
\\ curves of conductor N along with congruence conditions predetermined
\\ by M. Used by clnewform. M = [[1, 2,..., m - 1], m].
\\ If no value for mod is given it deferrs to an
\\ initialised value of 1.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
ellinput(N, mod = 1) = local(F, G);
  F = ellsearch(N);
  G = vector(0);
  m = vector(0);

  if(mod == 1,
  for(i = 1, length(F),
    G = concat(G, [[ellinit(F[i][2], 1), [0], 1]]));
  return(G););

  if(mod != 1,
  for(i = 1, mod - 1, m = concat(m, i));
  for(i = 1, length(F),
    G = concat(G, [[ellinit(F[i][2], 1), m, mod]])));
  return(G);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ ellgensearch(N)
\\ Lists the generators for all curves of conductor N.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
ellgensearch(N) = local(f, v);
  f = ellsearch(N);
  v = vector(0);
  for(i = 1, length(f),
    if(f[i][3]! = [], v = concat(v, f[i][3]), v = concat(v, [[0]])));
  return(v);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ elljsearch(N)
\\ Lists the j-invariants for all curves of conductor N. If two curves
\\ having the same conductor have the same j value, they will just be
\\ quadratic twists of each other.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
```

```
{
elljsearch(N) = local(f, v);
  f = ellsearch(N);
  v = vector(0);
  for(i = 1, length(f), v = concat(v, (ellinit(f[i][1]).j)));
  return(v);
}
```

Listing A.3: Functions Concerning EDSs & Related Seqences

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ elltoeds(e, p)
\\ Given as arguments an elliptic curve e, and a point p on e,
\\ outputs the first four terms of the elliptic curves associated
\\ elliptic sequence as a row vector.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
elltoeds(e, p) = local(a1, a2, a3, a4, a6, b2, b4, b6, b8, w);
  if(ellisoncurve(e, p) == 0, print("Point p is not on curve.");
    return(0));
  a1 = e.a1; a2 = e.a2; a3 = e.a3; a4 = e.a4; a6 = e.a6;
      \\ ai invariants of curve
  b2 = e.b2; b4 = e.b4; b6 = e.b6; b8 = e.b8;   \\ bi invariants of curve
  w = vector(4);

  w[1] = 1;
  w[2] = 2 * p[2] + a1 * p[1] + a3;
  w[3] = 3 * p[1]^4 + b2 * p[1]^3 + 3 * b4 * p[1]^2 + 3 * b6 * p[1] + b8;
  w[4] = w[2] * (2 * p[1]^6 + b2 * p[1]^5 + 5 * b4 * p[1]^4
  + 10 * b6 * p[1]^3 + 10 * b8 * p[1]^2 + (b2 * b8 - b4 * b6)
      * p[1] + b4 * b8 - b6^2);

  return(w);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ elltodds(e, p, n)
\\ Returns a vector of the first n terms of the DDS associated to the
\\ points [n]p on an elliptic curve e.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
elltodds(e, p, n) = local(vec);
  if(ellisoncurve(e, p) == 0, print("Point p is not on curve.");
    return(0));
  vec = vector(n);
  for(i = 1, n,
    vec[i] = round(sqrt(abs(denominator(ellpow(e, p, i)[1])))));
```

```
  return(vec);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ elltonormdds(e, p, n)
\\ Returns a vector of the first n terms of the normalised DDS
\\ associated to the points [n]p on an elliptic curve e.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
elltonormdds(e, p, n) = local(b1, vec);
  if(ellisoncurve(e, p) == 0, print("Point p is not on curve.");
    return(0));
  b1 = round(sqrt(abs(denominator(p[1]))));
  vec = vector(n);
  for(i = 1, n,
    vec[i] = round(sqrt(abs(denominator(ellpow(e, p, i)[1])))) / b1);
  return(vec);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ edsrankofapp(e, p, l)
\\ Given an eds w and a prime l returns the index of the first zero
\\ modulo l. Modified from code of Stange's to incorporate a check up to
\\ the Hasse bound.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
edsrankofapp(e, p, l) = local(v, vp, X, Xbase, HB);
  if(ellisoncurve(e, p) == 0, print("Point p is not on curve.");
        return(0));

  v = factor(denominator(p[1]));
      \\ checks l not a prime factor of denominator of p[1]
  vp = v[ , 1]~;
  for(i = 1, length(vp),
    if(l == vp[i], print("Prime divides denominator."); return(0), ));

  w = elltoeds(e, p);
  X = vector(5);
  Xbase = vector(5);
  HB = floor(2 * sqrt(l)) + l + 1;
  if(isprime(l) != 1, print("Term not prime."); return(0); );

      \\ 'X' stores at each round the most recent block of five terms
      \\ Start with the terms of eds, plus the zeroth term,
      \\ which is 0.  Return index if a zero is found.
  X[1] = 0;
  for(i = 1, 4, X[i + 1] = w[i];
    if(Mod(X[i + 1], l) == 0, return(i)));
```

```
      \\ 'Xbase' keeps a permanent record of these first five terms
      \\ for use in the recurrence which checks up to the Hasse bound
  Xbase = X;
  for(i = 5, HB, X = edsblockincrement(X, Xbase);
    if(Mod(X[5], l) == 0, return(i)));
  return(0);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ edstau(e, p, l)
\\ Given an elliptic curve e, a point p on e, and a prime l returns the
\\ arithmetic period of the sequence.
\\ These use formulae due to M. Ward.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
edstau(e, p, l) = local(v, r, w, b, wn, ep, k, a, tau);
  v = vector(5);
  wn = vector(4);
  r = edsrankofapp(e, p, l);

      \\ Rank must be greater than 3
  if(r <= 3,
    if(debug, print("Rank of " l " is " r
              ". Rank must be greater than 3.")); return(0));

      \\ l = 2 is not allowed explicitly and must be worked out for
      \\ each of 2 possible cases
  if(l == 2 && r == 4, return(1));
  if(l == 2 && r == 5, return(1));

  w = elltoeds(e, p);
    if(debug, print("Normal EDS: " w));
  b = round(sqrt(abs(denominator(p[1]))));
  for(i = 1, 4, wn[i] = w[i] * b^(i^2 - 1));
    if(debug, print("Normalised EDS: " wn));
  ep = znorder(Mod(wn[2] / edsget(wn, r - 2), l));
  k = znorder(Mod(edsget(wn, r - 1), l));
  a = 0;
  if(Mod(ep, 2) == 1 && Mod(k, 2) == 1, a = 1,
  if(valuation(ep, 2) == valuation(k, 2), a = -1)); tau = 2^a * lcm(ep, k);
  if(debug,
    print1("Rank = " r ", Order W(2)/W(r-2) = " ep ", Order W(r-1) = "
      k ", alpha = " a ", tau = " tau));
  return(tau);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ edsperiod(e, p, l)
```

```
\\ Given an elliptic curve e, a point p on e, edsperiod returns the
\\ rank, tau, and period of the sequence modulo a prime l.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
edsperiod(e, p, l) = local(r, tau, rt);
  r = edsrankofapp(e, p, l);
  if(r == 1, rt = 1; tau = 1);
  if(r == 2, rt = edsperiodr(e, p, l); tau = rt / r);
  if(r == 3, rt = edsperiodr(e, p, l); tau = rt / r);
  if(r > 3, tau = edstau(e, p, l); rt = r * tau);
  return([r, tau, rt]);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ edsperiodr(e, p, l)
\\ Returns the period of the sequence. Uses a linear method to calculate
\\ terms one after another until the period is found.
\\ 'Non-degerate' means the first, second, and third terms are non-zero.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
edsperiodr(e, p, l) = local(X, Xnew, Xbase, W);
  X = vector(5);
  Xnew = vector(5);
  Xbase = vector(5);

  W = elltoeds(e, p);
  W = W * Mod(1, l);
      \\ 'X' stores at each round the most recent block of five terms
      \\ Start with the terms of eds, plus the zeroth term, which is 0.
  X[1] = 0;
  for(i = 1, 4, X[i + 1] = W[i]);
      \\ 'Xbase' keeps a permanent record of these first five terms
      \\ for use in the recurrence
  Xbase = X;
      \\ loop up to max of 10^8 searching for a zero
  for(i = 1, 10^8, X = edsblockincrement(X, Xbase);
  if(X == Xbase, return(i)));
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ edsperiodbndrt(e, p, bnd, rtbnd)
\\ Returns a vector of 2-vectors [l, [r(l), t(l), rt(l)]] for primes in
\\ the range l = 2 up to bnd, where r(l), t(l), rt(l) are the rank, tau,
\\ and arithmetic period of l respectively w.r.t the eds w. The function
\\ returns all vectors for which the arithmetic period rt(l) is < rtbnd.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
```

```
edsperiodbndrt(e, p, bnd, rtbnd) = local(epp, u);
  epp = vector(0);
  u = vector(0);
  forprime(i = 1, bnd,
    epp = concat(epp, [[i, edsperiod(e, p, i)]]));
  for(j = 1, length(epp),
    if(epp[j][2][3] < rtbnd,
    u = concat(u,
      [[prime(j), [epp[j][2][1], epp[j][2][2], epp[j][2][3]]]])));
  return(u);
}
```

Listing A.4: Chinese Remainder Sieve Functions

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ chinchin(x, y)
\\ Input x = [x[1], x[2]], where x[1] is a vector of lifted intmods
\\ modulo m = x[2], and y is similar, with modulus n = y[2].
\\ gcdext(m, n) returns the vector [u, v, g] such that g is the
\\ gcd: mu + nv = gcd(m, n) = g (Bezout's identity).
\\ For those intmods in the same residue class modulo the gcd(m, n),
\\ i.e., if a = b (mod gcd(m, n)) then chinchin solves the
\\ system {z = a (mod m), z = b (mod n); which has as solution:
\\ z = (anv + bmu)/g (mod M), where M = lcm(m, n). (See proof below for
\\ an explanation.)
\\ chinchin first checks the sets of lifted intmods differ mod x[2], and
\\ if not returns the input. If they do differ chinchin then repeatedly
\\ works through each list of lifted intmods in x[1] and y[1] testing
\\ them to see if x[i] (Mod(G)) == y[j] (Mod(G)) (for index i in
\\ {1,..,length(x[1])}, and j in {1,..,length(y[1])}). If so the CRT
\\ can be used as explained above, and chinchin outputs the results as a
\\ sorted list of intmods modulo the lcm(m, n) = M.
\\ (Proof: mu + nv = g, so (mu + nv)/g = 1. Hence given the system
\\ {z = a (mod m), z = b (mod n); multiply by z to give
\\ (zmu + znv)/g = z. Now modulo m: (zmu + znv)/g = znv/g = z (mod m),
\\ and since z = a (mod m) we can replace z thus: anv/g = a (mod m).
\\ Similarly looking modulo n gives the result: bmu/g = b (mod n). Now
\\ if x is any solution we have x = z (mod m) and x = z (mod n) which
\\ implies m and n both divide x - z, and so M = lcm(m, n) divides
\\ x - z. This gives the general result as:
\\ z = (anv + bmu)/g (mod M)). q.e.d.)
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
chinchin(x, y) = local(a, b, v, w, bez, g, M, crt, crts);
  a = vector(0);
  b = vector(0);
  v = x[1];
  w = y[1];
  bez = gcdext(x[2], y[2]);
```

```
  g = bez[3];
    if(debug, print("g is " g));

  M = (x[2] * y[2]) / g; \\ lcm of x[2], y[2]
  crt = vector(0);

  if(debug, print("First check there is something to do."));
      \\ if g = x[2] and the sets x[1] and y[1](mod x[2]) do not
      \\ differ then return(y)
        if(g == x[2],
           if(setminus(Set(w * Mod(1, g)), Set(v)) == [], print("No!");
        return(y)));
        if(debug, print("Yes!"));
  for(i = 1, length(v), a = v[i];
        if(debug, print("The " i "th row of " length(v)));

    for(j = 1, length(w), b = w[j];
      if(Mod(a, g) == Mod(b, g),
        crt = concat(crt, Mod(lift(a) + bez[1] * x[2] * (lift(b) - lift(a)) / g,
                M)))));
  if(debug, print(crt));
  if(debug, print("Now time to sort."));

  crts = vecsort(lift(crt));
  return([crts * Mod(1, M), M]);
}
```

Listing A.5: Vector Comparison Functions

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ cutrep(x)
\\ Input vector x; cutrep strips any repetitions and outputs vector y.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
cutrep(x) = local(y, v, t);
        y = vector(0);
        t = 1;
        for(i = 1, length(x), v = x[i]; t = 1;
      for(j = 1, length(y),
        if(y[j] == v, t = 0));
      if(t == 1, y = concat(y, v)));
        return(y);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ compare(x, c)
\\ Given a vector x = [v, m], where v = ellapfreyn(e, p, l) is a vector
\\ of integers, with m and c integers; m will in general be a modulus,
\\ and c a trace of an elliptic curve: c = ellap(Y[i][1], l).
```

```
\\ compare(x, c) returns a 2-vector [w, m], where w is a concatenated
\\ (sorted) vector of lifts of the intmods Mod(i, m) when v[i] == c, and
\\ m = x[2].
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
compare(x, c) = local(w, v, m);
  v = x[1];
  m = x[2];
  w = vector(0);
  for(i = 1, length(v),
    if(v[i] == c, w = concat(w, lift(Mod(i, m)))));
  return([vecsort(w, , 8), m]);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ primeab(a, b)
\\ Given two integers a and b, primeab outputs the set of primes within
\\ the range [a, b].
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
primeab(a, b) = local(Q);
  Q=vector(0);
  for(i = a, b - 3,
    Q = concat(Q, nextprime(i)));
  return(vecsort(Q, , 8));
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ vecfactor(vec)
\\ Given a vector of n entries, returns the factorised entries.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
vecfactor(vec) = local(vf);
  n = matsize(vec)[2];
  vf = vector(n);
  for(i = 1, n,
    if(vec[i] == 1, vf[i] = [1, 1],
      if(vec[i] == -1, vf[i] = [-1, 1], vf[i] = factor(vec[i]))));
  return(vf);
}
```

Listing A.6: Newform Q-Series Coefficient Generation & Sieve Functions

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ ellapfreyn(e, p, l)
\\ Input an elliptic curve e, along with a point p on e, and l a prime.
\\ The function works out period = rt of the EDS w, along with the
```

```
\\ coefficients An, and Cn modulo l of the rt amount of Frey curves:
\\ Y^2 = X^3 - 3 * An + 2 * Cn.
\\ The EDS is first taken term-by-term modulo l and screened for trivial
\\ cases, then generated for rt + 1 values. Then the intmods An are
\\ computed via the values of the EDS and the use of the division
\\ polynomial formula for Phin(p), and the scaling
\\ An(P) = Phin(P) * B1(P)^{2n^2}.
\\ The Cn are then computed using the defining equation of the Mordell
\\ curve: y^2 = x^3 + D, from the just computed An, along with the
\\ scaling: Psin(P) * B1(P)^{n^2}.
\\ Each of the Frey curves are then initialised in turn, and for each
\\ curve computes the trace at l and outputs these as a vector.
\\ When working out the trace, since the discriminant of the Frey curve
\\ is d = 2^6 * 3^3 * (An^3 - Cn^2), then we take the trace of
\\ Y^2 = X^3 - 3 * (An  - l) + 2Cn,
\\ where it is understood An and Cn are taken modulo l as intmods,
\\ to force the curve to be nonsingular at l.
\\ Since the value Cn appears squared in the associated Diophantine
\\ equation, it is of no consequence if we take Cn = 1 (mod 4) when
\\ initiallising the Frey curve.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
ellapfreyn(e, p, l) = local(w, ep, D, r, rt, b1, W, a, b, c, ac, V, B);

  w = elltoeds(e, p);
  ep = edsperiod(e, p, l);
  D = p[2]^2 - p[1]^3;
  r = ep[1];
  rt = ep[3];
  b1 = Mod(round(sqrt(abs(denominator(p[1])))), l);
  if(r == 1, \\ rank = 1 so all terms 0 mod l
    W = vector(4) * Mod(0, l));
  if(r == 2 && rt == 2, \\ rank = 2 so every second term 0 mod l
    W = vector(4);
    W[1] = Mod(w[1], l);
    W[2] = Mod(w[2], l);
    W[3] = Mod(w[3], l);
    W[4] = Mod(w[4], l);
    );
  if(r == 2 && rt > 2, \\ rank = 2 so every second term 0 mod l;
    W = vector(rt + 1); \\ set the first 4 terms then use recurrence
    W[1] = Mod(w[1], l);
    W[2] = Mod(w[2], l);
    W[3] = Mod(w[3], l);
    W[4] = Mod(w[4], l);
    for(i = 5, rt + 1,
      if(Mod(i, 2) == Mod(0, 2),
        W[i] = Mod(0, l),
        W[i] = - W[3] * W[1] * W[i - 2]^2 / W[i - 4])));
```

```
  if(r >= 3 && rt > 0,  \\ w[1], w[2] mod l != 0 so
              \\ can use edsgen directly.
      W = edsgen(Mod(w, l), rt + 1));

  a = vector(rt);
  a[1] = Mod(numerator(p[1]), l);
  for(i = 2, rt,
    a[i] = (p[1] * W[i]^2 - W[i - 1] * W[i + 1]) * b1^(2 * i^2));
    \\if(debug, print("An vector ", lift(a)));

  c = vector(rt);
  for(i = 1, rt,
    c[i] = sqrt(a[i]^3 + D * (W[i] * b1^(i^2))^6));
  ac = vector(0);
  ac = lift([a, c]);
  V = vector(rt);
  for(i = 1, rt,
    V[i] =
    ellap(ellinit([0, 0, 0, -3 * (ac[1][i] - l), 2 * ac[2][i]]), l)
    );
  return(V);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ clnewform(e, p, Y, U, Q, l, bd)
\\ e and p are an elliptic curve-point pair,
\\ Y = ellinput(N, m), U = goodl(ellinit([0, 0, 0, 0, D], 1), p)
\\ Q = product of primes, l = prime, bd = bound.
\\ Returns a vector of indices modulo the period of the sequence for
\\ matching traces.
\\
\\ Program first checks l >= 5.
\\ Program then checks if l is a factor of the denominator of p[1], and
\\ if so skips this prime as we cannot use edsrankofapp in this case.
\\ clnewform uses the compare function to compare the traces at a prime
\\ l of the Frey curves, as given by ellapfreyn(e, p, l), with those of
\\ the set of elliptic curves of conductor N output by ellinput(N, m).
\\ Firstly it sets up the computation by disregarding any primes l with
\\ period M greater than the bound parameter bd.
\\
\\ The value Q is used by the program as another bound, this time in the
\\ size of the modulus the congruences are allowed to have. First it
\\ checks if gcd(Q, M) = 1, and if so returns Y.
\\
\\ If -1 is a square modulo l and all primes of bad reduction are
\\ squares modulo l then we can check the actual values of ellap with
\\ those traces of the Frey curves; otherwise we only check their
\\ absolute values.
\\
\\ The compare routine then outputs a 2-vector W of congruences W[1],
```

```
\\ and a modulus W[2]. We now compute m = gcd(W[2], Q^20) and set this
\\ as the new modulus. W then has any repetitions removed by the cutrep
\\ routine, and is then sorted w.r.t order modulo m, and subsequently
\\ stripped of any equivalent congruences by the routine cutallmod to
\\ output the new W = [W[1], W[2]].
\\ Now the algorithm uses the Chinese Remainder Theorem (CRT) to compare
\\ the sets of congruences contained in W with those associated with
\\ each curve in Y; it does this with the chinchin function. If we are
\\ lucky the output of chinchin is empty and we have lost a curve
\\ (equivalently a newform by modularity!), but if not we invoke
\\ cutallmod on the remaining congruences, and then concat them into a
\\ new vector with the associated form and modulus.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
clnewform(e, p, Y, U, Q, l, bd)
      = local(v, vp, D, ep, r, M, n, H, W, m, G, g, X, Z);
  if(l == 2 || l == 3, return(Y), );    \\ checks l >= 5

  v = factor(denominator(p[1]));
      \\ checks l not a prime factor of denominator of p[1]
  vp = v[ , 1]~;
  for(i = 1, length(vp),
    if(l == vp[i], return(Y), ));
  b = elltoeds(e, p);
  ep = edsperiod(e, p, l);
  r = ep[1];
  M = ep[3];
  if(debug, print("Start testing for prime " l "; period is " M "
          which factorizes as " factor(M)));
  if(M > bd, if(debug, print("Period is larger than the bound " bd "
          so skip this one."); return(Y)));
  n = gcd(M, Q^20);
  if(n == 1, if(debug, print("No Q-part.")); return(Y));
  H = vector(0);
  W = vector(0);
    if(debug, print("Call ellapfreyn."));
  X = ellapfreyn(e, p, l);

  for(i = 1, length(Y),
    if(debug, print("We are testing the " i "th form."));
      if(debug, print("Call compare."));
      \\ If -1 is a square mod l and all primes of bad
      \\ reduction are squares mod l then we can check the
      \\ actual values of ellap; otherwise only check
      \\ their absolute values.
  if(setsearch(U[1], lift(Mod(l, U[2]))) > 0,
    if(debug, print("Test actual value."));
    W = compare([X, M], ellap(Y[i][1], l)),
    if(debug, print("Test absolute value."));
```

```
    W = compare([abs(X), M], abs(ellap(Y[i][1], l))));

  if(debug, print("W is of length " length(W[1]) " and modulo " W[2]));
    m = W[2];
    n = gcd(m, Q^20);
    m = n;
    W = [vecsort(lift(cutrep(W[1] * Mod(1, m)))) * Mod(1, m), m];
    if(debug, print("After vecsort, W is of length "
          length(W[1]) " and modulo " W[2]));
    W = cutallmod(W, 100); \\ strips any equivalent congruences
    if(debug, print("After cutting, W is of length " length(W[1]) "
        and modulo " W[2]));
    m = W[2];
    g = Y[i][3];
  Z = chinchin(W, [Y[i][2], g]);
  if(Z[1] != [], if(debug, print("Call cutallmod."));
    G = cutallmod(Z, 100); if(debug, print("Call concat: too bad."));
    H = concat(H, [[Y[i][1], G[1], G[2]]]),
    if(debug, print("We have just lost the form " Y[i]));));
  return(H);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ clnewformall(e, p, Y, Q, L, M, bd)
\\ e, p, Y, Q, bd are as in clnewform; see there for description.
\\ L and M give lower and upper limits resp. for range of primes to
\\ use in clnewform.
\\ For each form there in Y there is initially one defining congruence.
\\ Whenever clnewform is run at a prime l, after the algorithm completes
\\ if any forms remain they make up the output, along with all the extra
\\ congruences that are generated to the new modulus.
\\ This output has the same form as the 3-vector Y, and we now rerun
\\ clnewform on it at the next prime. Doing so we seek to elliminate all
\\ newforms if possible, or get increased strengthing of our congruences
\\ of the index n.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
clnewformall(e, p, Y, Q, L, M, bd) = local(D, U);
  D = p[2]^2 - p[1]^3;  \\ D = Mordell curve a6 invariant
  U = goodl(ellinit([0, 0, 0, 0, D], 1), p);
  forprime(l = L, M, Y = clnewform(e, p, Y, U, Q, l, bd);
    if(Y == [], print("Finished at prime " l "."); return(Y););
      if(debug, print("We are at prime " l " and there are " length(Y[1][2]) "
        congruence possibilities."));
      if(length(Y[1][2]) > 1,
      if(debug, print("The minimum value is " Y[1][2][2] "
        where the modulo factorizes as " factor(Y[1][3])))));
    return(Y);
}
```

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ tracecl(e, p, Np, bnd)
\\ Input elliptic curve e, point p, level Np, lower bound 5, and upper
\\ bound bnd.
\\ tracecl tests for Frey curve traces = +/-1, indicating multiplicative
\\ reduction, then computes the difference
\\ a_l(E_{W,n}) * (l + 1) - c_l(f_i)
\\ for the multiplicative reduction case; otherwise computes the
\\ difference a_l(E_{W,n}) - c_l(f_i) in the good reduction case, and in
\\ both cases factors the results to show which primes p have E_{B,n}
\\ arise modulo p from the newform in question. The lower bound is
\\ hardcoded as 5, since this is the least prime we must check.
\\ This difference in the trace of Frey curve and newform coefficient is
\\ in accord with the theorem of Kraus and Oesterle and outputs primes
\\ we cannot deal with as explained in Proposition 8.5.1 of the thesis.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
tracecl(e, p, Np, bnd) = local(Y, X, PG, PM, P, pgm, L);
  Y = ellinput(Np);
  P = vector(0);
  PG = vector(0);
  PM = vector(0);
  pgm = vector(0);
  L = bnd;
  \\ First test for Frey curve traces al(E{Wn}) = +/-1, indicating
  \\ multiplicative reduction, then find the difference of the trace
  \\ of the Frey curve and newform coefficient in accord with Kraus
  \\ and Oesterle.
  forprime(l = 5, L, X = vecsort(cutrep(ellapfreyn(e, p, l)));
    if(debug, print1("Frey curve traces for " l ":" X));
    for(i = 1, length(X),
      for(j = 1, length(Y), if(X[i] == 1 || X[i] == -1,
        PM = vecsort(concat(PM, abs(X[i] * (l + 1) - ellap(Y[j][1], l))), , 8),
        PG = vecsort(concat(PG, abs(X[i] - ellap(Y[j][1], l))), , 8))));
      if(debug, print1("Multiplicative reduction case: " PM));
      if(debug, print1("Good reduction case: " PG));
          P = vecsort(concat(PM, PG), , 8);
      \\if(debug, print("Difference: " P));
    for(i = 1, length(P),
      if(P[i] != 0, pgm = concat(pgm, factor(abs(P[i]))[ , 1]~)));
  return(vecsort(pgm, , 8));
}
```

Listing A.7: Functions to Shrink the Dimension of Vectors of Intmods

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ cutmod(x, p)
\\ Checks if the gcd of the length l of vector v = x[1] and the modulus
```

```
\\ m = x[2] is 0 mod p, and if so sets m and l to m/p, l/p resp. Then
\\ starts a loop to check whether intmods mod p, from v[1] to v[l] equal
\\ the l blocks of intmods mod p starting from v[1 + l] up to
\\ v[l + l * (p - 1)], (where l = l/p is the 'new' l). If so returns the
\\ vector of shortened intmods modulo the smaller modulus.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
cutmod(x, p) = local(v, m, y, l);
  v = x[1];
  m = x[2];
  l = length(v);
  while(Mod(gcd(m, l), p) == Mod(0, p),
    m = m / p;
    l = l / p;
    y = vector(0);
    for(i = 1, l,
      for(j = 1, p - 1,
        if(Mod(v[i], m) != Mod(v[i + l * j], m),
    return([v, p * m])));
        y = concat(y, Mod(v[i], m)));
        v = y;
        );
  return([v, m]);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ cutallmod(x, n)
\\ cutallmod calls cutmod for each prime in range 1 to n.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
cutallmod(x, n) = forprime(i = 1, n, x = cutmod(x, i));
        return(x);
}
```

Listing A.8: Functions to Calculate the Conductor

```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ rad23(D)
\\ Given an integer D, returns the radical of D less any factors 2 and 3.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
rad23(D) = local(rad23, r23);
  rad23 = [];
  Df = factor(abs(D));

  for(i = 1, length(Df[ , 1]~),
    if(Df[, 1]~[i] != 2 && Df[ , 1]~[i] != 3,
```

```
      rad23 = concat(rad23, Df[ , 1]~[i]));
      if(debug,
        print("Radical{2, 3}("D") prime factors are " rad23));
    r23 = 1;
    for(i = 1, length(rad23), r23 = r23 * rad23[i]);
  return(r23);
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ f2(p)
\\ Gives the exponent f2 of the factor 2 of the conductor, N, of an
\\ elliptic Frey curve associated to a Mordell curve E_D, and point p
\\ on E_D. First checks that v_2(D) < 6. Next checks if B1 is even, and
\\ if so sets f2 = 1. If not it then checks valuation v_2(D)
\\ against the tables along with any conditions on the initial point.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
f2(p) = local(D, a, b, c, f2);
  D = p[2]^2 - p[1]^3;
  if(valuation(D, 2) >= 6,
    print("D has to be 6th power free."); return(0));
  if(ellisoncurve(ellinit([0, 0, 0, 0, D]), p) == 0,
    print("Point p is not on curve."); return(0));
  f2 = [];
  \\ Setup A1, B1, C1
  a = numerator(p[1]);
  b = round(sqrt(abs(denominator(p[1]))));
  c = numerator(p[2]);
    \\if(debug, print("[A, B, C] = " [a, b, c]));

    \\ If b is even, then every multiple of p has Bn even;
    \\ then since a, b, c are pairwise coprime, An, and Cn
    \\ are both odd for all n, and it doesn't matter about
    \\ the parity of D in this case, and f2 = 1 in all cases.
  if(Mod(b, 2) == 0, f2 = [1]; return(f2));
    \\ Set f2 = 1 to cover general case when Bn even.
    f2 = [1];

  if(valuation(D, 2) == 1, f2 = concat(f2, [7]));
  if(valuation(D, 2) == 2, f2 = concat(f2, [2, 3, 4]));
  if(valuation(D, 2) == 3, f2 = concat(f2, [5]));
  if(valuation(D, 2) == 4, f2 = concat(f2, [3]));
  if(valuation(D, 2) == 5, f2 = concat(f2, [3]));


  if(Mod(D, 8) == 1 && Mod(a, 2) == 0, f2 = concat(f2, [6]));
  if(Mod(D, 4) == 1 && Mod(c, 2) == 0, f2 = concat(f2, [5]));
  if(Mod(D, 4) == 3, f2 = concat(f2, [6]));
```

```
  return(vecsort(f2, ,8));
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ f3(p)
\\ Gives the exponent f3 of the factor 3 of the conductor, N, of an
\\ elliptic Frey curve associated to a Mordell curve E_D, and point pnt
\\ on E_D. First checks that v_3(D) < 6. If 3 divides B_1, 3 divides
\\ B_n for all terms and so exits with f3 =2.
\\ If not 3 divides B_n at some point so set f2 = [2] for this
\\ possibility. Now checks valuation v_3(D)
\\ against the tables along with any conditions on the initial point.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
f3(p) = local(D, a, b, c, c4, c6, c42, c63, f3, P2);
  D = p[2]^2 - p[1]^3;
  if(valuation(D, 3) >= 6,
    print("D has to be 6th power free."); return(0));
  if(ellisoncurve(ellinit([0, 0, 0, 0, D]), p) == 0,
    print("Point p is not on curve."); return(0));
  f3 = [];

  a = numerator(p[1]);
  b = round(sqrt(abs(denominator(p[1]))));
  c = numerator(p[2]);
      \\ If 3 divides b, then every multiple of pnt has b
      \\ divisible by 3, then since a, b, c are pairwise
      \\ coprime, 3 never divides An, Cn.
  if(Mod(b, 3) == 0, f3 = [2]; return(f3));
      \\ Set f3 = 2 to cover general case when 3\mid Bn.
  f3 = [2];

  if(valuation(D, 3) == 1, f3 = concat(f3, [4]));
  if(valuation(D, 3) == 2, f3 = concat(f3, [3]));
  if(3 <= valuation(D, 3) <= 5, f3 = concat(f3, [2]));

  \\ Test for Papadopolous's condition P2.
  \\ Set P2 = 1 if P2 is satisfied, and P2 = 0 if not.
  c4 = 2^4 * 3^2 * a;
  c6 = 2^6 * 3^3 * c;
  c42 = c4 / 3^2;
  c63 = c6 / 3^3;
  v3c4 = valuation(c4, 3);
  v3c6 = valuation(c6, 3);

  if(v3c4 >= 2 && v3c6 == 3 &&
        Mod(c63^2 + 2 - 3 * c42, 9) == 0, P2 = 1, P2 = 0);
    if(debug, print("P2 " P2));
  if(Mod(D, 3) == 1 && Mod(a, 3) == 0 && P2 == 1,
```

```
    f3 = concat(f3, [2]), f3 = concat(f3, []));

  if(Mod(D, 3) == 1 && Mod(a, 3) == 0 && P2 == 0,
    f3 = concat(f3, [3]), f3 = concat(f3, []));

  if((Mod(D, 9) == 1 || Mod(D, 9) == -1) && Mod(c, 3) == 0,
    f3 = concat(f3, [2, 3]));

  if(Mod(D, 3) == 2,
    if(P2 == 1, f3 = concat(f3, [2]), f3 = concat(f3, [3])));

  return(vecsort(f3, , 8));
}

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ ellmordnp(p)
\\ Gives the conductor, Np, after level lowering of an elliptic curve e.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

{
ellmordnp(p) = local(D, np, f2D, f3D, r23);
  D = p[2]^2 - p[1]^3;
  np = vector(0);
  f2D = f2(p);
  f3D = f3(p);
  r23 = rad23(D);

  if(debug, print("f2D: " f2D));
  if(debug, print("f3D: " f3D));

  for(i = 1, length(f2D),
    for(j = 1, length(f3D),
      np = concat(np, 2^f2D[i] * 3^f3D[j] * r23)));
  if(debug, print("Lowered level: " np));
  return(vecsort(np, , 8));
}
```

Listing A.9: Functions to Calculate EDSs by K. Stange

```
edstools.gp
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ edsblockincrement(wb, w)
\\ Given an eds w in the form of a vector of five terms
\\ (0th through 4th terms) or four terms (1st through 4th), and a block
\\ of length five in that eds, it calculates the block shifted one to the
\\ right. The sequence must be non-degenerate.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ edsgen(ws, len)
```

```
\\ Given an eds ws = [w1, w2, w3, w4] computes the first len terms.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\ edsblockships(w, len)
\\ Given an eds w and an integer len, returns a vector of length 5
\\ containing the terms len - 5  up through len of the sequence.
\\ Uses Shipsey's double-and-add method to generate the final terms in
\\ O(log (len)) time.  Very fast. Accepts negative len.
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
```

These are available as Pari/GP scripts at:
http://math.colorado.edu/~kstange/scripts.html
The file edstools.gp gives a number of Pari/GP programs for the evaluation of EDSs.

Notation

$+$, $-$	addition and negation on an elliptic curve, 14
$a_1, \ldots, a_6$	coefficients of a general Weierstrass equation, 10
$a_\ell(E)$	trace of Frobenius of E at a prime ℓ, 32
$\mathbb{A}^n$	affine n space, 5
$\mathbb{A}^n(K)$	set of K rational points of $\mathbb{A}^n$, 5
$\sim_p$	arises modulo p, 86
$b_1, \ldots, b_8$	quantities associated to a Weierstrass equation, 10
c_4, c_6	quantities associated to a Weierstrass equation, 11
$c_{4,k}$, $c_{6,k}$	$c_{4,k} = c_4/3^k$ and $c_{6,k} = c_6/3^k$, 92
$\chi(p, q, r)$	characteristic of a ternary Diophantine equation, 94
$\mathbb{C}(\Lambda)$	the field of elliptic functions for the lattice Λ, 39
$c_\ell(f)$	the ℓ^{th} Fourier coefficient of a newforms q-expansion, 81
$\Gamma_0(N)$	congruence subgroup, 81
$C(K)$	the set of K rational points on the algebraic curve C/K, 6
(B_n)	denominator divisibility sequence, 75
$\deg(D)$	degree of a divisor, 9
Δ, $\Delta(E)$	elliptic discriminant, 11

$\Delta_{\min}$	minimal discriminant of an elliptic curve E, 29
$\mathrm{Div}(C)$	divisor group of a curve, 9
Ψ_n, Φ_n, Ω_n	n^{th} division polynomials, 46
$\widehat{\Psi}_n$, $\widehat{\Phi}_n$, $\widehat{\Omega}_n$	n^{th} scaled division polynomials, 77
$\mathrm{div}(f)$	divisor of the function f, 9
$E_1(K)$	kernel of reduction modulo a prime p, 30
E_{ns}	nonsingular part of a Weierstrass equation, 19
$E_0(K)$	set of points of $E(K)$ with nonsingular reduction, 30
$E^{(d)}$	quadratic twist of elliptic curve E by d, 35
$\tilde{E}$	reduction of the elliptic curve E modulo p, 29
E_{tors}	torsion subgroup of the elliptic curve E, 21
$E[m]$	m-torsion subgroup of the elliptic curve E, 21
E_D	Mordell elliptic curve: $Y^2 = X^3 + D$, 102
(W_n)	elliptic divisibility sequence, 60
$E_{B,n}$	the Frey curve associated to an EDS, 110
$E_{W,n}$	the twist of the Frey curve $E_{B,n}$, 121
$E(K)$	group of K-rational points on the elliptic curve E/K, 14
$\varnothing$	the empty set, 129
f_2, f_3	exponents of 2, and 3 in level lowered conductor N_p, 96
$\mathfrak{F}_{E,P}$	the finite set of rational newforms of levels N_E corresponding to curve-point pair (E, P), 128
$\mathbb{F}_p$	finite field of p elements, 30
f	newform of weight 2 without character on $\Gamma_0(N)$, 81
g_2, g_3	Eisenstein series $60G_4$ and $140G_6$, 39
G_{2k}	Eisenstein series of weight $2k$, 38
$\mathrm{Gal}(L/K)$	the Galois group of L/K, 82
g	genus of an algebraic curve, 7
j, j_E	j-invariant of an elliptic curve E, 11

$K(C)$	function field of algebraic curve C, 6
$K(E)$	function field of elliptic curve E, 17
K	a number field, 5
$\bar{K}$	an algebraic closure of K, 5
Λ	lattice: $\langle \omega_1, \omega_2 \rangle \subset \mathbb{C}$, 37
Λ_τ	normalised lattice: $\langle 1, \tau \rangle \subset \mathbb{C}$, 37
$\left(\frac{a}{p}\right)$	Legendre symbol, 36
M_P	ideal associated to point P, 8
$M(P)$	$\mathrm{lcm}_{p \in \mathbb{P}}(r(P,p))$, 77
$M(\ell)$	period of eds modulo a prime ℓ, 129
$[m]$	multiplication-by-m map, 15
N, N_E	conductor of an elliptic curve, 31
N_p	level lowered conductor, 85
$\eta(\omega)$	quasiperiod associated to the period ω, 41
O	the identity element of an elliptic curve, 10
$O(1)$	a bounded function, 151
ω_1, ω_2	the periods of a rank 2 lattice, 36
$\pi_\ell(W_n)$	period of eds modulo a prime ℓ, 71
$\mathbb{P}^n$	projective n space, 7
$\mathbb{P}^n(K)$	set of K rational points of $\mathbb{P}^n$, 7
$\tilde{P}$	reduction of the point P modulo p, 29
q	abbreviation for $e^{2\pi i \tau}$, 81
Q_{opt}	optimal Q-part, 137
rad	radical of an integer, 92
r	rank of elliptic curve, 24
$r(\ell)$	rank of apparition of prime ℓ, 69
r_p	reduction map at prime p, 32
R	the ring of integers of a field K, 23
R_S	the ring of S-integers of a field K, 23
$r(P,p)$	order of P in finite group $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, 77
$\mathcal{S}_{f,\mathcal{L}}$	intersection of sets $\mathcal{S}_{f,\ell_i}$, where $\ell_i \in \mathcal{L}$, 129
$\mathcal{S}_{f,\ell}$	set of congruence conditions for rational newform f modulo $M(\ell)$, 128

$\tau(\ell)$	τ-function evaluated at prime ℓ, 71
$\mathcal{T}_\ell$	finite list of possible traces at ℓ, 129
$v_p(a)$	vauation of a at prime p, 58
x, y	Weierstrass coordinate functions, 17
$\wp(z)$	Weierstrass $\wp$-function, 38
$\sigma(z)$	Weierstrass σ-function, 42
$\zeta(z)$	Weierstrass ζ-function, 41

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Math. Appl. Chapman & Hall/CRC, Boca Raton, first edition, 2006.

[2] M. Ayad. Points S-entiers des courbes elliptiques. *Manuscripta Math.*, 76(3-4):305–324, 1992.

[3] M. Ayad. Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques. *Ann. Inst. Fourier (Grenoble)*, 43(3):585–618, 1993.

[4] C. F. Barros. *On the Lebesgue–Nagell equation and related subjects*. Ph.D. thesis, University of Warwick, 2010.

[5] I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian. *Applications of Finite Fields*. The Springer International Series in Engineering and Computer Science 199. Springer US, 1993.

[6] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic Curves in Cryptography*. Cambridge University Press, Cambridge, UK, 1999.

[7] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[8] Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers. *Ann. of Math. (2)*, 163(3):969–1018, 2006.

[9] K. Chandrasekharan. *Elliptic Functions*. Die Grundlehren der Mathematischen Wissenschaften, Band 281. Springer Berlin Heidelberg, 1985.

[10] J. Cheon and S. Hahn. Explicit valuations of division polynomials of an elliptic curve. *Manuscripta Math.*, 97:319–328, 1998.

[11] H. Cohen. *Number Theory: Analytic and Modern Tools v. 2*, volume 240 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2007.

[12] H. Cohen. *Number Theory: Tools and Diophantine Equations v. 1*, volume 239 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2007.

[13] J. E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, Cambridge, second edition, 1997. Available free online at http://homepages.warwick.ac.uk/staff/J.E.Cremona//book/.

[14] S. R. Dahmen. *Classical and Modular Methods Applied to Diophantine Equations*. Ph.D. thesis, Universeit Utrecht, 2008. http://igitur-archive.library.uu.nl/dissertations/2008-0820-200949/UUindex.html.

[15] H. Darmon and A. Granville. On the equations $z^m = f(x, y)$ and $ax^p + by^q = cz^r$. *Bull. London Math. Soc.*, (6):513–543, 1995.

[16] F. Diamond and J. Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[17] J. Diamond and K. Kramer. Modularity of a family of elliptic curves. *Math. Res. lett.*, 2:299–304, 1995.

[18] A. Enge. *Elliptic curves and their applications to cryptography*. Kluwer, 1999.

[19] G. Everest, J. Reynolds, and S. Stephens. On the denominators of rational points on elliptic curves. *Bull. London Math. Soc.*, (5):762–770, 2007.

[20] G. Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpen. *Invent. Math.*, 73:349–366, 1983.

[21] W. Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. Benjamin, New York, 1969.

[22] J. Gebel, A. Petho, and H. G. Zimmer. Computing integral points on elliptic curves. *Acta Arith.*, 68:171–192, 1994.

[23] P. Ingram. Multiples of integral points on elliptic curves. *J. Number Theory*, 129(1):182–208, 2009.

[24] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293:259–275, 1992.

[25] G. Martin. Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(n)$ and $\Gamma_1(n)$. *J. Number Theory*, 112, 2005.

[26] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44:129–162, 1978.

[27] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer Monographs in Mathematics. Springer, Berlin, Heidelberg, third edition, 2004.

[28] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 and 3. *J. Number Theory*, 44:119–152, 1993.

[29] J. Reynolds. Perfect powers in elliptic divisibility sequences. *J. Number Theory*, 132, 2012.

[30] K. Ribet. On the modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. *Invent. Math.*, 100(2):431–476, 1990.

[31] S. Schmitt and H. G. Zimmer. *Elliptic Curves - A Computational Approach*. De Gruyter Studies in Mathematics. Walter de Gruyter, 2004.

[32] R. Shipsey. *Elliptic divisibility sequences*. Ph.D. thesis, Goldsmiths College (University of London), 2000. http://homepages.gold.ac.uk/rachel/#PhD.

[33] C. L. Siegel. Über einige anwendungen diophantischer approximationen. *Abh. Preussischen Akademie der Wissenshaften*, 1929.

[34] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, New York, 1994.

[35] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2009.

[36] J. H. Silverman and N. Stephens. The sign of an elliptic divisibility sequence. *J. Ramanujan Math. Soc.*, 21(1):1–17, 2006.

[37] K. E. Stange. *Elliptic nets and elliptic curves*. Ph.D. thesis, Brown University, 2008.

[38] W. Stein. *Sage: Open Source Mathematical Software (Version* `6.5`*)*. The Sage Group, 2015. `http://sagemath.org`.

[39] C. Swart. *Elliptic curves and related sequences*. Ph.D. thesis, Royal Holloway and Bedford New College (University of London), 2003.

[40] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[41] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[42] The Computational Algebra Group, Sydney. *Magma Calculator*, 2012. Available from `http://magma.maths.usyd.edu.au/calc/`.

[43] The PARI Group, Bordeaux. *PARI/GP version* `2.7.0`, 2014. Available from `http://pari.math.u-bordeaux.fr/`.

[44] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris*, 273:238–241, 1971.

[45] M. Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.

[46] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography (Discrete Mathematics and Its Applications)*. Chapman and Hall/CRC, first edition, 2003.

[47] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Index