

# EXTENDING SIEGEL'S THEOREM FOR ELLIPTIC CURVES

A thesis

submitted to the School of Mathematics

of the University of East Anglia

in partial fulfilment of the requirements

for the degree of

Doctor of Philosophy

By

Jonathan Reynolds

January 2008

© This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with the author and that no quotation from the thesis, nor any information derived therefrom, may be published without the author's prior, written consent.

# Abstract

The Siegel-Mahler theorem says that, for an elliptic curve  $E$  defined over a number field  $K$  and function  $f$  having a pole at the identity of the Mordell-Weil group  $E(K)$ , there are finitely many  $K$ -rational points  $P$  with the denominator of  $f(P)$  divisible by no prime (ideal) in any given ring of  $S$ -integers. An important consequence of this is that there are finitely many integral points on an elliptic curve, and so finitely many terms in an elliptic divisibility sequence are one. The Siegel-Mahler theorem is extended in this thesis as follows. Firstly, given any integer  $n$  not dividing the order of  $f$  at the identity, it is shown that there are still finitely many choices for  $P$  when the denominator of  $f(P)$  is divisible by primes, as long as  $n$  divides the order of each of those primes. In the simplest case this shows that, for  $n > 1$ , there are finitely many  $n$ th powers in an elliptic divisibility sequence. The modular approach for Diophantine equations is used to give an example where the set of these exceptional points has empty intersection with the subgroup  $2E(K)$  when  $n > 5$  is a prime. Secondly, it is shown that when the generators of the Mordell-Weil group are simply magnified (which means they are the image of  $K$ -rational points under an isogeny with degree larger than one) there are finitely many  $K$ -rational points  $P$  with the denominator of  $f(P)$  divisible by less than two distinct primes in any given ring of  $S$ -integers. For the cubic Fermat-Thue curve this is shown unconditionally. Answering a question of Stephens, it is shown that the multiplication by two map will never produce an example of a magnified point (a point having a pre-image in an extension of degree less than four) which is not simply magnified. However, fourteen such examples are found using multiplication by three. Finally, two families of elliptic divisibility sequences whose terms are not prime powers beyond the fifth are given. One of these families includes a subset of the congruent number curves.

# Acknowledgements

I wish to thank Prof. Mike Bennett and Dr Samir Siksek for giving such a practical introduction to the modular approach for Diophantine equations at the Lorenz center in May 2007. This helped me partially answer a question raised by this thesis.

Also, I wish to thank Prof. Joseph Silverman for his many publications on elliptic curves and for suggesting a minor improvement to the text.

Shouts to all the postgrads I've met over the years who have made mathematics not quite such a lonely endeavour.

Finally, I wish to thank my supervisors, Graham and Shaun, for their support and advice.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Number Theory</b>	<b>5</b>
2.1	Basic Definitions . . . . .	5
2.2	Number Fields . . . . .	7
2.3	Heights . . . . .	11
<b>3</b>	<b>Curves</b>	<b>13</b>
3.1	Varieties . . . . .	13
3.2	Maps between Curves . . . . .	16
3.3	Curves of Genus $\geq 1$ . . . . .	18
<b>4</b>	<b>Elliptic Curves</b>	<b>19</b>
4.1	Fundamental Results . . . . .	19
4.2	Isogenies . . . . .	20
4.3	Properties of the Weierstrass Equation . . . . .	23
4.4	Elliptic Curves over $\mathbb{C}$ . . . . .	27
4.5	Heights on Elliptic Curves . . . . .	28
<b>5</b>	<b>Extending Siegel's Theorem</b>	<b>34</b>
5.1	The Siegel-Mahler Theorem . . . . .	35
5.2	Denominators Occurring as $n$ th powers . . . . .	36
5.3	Bounding $n$ using the Modular Approach . . . . .	41

<b>6</b>	<b>Magnified Points</b>	<b>47</b>
6.1	Existence . . . . .	48
6.2	Application to Primality . . . . .	54
<b>7</b>	<b>Elliptic Divisibility Sequences</b>	<b>65</b>
7.1	Definitions . . . . .	65
7.2	Explicit Bounds on Primality . . . . .	67
	<b>References</b>	<b>73</b>

# Chapter 1

## Introduction

A polynomial equation for which we seek only the integer solutions is known as a Diophantine equation. The study of these equations goes back at least to the time of Diophantus in the third century BC. The most famous Diophantine equation is the one appearing in “Fermat’s Last Theorem”. The problem of proving Fermat’s Last Theorem attracted the attention of huge numbers of both professional and amateur Mathematicians for over 350 years, and was finally solved by Wiles in 1994. The Diophantine equation appearing in Fermat’s Last Theorem naturally describes an algebraic curve.

The structure of the set of  $K$ -rational points  $C(K)$  on an algebraic curve  $C$  defined over a number field  $K$  is known to be determined by its genus. There are three cases. The genus 0 case was the first to be understood. If  $C$  has genus 0 then  $C(K)$  either contains no points or infinitely many and may be defined by a linear equation or a conic section. If  $C$  has genus 1 then by specifying a base point  $C$  becomes an elliptic curve and either  $C(K)$  is empty or, by the Mordell-Weil Theorem, is a finitely generated abelian group. Finally, in 1983 Faltings proved that if  $C$  has genus greater than 1 then  $C(K)$  is finite.

Siegel [45] proved that an elliptic curve defined over a number field has only finitely many integral points. Mahler [38] conjectured that Siegel’s Theorem is true for  $S$ -integral points and proved his conjecture for curves defined over the rationals. Lang [35] gave a modernized exposition and proved Mahler’s conjecture for number fields. An overview of the proof is given in the first section of chapter 5. It is well-known that Siegel did not approve of his work being modernized or generalized to the point of abstraction (see [36]).

The generalization given in the second section of chapter 5 can be viewed in a far from abstract way. It simply says that, given an integer  $n > 2$ , on an elliptic curve defined over a number field there are finitely many rational points for which the denominator of the  $x$ -coordinate is an  $n$ th power. (If the field does not have class number one then the numerator and denominator are coprime ideals.) An appropriate name for such points might be *n-power-integral*. Note that these points include the integral ones.

The proofs Siegel gave of his theorem do not provide a way of finding all of the integral points or bounding the number of integral points. Since it uses Faltings' theorem, the proof in the second section of chapter 5 is also ineffective. Methods have been developed by Baker, Evertse, Lang, Silverman and others in order to give a bound for the number of integral points. These methods are described briefly in the first section of chapter 5. Also, there are now many techniques which help find all of the integral points for large classes of elliptic curves. For example, recently in [18] it has been shown how to determine all of the integral points on the congruent number curve  $y^2 = x^3 - 2^{2a}p^{2b}x$  when  $p$  is a fixed odd prime and  $a, b$  are fixed positive integers.

Searching Cremona's tables [13], many curves have *n-power-integral* points which are not integral. However, there are curves which appear to have no such points. In many cases the *n-power-integral* points relate to solutions of Diophantine equations which are similar to the one in Fermat's Last Theorem. Intriguingly, the best example of this comes from a curve for which Fermat himself found all of the integral points. Namely, he showed that the only integral points on the curve  $E : y^2 = x^3 - 2$  are  $(3, \pm 5)$ . A few years ago, Siksek proposed that to successfully solve interesting Diophantine equations other than the one in Fermat's Last Theorem, Wiles' ideas must be combined with other, unrelated, methods from what is called "Diophantine analysis". This strategy was put into action by a team consisting of himself, Bugeaud and Mignotte. As a result, several famous problems have been resolved. The best known of these is the problem of finding all the perfect powers in the Fibonacci sequence [6]. Their work uses the results of Bennett and Skinner [2]. In the last section of chapter 5 the results in [2] are used to show that if  $n > 5$  is prime then there are no *n-power-integral* points on  $E : y^2 = x^3 - 2$  which belong to the

subgroup  $2E(\mathbb{Q})$ . It seems plausible that, for any  $n > 2$ , the only  $n$ -power-integral points in  $E(\mathbb{Q})$  are  $(3, \pm 5)$ , but a proof of this seems to be currently out of reach.

Let  $K$  be a field,  $E/K$  an elliptic curve,  $P \in E(K)$  and  $\phi : E' \rightarrow E$  an isogeny. Suppose that  $E'$ ,  $\phi$  and a point in  $\phi^{-1}(P)$  are all defined over a finite extension  $L/K$  with  $[L : K] < \deg \phi$ . Then  $P$  is called *magnified*. If  $L/K$  is Galois then  $P$  is called *Galois magnified*. If  $L = K$  then  $P$  is called *simply magnified*. In chapter 6 it is shown that for an elliptic curve defined over a number field, when the generators of the Mordell-Weil group are simply magnified then there are finitely many rational points whose  $x$ -coordinate has its denominator divisible by at most one prime. Note that this can also be viewed as an extension of Siegel's theorem, since again the integral points are included in the conclusion. Magnified points were defined by Everest, Miller and Stephens. They used them to prove that there are finitely many prime terms in certain elliptic divisibility sequences. For example,  $(3, 5)$  on  $E : y^2 : x^3 - 2$  is simply magnified. Hence, perhaps only the first term in the elliptic divisibility sequence generated by this point (or its inverse) is not divisible by two distinct primes. Subsequently, Everest and King introduced Galois magnified points and used the multiplication by 2 map to give examples of such points. Answering a question of Stephens, in the first section of chapter 6 it is shown that any Galois magnified point produced in this way is, in fact, simply magnified. It is also shown that this problem can be overcome by using the multiplication by 3 map instead. However, genuine examples appear to be rare. Everest, Miller and Stephens also gave an unconditional finiteness result for the cubic Fermat-Thue curve. Their work is built upon in the second section of chapter 6.

In the first section of chapter 7 it is explained that an elliptic divisibility sequence is the natural genus-1 analogue of classical divisibility sequences such as Mersenne and Fibonacci. Since the late 1980's, elliptic divisibility sequences have been the object of much research by workers including Chudnovsky and Chudnovsky, Elkies, Everest, Poonen, Silverman and Stephens. This has given rise to some exciting problems which can turn out to be applicable in other fields. For example, Silverman [47] showed that the terms of a given elliptic divisibility sequence will have a primitive divisor (a prime di-

visor which does not divide any previous term) from some point on; building upon this, Pheidas [42], Cornelissen and Zahidi [11], as well as Poonen [43], have found some fascinating connections with attempts to resolve Hilbert's Tenth Problem over the rationals, concerning the solution of Diophantine equations. The integral version of this decision problem was eventually settled by Matijasevich [39] whose proof brought about an interesting collision between Number Theory and Logic. Specifically, he reduced the problem to one in the arithmetic of the Fibonacci sequence.

Extending a theorem of Zsigmondy, Bilu, Hanrot and Voutier proved that for any Lucas or Lehmer sequence all terms beyond the 30th have a primitive divisor. Workers including Everest, Ingram, McLaren and Ward have asked if there are classes of elliptic divisibility sequences which have a primitive divisor beyond some explicit uniform index. For example, consider the elliptic divisibility sequence given by the congruent number curve  $F : y^2 = x^3 - T^2x$  with  $T$  square-free and a non-torsion point  $P \in F(\mathbb{Q})$ . Building on work of Everest, McLaren and Ward [21], Ingram [31] has shown that if  $x(P) < 0$  or  $x(P) + T$  is a rational square then every term beyond the second will have a primitive divisor. More recently [30], he has shown that if  $F$  is minimal then only one term after the first can be a unit. In the second section of chapter 7 it is shown that if  $x(P) < 0$  and  $x(P) + T$  is a rational square then every term beyond the fifth is divisible by the first term multiplied by two distinct primes. Also given is an infinite family of elliptic divisibility sequences whose terms are not prime powers beyond the second. For this family, both the curve and the point are parameterized. The point is always integral.

Chapters 2-4 give a brief overview of algebraic number theory, algebraic curves and elliptic curves. Attention is restricted to what is needed for the results in the last three chapters. For example, unique factorization into fractional ideals or in an  $S$ -integer ring is used heavily and so is explained thoroughly in chapter 2. Similarly for morphisms and properties of the Weierstrass equation in chapters 3 and 4.

# Chapter 2

## Number Theory

This chapter gives the needed facts from algebraic number theory. These are mainly taken from [40], but see also [37]. Section 2.1 is a collection of basic structures and objects of particular importance to this thesis. Section 2.2 explains how unique factorization is retained for number fields. Section 2.3 summarizes heights on projective space.

### 2.1 Basic Definitions

Let  $\mathcal{R}$  be a ring (commutative with a multiplicative identity).

**Definition 2.1.1.** An *ideal* of  $\mathcal{R}$  is a non-empty subset  $\mathfrak{a}$  of  $\mathcal{R}$  with the following properties:

- If  $a, b \in \mathfrak{a}$  then  $a - b \in \mathfrak{a}$ ,
- If  $a \in \mathfrak{a}$  and  $b \in \mathcal{R}$  then  $ab \in \mathfrak{a}$ .

An ideal  $\mathfrak{p} \neq \mathcal{R}$  is *prime* if for all  $a, b \in \mathcal{R}$ ,  $ab \in \mathfrak{p}$  implies that  $a$  or  $b$  is in  $\mathfrak{p}$ . An ideal  $\mathfrak{a} \neq \mathcal{R}$  is *maximal* if there exists no other ideal  $\mathfrak{b} \neq \mathcal{R}$  with  $\mathfrak{a} \subset \mathfrak{b}$ . The ideal  $\{0\}$  is called the *zero ideal* of  $\mathcal{R}$ . Every  $a \in \mathfrak{a}$  defines a *principal ideal*

$$(a) = a\mathcal{R} = \{ab : b \in \mathcal{R}\}.$$

The *product* of two ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  is given by

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

**Definition 2.1.2.** Let  $M$  be a set and suppose there are maps  $+ : M \times M \rightarrow M$  and  $\cdot : \mathcal{R} \times M \rightarrow M$ . Then  $(M, \mathcal{R}, +, \cdot)$  is an  $\mathcal{R}$ -module if the following properties hold:

- $(M, +)$  is an abelian group,
- $a(m_1 + m_2) = am_1 + am_2$  for all  $a \in \mathcal{R}$  and  $m_1, m_2 \in M$ ,
- $(a + b)m = am + bm$  for all  $a, b \in \mathcal{R}$  and  $m \in M$ ,
- $(ab)m = a(bm)$  for all  $a, b \in \mathcal{R}$  and  $m \in M$ ,
- $1m = m$  for all  $m \in M$ .

Let  $M$  be an  $\mathcal{R}$ -module. A subset  $N$  of  $M$  is a  $\mathcal{R}$ -submodule if  $N$  is a subgroup of  $(M, +)$  and  $an \in N$  whenever  $a \in \mathcal{R}$  and  $n \in N$ .

**Definition 2.1.3.** Let  $k$  be a field,  $k^*$  the non-zero elements of  $k$  and  $\bar{k}$  a fixed algebraic closure of  $k$ . *Affine  $n$ -space (over  $k$ )* is the set of  $n$ -tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{k}) = \{P = (x_1, \dots, x_n) : x_1, \dots, x_n \in \bar{k}\}.$$

Similarly, the set of  $k$ -rational points in  $\mathbb{A}^n$  is the set

$$\mathbb{A}^n(k) = \{P = (x_1, \dots, x_n) \in \mathbb{A}^n : x_1, \dots, x_n \in k\}.$$

Call an  $n$ -tuple *non-zero* if one  $x_i$  is non-zero. Given a non-zero  $(x_1, \dots, x_n) \in \mathbb{A}^n$ ,

$$[x_1, \dots, x_n] = \{(\lambda x_1 \dots \lambda x_n) : \lambda \in \bar{k}^*\}.$$

*Projective  $n$ -space (over  $k$ )* is the set

$$\mathbb{P}^n = \mathbb{P}^n(\bar{k}) = \{[x_0, \dots, x_n] : (x_0, \dots, x_n) \in \mathbb{A}^{n+1} \text{ is non-zero}\}.$$

The set of  $k$ -rational points in  $\mathbb{P}^n$  is the set

$$\mathbb{P}^n(k) = \{[x_0, \dots, x_n] : (x_0, \dots, x_n) \in \mathbb{A}^{n+1}(k) \text{ is non-zero}\}.$$

**Definition 2.1.4.** Let  $k$  be a field and  $k^*$  be the non-zero elements of  $k$ . A *discrete valuation* on  $k$  is a non-zero homomorphism  $\nu : k^* \rightarrow \mathbb{Z}$  such that  $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$  for all  $a, b \in k^*$ .

The following property of discrete valuations plays an important role in Chapter 5.

**Lemma 2.1.5.** *Let  $\nu$  be a discrete valuation on a field  $k$  and let  $a, b \in k^*$ . If  $\nu(a) > \nu(b)$  then  $\nu(a + b) = \nu(b)$ .*

*Proof.* First note that  $\nu(-1) + \nu(-1) = \nu(1) = 0$ . So  $\nu(-a) = \nu(-1) + \nu(a) = \nu(a)$ . Thus, if  $\nu(a) > \nu(b)$ ,

$$\nu(b) = \nu(a + b - a) \geq \min(\nu(a + b), \nu(a)) \geq \min(\nu(a), \nu(b)) = \nu(b).$$

So equality holds throughout and  $\nu(a + b) = \nu(b)$ . □

**Definition 2.1.6.** An *absolute value on a field  $k$*  is a function  $|\cdot| : k \rightarrow \{x \in \mathbb{R} : x \geq 0\}$  that satisfies the following conditions:

- $|x| = 0$  if and only if  $x = 0$ ,
- $|xy| = |x||y|$  for all  $x, y \in k$ ,
- $|x + y| \leq |x| + |y|$  for all  $x, y \in k$ .

An absolute value on  $k$  is *non-archimedean* if it satisfies the additional condition:

- $|x + y| \leq \max\{|x|, |y|\}$  for all  $x, y \in k$ ;

otherwise the absolute value is *archimedean*.

Two absolute values  $|\cdot|_1, |\cdot|_2$  on  $k$  are *equivalent* if there exists a positive real number  $\alpha$  such that  $|x|_2 = |x|_1^\alpha$  for all  $x \in k$ .

## 2.2 Number Fields

Let  $K$  and  $L$  be fields such that  $K \subset L$ . Then  $L$  is a vector space over  $K$ . If the dimension of  $L$  is finite then  $L$  is called a *finite extension of  $K$*  and its dimension is denoted by  $[L : K]$ . A *number field* is a finite extension of  $\mathbb{Q}$ . Let  $K$  be a number field. An element  $\alpha$  of  $K$  is said to be *integral over  $\mathbb{Z}$*  if it is the root of a monic polynomial with coefficients in  $\mathbb{Z}$ .

**Theorem 2.2.1.** *The set of elements of  $K$  integral over  $\mathbb{Z}$  forms a ring. Any element  $x \in K$  can be written as  $x = ab^{-1}$  where  $a$  and  $b \neq 0$  are elements of  $K$  integral over  $\mathbb{Z}$ .*

*Proof.* See Theorem 2.2 and Proposition 2.4 of [40]. □

The set of elements of  $K$  integral over  $\mathbb{Z}$  is called the *ring of integers of  $K$*  and is denoted by  $\mathcal{O}_K$ . Note that  $K$  is an  $\mathcal{O}_K$ -module (see Definition 2.1.2).

**Theorem 2.2.2.** *Every proper non-zero ideal  $\mathfrak{a}$  of  $\mathcal{O}_K$  can be written in the form*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

*where the distinct prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  and the positive integers  $r_1, \dots, r_n$  are uniquely determined. Every non-zero prime ideal of  $\mathcal{O}_K$  is maximal.*

*Proof.* See Section 3 of [40]. □

Let  $\mathfrak{p}$  be a non-zero prime ideal of  $\mathcal{O}_K$ . Since  $\mathfrak{p}$  is maximal, the quotient ring  $\mathcal{O}_K/\mathfrak{p}$  is a field. Let  $L$  be a finite extension of  $K$ . Then  $\mathfrak{p}$  factorizes into prime ideals of  $\mathcal{O}_L$ . If  $\mathfrak{q}$  is a prime ideal of  $\mathcal{O}_L$  occurring in the factorization of  $\mathfrak{p}$  then  $[\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$  is denoted by  $f(\mathfrak{q}/\mathfrak{p})$ .

**Definition 2.2.3.** *A fractional ideal of  $\mathcal{O}_K$  is a non-zero  $\mathcal{O}_K$ -submodule  $\mathfrak{a}$  of  $K$  such that*

$$d\mathfrak{a} = \{da : a \in \mathfrak{a}\} \subset \mathcal{O}_K$$

*for some non-zero  $d \in \mathcal{O}_K$ . Every non-zero  $x \in K$  defines a principal fractional ideal*

$$(x) = x\mathcal{O}_K = \{xa : a \in \mathcal{O}_K\}.$$

Note that a non-zero ideal is a fractional ideal but (in general) a fractional ideal is not an ideal. The product of two fractional ideals is defined in the same way as for ideals.

**Theorem 2.2.4.** *The set  $I(\mathcal{O}_K)$  of fractional ideals of  $\mathcal{O}_K$  forms a (multiplicative) group. Each fractional ideal  $\mathfrak{a} \neq \mathcal{O}_K$  can be written in the form*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

*where the distinct prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  and the non-zero integers  $r_1, \dots, r_n$  are uniquely determined.*

*Proof.* See Theorem 3.21 of [40]. □

**Definition 2.2.5.** Given a non-zero  $x \in K$ , let  $\text{ord}_{\mathfrak{p}}(x)$  denote the power to which the prime ideal  $\mathfrak{p}$  occurs in the factorization of  $(x)$ . It is conventional that  $\text{ord}_{\mathfrak{p}}(0) = \infty$ .

Note that, for each prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$ ,  $\text{ord}_{\mathfrak{p}}$  is a discrete valuation on  $K$ .

**Theorem 2.2.6.** Let  $P(\mathcal{O}_K)$  be the subgroup of  $I(\mathcal{O}_K)$  consisting of the principal fractional ideals of  $\mathcal{O}_K$ . The order of the quotient group  $\text{Cl}(\mathcal{O}_K) = I(\mathcal{O}_K)/P(\mathcal{O}_K)$  is finite and there is an effective algorithm for computing  $\text{Cl}(\mathcal{O}_K)$ .

*Proof.* See Section 4 of [40]. □

A subset  $\Sigma \subset \mathcal{O}_K$  is *multiplicative* if  $0 \notin \Sigma$ ,  $1 \in \Sigma$  and  $xy \in \Sigma$  whenever  $x, y \in \Sigma$ . If  $\Sigma \subset \mathcal{O}_K$  is multiplicative and  $\mathfrak{a} \in I(\mathcal{O}_K)$  then  $\Sigma^{-1}\mathfrak{a} := \{b^{-1}a : b \in \Sigma \text{ and } a \in \mathfrak{a}\}$ . Suppose  $\Sigma$  is a multiplicative subset of  $\mathcal{O}_K$  such that  $\Sigma^{-1}\mathcal{O}_K$  is not a field.

**Proposition 2.2.7.** The set  $\Sigma^{-1}\mathcal{O}_K$  is a ring and Theorem 2.2.4 holds when  $\mathcal{O}_K$  is replaced by  $\Sigma^{-1}\mathcal{O}_K$ .

*Proof.* See Proposition 3.3 of [40]. □

For any fractional ideal  $\mathfrak{a}$  of  $\mathcal{O}_K$ ,  $\Sigma^{-1}\mathfrak{a}$  is a fractional ideal of  $\Sigma^{-1}\mathcal{O}_K$ .

**Lemma 2.2.8.** The map  $\rho : I(\mathcal{O}_K) \rightarrow I(\Sigma^{-1}\mathcal{O}_K)$  given by  $\rho(\mathfrak{a}) = \Sigma^{-1}\mathfrak{a}$  is an epimorphism and  $\ker \rho = \{\mathfrak{a} \in I(\mathcal{O}_K) : \mathfrak{a} \cap \Sigma \neq \emptyset\}$ .

*Proof.* For any two fractional ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  of  $\mathcal{O}_K$ ,

$$\Sigma^{-1}(\mathfrak{a}\mathfrak{b}) = (\Sigma^{-1}\mathfrak{a})(\Sigma^{-1}\mathfrak{b})$$

so  $\rho$  is a homomorphism. If  $\mathfrak{a} \in I(\mathcal{O}_K)$  then

$$\mathfrak{a} \cap \Sigma \neq \emptyset \iff 1 \in \Sigma^{-1}\mathfrak{a} \iff \Sigma^{-1}\mathfrak{a} = \Sigma^{-1}\mathcal{O}_K.$$

It remains to show that  $\rho$  is surjective. If  $\mathfrak{a}'$  is an ideal of  $\Sigma^{-1}\mathcal{O}_K$  then

$$\mathfrak{a}' = \Sigma^{-1}(\mathfrak{a}' \cap \mathcal{O}_K)$$

and  $\mathfrak{a}' \cap \mathcal{O}_K$  is an ideal of  $\mathcal{O}_K$ . This extends to fractional ideals and the result follows. □

**Definition 2.2.9.** Let  $S$  be a fixed finite set of prime ideals of  $\mathcal{R} = \mathcal{O}_K$ . Define the ring of  $S$ -integers to be

$$\mathcal{R}_S = \{x \in K : \text{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

Define the (multiplicative) group of  $S$ -units to be

$$\mathcal{R}_S^* = \{x \in K : \text{ord}_{\mathfrak{p}}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}.$$

**Theorem 2.2.10.** Suppose  $\text{Cl}(\mathcal{R})$  has  $1+n$  elements. Let  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  be the non-principal ideals with fewest prime factors such that

$$\text{Cl}(\mathcal{R}) = \{P(\mathcal{R}), \mathfrak{a}_1 P(\mathcal{R}), \dots, \mathfrak{a}_n P(\mathcal{R})\}.$$

Let  $S$  contain the prime ideals dividing  $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ . Then  $\mathcal{R}_S$  is a principal ideal domain.

*Proof.* Let  $\Sigma = \{a \in \mathcal{R} : a \in \mathcal{R}_S^*\}$  then  $\Sigma^{-1}\mathcal{R} = \mathcal{R}_S$ . It is enough to show that every prime ideal of  $\mathcal{R}_S$  is principal. Consider the map  $\rho$  in Lemma 2.2.8. Since  $\rho$  is an epimorphism, a prime ideal of  $\mathcal{R}_S$  is of the form  $\rho(\mathfrak{a})$  for some ideal  $\mathfrak{a}$  of  $\mathcal{R}$ . But if  $\mathfrak{a}$  is not principal then  $\mathfrak{a} = (a)\mathfrak{a}_i$  for some  $a \in R$  and  $\mathfrak{a}_i \cap \Sigma \neq \emptyset$ . Hence  $\rho(\mathfrak{a}) = \rho((a))$  is principal.  $\square$

**Definition 2.2.11.** An *embedding of  $K$*  is a field homomorphism  $\sigma : K \rightarrow \mathbb{C}$ . If  $\sigma K \subset \mathbb{R}$  then  $\sigma$  is a *real embedding*. Otherwise  $\sigma$  is a *complex embedding*.

Note that an embedding of  $K$  fixes  $\mathbb{Q}$ . If  $\sigma : K \rightarrow \mathbb{C}$  is an embedding then there are exactly  $[L : K]$  embeddings of  $L$  which extend  $\sigma$ . Hence there are exactly  $[K : \mathbb{Q}]$  embeddings of  $K$ . If  $\sigma$  is a complex embedding of  $K$  then  $\bar{\sigma}$  given by  $\bar{\sigma}x = \overline{\sigma x}$  is another complex embedding of  $K$ . So there are an even number of complex embeddings of  $K$ . The following theorem is usually referred to as ‘‘Dirichlet’s S-Unit Theorem’’ although Dirichlet in fact proved it for rings of the form  $\mathbb{Z}[\alpha]$  rather than  $\mathcal{O}_K$ .

**Theorem 2.2.12.** Suppose there are  $r_1$  real embeddings and  $2r_2$  complex embeddings of  $K$ . Then  $\mathcal{R}_S^*$  is a finitely generated abelian group of rank  $r_1 + r_2 + \#S - 1$ .

*Proof.* See Theorem 5.9 of [40]  $\square$

## 2.3 Heights

Let  $K$  be a number field.

**Definition 2.3.1.** For each embedding  $\sigma : K \rightarrow \mathbb{C}$ , define  $|\cdot|_\sigma : K \rightarrow \mathbb{R}$  by

$$|x|_\sigma = |\sigma(x)|.$$

For each prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$ , define  $|\cdot|_{\mathfrak{p}} : K \rightarrow \mathbb{R}$  by

$$|x|_{\mathfrak{p}} = \begin{cases} 0 & \text{if } x = 0 \\ p^{-f_{\mathfrak{p}} \text{ord}_{\mathfrak{p}}(x)} & \text{otherwise,} \end{cases}$$

where  $f_{\mathfrak{p}} = f(\mathfrak{p}/(p))$  and  $p \in \mathbb{Z}$  is the unique prime such that  $\mathfrak{p}$  occurs in the factorization of  $(p)$ . Let  $M_K^\infty$  be the set of all embeddings of  $K$  and let  $M_K^0$  be the set of all prime ideals of  $\mathcal{O}_K$ . Put  $M_K = M_K^0 \cup M_K^\infty$ .

The following technical lemma shall be used in the proof of Theorem 6.2.1.

**Lemma 2.3.2.** *Suppose  $L/K$  is a Galois extension,  $\nu \in M_K^0$  is unramified in  $L$  and  $x \in L^*$ . Let  $\omega_1, \omega_2 \in M_L^0$  divide  $\nu$ . If  $\text{ord}_{\omega_1}(x) = \text{ord}_{\omega_2}(x)$  then  $|x|_{\omega_1} = |x|_{\omega_2}$ .*

*Proof.* Let  $p \in \mathbb{Z}$  be the unique prime such that  $\omega_1 \omega_2$  divides  $\mathfrak{p} = (p)$ . Since  $L/K$  is Galois,  $f(\omega_1/\nu) = f(\omega_2/\nu)$ . Hence

$$f(\omega_1/\mathfrak{p}) = f(\omega_1/\nu)f(\nu/\mathfrak{p}) = f(\omega_2/\nu)f(\nu/\mathfrak{p}) = f(\omega_2/\mathfrak{p})$$

and the result follows. □

**Theorem 2.3.3 (Product Formula).** *For all  $x \in K^*$ ,*

$$\prod_{\nu \in M_K} |x|_\nu = 1.$$

*Proof.* See Theorem 7.13 of [40]. □

**Definition 2.3.4.** Let  $P = [x_0, \dots, x_n] \in \mathbb{P}^n(K)$ . The *height of  $P$  (relative to  $K$ )* is defined by

$$H_K(P) = \prod_{\nu \in M_K} \max\{|x_0|_\nu, \dots, |x_n|_\nu\}.$$

**Proposition 2.3.5.** Let  $P \in \mathbb{P}^n(K)$ .

- The height  $H_K(P)$  is well defined. That is,  $H_K([\lambda x_0, \dots, \lambda x_n]) = H_K(P)$  for all  $\lambda \in K^*$ .
- $H_K(P) \geq 1$ .
- Let  $L/K$  be a finite extension. Then  $H_L(P) = H_K(P)^{[L:K]}$ .
- $H_{\mathbb{Q}}(P) = \max\{|x_0|, \dots, |x_n|\}$ , where  $|\cdot|$  is the usual absolute value.

*Proof.* See Proposition 5.4 in Chapter VII of [51]. □

**Definition 2.3.6.** Let  $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$ . The (absolute) height of  $P$ , denoted  $H(P)$ , is defined by

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

where  $K$  is a number field such that  $P \in \mathbb{P}^n(K)$ . The (absolute logarithmic) height is the function  $h : \mathbb{P}^n(\bar{\mathbb{Q}}) \rightarrow \mathbb{R}$  given by

$$h(P) = \log H(P).$$

By Proposition 2.3.5, the absolute height of a point in  $\mathbb{P}^n(\bar{\mathbb{Q}})$  is independent of the choice of field and  $h(P) \geq 0$  for all  $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$ .

**Definition 2.3.7.** For  $\nu \in M_K$  and  $x \in K$ , let

$$h_\nu(x) = \log \max\{1, |x|_\nu\}$$

and

$$h_{M_K^\infty}(x) = \sum_{\nu \in M_K^\infty} h_\nu(x).$$

# Chapter 3

## Curves

In this chapter  $k$  is either a field of characteristic 0 or  $k = \mathcal{O}_K/\mathfrak{p}$ , where  $K$  is a number field and  $\mathfrak{p}$  is a non-zero prime ideal of  $\mathcal{O}_K$ . Denote by  $\bar{k}$  a fixed algebraic closure of  $k$ .

### 3.1 Varieties

Let  $F \in k[X, Y]$  be irreducible over  $\bar{k}[X, Y]$ . Then the ideal  $(F) = F[X, Y]\bar{k}[X, Y]$  is prime and

$$V_{(F)} = \{P \in \mathbb{A}^2 : g(P) = 0 \text{ for all } g \in (F)\}$$

is called an (*affine*) *variety*. Since  $F \in k[X, Y]$ ,  $V_{(F)}$  is said to be *defined over  $k$*  and the set of  *$k$ -rational points of  $V_{(F)}$*  is the set

$$V_{(F)}(k) = V_{(F)} \cap \mathbb{A}^2(k).$$

**Example 3.1.1.** Let  $F = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \in k[X, Y]$ . Then  $F$  is irreducible over  $\bar{k}[X, Y]$  so  $V_{(F)}$  is an affine variety and

$$V_{(F)}(k) = \{(x, y) \in \mathbb{A}^2(k) : F(x, y) = 0\}.$$

The *affine coordinate ring of  $V_{(F)}$*  is defined by  $k[V_{(F)}] = k[X, Y]/(F)$ . Since  $(F)$  is prime,  $k[V_{(F)}]$  is an integral domain and its quotient field is denoted by  $k(V_{(F)})$ . Similarly,  $\bar{k}[V_{(F)}]$  and  $\bar{k}(V_{(F)})$  are defined by replacing  $k$  with  $\bar{k}$ .

**Definition 3.1.2.** A polynomial  $F \in \bar{k}[X, Y, Z]$  is *homogeneous of degree  $d$*  if

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z)$$

for all  $\lambda \in \bar{k}$ . An ideal  $I \subset \bar{k}[X, Y, Z]$  is *homogeneous* if it is generated by homogeneous polynomials.

Note that for a homogeneous polynomial  $F$ , it makes sense to ask whether  $F(P) = 0$  for a point  $P \in \mathbb{P}^2$ . Let  $F \in k[X, Y, Z]$  be homogeneous and irreducible over  $\bar{k}[X, Y, Z]$ . Then the ideal  $(F)$  is homogeneous and the set

$$V_{(F)} = \{P \in \mathbb{P}^2 : g(P) = 0 \text{ for all homogeneous } g \in (F)\}$$

is a *projective variety (of dimension 1)*. Projective varieties of dimension 1 are also called *curves*. The *set of  $k$ -rational points of  $V_{(F)}$*  is the set  $V_{(F)}(k) = V_{(F)} \cap \mathbb{P}^2(k)$ .

**Example 3.1.3.** Let

$$F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \in k[X, Y, Z].$$

Then  $F$  is homogeneous and irreducible over  $\bar{k}[X, Y, Z]$ . The set  $\{P \in \mathbb{P}^2 : F(P) = 0\}$  forms a curve. The  $k$ -rational points on the curve are given by  $\{P \in \mathbb{P}^2(k) : F(P) = 0\}$ .

**Definition 3.1.4.** Let  $V$  be a variety given by  $F(X_1 \dots X_n) = 0$ . If

$$\frac{\partial F}{\partial X_1}(P) = \dots = \frac{\partial F}{\partial X_n}(P) = 0.$$

then the point  $P \in V$  is *singular*. Otherwise,  $P$  is *non-singular*. If  $V$  contains a singular point then  $V$  is *singular*. Otherwise,  $V$  is *non-singular (or smooth)*.

**Example 3.1.5.** Let  $F$  be as in Example 3.1.3. The point  $\mathcal{O} = [0, 1, 0] \in V_{(F)}$  is non-singular since  $\partial F / \partial Z(\mathcal{O}) = 1 \neq 0$ .

**Definition 3.1.6.** The *function field of a projective variety  $V_{(F)}$* , denoted  $k(V_{(F)})$ , is the set of rational functions  $g/h$  such that:

- $g, h \in k[X, Y, Z]$  are homogeneous of the same degree;

- $h \notin (F)$ ;
- two functions  $g/h$  and  $g'/h'$  are identified if  $gh' - g'h \in (F)$ .

Similarly,  $\bar{k}(V_{(F)})$  is defined by replacing  $k$  with  $\bar{k}$ .

**Definition 3.1.7.** For a projective variety  $V$  and a point  $P \in V$ , let

$$\bar{k}[V]_P = \{f \in \bar{k}(V) : f = g/h \text{ with } h(P) \neq 0\}.$$

The functions in  $\bar{k}[V]_P$  are said to be *regular* (or *defined*) at  $P$ .

**Proposition 3.1.8.** *Let  $C$  be a curve. For every non-singular point  $P \in C$  there exists a discrete valuation on  $\bar{k}[C]_P$ .*

*Proof.* See Proposition 1.1 in Chapter II of [51]. □

**Definition 3.1.9.** Let  $C$  be a curve and  $P \in C$  a non-singular point. Denote by  $\text{ord}_P$  the discrete valuation on  $\bar{k}[C]_P$  given by Proposition 3.1.8. Extend  $\text{ord}_P$  to  $\bar{k}(C)$  by using

$$\text{ord}_P(g/h) = \text{ord}_P(g) - \text{ord}_P(h).$$

Let  $f \in \bar{k}(C)$ . If  $\text{ord}_P(f) > 0$ , then  $f$  has a *zero* at  $P$ ; if  $\text{ord}_P(f) < 0$ , then  $f$  has a *pole* at  $P$ . If  $\text{ord}_P(f) \geq 0$ , then  $f$  is *defined* at  $P$  and  $f(P)$  can be calculated. Otherwise  $f$  has a pole at  $P$ , written  $f(P) = \infty$ .

The following is Proposition 1.2 in Chapter II of [51].

**Proposition 3.1.10.** *Let  $C$  be a smooth curve and  $f \in \bar{k}(C)$ . Then there are finitely many points of  $C$  at which  $f$  has a pole or zero. Further, if  $f$  has no poles then  $f \in \bar{k}$ .*

Through a process of dehomogenization, every projective variety  $V$  has an affine subvariety  $W$ . The function field of  $V$  may also be thought of as  $k(W)$ . The points of  $V - W$  are called the *points at infinity* on  $V$ .

**Example 3.1.11.** Let  $V$  be the projective variety given in Example 3.1.3. Dehomogenizing, set  $x = X/Z$  and  $y = Y/Z$ . Then  $f(x, y) = 0$ , where  $f$  is as in Example 3.1.1. So  $V = V_{(f)} \cup \{\mathcal{O}\}$ , where  $\mathcal{O} = [0, 1, 0]$  is the point at infinity on  $V$ .

## 3.2 Maps between Curves

**Definition 3.2.1.** Let  $V_1$  and  $V_2 \subset \mathbb{P}^2$  be projective varieties. A *rational map from  $V_1$  to  $V_2$*  is a map  $\phi : V_1 \rightarrow V_2$  of the form  $\phi = [f_0, f_1, f_2]$ , such that for every point at which  $f_0, f_1, f_2 \in \bar{k}(V_1)$  are all defined,  $\phi(P) = [f_0(P), f_1(P), f_2(P)] \in V_2$ . If there is some  $\lambda \in \bar{k}^*$  so that  $\lambda f_0, \lambda f_1, \lambda f_2 \in k(V_1)$ , then  $\phi$  is said to be *defined over  $k$* .

Suppose that  $\phi = [f_0, f_1, f_2]$  is defined on  $A \subset V_1$  and  $\phi' = [f'_0, f'_1, f'_2]$  is defined on  $A' \subset V_1$ . Call  $\phi$  and  $\phi'$  *equivalent* if  $\phi|_{A \cap A'} = \phi'|_{A \cap A'}$ . Note that a rational map  $\phi : V_1 \rightarrow V_2$  is not necessarily a function on all of  $V_1$ . However, it is sometimes possible to evaluate  $\phi$  at points  $P$  of  $V_1$  where some  $f_i$  is not regular by replacing each  $f_i$  with  $gf_i$  for an appropriate  $g \in \bar{k}(V_1)$ .

**Definition 3.2.2.** A rational map  $\phi = [f_0, f_1, f_2] : V_1 \rightarrow V_2$  is *regular (or defined)* at  $P \in V_1$  if there is a function  $g \in \bar{k}(V_1)$  such that each  $gf_i$  is regular at  $P$  and at least one  $(gf_i)(P) \neq 0$ . If such a  $g$  exists, set  $\phi(P) = [(gf_0)(P), (gf_1)(P), (gf_2)(P)]$ . A rational map which is regular at every point of  $V_1$  is called a *morphism*.

**Example 3.2.3.** Assume that  $\text{char } k \neq 2$  and consider the two curves

$$\begin{aligned} C_1 & : Y^2Z = X^3 + aX^2Z + bXZ^2 \\ C_2 & : Y'^2Z' = X'^3 - 2aX'^2Z' + (a^2 - 4b)X'Z'^2 \end{aligned}$$

where  $a, b \in k$ . There is a rational map  $\phi : C_1 \rightarrow C_2$  given by

$$\phi = \left[ \frac{Y^2}{X^2}, \frac{Y(bZ^2 - X^2)}{ZX^2}, 1 \right].$$

The functions given are not defined at  $[0, 0, 1]$  but multiplying through by  $XY$  gives

$$\phi = \left[ Y \left( \frac{X^2}{Z} + aX + bZ \right), \frac{bZ^2 - X^2}{Z} \left( \frac{X^2}{Z} + aX + bZ \right), XY \right],$$

so  $\phi([0, 0, 1]) = [0, b^2, 0]$ . Similarly, multiplying through by  $X^3$  gives  $\phi(\mathcal{O}) = \mathcal{O}$ . Hence, if  $b$  is non-zero then  $\phi$  is a morphism.

Note that if  $C_1$  in Example 3.2.3 was smooth then  $\phi$  would be a morphism. This is true in general.

**Proposition 3.2.4.** *Let  $\phi : C_1 \rightarrow C_2$  be a rational map between curves. If  $P \in V_1$  is non-singular then  $\phi$  is regular at  $P$ . In particular, if  $C_1$  is smooth, then  $\phi$  is a morphism.*

*Proof.* See Proposition 2.1 in Chapter II of [51]. □

Dehomogenizing and solving a pair of simultaneous equations shows that  $\phi$  in Example 3.2.3 is surjective.

**Theorem 3.2.5.** *A morphism of curves is either constant or surjective.*

*Proof.* See 6.8 in Chapter II of [28]. □

Let  $C_1$  and  $C_2$  be curves defined over  $k$  and  $\phi : C_1 \rightarrow C_2$  a non-constant rational map defined over  $k$ . Define  $\phi^* : k(C_2) \rightarrow k(C_1)$  by  $\phi^* f = f \circ \phi$ . Then  $k(C_1)$  is a finite extension of  $\phi^* k(C_2)$  (see Theorem 2.4 in Chapter II of [51]). The *degree* of  $\phi$  is

$$\deg \phi = [k(C_1) : \phi^* k(C_2)]$$

and  $\phi$  is called *separable* (*inseparable*, *purely inseparable*) if the extension  $k(C_1)/\phi^* k(C_2)$  has the corresponding property.

**Example 3.2.6.** Let  $\phi$  be as in Example 3.2.3. Dehomogenizing,  $k(C_1) = k(x, y)$  and

$$\phi^* k(C_2) = \left\{ f \left( \frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2} \right) : f \in k(C_2) \right\} = k \left( \frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2} \right).$$

Hence  $\deg \phi = [k(C_1) : \phi^* k(C_2)] = 2$ .

**Example 3.2.7.** Let  $\phi : C_1 \rightarrow C_2$  be a non-constant rational map where  $\phi, C_1$  and  $C_2$  are all defined over a number field  $K$ . Then  $\text{char } \phi^* K(C_2) = 0$  so every finite extension of  $\phi^* K(C_2)$  is separable. Hence  $\phi$  is separable.

The following is Corollary 2.4.1 in Chapter II of [51].

**Theorem 3.2.8.** *Let  $C_1$  and  $C_2$  be smooth curves. If  $\phi : C_1 \rightarrow C_2$  is a map of degree 1 then  $\phi$  is an isomorphism.*

### 3.3 Curves of Genus $\geq 1$

Associated to every curve  $C$  is an integer  $g \geq 0$ , called the *genus* of  $C$ , which gives a lot of information about  $C$ . The details of how genus is defined are given in Part A of [29]. The following theorem gives formulas which are adequate for this thesis.

**Theorem 3.3.1.** *Let  $C$  be a curve given by  $F(X, Y, Z) = 0$  for some homogeneous irreducible polynomial  $F \in \bar{k}[X, Y, Z]$ . If  $C$  is non-singular, then the genus of  $C$  equals*

$$\frac{(\deg F - 1)(\deg F - 2)}{2}.$$

*Suppose that  $\text{char } k \neq 2$  and  $C : y^2 = F(x)$ , where  $F(x) \in \bar{k}[x]$  has  $\deg F > 0$  distinct roots. Then the genus  $g$  of  $C$  is given by*

$$g = \begin{cases} \frac{1}{2}(\deg F - 1) & \text{if } \deg F \text{ is odd} \\ \frac{1}{2}(\deg F - 2) & \text{otherwise.} \end{cases}$$

*Proof.* See p.199 of [26] and p.82 of [29]. □

**Theorem 3.3.2** (Faltings [24]). *Let  $C$  be a curve defined over a number field  $K$ . If  $C$  has genus  $g > 1$  then  $C(K)$  is a finite set.*

**Example 3.3.3.** Let  $m$  be a positive integer. The curve

$$C : X^{2m} + Y^{2m} = Z^{2m}$$

has genus  $(2m - 1)(m - 1)$ . So if  $m > 1$  and  $K$  is a number field, then  $C(K)$  is finite.

**Example 3.3.4.** The curve

$$C : Y^2Z + XYZ + YZ^2 = X^3 - X^2Z + 4XZ^2 + 6Z^3$$

is non-singular over any number field and has genus 1.

# Chapter 4

## Elliptic Curves

In this chapter  $k$  is either a field of characteristic 0 or a finite field. Denote by  $\bar{k}$  a fixed algebraic closure of  $k$ .

An *elliptic curve* is a pair  $(E, O)$ , where  $E$  is a smooth curve of genus 1 and  $O \in E$ . An elliptic curve  $(E, O)$  is *defined over*  $k$ , written  $E/k$ , if  $O \in E(k)$  and  $E$  is defined over  $k$ . An elliptic curve is often just denoted by  $E$  when the point  $O$  is understood.

### 4.1 Fundamental Results

**Proposition 4.1.1.** *Let  $(E, O)$  be an elliptic curve defined over  $k$ .*

(a) *There exist functions  $x, y \in k(E)$  such that  $\phi = [x, y, 1]$  gives a map of degree 1 from  $E/k$  to a smooth curve  $C$  given by a Weierstrass equation*

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

*with coefficients  $a_1, \dots, a_6 \in k$ ; and such that  $\phi(O) = [0, 1, 0]$ .*

(b) *Any two Weierstrass equations for  $E$  are related by a linear change of variables*

$$\begin{aligned} X &= u^2X' + r \\ Y &= u^3Y' + su^2X' + t \end{aligned}$$

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

(c) *Let  $x, y$  be as in (a). Then  $x$  has exactly one pole,  $\text{ord}_O(x) = -2$  and  $\text{ord}_O(y) = -3$ .*

(d) *Conversely, every smooth cubic curve  $C$  given by a Weierstrass equation together with the point  $[0, 1, 0]$  is an elliptic curve.*

*Proof.* See Proposition 3.1 in Chapter III of [51] □

**Definition 4.1.2.** The functions  $x, y \in k(E)$  in Proposition 4.1.1 are called the Weierstrass coordinate functions on  $E$ .

**Remark 4.1.3.** The map  $\phi$  in Proposition 4.1.1 is actually a bijection since it is a map of degree 1 between smooth curves (see Theorem 3.2.8).

If  $E$  is an elliptic curve then there exists a binary operation  $+$  on  $E$  such that  $(E, +)$  is an abelian group (See Chapter III of [51]). Further,  $E(k)$  is a subgroup of  $E$ . The formulas for this group operation when  $E$  is given by a Weierstrass equation shall be described below (see Section 4.3).

**Theorem 4.1.4 (Mordell-Weil).** *Let  $K$  be a number field and  $E/K$  an elliptic curve. The group  $E(K)$  is finitely generated.*

*Proof.* See Chapter VIII of [51]. □

Let  $K$  be a number field. Using the Mordell-Weil theorem,  $E(K)$  is a finitely generated abelian group. Hence  $E(K) \cong E_{tors}(K) \times \mathbb{Z}^r$ , where the *torsion subgroup*  $E_{tors}(K)$  is finite and the *rank*  $r$  of  $E(K)$  is a non-negative integer.

## 4.2 Isogenies

**Definition 4.2.1.** Let  $E_1$  and  $E_2$  be elliptic curves. An *isogeny* between  $E_1$  and  $E_2$  is a morphism  $\phi : E_1 \rightarrow E_2$  satisfying  $\phi(O) = O$ .

Proposition 3.2.4 shows that isogenies are given by rational maps. Notice that from Theorem 3.2.5, an isogeny  $\phi$  satisfies either  $\phi(E_1) = \{O\}$  or  $\phi(E_1) = E_2$ . By convention, the constant isogeny has degree 0.

**Example 4.2.2.** If  $B \neq 0$  then  $E' : Y'^2 = X'^3 - \frac{B}{27}Z'^6$  and  $E : Y^2 = X^3 + BZ^6$  are elliptic curves. Hence,  $\phi : E' \rightarrow E$  given by

$$\phi = \left[ \frac{X'}{Z'} - \frac{4BZ'^2}{27X'^2}, \frac{Y'}{Z'} \left( 1 + \frac{8BZ'^3}{27X'^3} \right), 1 \right]$$

is a morphism. Multiplying through by  $Z'X'^3$  shows that  $\phi([0, 1, 0]) = [0, 1, 0]$  and so  $\phi$  is an isogeny.

**Definition 4.2.3.** For each  $m \in \mathbb{Z}$ , define the *multiplication by m map*  $[m] : E \rightarrow E$  by

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

If  $P \in E$ , the point  $[m]P$  is usually written as  $mP$ . The *m-torsion sub-group of E*, denoted  $E[m]$ , is given by

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

**Theorem 4.2.4.** *Let m be a non-zero integer.*

- (a) *The multiplication by m map is an isogeny.*
- (b) *Assume that either  $\text{char } k = 0$  or  $\text{char } k$  is coprime to  $m$ . If  $E$  is defined over  $k$ , then the multiplication by m map is separable.*

*Proof.* See Theorem 3.6 and Corollary 5.4 in Chapter III of [51]. □

The following proposition collects the needed facts about isogenies.

**Proposition 4.2.5.** *Let  $\phi : E_1 \rightarrow E_2$  be a non-constant isogeny of degree  $d$ .*

- (a) *The map  $\phi$  is a group homomorphism.*
- (b) *If  $\phi$  is separable then for every  $Q \in E_2$ ,  $\#\phi^{-1}(Q) = d$ .*
- (c) *Let  $\psi : E_1 \rightarrow E_3$  be a non-constant isogeny and assume that  $\phi$  is separable. If  $\ker \phi \subset \ker \psi$  then there is a unique isogeny  $\lambda : E_2 \rightarrow E_3$  such that  $\psi = \lambda \circ \phi$ .*

(d) *There exists a unique isogeny  $\hat{\phi} : E_2 \rightarrow E_1$  satisfying  $\hat{\phi} \circ \phi = [d]$ .*

*Proof.* See Theorem 4.8, Theorem 4.10, Corollary 4.11 and Theorem 6.1 in Chapter III of [51]. □

Given an elliptic curve  $E$  and a finite subgroup  $G \subset E$ , Vélu has given an explicit construction of an isogeny  $\phi : E \rightarrow E'$  with  $\ker \phi = G$ .

**Theorem 4.2.6** (Vélu [53]). *Let  $E/\bar{k}$  be an elliptic curve given by a Weierstrass equation*

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

*and let  $G \subset E(\bar{k})$  be a finite subgroup. Denote by  $G_2$  the set of points of order 2 in  $G$  and let  $R$  be such that  $R, -R$  forms a partition of  $F \setminus F_2 \cup \{\mathcal{O}\}$ . Put  $S = F_2 \cup R$  and for  $T = (t, y_T) \in S$  set*

$$\begin{aligned} g_T^x &= 3t^2 + 2a_2t + a_4 - a_1y_T, \\ g_T^y &= -2y_T - a_1t - a_3, \\ u_T &= 4t^3 + b_2t^2 + 2b_4t + b_6, \\ v_T &= \begin{cases} g_T^x & \text{if } T \in F_2 \\ 6t^2 + b_2t + b_4 & \text{if } T \notin F_2, \end{cases} \\ v &= \sum_{T \in S} v_T, \\ w &= \sum_{T \in S} (u_T + tv_T). \end{aligned}$$

*There exists an elliptic curve*

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

*so that the isogeny  $\phi : E \rightarrow E'$  given by*

$$\begin{aligned} x' &= x + \sum_{T \in S} \left( \frac{v_T}{x-t} + \frac{u_T}{(x-t)^2} \right), \\ y' &= y - \sum_{T \in S} \left( u_T \frac{2y + a_1x + a_3}{(x-t)^3} + v_T \frac{a_1(x-t) + y - y_T}{(x-t)^2} + \frac{a_1t - g_T^x g_T^y}{(x-t)^2} \right) \end{aligned}$$

*has kernel  $G$ .*

### 4.3 Properties of the Weierstrass Equation

Let  $E/k$  be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (4.1)$$

**Lemma 4.3.1.** *Let  $k$  be a number field and  $(x, y)$  a  $k$ -rational point on (4.1) with  $xy \neq 0$ . Suppose that the coefficients of (4.1) satisfy  $\text{ord}_p(a_i) \geq 0$ . If  $\text{ord}_p(x) < 0$  or  $\text{ord}_p(y) < 0$ , then  $3 \text{ord}_p(x) = 2 \text{ord}_p(y)$ .*

*Proof.* Note that for all  $a, b \in k$ ,  $\text{ord}_p(a + b) \geq \min\{\text{ord}_p(a), \text{ord}_p(b)\}$ . If  $\text{ord}_p(x) < 0$  and  $2 \text{ord}_p(y) > 3 \text{ord}_p(x)$ , then the valuation of every term in (4.1) is greater than  $3 \text{ord}_p(x)$ . But  $\text{ord}_p(x^3) = 3 \text{ord}_p(x)$ . So if  $\text{ord}_p(x) < 0$  then  $2 \text{ord}_p(y) \leq 3 \text{ord}_p(x)$ . Similarly, if  $\text{ord}_p(y) < 0$  then  $3 \text{ord}_p(x) \leq 2 \text{ord}_p(y) < 0$ .  $\square$

If  $\text{char } k \neq 2$ , completing the square in (4.1) gives

$$\left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} \quad (4.2)$$

where  $b_2 = a_1^2 + 4a_2$ ,  $b_4 = 2a_4 + a_1a_3$  and  $b_6 = a_3^2 + 4a_6$ . Also define the quantities

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4,$$

$$c_6 = b_2^3 + 36b_2b_4 - 216b_6,$$

$$\Delta_E = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

$$j_E = c_4^3/\Delta_E.$$

The quantity  $\Delta_E$  given above is called the *discriminant* of the Weierstrass equation and  $j_E$  is called the *j-invariant* of the elliptic curve  $E$ .

**Proposition 4.3.2.** *A curve given by a Weierstrass equation (4.1) is non-singular if and only if  $\Delta_E \neq 0$ . Two elliptic curves are isomorphic (over  $\bar{k}$ ) if and only if they have the same *j-invariant*.*

*Proof.* See Proposition 1.4 in Chapter 3 of [51].  $\square$

If  $\text{char } k \neq 2, 3$ , then (4.1) can be written as

$$(108(2y + a_1x + a_3))^2 = (36x + 3b_2)^3 - 27c_4(36x + 3b_2) - 54c_6. \quad (4.3)$$

If  $P_0 = (x_0, y_0) \in E$  then  $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$ . Suppose  $P_1 = (x_1, y_1) \in E$  and  $P_2 = (x_2, y_2) \in E$ . The *addition formula* for  $P_1 \neq \pm P_2$  is

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

and the *duplication formula* for  $P = (x, y) \in E$  is

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

**Proposition 4.3.3.** *Let  $E$  be a (possibly singular) curve given by a Weierstrass equation (4.1). Denote by  $E_{ns}$  the set of non-singular points of  $E$ . Similarly, denote by  $E_{ns}(k)$  the set of non singular points of  $E(k)$ . Then  $(E_{ns}, +)$  is an abelian group. Moreover,  $E_{ns}(k)$  is a subgroup of  $E_{ns}$ .*

*Proof.* See Proposition 2.5 in Chapter 3 of [51]. □

**Definition 4.3.4.** *A function  $f \in \bar{k}(E)$  is called even if  $f(P) = f(-P)$  for all  $P \in E$ .*

**Lemma 4.3.5.** *A function  $f \in k(E)$  is even if and only if  $f \in k(x)$ .*

*Proof.* From the definition of  $-P$  above, if  $f \in k(x)$  then  $f$  is even. Suppose now that  $f \in k(x, y)$  is even. Using (4.1),

$$f(x, y) = \frac{g_1(x) + h_1(x)y}{g_2(x) + h_2(x)y}$$

for some  $g_1, h_1, g_2, h_2 \in k[x]$ . Hence

$$\frac{g_1(x) + h_1(x)y}{g_2(x) + h_2(x)y} = \frac{g_1(x) + h_1(x)(-y - a_1x - a_3)}{g_2(x) + h_2(x)(-y - a_1x - a_3)}.$$

Thus

$$(g_1(x)h_2(x) - g_2(x)h_1(x))(2y + a_1x + a_3) = 0.$$

So either  $g_1h_2 = g_2h_1$ , or else  $2 = a_1 = a_3 = 0$ . The latter implies that  $\Delta_E = 0$ , contradicting Proposition 4.3.2. Therefore it follows that  $f(x, y) \in k(x)$ . □

Define the *division polynomials*  $\omega_m \in k[E]$  as follows:

$$\begin{aligned}\omega_1 &= 1, \\ \omega_2 &= 2y + a_1x + a_3, \\ \omega_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\ \omega_4 &= (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2)\omega_2, \\ \omega_{2n+1} &= \omega_{n+2}\omega_n^3 - \omega_{n-1}\omega_{n+1}^3 \text{ for } n \geq 2, \\ \omega_2\omega_{2n} &= (\omega_{n+2}\omega_{n-1}^2 - \omega_{n-2}\omega_{n+1}^2)\omega_n \text{ for } n \geq 3.\end{aligned}$$

Also set  $\omega_0 = 0$  and  $\omega_{-n} = -\omega_n$  for  $n < 0$ . Define  $\theta_m \in k[x, y]$  by

$$\theta_m = x\omega_m^2 - \omega_{m+1}\omega_{m-1}.$$

The multiplication by  $m$  map on  $E$  is given by

$$[m] = \left[ \frac{\theta_m}{\omega_m^2}, \frac{\gamma_m}{\omega_m^3}, 1 \right]$$

where  $\gamma_m \in k[E]$  can be expressed in terms of  $\theta_m$  and  $\omega_m$ . Note that  $\theta_m/\omega_m^2 \in K(x)$ .

Now assume that  $\text{char } k \neq 2, 3$ . Given the  $x$ -coordinate  $t$  of a point in  $E[2]$ , let  $E_t$  be an elliptic curve given by a Weierstrass equation

$$E_t : y_1^2 = x_1^3 + A_t x_1^2 + B_t x_1$$

where  $A_t = 3t + \frac{b_2}{4}$  and  $B_t = 3t^2 + \frac{b_2}{2}t + \frac{b_4}{2}$ . An isomorphism  $E \rightarrow E_t$  is given by

$$\left[ x - t, y + \frac{a_1}{2}x + \frac{a_3}{2}, 1 \right].$$

Put  $d_t = A_t^2 - 4B_t$  and let  $F_t$  be an elliptic curve given by a Weierstrass equation

$$F_t : y_2^2 = x_2^3 - 2A_t x_2^2 + d_t x_2.$$

**Proposition 4.3.6.** *There are isogenies  $\phi : E_t \rightarrow F_t$  and  $\hat{\phi} : F_t \rightarrow E_t$  given by*

$$\phi = \left[ \frac{y_1^2}{x_1^2}, \frac{y_1(B_t - x_1^2)}{x_1^2}, 1 \right] \text{ and } \hat{\phi} = \left[ \frac{y_2^2}{4x_2^2}, \frac{y_2(d_t - x_2^2)}{8x_2^2}, 1 \right]$$

*such that  $\hat{\phi} \circ \phi = [2]$  on  $E_t$ . Given  $P = (X, Y) \in E_t$ , the solutions of  $\hat{\phi}(Q) = P$  are*

$$Q = (2X + A_t \mp 2YX^{-1/2}, \pm 2X^{1/2}(2X + A_t \mp 2YX^{-1/2})).$$

*Proof.* In Example 3.2.3 it was shown that  $\phi$  is a morphism. Similarly,  $\hat{\phi}$  is a morphism.

Solving

$$\frac{y_2^2}{4x_2^2} = X \text{ and } \frac{y_2(d_t - x_2^2)}{8x_2^2} = Y$$

for  $x_2$  and  $y_2$  gives the required solutions. So  $\hat{\phi}$  is a surjection. Similarly,  $\phi$  is a surjection.

In particular,  $\phi$  and  $\hat{\phi}$  are isogenies. A computation shows that  $\hat{\phi} \circ \phi$  agrees with the duplication formula on  $E_t$ .  $\square$

The following homomorphism is traditionally used to help find generators of the Mordell-Weil Group (see for example Chapter 14 in [9]). It will serve another purpose in this thesis.

**Lemma 4.3.7.** *If  $t \in k$ , define a map  $\alpha : E_t(k) \rightarrow k^*/k^{*2}$  by*

$$\alpha((x, y)) = xk^{*2}, \text{ if } x \neq 0,$$

$$\alpha((0, 0)) = B_t k^{*2},$$

$$\alpha(\mathcal{O}) = k^{*2}.$$

*Then  $\alpha$  is a group homomorphism.*

*Proof.* Let  $P_1, P_2, P_3 \in E_t(k)$  be such that  $P_1 + P_2 = -P_3$ . If any of the points are zero then the result follows immediately from the definition of  $\alpha$ . Otherwise, they lie on a line  $y_1 = qx_1 + r$  where  $q, r \in k$ . Substituting in the equation for  $E_t$ , we have

$$x_1(x_1^2 + A_t x_1 + B_t) - (qx_1 + r)^2 = (x_1 - x(P_1))(x_1 - x(P_2))(x_1 - x(P_3))$$

Comparing coefficients gives

$$x(P_1)x(P_2)x(P_3) = r^2$$

and

$$x(P_1)x(P_2) = B_t - 2rq - x(P_3)(x(P_1) + x(P_2)).$$

Hence if  $x(P_1)x(P_2)x(P_3) \neq 0$ , then  $\alpha(-P_3) = \alpha(P_3) = \alpha(P_1)\alpha(P_2)$ . If  $x(P_3) = 0$ , then  $r = 0$  and  $\alpha(P_1)\alpha(P_2) = B_t(k^*)^2$ . The case  $x(P_1)x(P_2) = 0$  is similar.  $\square$

## 4.4 Elliptic Curves over $\mathbb{C}$

Here the definitions and theorems are collected from Chapter VI of [51]. These are needed since the next section uses linear forms in elliptic logarithms.

**Definition 4.4.1.** Let  $\omega_1, \omega_2 \in \mathbb{C}$  be linearly independent over  $\mathbb{R}$ . Then

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

is called a *lattice*.

Let  $\Lambda = \langle \omega_1, \omega_2 \rangle$  be a lattice.

**Definition 4.4.2.** An *elliptic function* (relative to the lattice  $\Lambda$ ) is a meromorphic function  $f(z)$  on  $\mathbb{C}$  which satisfies  $f(z + \omega) = f(z)$  for all  $\omega \in \Lambda, z \in \mathbb{C}$ .

**Definition 4.4.3.** A *fundamental parallelogram* for  $\Lambda$  is a set of the form

$$\mathcal{P} = \{a + t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 < 1\}$$

where  $a \in \mathbb{C}$ . Denote the closure of  $\mathcal{P}$  in  $\mathbb{C}$  by  $\bar{\mathcal{P}}$ .

**Definition 4.4.4.** The *Weierstrass  $\wp$ -function* (relative to  $\Lambda$ ) is defined by the series

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left( \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)$$

(For notational convenience, write  $\wp(z)$  if the lattice  $\Lambda$  has been fixed.)

**Theorem 4.4.5.** *The series defining the Weierstrass  $\wp$ -function converges absolutely and uniformly on every compact subset of  $\mathbb{C} \setminus \Lambda$ . It defines a meromorphic function on  $\mathbb{C}$  having a double pole with residue 0 at each lattice point and no other poles. Moreover, the Weierstrass  $\wp$ -function is an elliptic function.*

Since the series for  $\wp$  is uniformly convergent, it can be differentiated term by term to obtain

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

**Theorem 4.4.6.** Let  $E/\mathbb{C}$  be an elliptic curve given by an equation

$$Y^2 = 4X^3 - g_2X - g_3.$$

There exists a lattice  $\Lambda \subset \mathbb{C}$  such that  $\theta : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$  given by

$$\theta(z) = \begin{cases} [\wp(z, \Lambda), \wp'(z, \Lambda), 1] & \text{if } z \neq \Lambda \\ \mathcal{O} & \text{if } z = \Lambda \end{cases}$$

is an isomorphism.

## 4.5 Heights on Elliptic Curves

Let  $K$  be a number field and  $E/K$  an elliptic curve.

**Definition 4.5.1.** For  $f \in \bar{K}(E)$  and  $P \in E(\bar{K})$ , let

$$h_f(P) = \begin{cases} 0 & \text{if } P \text{ is a pole of } f \\ h([f(P), 1]) & \text{otherwise.} \end{cases}$$

**Proposition 4.5.2.** Let  $f \in K(E)$  be a non-constant function. Then for any constant  $C$ ,

$$\{P \in E(K) : h_f(P) \leq C\}$$

is a finite set.

*Proof.* See Proposition 6.1. in Chapter VIII of [51] □

**Proposition 4.5.3.** Let  $P \in E(\bar{K})$  and  $f \in K(E)$  be non-constant even function. The limit

$$\frac{1}{\deg(f)} \lim_{N \rightarrow \infty} \frac{h_f(2^N P)}{4^N}$$

exists, and is independent of  $f$ . Denote the limit by  $\hat{h}(P)$ .

(a) For all  $P, Q \in E(\bar{K})$ ,

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

(b) Let  $f \in K(E)$  be an even function. Then

$$(\deg f)\hat{h} = h_f + O(1),$$

where the implied constant depends only on  $E$  and  $f$ .

(c) For all  $P \in E(\bar{K})$  and  $m \in \mathbb{Z}$ ,  $\hat{h}(mP) = m^2\hat{h}(P)$ .

(d) Let  $P \in E(\bar{K})$ . Then  $\hat{h}(P) \geq 0$ , and  $\hat{h}(P) = 0$  if and only if  $P$  is a torsion point.

(e) Suppose  $\phi : E \rightarrow E'$  is a  $d$ -isogeny. For all  $P \in E(\bar{K})$ ,  $\hat{h}(\phi(P)) = d\hat{h}(P)$ .

*Proof.* For the existence claim and properties (a)-(d) see §9 of Chapter VIII in [51].

(e). Let  $x$  and  $y$  be Weierstrass coordinate functions on  $E$ . Since  $x$  is an even function and  $\phi$  is a homomorphism,  $x(\phi(-P)) = x(\phi(P))$  for all  $P \in E$ . Thus  $x \circ \phi$  is a non-constant even function. Therefore, for all  $P \in E(\bar{K})$ ,

$$\begin{aligned} \hat{h}(\phi(P)) &= \frac{1}{\deg x} \lim_{N \rightarrow \infty} \frac{h_x(2^N \phi(P))}{4^N} \\ &= \frac{1}{\deg x} \lim_{N \rightarrow \infty} \frac{h_{x \circ \phi}(2^N P)}{4^N} \\ &= \frac{\deg(x \circ \phi)}{\deg x} \hat{h}(P) \\ &= d\hat{h}(P). \end{aligned}$$

□

**Remark 4.5.4.** Regarding Proposition 4.5.3(b), when  $P \in E(K)$  explicit bounds for

$$\hat{h}(P) - \frac{1}{2}h_x(P)$$

which depend only on  $E$  are given in [49] (see Theorem 7.2.1).

The following is a special case of a recent improvement on David's theorem [16]. It should be noted that David's theorem, which gives a bound of the form

$$-C \log B (\log \log B)^{r+1}$$

rather than  $-C \log B$ , would be sufficient for this thesis. In particular, David's theorem can be used to prove Theorem 6.2.1.

**Theorem 4.5.5** ([17]). *Let  $F/K$  be an elliptic curve given by an equation*

$$Y^2 = 4X^3 - g_2X - g_3$$

*and  $\mathcal{L}(\mathbf{z}) = \beta_0 z_0 + \dots + \beta_r z_r$  be a non-zero linear form on  $\mathbb{C}^{r+1}$  with  $\beta_i \in \mathbb{Z}$  and at least one  $|\beta_i| > 2$ . Moreover, let  $u_1 \dots u_r \in \mathbb{C}$  be such that*

$$\gamma_i = (\wp(u_i), \wp'(u_i)) \in F(K)$$

*if  $u_i \notin \Lambda$  and  $\gamma_i = \mathcal{O}_F$  if  $u_i \in \Lambda$ , where  $\Lambda$  is given by Theorem 4.4.6. Put*

$$\mathbf{v} = (1, u_1, \dots, u_r).$$

*There exists  $C > 0$  depending only on  $r$ ,  $F$  and  $[K : \mathbb{Q}]$  such that if  $\mathcal{L}(\mathbf{v}) \neq 0$  then*

$$\log |\mathcal{L}(\mathbf{v})| \geq -C \log B$$

*where  $B = \max\{|\beta_0|, \dots, |\beta_r|\}$ .*

**Remark 4.5.6.** The bound in [17] is effective and is given as follows. Keep the notation of Theorem 4.5.5. Let  $\omega_1, \omega_2$  be a pair of generators for  $\Lambda$  such that  $\tau = \frac{\omega_2}{\omega_1}$  lies in the fundamental domain

$$\mathcal{F} = \left\{ z \in \mathbb{C} : \text{Im}(z) > 0, |\text{Re}(z)| \leq \frac{1}{2} \right\}.$$

Put  $h = \max\{1, h([1, g_2, g_3])\}$  and  $D = [K : \mathbb{Q}]$ . Let  $U, V_1 \dots V_r$  be real numbers such that  $V_1 \geq \dots \geq V_r$ ,

$$\log V_i \geq \max \left\{ e, \hat{h}(\gamma_i), \frac{|u_i|^2}{D|\omega_1|^2 \text{Im } \tau} \right\}$$

and

$$e \leq U \leq \min \left\{ \frac{|\omega_1| (\text{Im } \tau \cdot D \log V_i)^{1/2}}{|u_i|} : 1 \leq i \leq r \right\}.$$

If  $\mathcal{L}(\mathbf{v}) \neq 0$  then there exists an effective function  $C > 0$  of  $r$  with

$$\begin{aligned} \log |\mathcal{L}(\mathbf{v})| \geq & -CD^{2r+2}(\log U)^{-2r-1}(\log B + \log(DU) + h + \log \log V_1) \\ & \times (\log(DU) + h + \log \log V_1)^{r+1} \prod_{i=1}^r (h + \log(V_i)). \end{aligned}$$

**Lemma 4.5.7.** *Suppose that  $x$  and  $y$  are coordinate functions on a Weierstrass equation for  $E$  which has coefficients in  $\mathcal{O}_K$ . Fix a non-torsion point  $P \in E(K)$  and let  $\mathfrak{p} \in M_K^0$  be a prime ideal dividing  $(p) \in M_{\mathbb{Q}}^0$ .*

(a) *For any pair  $n, m \in \mathbb{N}$ , if  $\text{ord}_{\mathfrak{p}}(x(nP)) \leq -2$  then*

$$-\frac{1}{2} \text{ord}_{\mathfrak{p}}(x(mnP)) \geq -\frac{1}{2} \text{ord}_{\mathfrak{p}}(x(nP)).$$

(b) *For any pair  $n, m \in \mathbb{N}$ , if  $\text{ord}_{\mathfrak{p}}(x(mP)) < -\frac{2 \text{ord}_{\mathfrak{p}}(p)}{p-1}$  then*

$$-\frac{1}{2} \text{ord}_{\mathfrak{p}}(x(nmP)) = -\frac{1}{2} \text{ord}_{\mathfrak{p}}(x(mP)) + \text{ord}_{\mathfrak{p}}(n).$$

(c) *Let  $m_0$  be the smallest positive integer such that  $\text{ord}_{\mathfrak{p}}(x(m_0P)) < 0$ . For every natural number  $m$ ,*

$$\text{ord}_{\mathfrak{p}}(x(mP)) < 0 \iff m_0 | m.$$

(d) *For every natural number  $m$ , if  $\text{ord}_{\mathfrak{p}}(x(mP)) < 0$  then*

$$-\frac{1}{2} \text{ord}_{\mathfrak{p}}(x(mP)) \leq \text{ord}_{\mathfrak{p}}(m) + C$$

*where  $C$ , which can be determined explicitly, depends only on  $E, P$  and  $\mathfrak{p}$ .*

*Proof.* See Sections 2 and 4 in Chapter IV of [52]. For (b), see also [48]. □

**Theorem 4.5.8.** *Suppose that  $x$  and  $y$  are coordinate functions on a Weierstrass equation for  $E$  which has coefficients in  $\mathcal{O}_K$ . Fix  $\nu \in M_K$  and a non-torsion point  $P \in E(K)$ . For all  $m > 2$ ,*

$$h_{\nu}(x(mP)) \leq C \log m$$

*where  $C > 0$ , which can be determined explicitly, depends only on  $E, P, \nu$  and  $[K : \mathbb{Q}]$ .*

*Proof.* Firstly, suppose that  $\nu \in M_K^{\infty}$  fixes  $K$ . Then  $|\cdot|_{\nu}$  is the usual absolute value on  $\mathbb{C}$ . Using (4.3),  $36x(P) + 3b_2 = X(Q)$  where  $Q$  lies on an elliptic curve  $F/K$  given by

$$Y^2 = 4X^3 - g_2X - g_3.$$

Using Theorem 4.4.6, let  $\Lambda = \langle \omega_1, \omega_2 \rangle$  be the lattice such that  $\theta : \mathbb{C}/\Lambda \rightarrow F(\mathbb{C})$  given by

$$\theta(z) = \begin{cases} [\wp(z, \Lambda), \wp'(z, \Lambda), 1] & \text{if } z \neq \Lambda \\ \mathcal{O} & \text{if } z = \Lambda \end{cases}$$

is an isomorphism. Fix  $z_P \in \mathbb{C}$  such that  $\wp(z_P) = X(Q)$ . Then  $\wp(mz_P) = X(mQ)$ . Note that  $mz_P \notin \Lambda$  since  $P$  is non-torsion. Let

$$\mathcal{P} = \left\{ t_1\omega_1 + t_2\omega_2 : -\frac{1}{2} \leq t_i < \frac{1}{2} \right\}$$

be a fundamental parallelogram for  $\Lambda$ . Write  $z_P = t_1\omega_1 + t_2\omega_2$  for some  $t_1, t_2 \in \mathbb{R}$ . For  $t \in \mathbb{R}$ , let  $[t]$  denote the greatest integer less than  $t$ ,  $\lceil t \rceil$  the smallest integer bigger than  $t$  and  $\{t\} = t - [t]$ . Put

$$m_i = \begin{cases} [mt_i] & \text{if } \{mt_i\} < 0.5 \\ \lceil mt_i \rceil & \text{if } \{mt_i\} \geq 0.5. \end{cases}$$

Then  $mz_P - m_1\omega_1 - m_2\omega_2 \in \mathcal{P}$ . Also, since  $mz_P \notin \Lambda$ ,  $mz_P - m_1\omega_1 - m_2\omega_2$  is non-zero. The only pole of the Weierstrass  $\wp$ -function lying in  $\bar{\mathcal{P}}$  is 0, so  $z^2\wp(z)$  is holomorphic on  $\bar{\mathcal{P}}$ . Since  $\bar{\mathcal{P}}$  is compact,  $z^2\wp(z)$  is bounded and attains its bounds on  $\bar{\mathcal{P}}$ . It follows that

$$\log |\wp(mz_P)| \leq -2 \log |mz_P - m_1\omega_1 - m_2\omega_2| + C_1$$

where  $C_1$  depends only upon  $E$ . Assume that  $m > 2$ . By Theorem 4.5.5, there exists  $C_2 > 0$  depending only on  $E$  and  $[K : \mathbb{Q}]$  such that

$$\log |mz_P - m_1\omega_1 - m_2\omega_2| \geq -C_2 \log \max\{|m|, |m_1|, |m_2|\}.$$

But  $m_i = mt_i + c$ , where  $|c| < 1$ . Hence, the result follows for the usual  $\nu \in M_K^\infty$ .

If  $\sigma \in M_K^\infty$  then  $\sigma(K)$  is a number field of the same degree as  $K$ . Now the point

$$\sigma(mP) = (\sigma(x(mP)), \sigma(y(mP)))$$

lies on an elliptic curve defined over  $\sigma(K)$  given by a Weierstrass equation depending on  $\sigma$ . Hence, from above, the required bound for  $\log \max\{1, |\sigma(x(mP))|\}$  follows.

Now suppose that  $\mathfrak{p} \in M_K^0$ . Let  $p \in \mathbb{Z}$  be the unique prime such that  $\mathfrak{p} \mid (p)$ . Assume that

$$1 < |x(mP)|_{\mathfrak{p}} = p^{-f_{\mathfrak{p}} \text{ord}_{\mathfrak{p}}(x(mP))},$$

then  $\text{ord}_p(x(mP)) < 0$ . Taking logarithms,

$$\log |x(mP)|_p = -f_p \text{ord}_p(x(mP)) \log p$$

By Lemma 4.5.7,  $-\text{ord}_p(x(mP)) \leq 2 \text{ord}_p(m) + C_1$  where  $C_1$  depends only on  $E, P$  and  $p$ . Note that  $\text{ord}_p(m) = c \text{ord}_p(m)$  where  $1 \leq c \leq [K : \mathbb{Q}]$ . Write

$$m = p^{\text{ord}_p(m)} \prod_{\text{primes } q \neq p} q^{\text{ord}_q(m)}$$

Taking logarithms shows that  $\text{ord}_p(m) \leq \log m / \log 2$  and the result follows.  $\square$

**Corollary 4.5.9.** *Suppose that  $x$  and  $y$  are coordinate functions on a Weierstrass equation for  $E$  which has coefficients in  $\mathcal{O}_K$ . Fix a finite subset  $S$  of  $M_K$  and a non-torsion point  $P$ . Then for all  $m > 2$ ,*

$$\sum_{v \in S} h_v(x(mP)) \leq C \log m$$

where  $C > 0$ , which can be determined explicitly, depends only on  $E, P, S$  and  $[K : \mathbb{Q}]$ .

# Chapter 5

## Extending Siegel's Theorem

In this chapter  $K$  is a number field,  $S$  a fixed finite set of prime ideals of  $\mathcal{O}_K$  and  $\mathcal{R}_S$  is the corresponding ring of  $S$ -integers. Suppose  $C/K$  is a smooth curve of genus 1, and let  $f \in K(C)$  have a pole at  $O \in C$ . Theorem 3.1.10 says that there are only finitely many  $P \in C(K)$  at which  $f$  has a pole or a zero. Define

$$C_f(K) = \{P \in C(K) : f \text{ does not have a pole or a zero at } P\}$$

and for  $P \in C_f(K)$ , let

$$S_f(P) = \{\mathfrak{p} \notin S : \text{ord}_{\mathfrak{p}}(f(P)) < 0\}.$$

The Siegel-Mahler theorem gives that  $\{P \in C(K) : f(P) \in \mathcal{R}_S\}$  is a finite set. This is equivalent to saying that  $\{P \in C_f(K) : S_f(P) = \emptyset\}$  is a finite set. Section 5.1 gives a brief overview of how the Siegel-Mahler theorem has been proven and how these proofs have been made effective. In section 5.2 it is shown that for all  $n \nmid \text{ord}_O(f)$ , the set

$$\Upsilon_f^n = \{P \in C_f(K) : n \mid \text{ord}_{\mathfrak{p}}(f(P)) \text{ for all } \mathfrak{p} \in S_f(P)\}$$

is finite. Note that  $S_f(P)$  in  $\Upsilon_f^n$  can be non-empty.

Let  $K = \mathbb{Q}$ ,  $S = \emptyset$ , and let  $E/\mathbb{Q}$  be an elliptic curve with Weierstrass coordinate functions  $x, y$ . If  $E(\mathbb{Q})$  has positive rank then the points in  $\Upsilon_x = \cup_{n>2} \Upsilon_x^n$  give rise to perfect powers in elliptic divisibility sequences (see Chapter 7). Using a technique for solving Diophantine equations known as the “modular approach”, it is shown in [6] that

the only perfect powers in the Fibonacci sequence are 0, 1, 8 and 144. In Section 5.3 it is shown that if  $E : y^2 = x^3 - 2$  and  $Q$  is the generator of  $E(\mathbb{Q})$  then  $\Upsilon_x^p \cap \langle 2Q \rangle$  is empty for any prime  $p > 5$ . Finding  $E$  for which  $E(\mathbb{Q})$  is infinite but the whole of  $\Upsilon_x$  can be proven finite seems too difficult for current techniques (see [2], [5], [32], and [46]). The special subset of points in  $E_x(\mathbb{Q})$  having both the denominator and the numerator of their  $x$ -coordinate an  $n$ th power appears more accessible. It is shown in Section 5.3 that if  $E : y^2 = x^3 - 25x$  and  $Q$  is the non-torsion generator of  $E(\mathbb{Q})$  then the set

$$\{P \in \langle Q \rangle : x(P) = u^p \text{ for some } u \in \mathbb{Q}^*\} \subset \Upsilon_x^p$$

is empty for any prime  $p > 5$ .

## 5.1 The Siegel-Mahler Theorem

Let  $E/K$  be an elliptic curve with Weierstrass coordinate functions  $x$  and  $y$ . There are two well-known proofs that  $\{P \in E_x(K) : S_x(P) = \emptyset\}$  is a finite set. The first is to deduce it from the following Diophantine approximation result.

**Theorem 5.1.1** (Siegel). *Suppose  $\#E(K) = \infty$ . Let  $\nu \in M_K$  and*

$$d_\nu(P, O) = \min\{|x(P)|_\nu^{-1/2}, 1\}.$$

*Then*

$$\lim_{h_x(P) \rightarrow \infty} \frac{\log d_\nu(P, O)}{h_x(P)} = 0.$$

This yields an ineffective proof. However, quantitative statements have been deduced.

**Theorem 5.1.2** (Silverman). *Let  $E/K$  be an elliptic curve and suppose  $E(K)$  has rank  $r$ . There exist Weierstrass coordinate functions  $x, y$  on  $E$  and a constant  $\kappa$  depending only on  $K$  such that*

$$\#\{P \in E_x(K) : S_x(P) = \emptyset\} \leq \kappa^{(1+r)(1+\delta)+\#S},$$

where  $\delta = \#\{\mathfrak{p} \in M_K^0 : \text{ord}_{\mathfrak{p}}(j_E) < 0\}$ .

*Proof.* See exercise 8.14(c) in [51] and [47]. □

**Remark 5.1.3.** Note that  $x, y$  in Theorem 5.1.2 are described explicitly in exercise 8.14(c) of [51] but are not necessarily unique. Further explicit conditions on the Weierstrass equation for  $E$  allow the constant  $\kappa$  to be computed (see [27]).

A second proof of the Siegel-Mahler theorem comes from Siegel's reduction of  $S$ -integral points on hyperelliptic curves. This is followed in Section 5.2. The reduction shows that it is enough to find the solutions of

$$au + bv = 1, \tag{5.1}$$

when  $a, b$  are fixed in a given number field and  $u, v$  are  $\mathcal{S}$ -units in that field for a fixed set  $\mathcal{S}$ . Using Dirichlet's  $S$ -unit theorem (Theorem 2.2.12),  $u, v$  in (5.1) may be replaced by  $u^n, v^n$  for any choice of  $n \in \mathbb{N}$ . This gives

$$au^n + bv^n = 1 \tag{5.2}$$

for  $\mathcal{S}$ -units  $u, v$ . Choosing  $n$  large enough, Roth's theorem [15] proves that there are finitely many solutions to (5.2). Roth's theorem is essentially the best possible result from a long line of similar results on Diophantine approximation, and so is ineffective. Evertse [23] has given an explicit bound for the number of solutions of (5.1) which depends only upon the degree of the number field and the size of  $\mathcal{S}$ . It is possible (see for example Chapter 4 of [1]) to use linear forms in logarithms on the  $\mathcal{S}$ -unit equation to give an explicit upper bound for the height of any  $S$ -integral point of  $E(K)$  in terms of  $K, S$  and  $E$ . Moreover, this explicit bound can be computed easily (i.e. it does not depend upon the generators of the Mordell-Weil group  $E(K)$ ).

Choosing  $n > 3$  in (5.2) shows that there are finitely many solutions by Faltings' theorem (see Example 3.3.3). This may seem heavy-handed, but in the next section it will be shown that it proves considerably more than the Siegel-Mahler theorem.

## 5.2 Denominators Occurring as $n$ th powers

Suppose that  $E/\mathbb{Q}$  is an elliptic curve given by a Weierstrass equation

$$E : y^2 + xy = x^3 + x^2 - 7x + 5.$$

Then  $E(\mathbb{Q}) = \langle P \rangle$ , where  $P = (2, -3)$ . Write  $x(mP) = A_m/B_m^2$  in lowest terms. Then  $B_m = 1$  for  $m = 1, 2, 3, 4, 7$  and  $B_{12} = 2^7$  but are there finitely many 7th powers in this sequence? Similarly, given any  $n > 1$ , are there finitely many  $n$ th powers in this sequence? The following theorem gives positive answers to these questions and generalizes the Siegel-Mahler theorem. The proof is based on Siegel's reduction of  $S$ -integral points on hyperelliptic curves and invokes Faltings' theorem at a critical stage.

**Theorem 5.2.1.** *Let  $E/K$  be an elliptic curve with Weierstrass coordinate functions  $x$  and  $y$ . For all  $n > 2$ ,*

$$\Upsilon_x^n = \{P \in E_x(K) : n \mid \text{ord}_{\mathfrak{p}}(x(P)) \text{ for all } \mathfrak{p} \in S_x(P)\}$$

*is a finite set.*

*Proof.* From (4.2), a Weierstrass equation for  $E$  may be taken as

$$y^2 = x^3 + B_2x^2 + B_4x + B_6. \quad (5.3)$$

Note that the coordinate function  $x$  has not been changed. Let  $\alpha_1, \alpha_2, \alpha_3$  be the distinct zeros of  $x^3 + B_2x^2 + B_4x + B_6$  and put  $\dot{K} = K(\alpha_1, \alpha_2, \alpha_3)$ . Using Theorem 2.2.10, let  $\dot{S} \subset M_{\dot{K}}$  be such that

- $\dot{S}$  contains the primes lying above the primes in  $S$ ;
- $B_i \in \mathcal{R}_{\dot{S}}$ ;
- $2, \alpha_i - \alpha_j$  are  $\dot{S}$ -units for all  $i \neq j$ ;
- the ring of  $\dot{S}$ -integers in  $\dot{K}$ , denoted  $\dot{\mathcal{R}}_S$ , is a unique factorization domain.

By Lemma 4.3.1, for an element  $P \in E(K)$ ,

$$(x(P), y(P)) = \left( \frac{A_P}{B_P^2}, \frac{C_P}{B_P^3} \right) \quad (5.4)$$

where  $A_P C_P$  and  $B_P$  are coprime in  $\dot{\mathcal{R}}_S$ . So if  $n > 2$  and  $P \in \Upsilon_x^n$ , then there is an integer  $m > 1$  such that  $B_P = z^m$  for some  $z \in \dot{\mathcal{R}}_S$ . Substituting (5.4) into (5.3) gives

$$C_P^2 = (A_P - \alpha_1 B_P^2)(A_P - \alpha_2 B_P^2)(A_P - \alpha_3 B_P^2) \quad (5.5)$$

Let  $\wp$  be a prime of  $\mathcal{R}_S$  dividing  $A_P - \alpha_i B_P^2$ ; then  $\wp$  cannot divide  $B_P$ , since  $A_P$  and  $B_P$  are coprime. Hence the factors  $A_P - B_P^2 \alpha_i$  are coprime in  $\mathcal{R}_S$ , since if  $\wp$  divides both  $A_P - \alpha_i B_P^2$  and  $A_P - \alpha_j B_P^2$  then it divides  $(\alpha_i - \alpha_j) B_P^2$ . Now let  $L/\dot{K}$  be the extension obtained by adjoining to  $\dot{K}$  the square root of every  $\dot{S}$ -unit. Note that  $L/\dot{K}$  is finite from Dirichlet's  $S$ -unit theorem (Theorem 2.2.12). Further let  $\mathcal{S}$  be the finite set containing the prime ideals of  $\mathcal{O}_L$  which lie above the ideals in  $\dot{S}$  and any extra prime ideals required to make the ring of  $\mathcal{S}$ -integers in  $L$ , denoted  $\mathfrak{R}_S$ , a unique factorization domain. From (5.5) it follows that there are  $z_i \in \mathfrak{R}_S$  such that

$$A_P - \alpha_i B_P^2 = z_i^2. \quad (5.6)$$

Taking the difference of any two of these equations yields

$$(\alpha_j - \alpha_i) B_P^2 = (z_i - z_j)(z_i + z_j).$$

Note that  $z_i \pm z_j$  are coprime in  $\mathfrak{R}_S$  since if  $\pi | B_P$  divides  $z_i$  then, by (5.6),  $\pi$  divides  $A_P$ .

Fix an integer  $m > 1$  and suppose  $B_P = z^m$  for some  $z \in \mathcal{R}_S$ . *Siegel's identity*:

$$\frac{z_1 \pm z_2}{z_1 - z_3} \mp \frac{z_2 \pm z_3}{z_1 - z_3} = 1$$

becomes the equation

$$\alpha u^{2m} + \beta v^{2m} = 1, \quad u, v \in L$$

where, using Dirichlet's  $S$ -unit theorem, there are finitely many choices for  $\alpha, \beta \in \mathfrak{R}_S^*$ .

By Faltings' Theorem, there are finitely many choices for

$$\alpha u^{2m} = \frac{z_1 \pm z_2}{z_1 - z_3}$$

(see Example 3.3.3). Multiplying these two numbers, there are finitely many choices for

$$\frac{(z_1 + z_2)(z_1 - z_2)}{(z_1 - z_3)^2} = \frac{(\alpha_2 - \alpha_1) B_P^2}{(z_1 - z_3)^2},$$

hence finitely many for

$$\frac{B_P}{z_1 - z_3},$$

and so finitely many for

$$\frac{z_1}{B_P} = \frac{1}{2} \left[ \frac{z_1 - z_3}{B_P} + \frac{z_1 + z_3}{B_P} \right] = \frac{1}{2} \left[ \frac{z_1 - z_3}{B_P} + \frac{(\alpha_3 - \alpha_1) B_P}{z_1 - z_3} \right].$$

But

$$x(P) = \frac{A_P}{B_P^2} = \alpha_1 + \frac{z_1^2}{B_P^2},$$

so there are only finitely many choices for  $x(P)$ . For each choice of  $x(P)$  there are at most two choices for  $y(P)$ .  $\square$

**Remark 5.2.2.** Using results of Farhi [25] it is thought possible to give an explicit upper bound for the number of points in  $\Upsilon_x^n$  (where  $n > 2$  is fixed). This bound will depend upon  $E$ ,  $S$  and  $n$  as well as the maximal  $L$ -rank of a finite number of Abelian varieties. The dependence upon  $E$  arises as the maximal naive height of the identity elements on these varieties; hence it manifests as the height of a very complicated rational number which is a rational function in the coordinates of the curve. An explicit formulation of this bound will not be pursued here.

**Corollary 5.2.3.** *Let  $C/K$  be a smooth curve of genus 1, and let  $f \in K(C)$  have a pole at  $O \in C$ . For all  $n \nmid \text{ord}_O(f)$ ,*

$$\Upsilon_f^n = \{P \in C(K) : n \mid \text{ord}_{\mathfrak{p}}(f(P)) \text{ for all } \mathfrak{p} \in S_f(P)\}$$

*is a finite set.*

*Proof.* By extending  $K$ , it may be assumed that  $O \in C(K)$ . Then  $(C, O)$  is an elliptic curve defined over  $K$ . Let  $x, y$  be coordinates on a Weierstrass equation for  $(C, O)$ , which from (4.2) may be taken as

$$y^2 = x^3 + B_2x^2 + B_4x + B_6.$$

Now  $f \in K(C) = K(x, y)$  and  $[K(x, y) : K(x)] = 2$  give

$$f(x, y) = \frac{\phi(x) + \psi(x)y}{\eta(x)}$$

where  $\phi(x), \psi(x), \eta(x) \in K[x]$ . Lemma 2.1.5 and Proposition 4.1.1 (c) give

$$\text{ord}_O(\phi) = \text{ord}_O(x^{\deg \phi}) = -2 \deg \phi.$$

Similarly,  $\text{ord}_O(\psi) = -2 \deg \psi$  and  $\text{ord}_O(\eta) = -2 \deg \eta$ . Since  $O$  is a pole of  $f$ ,

$$\text{ord}_O(f) = \text{ord}_O(\phi + \psi y) - \text{ord}_O(\eta) < 0.$$

But

$$\text{ord}_O(\phi + \psi y) \geq \min\{\text{ord}_O(\phi), \text{ord}_O(\psi) + \text{ord}_O(y)\}$$

and  $\text{ord}_O(y) = -3$ , thus

$$2 \deg \eta < \max\{2 \deg \phi, 2 \deg \psi + 3\}.$$

Using Theorem 2.2.10, let  $\dot{S} \subset M_K^0$  be such that:

- $S \subset \dot{S}$ ;
- $B_i \in \mathcal{R}_{\dot{S}}$ ;
- $\mathcal{R}_{\dot{S}}$  is a unique factorization domain;
- $\phi(x), \psi(x), \eta(x) \in \mathcal{R}_{\dot{S}}[x]$  and their leading coefficients are units.

Applying Lemma 4.3.1 to an element  $P \in E(K)$  gives

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

where  $A_P C_P$  and  $B_P$  are coprime in  $\mathcal{R}_{\dot{S}}$ . Firstly assume that  $3 + 2 \deg \psi > 2 \deg \phi$  and write

$$f(P) = \frac{B_P^{3+2(\deg \psi - \deg \phi)} \left( B_P^{2 \deg \phi} \phi \left( \frac{A_P}{B_P^2} \right) \right) + C_P \left( B_P^{2 \deg \psi} \psi \left( \frac{A_P}{B_P^2} \right) \right)}{B_P^{3+2(\deg \psi - \deg \eta)} \left( B_P^{2 \deg \eta} \eta \left( \frac{A_P}{B_P^2} \right) \right)}.$$

Now  $B_P$  is coprime with both the numerator and  $B_P^{2 \deg \eta} \eta(x(P))$ . Hence if

$$n \nmid 3 + 2(\deg \psi - \deg \eta)$$

and  $P \in \Upsilon_f^n$  then  $P \in \Upsilon_x^{2n'}$  for some  $n' > 1$ . Similarly if  $3 + 2 \deg \psi < 2 \deg \phi$  and

$$n \nmid 2(\deg \phi - \deg \eta),$$

then  $P \in \Upsilon_f^n$  implies that  $P \in \Upsilon_x^{2n'}$  for some  $n' > 1$ . Thus, the result follows from Theorem 5.2.1. □

For the special subset of  $K$ -rational points on an elliptic curve whose  $x$ -coordinate is roughly an  $n$ th power Faltings' theorem is more directly applicable. Moreover, Faltings' theorem applies in the case  $n = 2$  when the Weierstrass equation (4.1) has  $b_6 \neq 0$ .

**Theorem 5.2.4.** *Let  $E/K$  be an elliptic curve and  $x, y$  coordinates on a Weierstrass equation (4.1) for  $E$ . Put*

$$n_0 = \begin{cases} 1 & \text{if } b_6 \neq 0 \\ 2 & \text{otherwise.} \end{cases}$$

For all  $n > n_0$ ,

$$\Theta_x^n = \{P \in E_x(K) : n \mid \text{ord}_{\mathfrak{p}}(x(P)) \text{ for all } \mathfrak{p} \notin S\}$$

is a finite set.

*Proof.* A proof is detailed for the case where  $b_6 \neq 0$  and  $n = 2$ . A similar approach or Theorem 5.2.1 proves the other cases. Using Theorem 2.2.10, choose  $\dot{S} \subset M_K^0$  containing  $S$  so that  $R_{\dot{S}}$  is a principal ideal domain. Suppose that  $P \in \Theta_x^2$ . Then  $x(P) = \alpha u(P)^2$  for some  $u(P) \in K^*$ , where, using Dirichlet's  $S$ -unit theorem (Theorem 2.2.12), there are finitely many choices for  $\alpha \in R_{\dot{S}}^*$ . Let  $Y = y + \frac{a_1}{2}x + \frac{a_3}{2}$ . Substituting  $x(P)$  into (4.2) shows that  $(u(P), Y(P))$  lies on the curve

$$C : Y^2 = \alpha^3 u^6 + \alpha^2 \frac{b_2}{4} u^4 + \alpha \frac{b_4}{2} u^2 + \frac{b_6}{4}$$

where  $b_6 \neq 0$ . The discriminant

$$-\frac{1}{256} \alpha^{15} b_6 (108b_6^2 - 36b_6 b_2 b_4 - b_2^2 b_4^2 + b_2^3 b_6 + 32b_4^3)^2$$

is non-zero. Hence  $C$  is a hyperelliptic curve and so, by Theorem 3.3.1, has genus 2. The required result follows from Faltings' theorem (Theorem 3.3.2).  $\square$

### 5.3 Bounding $n$ using the Modular Approach

In the proof of Theorem 5.2.1 it was shown that if  $n > 2$  and  $\Upsilon_x^n$  is non-empty then

$$\alpha u^n + \beta v^n = 1$$

for some  $u, v \in L^*$ , where  $L$  is a number field of degree at least 2 and, using Dirichlet's  $S$ -unit theorem, there are finitely many choices for the  $S$ -units  $\alpha, \beta$ . Despite such equations being generalizations of the Fermat equation to number fields there has been little study of

them. In [33] Jarvis and Meekin prove a version of “Fermats Last Theorem” over  $\mathbb{Q}(\sqrt{2})$  but also explain that their method will not work for any other quadratic field.

Other reduction processes for specific curves shall be highlighted in this section. The equations arising from these processes are ternary Diophantine equations of signature  $(p, p, 2)$ . Adapting Wiles’ proof [55] of Fermats Last Theorem to solve other Diophantine equations is known as the “modular approach” (see [2], [5], [32] and [46]). In this section results from [2] are used. It should be noted that there is much more to these results than the recipe stated below but any further adaptation is beyond the scope of this thesis. For the definition of a cuspidal newform of weight 2 and level  $N$  see Chapter III of [12].

**Theorem 5.3.1** (Bennett and Skinner [2]). *Consider the Diophantine equation*

$$AX^p + BY^p = CZ^p,$$

where:

- $AX, BY, CZ$  are non-zero and pairwise coprime;
- $XY \neq \pm 1$ ;
- $p > 5$  is prime;
- $p > \max\{\text{ord}_q(A), \text{ord}_q(B)\}$  for all primes  $q$ ;
- $C$  is square-free.

Without loss of generality one of the following holds:

- (i)  $ABCXY$  is odd and  $Y + BC$  is divisible by 4.
- (ii)  $XY$  is odd and either  $\text{ord}_2(B) = 1$  or  $\text{ord}_2(C) = 1$ .
- (iii)  $XY$  is odd,  $\text{ord}_2(B) = 2$  and  $BY/4 + Z$  is divisible by 4.
- (iv)  $XY$  is odd,  $\text{ord}_2(B) \in \{3, 4, 5\}$  and  $Z - C$  is divisible by 4.
- (v)  $Y$  is even and  $Z - C$  is divisible by 4.

In cases (i) and (ii) let

$$E_1 : y_1 = x_1^3 + 2CZx_1^2 + BCY^p x_1.$$

In cases (iii) and (iv) let

$$E_2 : y_2^2 = x_2^3 + CZx_2^2 + \frac{BCY^p}{4}x_2,$$

and in case (v) let

$$E_3 : y_3^2 + x_3y_3 = x_3^3 + \frac{CZ-1}{4}x_3^2 + \frac{BCY^p}{64}x_3.$$

Then the Galois representation

$$\rho_p^{E_i} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E_i[p])$$

arises from a cuspidal newform of weight 2 and level

$$N_p(E_i) = 2^n C^2 \prod_{q|AB} q,$$

where

$$n = \begin{cases} 5 & \text{case (i)} \\ 6 & \text{case (ii)} \\ 1 & \text{case (iii), } \text{ord}_2(B) = 2 \text{ and } BC/4 + Y \text{ is divisible by 4} \\ 2 & \text{case (iii), } \text{ord}_2(B) = 2 \text{ and } BC/4 - Y \text{ is divisible by 4} \\ 4 & \text{case (iv) and } \text{ord}_2(B) = 3 \\ 2 & \text{case (iv) and } \text{ord}_2(B) = 4 \text{ or } 5 \\ 0 & \text{case (v) and } \text{ord}_2(B) \neq 0 \text{ or } 6 \\ 1 & \text{case (v) and } \text{ord}_2(B) = 0 \\ -1 & \text{case (v) and } \text{ord}_2(B) = 6. \end{cases}$$

**Remark 5.3.2.** The definition of a Galois representation arising from a newform is given on p.31 of [2] and will not be needed here.

For the rest of this section,  $K = \mathbb{Q}$  and  $S = \emptyset$ .

**Proposition 5.3.3.** *Let  $D = -2$  or  $-11$  and  $E : y^2 = x^3 + D$ . Suppose that  $P \in \Upsilon_x^n$ . Put  $n' = n$  if  $n$  is odd and  $n' = n/2$  otherwise. Write  $x(P) = X/Z^{2n'}$  and  $y(P) = Y/Z^{3n'}$ , where  $XY$  and  $Z$  are coprime. Then  $X = a^2 - b^2D$ ,  $Y = a(a^2 + 3Db^2)$  and*

$$Z^{3n'} = b(3a^2 + Db^2), \quad (5.7)$$

where  $a + b\sqrt{D}$  is an algebraic integer in  $\mathbb{Q}(\sqrt{D})$ .

*Proof.* The proof follows Fermat's deduction that the only integral points on  $y^2 = x^3 - 2$  are  $(3, \pm 5)$ . Let  $\mathcal{R}$  be the ring of algebraic integers in  $\mathbb{Q}(\sqrt{D})$ . Substituting  $x(P)$  and  $y(P)$  into the equation for  $E$  gives

$$X^3 = Y^2 - DZ^{6n'} = (Y + \sqrt{D}Z^{3n'})(Y - \sqrt{D}Z^{3n'}).$$

The greatest common divisor of  $Y + \sqrt{D}Z^{3n'}$  and  $Y - \sqrt{D}Z^{3n'}$  in  $\mathcal{R}$  divides  $2\sqrt{D}$ . Since

$$2\sqrt{D} = \begin{cases} -(\sqrt{D})^3 & \text{if } D = -2 \\ 2\sqrt{D} & \text{if } D = -11, \end{cases}$$

and the only units in  $\mathcal{R}$  are  $\pm 1$ , it follows that

$$Y + \sqrt{D}Z^{3n'} = \zeta^3$$

for some  $\zeta \in \mathcal{R}$ . Substituting  $\zeta = a + b\sqrt{D}$  into

$$2\sqrt{D}Z^{3n'} = \zeta^3 - \bar{\zeta}^3 = (\zeta - \bar{\zeta})(\zeta^2 + \zeta\bar{\zeta} + \bar{\zeta}^2)$$

yields (5.7). Working back, the same substitution gives  $Y$  and  $X$  as required.  $\square$

**Example 5.3.4.** Let  $E : y^2 = x^3 - 2$ . Then  $E(\mathbb{Q}) = \langle Q \rangle$  where  $Q = (3, 5)$ . It will be shown that  $\langle 2Q \rangle \cap \Upsilon_x^p$  is empty for any prime  $p > 5$ . Suppose that  $P \in \langle 2Q \rangle \cap \Upsilon_x^p$ , where  $p > 5$  is prime. The denominator of  $x(2Q)$  is even. By Lemma 4.5.7(b) the denominator of  $x(P)$  is even. Write  $x(P) = X/Z^{2p}$  and  $y(P) = Y/Z^{3p}$ , where  $XY$  and  $Z$  are coprime. If  $3 \nmid Z$  then Proposition 5.3.3 gives

$$Z_1^p + 2Z_2^p = 3a^2,$$

where  $Z_1, 2Z_2, 3a$  are pairwise coprime and  $Z_2$  is even. Now follow the recipe of Bennett and Skinner (see Theorem 5.3.1 above). Consider

$$E_3 : y_3^2 + x_3y_3 = x_3^3 + \frac{3a-1}{4}x_3^2 + \frac{3Z_2^P}{32}x_3.$$

Since  $Z \neq 1$ , there exists a cuspidal newform of weight 2 and level

$$N_p(E_3) = 2^0 \cdot 3^2 \cdot 2 = 18.$$

But a computation on MAGMA [3] shows that there are no such newforms. If  $3|Z$  then, using Proposition 4.5.7(b),  $P = 2mQ$  where  $3|m$ . Write  $m = 3^s m'$  where  $3 \nmid m'$ . Using Proposition 4.5.7,  $P' = 2m'Q \in \Upsilon_x^p$ . It follows that  $\langle 2Q \rangle \cap \Upsilon_x^p$  is empty.

If attention is restricted to points in  $E_x(\mathbb{Q})$  whose  $x$ -coordinate is an  $n$ th power and if  $E$  has  $\mathbb{Q}$ -rational 2-torsion then Lemma 4.3.7 gives rise to ternary Diophantine equations of signature  $(p, p, 2)$ .

**Proposition 5.3.5.** Let  $E : y^2 = x^3 - 25x$  and let  $Q = (-4, 6)$  denote the non-torsion generator of  $E(\mathbb{Q})$ . The set

$$\Theta_x^p = \{m : x(mQ) = u^p \text{ for some } u \in \mathbb{Q}^*\}$$

is empty for any prime  $p > 5$ .

*Proof.* Using Lemma 4.3.7 with  $t = 0$ , write  $x(mQ) = \pm A_m^2/B_m^2$  in lowest terms. Using Lemma 4.3.7 with  $t = \pm 5$  shows that

$$A_m^2 + 5B_m^2 = Z^2$$

for some non-zero  $Z \in \mathbb{Z}$ . Note that 5 does not divide  $A_m$ . suppose that  $A_m = X^p$  and  $B_m = Y^p$  for some prime  $p \geq 3$ . Then

$$X^{2p} + 5Y^{2p} = Z^2$$

where  $X, 5Y, Z$  are non-zero and pairwise coprime. Assume that  $p \geq 7$ . Now follow the recipe of Bennett and Skinner (see Theorem 5.3.1 above). One of  $X$  or  $Y$  is even so consider

$$E_3 : y_3^2 + x_3y_3 = x_3^3 + \frac{Z-1}{4}x_3^2 + \frac{BY^{2p}}{64}x_3,$$

where  $B = 1$  or  $5$ . Since  $XY \neq \pm 1$  and  $B$  is odd, there exists a cuspidal newform of weight 2 and level

$$N_p(E_3) = 2^1 \cdot 1 \cdot 5 = 10.$$

But a computation on MAGMA shows that there are no such newforms. Therefore  $p \leq 5$ .

□

# Chapter 6

## Magnified Points

In this chapter  $K$  is a number field,  $S$  a fixed finite set of prime ideals of  $\mathcal{O}_K$  and  $\mathcal{R}_S$  is the corresponding ring of  $S$ -integers. Suppose  $C/K$  is a smooth curve of genus 1, and let  $f \in K(C)$  be a non-constant function. Theorem 3.1.10 says that there are only finitely many  $P \in C(K)$  at which  $f$  has a pole or a zero. Define

$$C_f(K) = \{P \in C(K) : f \text{ does not have a pole or a zero at } P\}$$

and for  $P \in C_f(K)$ , let

$$S_f(P) = \{\mathfrak{p} \notin S : \text{ord}_{\mathfrak{p}}(f(P)) < 0\}.$$

Two elliptic curves  $E/\mathbb{Q}$ ,  $E'/\mathbb{Q}$  lie in the same isogeny class if there is an isogeny between them which is defined over  $\mathbb{Q}$ . Velu's formulae (Theorem 4.2.6) and the Weierstrass parameterization of the elliptic curve (Theorem 4.4.6) can be used to find the elliptic curves in an isogeny class. This is best illustrated in an algorithm developed by Cremona (see Section 3.8 of [14]). Cremona has used his algorithm to produce tables [13] of isogeny classes. Given an isogeny class, it is not always clear whether a rational point on a curve in the class is the image of another rational point. For an elliptic curve  $E/\mathbb{Q}$ , the definition of  $P \in E(\mathbb{Q})$  being (simply) magnified was first given in [22] and related to prime appearance in elliptic divisibility sequences. Such a point is the image of another rational point under an isogeny of degree larger than 1. The definition was generalized in [20] and [34] to include Galois magnified points on elliptic curves defined

over number fields. But all of the examples given in these publications use points which are, in fact, simply magnified. In Section 6.1 it is shown that the multiplication by 2 map will never produce a genuine example of a Galois magnified point. However, fourteen such examples are found using multiplication by 3.

Let  $(E, O)$  be an elliptic curve defined over  $K$  and suppose that  $f \in K(E)$  has a pole at  $O$ . In Section 6.2, the known results on primality ([20], [22]) are built upon. In particular, it is shown that if the generators of  $E(K)$  are simply magnified then

$$\{P \in E_f(K) : |S_f(P)| \leq 1\} \quad (6.1)$$

is a finite set whose size is determined by the Siegel-Mahler theorem. Fix  $D \in K^*$ . For the cubic Fermat-Thue equation

$$E_D : U^3 + V^3 = D,$$

the set in (6.1) is shown to be finite unconditionally. In recent times, Elkies [19] has studied the group  $E_D(\mathbb{Q})$ . It is known that its rank can be at least 11 and is conjectured to grow arbitrarily large. Section 6.2 ends by showing that, for  $K = \mathbb{Q}$ ,  $S = \emptyset$ ,  $E = E_D$ ,  $f = U$  and  $D \in \mathbb{Z}$  cube free, the set in (6.1) is bounded independently of rank.

## 6.1 Existence

Let  $E/K$  be an elliptic curve. The following adapts the definitions given in [22] and [20].

**Definition 6.1.1.** A point  $P \in E(K)$  is called *magnified* if  $\phi(Q) = P$  for  $Q \in E'(L)$  where  $L$  is a number field,  $E'/L$  is an elliptic curve and  $\phi : E' \rightarrow E$  is an isogeny defined over  $L$  with  $\deg \phi > [L : K]$ . If  $L/K$  is also Galois then  $P$  is called *Galois magnified*. If  $L = K$  then  $P$  is called *simply magnified*.

In all of the examples in [20] and [34], a point which is magnified is also simply magnified.

**Example 6.1.2** ([20]). Consider  $P = (3, 2)$  on

$$E : y^2 = x^3 - x^2 - 4x - 2.$$

Here  $2Q_1 = P$ , where  $Q_1 = (2 + 2\sqrt{2}, 4 + 3\sqrt{2})$  and  $2Q_2 = Q_1$  has a solution with coordinates in  $\mathbb{Q}(\sqrt{2 + 2\sqrt{2}})$ . In fact,  $P$  and  $Q_1$  are Galois magnified because the extensions are quadratic. But  $E$  has a 2-torsion point which has  $x$ -coordinate  $t = -1$  with  $x(P) - t$  a square in  $\mathbb{Z}$ . The condition  $x(P) - t$  being a square ensures that  $P \in E(\mathbb{Q})$  is simply magnified by a 2-isogeny (see §14 of [9] or Lemma 4.3.6). Similarly,  $Q_1 \in E(\mathbb{Q}(\sqrt{2}))$  is simply magnified by a 2-isogeny.

Nelson Stephens asked if a non-torsion point  $P \in E(K)$  is simply magnified whenever it is magnified by doubling a point. Theorem 6.1.4 gives a positive answer to this question. Let  $x$  and  $y$  be Weierstrass coordinate functions on  $E$  and recall the definitions of  $\theta_m, \omega_m$  from Section 4.3.

**Lemma 6.1.3.** *Fix  $m > 0$  and  $P \in E(K) \setminus E[2]$ . If  $mR = P$  then  $y(R) \in K(x(R))$ .*

*Proof.* Using the division polynomials,

$$x(R + P) = x((m + 1)R) = \frac{\theta_{m+1}(R)}{\omega_{m+1}(R)^2} \in K(x(R)).$$

If  $R = \pm P$ , then  $R \in E(K)$ . Otherwise, by the addition formula

$$\left( \frac{y(P) - y(R)}{x(P) - x(R)} \right)^2 + a_1 \left( \frac{y(P) - y(R)}{x(P) - x(R)} \right) - a_2 - x(R) - x(P) \in K(x(R)).$$

Multiplying through by  $(x(P) - x(R))^2$  and collecting terms gives

$$y(R)^2 + a_1 x(R) y(R) + y(R)(-2y(P) - a_1 x(P)) \in K(x(R)).$$

Using (4.1) gives

$$y(R)(-2y(P) - a_1 x(P) - a_3) \in K(x(R)).$$

Since  $P \notin E[2]$ ,  $2y(P) + a_1 x(P) + a_3 \neq 0$  and the result follows.  $\square$

For  $m > 0$  and  $P \in E(K)$ , define  $\delta_m(E, P) \in K[x]$  by

$$\delta_m(E, P) = \theta_m - x(P)\omega_m^2.$$

Then  $\delta_m(E, P)$  is monic and has degree  $m^2$ . The zeros of  $\delta_m(E, P)$  give the values of  $x(R)$  for which  $mR = P$  and so, by Lemma 6.1.3, they determine where the solutions to  $mR = P$  are defined.

Let  $T \in E[2]$  and  $t = x(T)$ . Composing the 2-isogeny  $\hat{\phi} : F_t \rightarrow E_t$  (see Proposition 4.3.6) with an isomorphism  $E_t \rightarrow E$  creates a 2-isogeny  $\psi : F_t \rightarrow E$ .

**Theorem 6.1.4.** *Let  $P \in E(K) \setminus E[2]$ . Suppose  $P$  is not double a  $K$ -rational point. Then the following are equivalent:*

1.  $2R = P$  has a solution with  $[K(x(R), y(R)) : K] = 2$ ;
2. there exists  $T \in E(K)[2]$  such that  $P \in \psi F_{x(T)}(K)$ .

*Proof.*  $1 \Rightarrow 2$ . Put  $L = K(x(R), y(R))$ . Let  $\sigma$  be the generator of  $\text{Gal}(L/K)$ , then the point  $T = \sigma(R) - R$  is a 2-torsion point since  $2T = \sigma(2R) - 2R = \mathcal{O}$ . Also  $T \in E(K)$  since  $\sigma(T) = R - \sigma(R) = -T = T$ . Let  $x(T) = t$ , then

$$\sigma(\hat{\psi}(R)) = \hat{\psi}(\sigma(R)) = \hat{\psi}(R + T) = \hat{\psi}(R),$$

where  $\hat{\psi}$  is the dual of  $\psi$ . So  $\hat{\psi}(R) \in F_t(K)$  and  $\psi(\hat{\psi}(R)) = 2R = P$ .

$2 \Rightarrow 1$ . Suppose  $T \in E(K)[2]$ ,  $P \in \psi F_t(K)$  and  $P = \psi(Q)$ . A non-zero isogeny is surjective, so there exists  $R$  on  $E$  with  $\hat{\psi}(R) = Q$ . Since  $P$  is not double a  $K$ -rational point and  $x(R)$  satisfies a quadratic polynomial,  $[K(x(R)) : K] = 2$ . But  $2R = P$ , so applying Lemma 6.1.3 gives the required result.  $\square$

To see that  $P$  must not be a 2-torsion point in Theorem 6.1.4, consider the following

**Example 6.1.5.** Let  $P = (0, 0)$  on

$$E : y^2 = x^3 + x = x(x+i)(x-i).$$

Then  $2(1, \sqrt{2}) = P$ . None of  $0, \pm i$  are squares in  $\mathbb{Q}^*$ , so Theorem 6.1.4 is contradicted.

Extending Stephens' question, it is natural to ask if a non-torsion point  $P \in E(K)$  is simply magnified whenever it is magnified by tripling a point. More generally, one can ask if a non-torsion point  $P \in E(K)$  is simply magnified whenever it is Galois magnified. Example 6.1.8 gives negative answers to these questions and so shows that the definition of Galois magnified is necessary.

**Example 6.1.6.** Let  $K = \mathbb{Q}$ ,  $B \in \mathbb{Z}$  and  $E : y^2 = x^3 + B$ . Consider the 3-isogeny  $\phi : E' \rightarrow E$  given in Example 4.2.2. Put  $B = -2$  and  $P = (3, 5)$ . Then  $\delta_3(E, P)$  has an irreducible cubic factor and  $\phi(\frac{1}{3}, -\frac{1}{3}) = P$ . Note that the splitting field of an irreducible cubic can have degree at most 6. So, using Lemma 6.1.3,  $P$  is Galois magnified by tripling a point and  $P$  is simply magnified. The same method works for  $B = -4$  when  $P = (2, 2)$ ,  $B = -11$  when  $P = (3, 4)$ , and many other pairs  $(B, P)$ .

Examples where  $\delta_3(E, P)$  factorizes (over  $K$ ) but  $P$  is not simply magnified are relatively hard to find. Let  $K = \mathbb{Q}$ . The first 12 of Cremona's "generators" tables from [13] were considered. There were 22,962 pairs  $(E, P)$  found such that  $\delta_3(E, P)$  factorizes (over  $\mathbb{Q}$ ). In all but 14 of these pairs,  $P$  is simply magnified by a 3-isogeny. As in Example 6.1.7, the 3-isogeny is constructed using Vélú's formulae [53] (see Theorem 4.2.6) and a rational zero of  $\omega_3$ . The 14 counterexamples found are listed in Table 6.1. They are given in the same format as Cremona uses, where  $N$  is the conductor,  $C$  is the isogeny class and  $\#$  is the number of the curve in the class. Each curve listed has rank 1 and  $P$  is taken to be the generator which Cremona gives. Moreover, they each lie in an isogeny class of size two.

**Example 6.1.7.** Take  $P = (-1, 3)$  and

$$E : y^2 + y = x^3 + x^2 - 7x + 5$$

(Cremona reference 91b1). Then

$$\delta_3(E, P) = (x^3 - 7x + 7)(x^6 + 9x^5 + 115x^4 - 628x^3 + 1120x^2 - 875x + 259)$$

and  $\omega_3 = (x - 1)(3x^3 + 7x^2 - 35x + 28)$ . The translation  $x_1 = x - 1$  gives

$$E_1 : y^2 + y = x_1^3 + 4x_1^2 - 2x_1$$

Note that  $P_1 = (-2, 3) \in E_1(\mathbb{Q})$ ,  $T = (0, 0)$  is a 3-torsion point and

$$\delta_3(E_1, P_1) = (x^3 + 3x^2 - 4x + 1)(x^6 + 15x^5 + 175x^4 - 58x^3 + 31x^2 - 8x + 1) \quad (6.2)$$

To show that  $P$  is simply magnified it is enough to show that there exists a 3-isogeny  $\phi : E_1 \rightarrow E'$  which is defined over  $\mathbb{Q}$  and which maps a solution of  $3R = P_1$  to a

$\mathbb{Q}$ -rational point  $Q$  on  $E'/\mathbb{Q}$ . Putting  $G = \langle T \rangle$  and  $t = 0$  in Theorem 4.2.6 gives

$$E' : y'^2 + y' = x'^3 + 4x'^2 + 18x' + 57$$

and a 3-isogeny  $\phi : E_1 \rightarrow E'$ , where

$$x_1(R)^3 - x'(Q)x_1(R)^2 - 4x_1(R) + 1 = 0.$$

Now (6.2) shows that  $R$  can be chosen so that  $Q = (-3, 3)$ . To construct the dual of  $\phi$ , use Theorem 4.2.6 on  $E'$  with  $t = -16/3$  to get an elliptic curve

$$E_2 : y_2^2 + y_2 = x_2^3 + 4x_2^2 - \frac{1766}{3}x_2 + \frac{129394}{27}$$

and an isogeny  $\psi : E' \rightarrow E_2$  given by

$$\begin{aligned} x_2 &= x' + \frac{364}{3(x' - t)} - \frac{8281}{27(x' - t)^2}, \\ y_2 &= y' + \frac{8281(2y' + 1)}{27(x' - t)^3} - \frac{364y' + 182}{3(x' - t)^2}. \end{aligned}$$

By Proposition 4.2.5(c), Theorem 3.2.8 and Proposition 4.1.1(b), composing  $\psi$  with a simple linear transformation maps back to  $E$ . Indeed, this linear transformation is given by  $x_2 = 3^2x + \frac{5}{3}$  and  $y_2 = 3^3y + 13$ .

**Example 6.1.8.** The entry in Table 6.1 with conductor 70470 gives

$$E : y^2 + xy = x^3 - x^2 + 6546x - 197740.$$

and  $P = (124, 1522)$ . Looking at Cremona's table, the only other curve lying in the same isogeny class as  $E$  is

$$E' : y'^2 + x'y' = x'^3 - x'^2 - 2094x' - 36652.$$

This curve has rank 1 and  $E'(\mathbb{Q}) = \langle Q \rangle$ , where

$$Q = \left( \frac{54604}{441}, \frac{11107426}{9261} \right).$$

If  $P$  is simply magnified by a  $d$ -isogeny then it is the image of  $mQ$ , for some non-zero integer  $m$  and, using Proposition 4.5.3,  $dm^2\hat{h}(Q) = \hat{h}(P)$ . But in fact,  $\hat{h}(Q) = 3\hat{h}(P)$ .

Table 6.1: Counterexamples.

$N$	$C$	#	$N$	$C$	#	$N$	$C$	#
17739	g	1	47526	f	1	70470	m	2
19926	l	2	49818	j	1	92055	u	1
26730	y	2	57222	bw	2	113866	d	1
39710	z	1	62814	r	1	119646	dd	2
45662	h	1	64395	f	1			

So

$$\delta_3(E, P) = (x^3 - 966x^2 - 233916x - 31751344)(x^3 - 102x^2 - 1068x - 122896) \\ \times (x^3 - 48x^2 + 8868x - 295696)$$

factorizes but  $P$  is not simply magnified. However, all of the zeros of

$$x^3 - 48x^2 + 8868x - 295696$$

lie in  $L = \mathbb{Q}(\sqrt{-3}, 3^{\frac{1}{3}})$  so  $P$  is Galois magnified.

It was shown in the proof of Theorem 6.1.4 that if  $\delta_2(E, P)$  has a quadratic factor over  $K$ , then  $\omega_2^2$  has a zero in  $K$ . For an odd prime  $l$ , denote by  $\Sigma_l$  the set of pairs  $(E, P)$  found in Cremona's first 12 tables such that  $\delta_l(E, P)$  factorizes. Let  $\nu(\omega_l)$  be the smallest degree occurring in the factorization of  $\omega_l$  over  $\mathbb{Q}$ . Table 6.2 gives data relating magnification by  $[l]$  to  $\nu(\omega_l)$ , where  $\# \nu(\omega_l) = 1$  means the number of curves in  $\Sigma_l$  with  $\nu(\omega_l) = 1$ . The data suggests that  $\nu(\omega_l) \leq (l-1)/2$  when  $\delta_l(E, P)$  factorizes. Such a result would provide a way of eliminating the possibility of magnification by  $[l]$  which is independent of rank.

Table 6.2: Comparing  $\Sigma_l$  with  $\nu(\omega_l)$ .

$l$	$ \Sigma_l $	$\# \nu(\omega_l) = 1$	$\# \nu(\omega_l) = 2$	$\# \nu(\omega_l) = 3$
3	22,962	22,962	0	0
5	1,911	539	1,372	0
7	443	45	0	398

## 6.2 Application to Primality

In [22] it was proven that when  $K = \mathbb{Q}$ ,  $E$  is an elliptic curve given by a Weierstrass equation with integral coefficients and  $P \in E(\mathbb{Q})$  is a non-torsion simply magnified point then there finitely many  $m$  with  $|\emptyset_x(mP)| \leq 1$ . In [20] this result was proven for number fields and the condition on  $P$  was weakened to include Galois magnified points.

**Theorem 6.2.1.** *Let  $E/K$  be an elliptic curve having coordinates  $x$  and  $y$  on a Weierstrass equation with coefficients in  $\mathcal{O}_K$ . Suppose that a fixed non-torsion point  $P \in E(K)$  is Galois magnified by*

$$\phi : (E', \mathcal{O}') \rightarrow (E, \mathcal{O}),$$

where  $E'$  and  $\phi$  are defined over a number field  $L$ . Let  $m$  be such that  $mP \in E_x(K)$  and  $|S_x(mP)| \leq 1$ . Then there are finitely many choices for  $m$ . Moreover, a bound for  $m$  which depends only on  $E, E', \phi, S, K, L$  and  $P$  can be explicitly determined.

*Proof.* Let  $x'$  and  $y'$  be coordinates on a Weierstrass equation for  $E'/L$  which, from (4.2), may be taken as

$$y'^2 = x'^3 + B_2x'^2 + B_4x' + B_6.$$

Since  $f' = x \circ \phi \in L(E') = L(x', y')$  is an even function, Lemma 4.3.5 gives

$$f'(x') = \frac{\psi(x')}{\eta(x')}$$

where  $\psi(x'), \eta(x') \in L[x']$ . Let  $\mathcal{S}$  be the finite set containing:

- the prime ideals of  $\mathcal{O}_L$  which lie above the ideals in  $S$ ;
- the prime ideals of  $\mathcal{O}_L$  which lie above the finitely many prime ideals of  $\mathcal{O}_K$  which ramify in  $L$ ;
- the prime ideals of  $\mathcal{O}_L$  so that the ring of  $\mathcal{S}$ -integers in  $L$ , denoted  $\mathfrak{R}_{\mathcal{S}}$ , is a principal ideal domain;

- the prime ideals of  $\mathcal{O}_L$  so that  $B_i \in \mathfrak{R}_S$ ;
- the prime ideals of  $\mathcal{O}_L$  so that  $\psi(x'), \eta(x') \in \mathfrak{R}_S[x']$  and their leading coefficients are units in  $\mathfrak{R}_S$ .

Suppose that  $P$  is Galois magnified from  $Q \in E'(L)$ . Note that  $\phi(mQ) = mP$  and  $y'(mQ) \neq 0$  since  $P$  is non-torsion. By Lemma 4.3.1, if  $x'(Q) \neq 0$ ,

$$(x'(Q), y'(Q)) = \left( \frac{A_Q}{B_Q^2}, \frac{C_Q}{B_Q^3} \right)$$

where  $A_Q C_Q$  and  $B_Q$  are coprime in  $\mathfrak{R}_S$ . Since

$$\text{ord}_{\mathcal{O}'}(f') = \text{ord}_{\mathcal{O}'}(\psi) - \text{ord}_{\mathcal{O}'}(\eta) = \text{ord}_{\mathcal{O}}(x) = -2,$$

$\deg \psi - \deg \eta = 1$ . Thus

$$x(P) = f'(Q) = \frac{\left( B_Q^{2 \deg \psi} \psi \left( \frac{A_Q}{B_Q^2} \right) \right)}{B_Q^2 \left( B_Q^{2 \deg \eta} \eta \left( \frac{A_Q}{B_Q^2} \right) \right)} \quad (6.3)$$

where  $B_Q$  is coprime with both the numerator and  $B_Q^{2 \deg \eta} \eta(x'(Q))$ .

Assume that  $mP \in E_x(K)$  and  $|S_x(mP)| \leq 1$ . Since  $x'$  is an even function, Proposition 4.5.3 gives

$$2\hat{h}(mQ) = h_{x'}(mQ) + O(1) \quad (6.4)$$

where the implied constant depends on  $E'$ . If  $x'(mQ) = 0$  then  $2m^2\hat{h}(Q) = O(1)$ . So assume that  $mQ \in E'_{x'}(L)$ . If  $|S_{x'}(mQ)| = 0$  then, using Corollary 4.5.9, for all  $m > 2$ ,

$$\begin{aligned} 2m^2\hat{h}(Q) &= \frac{1}{[L : \mathbb{Q}]} \sum_{\omega \in M_L} \log \max\{1, |x'(mQ)|_{\omega}\} + O(1) \\ &= \frac{1}{[L : \mathbb{Q}]} \sum_{\mathfrak{q} \in \mathcal{S}} h_{\mathfrak{q}}(x'(mQ)) + \frac{h_{M_L^{\infty}}(x'(mQ))}{[L : \mathbb{Q}]} + O(1) \\ &\leq C \log m \end{aligned}$$

where  $C > 0$  only depends on  $E', P, \phi, S, K$  and  $L$ . So assume that  $\mathfrak{q}_m \in \mathcal{S}_{x'}(mQ)$ . Let  $\mathfrak{p}_m$  be the prime ideal in  $M_K^0$  which  $\mathfrak{q}_m$  divides. Looking at (6.3), note that each prime ideal  $\mathfrak{q} \in \mathcal{S}_{x'}(mQ)$  divides  $\mathfrak{p}_m$  and, since  $\mathfrak{p}_m$  is unramified in  $L$ ,  $\text{ord}_{\mathfrak{q}}(x'(mQ))$  is the

same for each  $\mathfrak{q} \in \mathcal{S}_{x'}(mQ)$ . Using Lemma 2.3.2,

$$\begin{aligned}
[L : \mathbb{Q}]h_{x'}(mQ) &= \sum_{\omega \in M_L} \log \max\{1, |x'(mQ)|_\omega\} \\
&= \sum_{\mathfrak{q} \in \mathcal{S}_{x'}(mQ)} \log |x'(mQ)|_{\mathfrak{q}} + \sum_{\mathfrak{q} \in \mathcal{S}} h_{\mathfrak{q}}(x'(mQ)) + h_{M_L^\infty}(x'(mQ)) \\
&= |\mathcal{S}_{x'}(mQ)| \log |x'(mQ)|_{\mathfrak{q}_m} + \sum_{\mathfrak{q} \in \mathcal{S}} h_{\mathfrak{q}}(x'(mQ)) + h_{M_L^\infty}(x'(mQ))
\end{aligned}$$

So, using Corollary 4.5.9,

$$[L : \mathbb{Q}]h_{x'}(mQ) = |\mathcal{S}_{x'}(mQ)| \log |x'(mQ)|_{\mathfrak{q}_m} + O(\log m). \quad (6.5)$$

Since  $x$  is an even function, Proposition 4.5.3 gives

$$2\hat{h}(mP) = h_x(mP) + O(1) \quad (6.6)$$

where the implied constant depends on  $E$ . Looking at (6.3), note that  $\mathfrak{q}_m \in \mathcal{S}_{f'}(mQ)$ , each  $\mathfrak{q} \in \mathcal{S}_{f'}(mQ)$  divides  $\mathfrak{p}_m$  and that  $\text{ord}_{\mathfrak{q}}(f'(mQ))$  is the same for each  $\mathfrak{q} \in \mathcal{S}_{f'}(mQ)$ .

Using Lemma 2.3.2,

$$\begin{aligned}
[L : \mathbb{Q}]h_x(mP) &= \sum_{\omega \in M_L} \log \max\{1, |x(mP)|_\omega\} \\
&= \sum_{\mathfrak{q} \in \mathcal{S}_{f'}(mQ)} \log |f'(mQ)|_{\mathfrak{q}} + \sum_{\mathfrak{q} \in \mathcal{S}} h_{\mathfrak{q}}(x(mP)) + h_\infty(x(mP)) \\
&= |\mathcal{S}_{f'}(mQ)| \log |f'(mQ)|_{\mathfrak{q}_m} + \sum_{\mathfrak{q} \in \mathcal{S}} h_{\mathfrak{q}}(x(mP)) + h_\infty(x(mP)).
\end{aligned}$$

From (6.3),  $\text{ord}_{\mathfrak{q}_m}(f'(mQ)) = \text{ord}_{\mathfrak{q}_m}(x'(mQ))$ . Thus, using Corollary 4.5.9,

$$[L : \mathbb{Q}]h_x(mP) = |\mathcal{S}_{f'}(mQ)| \log |x'(mQ)|_{\mathfrak{q}_m} + O(\log m) \quad (6.7)$$

Let  $d = \deg \phi$ . By Proposition 4.5.3,

$$2d[L : \mathbb{Q}]\hat{h}(mQ) = 2[L : \mathbb{Q}]\hat{h}(mP).$$

Substituting in (6.4) and (6.6) gives

$$d[L : \mathbb{Q}]h_{x'}(mQ) = [L : \mathbb{Q}]h_x(mP) + O(1)$$

where the implied constant depends on  $E$  and  $E'$ . Substituting in (6.5) and (6.7) shows that for all  $m > 2$ ,

$$(d|\mathcal{S}_{x'}(mQ)| - |\mathcal{S}_{f'}(mQ)|) \log |x'(mQ)|_{q_m} \leq C_1 \log m \quad (6.8)$$

where  $C_1 > 0$  depends only on  $E, E', \phi, S, K, L$  and  $P$ . But

$$d|\mathcal{S}_{x'}(mQ)| - |\mathcal{S}_{f'}(mQ)| \geq d - [L : K] > 0,$$

so substituting (6.8) into (6.7) and (6.6) shows that for all  $m > 2$ ,

$$m^2 \hat{h}(P) \leq C \log m$$

where  $C > 0$  depends only on  $E, E', \phi, S, K, L$  and  $P$ . The required result follows.  $\square$

**Remark 6.2.2.** Keep the notation of Theorem 6.2.1 but suppose that  $\deg \phi = [L : K]$ ,  $mP \in E_x(K)$  and  $S_x(mP) = \{\mathfrak{p}\}$  where  $\mathfrak{p}$  does not split completely in  $L$ . Then (6.8) gives that there are finitely many choices for  $m$ .

**Remark 6.2.3.** Because elliptic transcendence theory is used (Theorem 4.5.5), the constant constructed in the proof of Theorem 6.2.1 is too unwieldy for the purpose of producing examples with explicit bounds. Using results of Silverman [49], in Chapter 7 bounds on height which do not come from elliptic transcendence theory are used and infinite families of examples are produced (see Proposition 7.2.5 and Proposition 7.2.6).

**Corollary 6.2.4.** *Let  $(E, O)$  be an elliptic curve defined over  $K$  and  $f \in K(E)$  be such that  $O$  is a pole of  $f$ . Suppose that a fixed non-torsion point  $P \in E(K)$  is Galois magnified by*

$$\phi : (E', O') \rightarrow (E, O),$$

where  $E'$  and  $\phi$  are defined over a number field  $L$ . Let  $m$  be such that  $mP \in E_f(K)$  and  $|S_f(mP)| \leq 1$ . Then there are finitely many choices for  $m$ . Moreover, a bound for  $m$  which depends only on  $E, E', \phi, S, K, L, P$  and  $f$  can be explicitly determined.

*Proof.* Let  $x$  and  $y$  be coordinates on a Weierstrass equation for  $E/K$  which, from (4.2), may be taken as

$$y^2 = x^3 + B_2x^2 + B_4x + B_6.$$

Now  $f \in K(E) = K(x, y)$  gives

$$f(x, y) = \frac{\psi_1(x) + \psi_2(x)y}{\eta(x)}$$

where  $\psi_1(x), \psi_2(x), \eta(x) \in K[x]$ . Using Theorem 2.2.10, choose  $\dot{S} \subset M_K^0$  so that:

- $S \subset \dot{S}$ ;
- $\mathcal{R}_{\dot{S}}$  is a unique factorization domain;
- $\psi_1(x), \psi_2(x), \eta(x) \in \mathcal{R}_{\dot{S}}[x]$  and their leading coefficients are units;
- $B_i \in \mathcal{R}_{\dot{S}}$ .

If  $x(mP) = 0$  then Proposition 4.5.3 gives that  $2m^2\hat{h}(P) = O(1)$ . So assume that  $mP \in E_x(K)$ . By Lemma 4.3.1, if  $x(P) \neq 0$ ,

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

where  $A_P C_P$  and  $B_P$  are coprime in  $\mathcal{R}_{\dot{S}}$ . As in the proof of corollary 5.2.3,  $O$  being a pole of  $f$  implies that

$$2 \deg \eta < \max\{2 \deg \psi_1, 2 \deg \psi_2 + 3\}.$$

If  $3 + 2 \deg \psi_2 > 2 \deg \psi_1$ , write

$$f(P) = \frac{B_P^{3+2(\deg \psi_2 - \deg \psi_1)} \left( B_P^{2 \deg \psi_1} \psi_1 \left( \frac{A_P}{B_P^2} \right) \right) + C_P \left( B_P^{2 \deg \psi_2} \psi_2 \left( \frac{A_P}{B_P^2} \right) \right)}{B_P^{3+2(\deg \psi_2 - \deg \eta)} \left( B_P^{2 \deg \eta} \eta \left( \frac{A_P}{B_P^2} \right) \right)}.$$

If  $3 + 2 \deg \psi_2 < 2 \deg \psi_1$ , write

$$f(P) = \frac{\left( B_P^{2 \deg \psi_1} \psi_1 \left( \frac{A_P}{B_P^2} \right) \right) + B_P^{2(\deg \psi_1 - \deg \psi_2) - 3} C_P \left( B_P^{2 \deg \psi_2} \psi_2 \left( \frac{A_P}{B_P^2} \right) \right)}{B_P^{2(\deg \psi_1 - \deg \eta)} \left( B_P^{2 \deg \eta} \eta \left( \frac{A_P}{B_P^2} \right) \right)}.$$

Note that  $B_P$  is coprime (in  $\mathcal{R}_{\dot{S}}$ ) with both the numerator and  $B_P^{2 \deg \eta} \eta(x(P))$ . Hence, if  $|S_f(mP)| \leq 1$  then  $|\dot{S}_x(mP)| \leq 1$  and the result follows from Theorem 6.2.1.  $\square$

For points which are simply magnified, the number of exceptional points is bounded by the Siegel-Mahler Theorem (see Remark 6.2.6).

**Theorem 6.2.5.** *Let  $(E, O)$  be an elliptic curve defined over  $K$ . Suppose that  $G \subset E(K)$  is a set of points which are simply magnified. If  $f \in K(E)$  has a pole at  $O$  then there are finitely many  $P \in G \cap E_f(K)$  with  $|S_f(P)| \leq 1$ .*

*Proof.* Let  $P \in G$  be simply magnified from  $Q \in E'(K)$  by an isogeny

$$\phi : (E', O') \rightarrow (E, O)$$

of degree  $d$ . Let  $x'$  and  $y'$  the coordinates on a Weierstrass equation for  $E'/K$  which, from (4.2), may be taken as

$$y'^2 = x'^3 + B_2x'^2 + B_4x' + B_6.$$

Put  $f' = f \circ \phi \in \phi^*K(E) \subset K(E') = K(x', y')$ . Then  $f'(Q) = f(P)$ . Write

$$f'(x', y') = \frac{\psi_1(x') + \psi_2(x')y'}{\eta(x')}$$

where  $\psi_1(x'), \psi_2(x'), \eta(x') \in K[x']$ . Using Theorem 2.2.10, choose  $\dot{S} \subset M_K^0$  so that:

- $S \subset \dot{S}$ ;
- $\mathcal{R}_{\dot{S}}$  is a unique factorization domain;
- $\psi_1(x'), \psi_2(x'), \eta(x') \in \mathcal{R}_{\dot{S}}[x']$  and their leading coefficients are units;
- $B_i \in \mathcal{R}_{\dot{S}}$ .

Assume that  $x'(Q)$  and  $y'(Q)$  are non-zero. Using Lemma 4.3.1, write  $x'(Q) = A_Q/B_Q^2$  where  $A_Q$  and  $B_Q$  are coprime in  $\mathcal{R}_{\dot{S}}$ . Then the denominator of  $f'(Q) = f(P)$  is divisible by  $B_Q$ . Thus, if  $x'(Q)$  is not an  $\dot{S}$ -integer then  $\text{ord}_\nu(f(P)) < 0$  for some prime  $\nu \notin S$ .

By Proposition 4.2.5 and Example 3.2.7, there exists a non-zero  $d$ -torsion point  $T$  in the kernel of  $\phi$ . Note that  $f'(Q + T) = f'(Q)$ . Let  $L = K(x'(T), y'(T))$ . Using Theorem 2.2.10, choose  $\mathcal{S} \subset M_L^0$  so that:

- $\mathcal{S}$  contains the prime ideals of  $\mathcal{O}_L$  which lie above the ideals in  $\dot{S}$ ;
- the ring of  $\mathcal{S}$ -integers in  $L$ , denoted  $\mathfrak{R}_{\mathcal{S}}$ , is a unique factorization domain;
- $x'(T) \in \mathfrak{R}_{\mathcal{S}}$ .

Then the addition formula shows that the denominator of  $x'(Q + T)$  divides

$$(A_Q - x'(T)B_Q^2)^2,$$

and so is coprime with  $B_Q$  in  $\mathfrak{R}_{\mathcal{S}}$ . The denominator of  $x'(Q + T)$  also divides the denominator of  $f'(Q + T) = f'(P)$ . Thus, if  $x'(Q + T)$  is not an  $\mathcal{S}$ -integer then  $\text{ord}_{\omega}(f'(P)) < 0$  for some prime  $\omega \notin \mathcal{S}$ . So if  $x'(Q + T)$  and  $x'(Q)$  are not  $\mathcal{S}$ -integers then  $|S_f(P)| > 1$ . Conversely, if  $|S_f(P)| \leq 1$  then  $P$  is the image under  $\phi$  of a point  $Q \in E'(L)$  with  $x'(Q) \in \mathfrak{R}_{\mathcal{S}}$ .  $\square$

**Remark 6.2.6.** Keep the notation of Theorem 6.2.5. In the proof of Theorem 6.2.5, choose  $x', y'$  as in Theorem 5.1.2. Then it follows that there exists a constant  $\kappa$  depending only on  $L$  such that

$$\#\{P \in G \cap E_f(K) : |S_f(P)| \leq 1\} \leq \kappa^{(1+r)(1+\delta)+\#\mathcal{S}},$$

where  $r$  is the rank of  $E'(L)$  and  $\delta = \#\{\mathfrak{p} \in M_L^0 : \text{ord}_{\mathfrak{p}}(j_{E'}) < 0\}$ .

**Example 6.2.7.** Take  $K = \mathbb{Q}$ , let  $(E, \mathcal{O})$  be an elliptic curve given by

$$y^2 = x^3 - 2611x - 51330,$$

and suppose that  $f \in \mathbb{Q}(E)$  has a pole at  $\mathcal{O}$ . Using [13] and PARI/GP,

$$E(\mathbb{Q}) = \langle (70, 330), (259, 4080), T_1, T_2 \rangle$$

where  $T_1 = (59, 0)$  and  $T_2 = (-29, 0)$  are 2-torsion points. Consider the subgroup

$$G = \langle (70, 330), (259, 4080), T_2 \rangle.$$

Putting  $t = -30$  in Proposition 4.3.6 shows that there exists an elliptic curve

$$E' : y'^2 = x'^3 + 180x'^2 + 7744x'$$

and a 2-isogeny  $\psi : E' \rightarrow E$  such that

$$\psi \langle (176, -3520), (968, -32912), (-88, 176) \rangle = G.$$

So by Theorem 6.2.5, there are finitely many  $P \in E_f(\mathbb{Q}) \cap G$  with  $|S_f(P)| \leq 1$ .

There do exist elliptic curves  $E$  for which the whole of the Mordell-Weil Group  $E(\mathbb{Q})$  is simply magnified.

**Example 6.2.8.** Take  $K = \mathbb{Q}$ , let  $(E, \mathcal{O})$  be an elliptic curve given by

$$y^2 = x^3 + B,$$

and suppose that  $f \in \mathbb{Q}(E)$  has a pole at  $\mathcal{O}$ . Let  $\phi$  be as in Example 4.2.2. If  $B = -2$  then

$$E(\mathbb{Q}) = \langle (3, 5) \rangle$$

and  $\phi(\frac{1}{3}, \frac{1}{3}) = (3, 5)$ . If  $B = -11$  then, using [13] and PARI/GP,

$$E(\mathbb{Q}) = \langle (3, 4), (15, 58) \rangle$$

and  $\phi(\langle (-\frac{2}{3}, \frac{1}{3}), (\frac{1}{3}, -\frac{2}{3}) \rangle) = E(\mathbb{Q})$ . So by Theorem 6.2.5, if  $B = -2, -11$  then there are finitely many  $P \in E_f(\mathbb{Q})$  with  $|S_f(P)| \leq 1$ .

Fix  $D \in K^*$ . For the cubic Fermat-Thue curve  $E : U^3 + V^3 = D$ , the magnified condition in Theorem 6.2.5 is known to be unnecessary. The following is an extension to number fields of Theorem 4.1 in [22].

**Theorem 6.2.9.** *For non-zero  $D \in K$ , let*

$$E : U^3 + V^3 = D.$$

*If  $f \in K(E)$  has a pole at  $O = [1, -1, 0]$  then there are finitely many  $P \in E_f(K)$  with  $|S_f(P)| \leq 1$ . The number of such points is given by the Siegel-Mahler Theorem.*

*Proof.* Using Theorem 2.2.10, choose  $\dot{S} \subset M_K^0$  so that:

- $S \subset \dot{S}$ ;
- $\mathcal{R}_{\dot{S}}$  is a unique factorization domain;
- $2, 3, D \in \mathcal{R}_{\dot{S}}^*$ .

Let  $C : Y^2 = X^3 - 2^4 3^3 D^2$ . There is an isomorphism  $\phi : C \rightarrow E$  given by

$$\phi = \left[ \frac{2^2 3^2 D + Y}{6X}, \frac{2^2 3^2 D - Y}{6X}, 1 \right].$$

Let  $P \in E_U(K)$ . Now  $P = \phi(Q)$  for some  $Q \in C(K)$ . Using Lemma 4.3.1, write  $X(Q) = A_Q/B_Q^2$  and  $Y(Q) = C_Q/B_Q^3$  where  $A_Q, B_Q, C_Q$  are pairwise coprime in  $\mathcal{R}_{\dot{S}}$ .

Then

$$U(P) = \frac{2^2 3^2 D + Y(Q)}{6X(Q)} = \frac{2^2 3^2 D B_Q^3 + C_Q}{6A_Q B_Q}$$

and  $V(P)$  is similar. Note that both  $A_Q$  and  $B_Q$  are coprime with the numerator in  $\mathcal{R}_{\dot{S}}$ .

Let  $L = K(\sqrt{-3})$ . Further, let  $\mathcal{S} \subset M_L^0$  be such that:

- $\mathcal{S}$  contains the prime ideals of  $\mathcal{O}_L$  which lie above the ideals in  $\dot{S}$ ;
- the ring of  $\mathcal{S}$ -integers in  $L$ , denoted  $\mathfrak{R}_{\mathcal{S}}$ , is a unique factorization domain.

Consider  $T = (0, 2^2 3 D \sqrt{-3}) \in C(L)$ . The denominator of  $X(Q+T)$  divides  $A_Q$  in  $\mathfrak{R}_{\mathcal{S}}$ .

Put  $\psi = [3] \circ \phi$ , then  $\psi(Q+T) = \psi(Q) = 3P$ . Assume that  $|S_U(P)| \leq 1$ . Then  $3P$  is the image of an  $\mathcal{S}$ -integral point under  $\psi$ . So, there are at most  $|\{Q \in C(L) : X(Q) \in \mathfrak{R}_{\mathcal{S}}\}|$  choices for  $3P$ . From Proposition 4.2.5(b), for each choice of  $3P$  there are at most 9 choices for  $P$ .

The inverse of  $\phi$  is given by

$$X = 2^2 3(U^2 - UV + V^2) \quad \text{and} \quad Y = 2^2 3^2(U^2 - UV + V^2)(U - V).$$

For  $P \in E_U(K)$  write  $U(P) = A_P/B_P$  and  $V(P) = C_P/B_P$  where  $A_P, B_P$  and  $C_P$  are pairwise coprime in  $\mathcal{R}_{\dot{S}}$ . Thus

$$X(P) = \frac{2^2 3(A_P - A_P C_P + C_P^2)}{B_P^2}.$$

So, if  $|S_X(P)| \leq 1$  then  $|\dot{S}_U(P)| \leq 1$ . Now suppose that  $f \in K(E) = K(X, Y)$  has a pole at  $O$ . Following the proof of Corollary 5.2.3, there exists a set  $\dot{S} \subset M_K^0$  so that  $|S_f(P)| \leq 1$  implies  $|\dot{S}_X(P)| \leq 1$ . Hence, the required result follows.  $\square$

When  $K = \mathbb{Q}$ ,  $f = U$  and  $S = \emptyset$ , the number of points in Theorem 6.2.9 can be bounded independently of rank. For non-zero  $D \in \mathcal{O}_K$ , let

$$l_K(D) = \sum_{\text{ord}_{\mathfrak{p}}(D) > 0} 1$$

and

$$l'_K(D) = \sum_{\text{ord}_p(D) > 0} \text{ord}_p(D).$$

**Theorem 6.2.10.** *For non-zero cube-free  $D \in \mathbb{Z}$ , let*

$$E : U^3 + V^3 = D.$$

*Then*

$$\{P \in E(\mathbb{Q}) : |\emptyset_U(P)| \leq 1\} \leq 48 \cdot 2^{6l_{\mathbb{Q}}(D)} \cdot 7^{27(2l_{\mathbb{Q}}(D)+3)}.$$

*Proof.* Firstly, suppose that  $U(P) = u \in \mathbb{Z}$ . Then  $V(P) = v \in \mathbb{Z}$  and it may be assumed that  $(u, v) = 1$ . Factorizing,

$$(u + v)(u^2 - uv + v^2) = D.$$

So  $u + v = z_1$  and  $u^2 - uv + v^2 = z_2$  for  $z_1, z_2 \in \mathbb{Z}$ . Since  $D$  is cube-free, there are at most  $2 \cdot 2^{l'_{\mathbb{Q}}(D)} \leq 2 \cdot 2^{2l_{\mathbb{Q}}(D)}$  choices for  $z_2$ . Put  $K = \mathbb{Q}(\zeta)$  where  $\zeta$  is non-trivial cube root of unity. Then  $K = \mathbb{Q}(\sqrt{-3})$  and

$$u^2 - uv + v^2 = (u + \zeta v)(u + \zeta^2 v) = z_2.$$

Put  $u + \zeta v = w_1$  and  $u + \zeta^2 v = w_2$ . There are 6 units in  $\mathbb{Z}[\zeta]$ . For each choice of  $z_2$ , there are at most  $6 \cdot 2^{l'_K(z_2)}$  choices for  $\{w_1, w_2\}$ . But

$$l'_K(z_2) \leq l'_K(D) \leq 2l'_{\mathbb{Q}}(D) \leq 4l_{\mathbb{Q}}(D),$$

so there are at most  $12 \cdot 2^{6l_{\mathbb{Q}}(D)}$  choices for  $\{w_1, w_2\}$ . For each choice of  $\{w_1, w_2\}$ , there is exactly one choice for

$$u = \frac{\zeta w_1 - w_2}{\zeta - 1} \quad \text{and} \quad v = \frac{w_2 - w_1}{\zeta(\zeta - 1)}.$$

Now suppose that  $U(P) = u/q$  with  $u \in \mathbb{Z}$  and  $q$  a prime power. Then

$$(u + v)(u^2 - uv + v^2) = Dq^3$$

where  $u, v, q$  are pairwise coprime. Assume that  $q$  is not a power of 3. A prime which divides  $u + v$  and  $u^2 - uv + v^2$ , also divides 3. If  $q$  does not divide  $u^2 - uv + v^2$ , then the number of solutions is bounded as before. Hence, assume that

$$u + v = z_1 \quad \text{and} \quad u^2 - uv + v^2 = z_2 q^3.$$

A prime which divides  $u + \zeta v$  and  $u + \zeta^2 v$ , also divides

$$\zeta u + \zeta^2 v - u - \zeta^2 v = (\zeta - 1)u = u \left( \frac{1}{2} \pm \frac{1}{2} \sqrt{-3} \right) \sqrt{-3}.$$

Thus, one of  $u + \zeta v$ ,  $u + \zeta^2 v$  is equal to  $w\rho^3$  where  $w$  divides  $z_2$  and  $\rho$  divides  $q$  in  $\mathbb{Z}[\zeta]$ . As before, there are at most  $12 \cdot 64^{l_{\mathbb{Q}}(D)}$  choices for  $\{z_1, z_2, w\}$ . Put  $w = c + d\zeta$  and  $\rho = a + b\zeta$  with  $a, b, c, d \in \mathbb{Z}$ . Comparing coefficients, write  $u$  and  $v$  explicitly in terms of  $a, b, c$  and  $d$ . Substituting into the equation  $u + v = z_1$  then gives

$$(c + d)a^3 + (3c - 6d)a^2b + (3d - 6c)ab^2 + (c + d)b^3 = z_1$$

or

$$(c - 2d)a^3 + (3d - 6c)a^2b + (3c + 3d)ab^2 + (c - 2d)b^3 = z_1.$$

Both of these Thue equations are non-singular since their corresponding cubic polynomials have discriminant

$$729(d^2 - cd + c^2)^2 \neq 0.$$

By Corollary 2 of [23], for each choice of  $z_1$  and  $w$  there are at most

$$7^{27(2l_{\mathbb{Q}}(z_1)+3)} \leq 7^{27(2l_{\mathbb{Q}}(D)+3)} \quad (6.9)$$

choices for  $\{a, b\}$ . Hence, multiplying by  $12 \cdot 64^{l_{\mathbb{Q}}(D)}$  gives the required bound.

Finally, assume that  $q = 3^n$ . The greatest common divisor  $z = \gcd(u+v, u^2-uv+v^2)$  divides 3. It may be assumed that

$$u + v = zz_1 \quad \text{and} \quad u^2 - uv + v^2 = z^{-1}3^3(3^{n-1})^3 z_2.$$

Note that  $\sqrt{-3}$  is prime in  $\mathbb{Z}[\zeta]$  and that the greatest common divisor of  $u + \zeta v$ ,  $u + \zeta^2 v$  divides  $\sqrt{-3}$ . It follows that one of  $u + \zeta v$ ,  $u + \zeta^2 v$  is equal to  $w'w(3^{n-1})^3$  where  $w$  divides  $z_2$  and  $w' = z^{-1}3^3$  or  $w' = z^{-1}(\sqrt{-3})^5$ . So there are at most  $48 \cdot 64^{l_{\mathbb{Q}}(D)}$  choices for  $\{z, z_1, z_2, w'w\}$ . Multiplying with (6.9) gives the required bound.  $\square$

# Chapter 7

## Elliptic Divisibility Sequences

Let  $E/\mathbb{Q}$  be an elliptic curve given by a Weierstrass equation with integral coefficients and suppose that there exists a non-torsion point  $P \in E(\mathbb{Q})$  which is Galois magnified. Theorem 6.2.1 gives that there are finitely many prime power terms in the corresponding elliptic divisibility sequence. A brief overview of how these sequences are defined and what is known about them is given Section 7.1. Two families of elliptic divisibility sequences whose terms are not prime powers beyond the fifth are given in Section 7.2. One of these families includes a subset of the congruent number curves.

### 7.1 Definitions

Let  $(h_n)$  be an infinite sequence of integers  $\dots, h_{-2}, h_{-1}, h_0, h_1, h_2, \dots$  such that  $h_n | h_m$  whenever  $n | m$  and

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \quad (7.1)$$

for all  $m, n \in \mathbb{Z}$ . Suppose further that  $h_2$  and  $h_3$  are non-zero. These were first studied in detail by Ward in [54]. They include the Fibonacci sequence (up to sign) and the Mersenne sequence (up to a power of 2). For a detailed description of the sign of  $(h_n)$  see [50].

Building on work of Ward, Shipsey [44] has given a formula for a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x \quad (7.2)$$

such that  $a_3a_4$  is non-zero and the sequence  $(\omega_n(0, 0))$  of division polynomials (see Section 4.3) is  $(h_n)$ . Moreover, if the coefficients  $a_i$  are integers and  $(a_3, a_4) = 1$  then  $Z_n^2 = h_n^2$ , where  $x(n(0, 0)) = X_n/Z_n^2$  is written in lowest terms. Traditionally [54], the sequence  $(h_n)$  has been called an elliptic divisibility sequence. However, the Weierstrass equation (7.2) is, crucially, not always non-singular.

**Example 7.1.1.** Let  $(F_n)$  be the Fibonacci sequence and  $P = (0, 0)$  on

$$C : y^2 + xy + y = x^3 - 2x^2.$$

Then  $Z_n = |F_n|$ , where  $x(nP) = X_n/Z_n^2$  is written in lowest terms. Note that  $P$  is non-singular but  $(1, -1)$  is singular on  $C$ .

Now let  $E/\mathbb{Q}$  be an elliptic curve such that  $E(\mathbb{Q})$  has positive rank. In [44] Shipsey proves that  $E$  has a Weierstrass equation (7.2) with integer coefficients such that  $a_3a_4$  is non-zero and  $(Z_n)$  satisfies (7.1) (up to sign), where  $(0, 0)$  is a non-torsion point and  $x(n(0, 0)) = X_n/Z_n^2$  is written in lowest terms. This motivates the following definition, which has been used and studied by Everest [22], Cornelissen [11], Silverman [48], Streng [52] et al.

**Definition 7.1.2.** Let  $E/\mathbb{Q}$  be an elliptic curve given by a Weierstrass equation (4.1) with coefficients in  $\mathbb{Z}$ . Suppose there exists a non-torsion point  $P \in E(\mathbb{Q})$  and, for  $n \neq 0$ , write  $x(nP) = X_n/Z_n^2$  in lowest terms. Then the sequence  $(Z_n)$  is called an *elliptic divisibility sequence given by  $(E, P)$* .

Note that if  $(Z_n)$  is as in Definition 7.1.2 then, from Lemma 4.5.7(a),  $Z_n|Z_m$  whenever  $n|m$ . It is shown in [6] that the only perfect powers in the Fibonacci sequence are 0, 1, 8 and 144. Fix an integer  $n_0 > 1$ . A consequence of Theorem 5.2.1 is that there are only finitely many  $n_0$ th powers in an elliptic divisibility sequence. The Fibonacci and Mersenne sequences are believed to have infinitely many prime terms (see [7] and [8]). The latter has produced the largest primes known to date. In [10] Chudnovsky and Chudnovsky considered the likelihood that an elliptic divisibility sequence might be a source of large primes.

**Example 7.1.3.** Let  $P$  denote the point  $(-386, -3767)$  on the elliptic curve

$$y^2 + xy = x^3 - 141875x + 18393057$$

The values  $x(nP)$  have prime square denominators for 32 values of  $n$ , ending (perhaps) with  $n = 1811$ . These computations were performed on PARI/GP [41].

Theorem 6.2.1 says that if  $(E, P)$  determines an elliptic divisibility sequence and  $P$  is Galois magnified then there are finitely many prime terms, moreover, if  $nP$  yields a prime term then  $n$  can be explicitly bounded. In the next section, it will be shown that this bound is uniform for certain families of curves.

## 7.2 Explicit Bounds on Primality

Here the proof of Theorem 6.2.5 will be carried out explicitly for two families of curves using the 2-isogeny given by Proposition 4.3.6. Estimates for the difference between the Weil height and the canonical height (see Proposition 4.5.3(b)) shall also be used heavily. The following theorem is Theorem 1.1 of [49].

**Theorem 7.2.1.** ([49]) *Let  $K$  be a number field. For  $x \in K$ , denote  $h([x, 1])$  by  $h(x)$ . Let  $E/K$  be an elliptic curve given by a Weierstrass equation (4.1) whose coefficients are in the ring of integers of  $K$ . Let  $\Delta$  be the discriminant of (4.1),  $j$  be the  $j$ -invariant of  $E$  and*

$$2^* = \begin{cases} 2 & \text{if } b_2 \neq 0 \\ 1 & \text{if } b_2 = 0. \end{cases}$$

*Define*

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

*Then for all  $P \in E(\bar{K})$ ,*

$$-\frac{h(j)}{24} - \mu(E) - 0.973 \leq \hat{h}(P) - \frac{h_x(P)}{2} \leq \mu(E) + 1.07.$$

**Corollary 7.2.2.** ([49]) *Let  $K$  be a number field. For  $x \in K$ , denote  $h([x, 1])$  by  $h(x)$ .*

*Let  $E/K$  be an elliptic curve given by a Weierstrass equation*

$$y^2 = x^3 + Ax + B \tag{7.3}$$

whose coefficients are in the ring of integers of  $K$ . Let  $\Delta$  be the discriminant of (7.3) and let  $j$  be the  $j$ -invariant of  $E$ . Then for all  $P \in E(\bar{K})$ ,

$$-\frac{h(j)}{8} - \frac{h(\Delta)}{12} - 0.973 \leq \hat{h}(P) - \frac{h_x(P)}{2} \leq \frac{h(j)}{12} + \frac{h(\Delta)}{12} + 1.07.$$

**Example 7.2.3.** For an integer  $T > 1$ , let

$$F : y^2 = x^3 + 2(T^4 + T^2 + 2)x^2 + T^4(T^2 - 1)^2x.$$

Then Theorem 7.2.1 gives  $h_x(Q) \geq 2\hat{h}(Q) - 2\mu(F) - 2.14$  for all  $Q \in F(\mathbb{Q})$ , where

$$2\mu(F) = \frac{1}{2} \log(T^8 + 14T^6 + 17T^4 + 16T^2 + 16) + \log(T^4 + T^2 + 2) + 3 \log 2 - \log 3.$$

For any positive integer  $m$  and  $Q \in F(\mathbb{Q})$ , the lower bound in Theorem 7.2.1 gives

$$2\hat{h}(mQ) \geq h_x(mQ) + \frac{8}{12} \log 2 - \frac{3}{12} \log(T^8 + 14T^6 + 17T^4 + 16T^2 + 16) - 2\mu(F) - 1.946.$$

**Lemma 7.2.4.** Let  $\phi$  be as in Proposition 4.3.6 with  $t, A_t, B_t \in \mathbb{Z}$ . Given  $P \in E_t(\mathbb{Q})$ , suppose there exists  $Q \in F_t(\mathbb{Q})$  such that  $\hat{\phi}(Q) = P$ . Then the denominators of  $x_2(Q)$  and  $x_2(Q + (0, 0))$  are coprime. Moreover, they divide the denominator of  $x_1(P)$ .

*Proof.* Write

$$P = \left( \frac{X}{Z^2}, \frac{Y}{Z^3} \right)$$

where  $X, Y, Z \in \mathbb{Z}$  with  $(XY, Z) = 1$  and

$$Q = \left( \frac{X_Q}{Z_Q^2}, \frac{Y_Q}{Z_Q^3} \right)$$

where  $X_Q, Y_Q, Z_Q \in \mathbb{Z}$  with  $(X_Q Y_Q, Z_Q) = 1$ . Then

$$x_1(\phi(Q)) = \frac{X_Q^2 - 2A_t X_Q Z_Q^2 + d_t Z_Q^4}{4Z_Q^2 X_Q} = \frac{X}{Z^2} = x(P).$$

so  $Z_Q$  occurs in the denominator of  $x(P)$ . Also

$$|x_2(Q + (0, 0))| = \left| \frac{Y_Q^2}{Z_Q^2 X_Q^2} + 2A_t - \frac{X_Q}{Z_Q^2} \right| = \left| \frac{d_t Z_Q^2}{X_Q} \right|$$

so the denominator of  $x_2(Q + (0, 0))$  occurs in the denominator of  $x_1(P)$  and the result follows.  $\square$

For the rest of this section,  $E$  is an elliptic curve given by a Weierstrass equation (4.1) with coefficients in  $\mathbb{Z}$ . Also, for a non-torsion point  $P \in E(\mathbb{Q})$  write  $x(nP) = X_n/Z_n^2$  where  $X_n, Z_n \in \mathbb{Z}$  are coprime.

The first family given parameterizes both the curve and the point.

**Proposition 7.2.5.** *For an integer  $T > 1$ , let  $P = (0, T^3)$  on*

$$E : y^2 = (x + 1)(x - T^2)(x - T^4).$$

*Then for  $n > 2$ ,  $Z_n$  is divisible by at least two distinct primes.*

*Proof.* It is enough to prove the result for  $P_{-1} = (1, T^3)$  on

$$E_{-1} : y^2 = x^3 - (T^4 + T^2 + 2)x^2 + (T^4 + 1)(T^2 + 1)x.$$

Putting  $t = -1$  in Lemma 4.3.7 gives that  $x(nP_{-1})$  is a non-zero square. Using Proposition 4.3.6,

$$Q = (-T^2(T + 1)^2, -2T^2(T + 1)^2) \in F(\mathbb{Q})$$

is such that  $\hat{\phi}(nQ) = nP_{-1}$  where  $F$  is as in Example 7.2.3. By Lemma 7.2.4, it is enough to show that if  $nQ$  or  $nQ + (0, 0)$  is integral then  $n \leq 2$ . Assume firstly that  $n$  is odd. Lemma 4.3.7 gives that  $x'(nQ) < 0$ . So  $nQ$  and  $nQ + (0, 0)$  lie on the bounded part of  $F$ . Without loss of generality assume that  $nQ$  is integral. Then

$$h_{x'}(nQ) < \log |A_{-1} - 2B_{-1}^{1/2}| < \log d_{-1}.$$

The estimates in Example 7.2.3 yield

$$8\hat{h}(nQ) \leq 2 \log (T^8(T^2 - 1)^4(T^4 + T^2 + 2)^2(T^8 + 14T^6 + 17T^4 + 16T^2 + 16)) + \theta$$

where  $\theta = 4(3 \log 2 - \log 3 + 2.14)$  and

$$8\hat{h}(5Q) \geq 4h_{x'}(5Q) - \log((T^4 + T^2 + 2)^4(T^8 + 14T^6 + 17T^4 + 16T^2 + 16)^3) + \eta$$

where  $\eta = 4(\log 3 - \frac{7}{3} \log 2 - 1.946)$ . Put

$$f(T) = T^{12} + 3T^{10} - 6T^9 + 6T^8 - 4T^7 + 3T^6 - 2T^5 + 2T^4 - 4T^3 - T^2 + 2T + 1$$

then

$$x'(5Q) = -\frac{T^2(T+1)^2 f(T)^2}{f(-T)^2}$$

and it follows that  $h_{x'}(5Q) = 2 \log(T(T+1)f(T))$ . Hence

$$8\hat{h}(5Q) \geq \log \left( \frac{T^8(T+1)^8 f(T)^8}{(T^4 + T^2 + 2)^4 (T^8 + 14T^6 + 17T^4 + 16T^2 + 16)^3} \right) + \eta$$

and so

$$\frac{n^2}{25} \leq \frac{2 \log(T^8(T^2-1)^4(T^4+T^2+2)^2(T^8+14T^6+17T^4+16T^2+16)) + \theta}{\log \left( \frac{T^8(T+1)^8 f(T)^8}{(T^4+T^2+2)^4 (T^8+14T^6+17T^4+16T^2+16)^3} \right) + \eta}.$$

Thus  $n \leq 6.2$  for all  $T > 1$ . Since  $n$  is odd, it follows that  $n \leq 5$ . But

$$x'(3Q) = -\frac{T^2(T+1)^2(T^4+T^2-2T+1)^2}{(T^4+T^2+2T+1)^2}$$

and  $(T^4 + T^2 \pm 2T + 1), f(\pm T) > 1$  when  $T > 1$ .

It remains to show that for all integers  $m > 0$ ,  $Z_{2(m+1)}$  is divisible by at least two distinct primes. This can be done by strong induction on  $m$  as follows.

*Base step.* A computation shows that

$$x(4P_{-1}) = \frac{(T^{16} + 4T^{14} + 10T^{12} + 3T^8 - 6T^4 + 4T^2 + 1)^2}{16T^2(T^2 - T + 1)^2(T^2 + T + 1)^2(T^4 - T^2 + 1)^2(T^4 + T^2 - 1)^2}.$$

*Inductive step.* Assume that  $m > 1$  and the statement is true for all positive integers less than  $m$ . Now use that  $Z_{m+1}$  divides  $Z_{2(m+1)}$ . If  $m+1$  is odd then, from above,  $Z_{m+1}$  is divisible by at least two distinct primes. If  $m+1$  is even then, by the inductive hypothesis,  $Z_{m+1}$  is divisible by at least two distinct primes.  $\square$

For the second family, the curves are the congruent number curves and the point is allowed to be any non-torsion point lying on the connected component which is the image of a rational point under a specific 2-isogeny. Table 7.1 gives examples of elliptic divisibility sequences with the required properties. All of the terms  $Z_n/Z_1$  with  $n > n_0$  are divisible by at least two distinct primes. The curves in the tables are sufficiently different since no two are isomorphic over  $\mathbb{Q}$ . It is not known whether there are infinitely many such examples.

**Proposition 7.2.6.** *For a positive square-free integer  $T$ , let  $P \in E(\mathbb{Q})$  be a non-torsion point on*

$$E : y^2 = x^3 - T^2x$$

*with  $x(P) < T$  and  $x(P) + T$  a square. If  $Z_n/Z_1$  is a prime power then  $n \leq 5$ .*

*Proof.* Firstly suppose that  $n > 5$  is composite. Then  $Z_n/Z_1$  is divisible by  $Z_{n'}$  for some  $n' > 2$ . By Theorem 1 in [31],  $Z_{n'}$  and  $Z_n$  have a primitive divisor. Thus,  $Z_n/Z_1$  cannot be a prime power.

Now suppose that  $n$  is an odd prime. The point  $P_{-T} = (x(P) + T, y(P))$  lies on

$$E_{-T} : y^2 = x_1^3 - 3Tx_1^2 + 2T^2x_1.$$

Putting  $t = -T$  in Lemma 4.3.7 gives that  $x(nP) + T$  is a non-zero square. Using Proposition 4.3.6, let  $Q \in F(\mathbb{Q})$  be such that  $\hat{\phi}(nQ) = nP_{-T}$  where

$$F : y_2^2 = x_2^3 + 6Tx_2^2 + T^2x_2 = x_2(x_2 - (-3 - 2\sqrt{2})T)(x_2 - (-3 + 2\sqrt{2})T).$$

By Lemma 7.2.4, it is enough to show that if the denominator of  $x_2(nQ)$  or  $x_2(nQ + (0, 0))$  divides  $Z_1$  then  $n \leq 5$ . Since  $x(P) < T$ ,  $x(Q) < 0$  and Lemma 4.3.7 gives that  $nQ$  and  $nQ + (0, 0)$  lie on the bounded part of  $F$ . Without loss of generality assume that the denominator of  $x_2(nQ)$  divides  $Z_1$ . Let  $Q'$  be the image of  $Q$  under the translation given by  $x_3 = x_2 + 2T$ . Then  $nQ'$  lies on the bounded part of

$$F' : y_3^2 = x_3^3 - 11T^2x_3 + 14T^3 = (x_3 - 2T)(x_3 - (-1 - 2\sqrt{2})T)(x_3 - (-1 + 2\sqrt{2})T).$$

Since the denominator of  $x_3(nQ')$  divides  $Z_1$ ,

$$h_x(nQ') \leq \log T + \log(1 + 2\sqrt{2}) + \log Z_1.$$

The upper bound in Corollary 7.2.2 yields

$$\hat{h}(nQ') \leq \log T + 3.3085 + \frac{1}{2} \log Z_1. \quad (7.4)$$

The inequality (15) in [4] is

$$-\frac{1}{2} \log T - \frac{1}{4} \log 2 \leq \hat{h}(P) - \frac{1}{2} h_x(P) \leq \frac{1}{4} \log(T^2 + 1) + \frac{1}{12} \log 2.$$

Substituting the lower bound into (7.4) gives

$$\hat{h}(nQ') - \hat{h}(P) \leq \frac{3}{2} \log T + 3.4818$$

From Proposition 4.5.3,  $2\hat{h}(Q') = \hat{h}(P)$  and in [4] it is shown that

$$\hat{h}(P) \geq \frac{1}{16} \log(2T^2).$$

Hence

$$\frac{1}{16} \left( \frac{n^2}{2} - 1 \right) \leq \frac{\frac{3}{2} \log T + 3.4818}{2 \log T + \log 2}.$$

The existence of the non-torsion point  $P$  implies that  $T \geq 5$ . It follows that  $n \leq 5$  when  $T > 5$ . When  $T = 5$ ,  $\hat{h}(P) \geq \hat{h}((-4, 6))$  and the result follows.  $\square$

Table 7.1: Examples of Proposition 7.2.6

$T$	$P$	$n_0$
5	$(-4, 6)$	1
6	$(-2, 8)$	2
7	$(-63/16, 735/64)$	1
13	$(-36/25, 1938/125)$	1
14	$(-7/4, 147/8)$	1
29	$(-4900/169, 6930/2197)$	1
65	$(-16, 252)$	1
85	$(-36, 462)$	1

# References

- [1] A. Baker. *Transcendental Number Theory*. Cambridge Univ. Press, 1975.
- [2] M. A. Bennet and C. M. Skinner. Ternary diophantine equations via galois representations and modular forms. *Canad. J. Math.* 56:23-54, 2004.
- [3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.* 24(3-4):235-265, 1997.
- [4] A. Bremner and J. H. Silverman. Integral Points in Arithmetic Progression on  $y^2 = x(x^2 - n^2)$ . *Journal of Number Theory*, 80:473–486, 2000.
- [5] Y. Bugeaud, F. Luca, M. Mignotte, and S. Siksek. Perfect powers from products of terms in Lucas sequences. *Crelle*. (to appear).
- [6] Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential diophantine equations I. Fibonacci and Lucas perfect powers. *Ann. of Math.* 163:169-1081, 2006.
- [7] Chris Caldwell. *Mersenne Primes: History, Theorems and Lists*. <http://primes.utm.edu/mersenne/index.html>.
- [8] Chris Caldwell. *The Prime Pages: Fibonacci prime*. <http://primes.utm.edu/glossary/page.php?sort=FibonacciPrime>.
- [9] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.
- [10] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.* 7:385-434, 1986.

- [11] Gunther Cornelissen and Karim Zahidi. Elliptic divisibility sequences and undecidable problems about rational points. *J. reine und angew. Math.* (to appear).
- [12] G. Cornell, J. Silverman, and G. Stevens. *Modular forms and Fermat's Last Theorem*. Springer-Verlag, New York, 1997.
- [13] J. E. Cremona. Elliptic curve data, updated 2006-09-24. <http://www.warwick.ac.uk/~masgaj/ftp/data/>.
- [14] J. E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, second edition, 1997.
- [15] H. Davenport and K. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:160–167, 1955.
- [16] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France*, 62, 1995.
- [17] S. David and N. Hirata-Kohno. Linear forms in elliptic logarithms. *Journal für die reine und angewandte Mathematik*, (to appear). See also <http://hdl.handle.net/2433/41268>.
- [18] K. Draziotis and D. Poulakis. Practical solution of the diophantine equation  $y^2 = x(x + 2^a p^b)(x - 2^a p^b)$ . *Mathematics of Computation*, 75(255):1585–1593, 2006.
- [19] N. D. Elkies and M. Watkins. Elliptic curves of large rank and small conductor. *Lecture Notes in Computer Science*, 3076, 2004.
- [20] G. Everest and H. King. Prime powers in elliptic divisibility sequences. *Math. Comp.* 74(252):2061–2071 (electronic), 2005.
- [21] G. Everest, G. McLaren, and T. Ward. Primitive divisors of elliptic divisibility sequences. *Journal of Number Theory*, 118:71–89, 2006.
- [22] G. Everest, V. Miller, and N. Stephens. Primes generated by elliptic curves. *Proc. Amer. Math. Soc.* 132:955-963, 2004.
- [23] J. H. Evertse. On equations in S-units and the Thue-Mahler equation. *Invent. math.* 75:561-584, 1984.

- [24] G. Faltings. Endlichkeitsätze für Abelschen Varietäten über Zahlkörper. *Invent. Math.*, 73:349–366, 1983.
- [25] B. Farhi. Une approche polynomiale du théorème de Faltings. *C. R. Math. Acad. Sci. Paris*, 340(340):103–106, 2005.
- [26] W. Fulton. *Algebraic curves: An introduction to algebraic geometry*. Benjamin, New York, 1969.
- [27] R. Gross and J. Silverman. S-integer points on elliptic curves. *Pacific J. Math.*, 167:266–288, 1995.
- [28] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.
- [29] M. Hindry and J. H. Silverman. *Diophantine Geometry: An Introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer, New York, 2000.
- [30] Patrick Ingram. Multiples of integral points on elliptic curves. (submitted).
- [31] Patrick Ingram. Elliptic divisibility sequences over certain curves. *Journal of Number Theory*, pages 473–486, 2007.
- [32] W. Ivorra and A. Kraus. Quelques résultats sur les équations  $ax^p + by^p = cz^2$ . *Canad. J. Math.* 58:115-153, 2006.
- [33] F. Jarvis and P. Meekin. The Fermat equation over  $\mathbb{Q}(\sqrt{2})$ . *Journal of Number Theory*, 109:182–196, 2004.
- [34] Helen King. *Prime Appearance in Elliptic Divisibility Sequences*. PhD thesis, University of East Anglia, 2005.
- [35] S. Lang. Integral points on curves. *Publications Mathématiques de l’IHÉS*, pages 27–43, 1960.
- [36] S. Lang. Mordell’s review, Siegel’s letter to Mordell, Diophantine geometry, and 20th century mathematics. *Notices Amer. Math. Soc.* 42(3):339-350, 1995.
- [37] Serge Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd edition, 1994.

- [38] K. Mahler. Über die rationalen punkte auf kurven vorn geschlecht eins. *J. Reine Angew. Math.* 170:168-178, 1934.
- [39] Y. Matijasevich. Enumerable sets are diophantine. *Doklady Akademii Nauka SSSR*, 191:272–282, 1970.
- [40] J. S. Milne. Algebraic number theory, on-line notes. <http://www.jmilne.org/math/>.
- [41] The PARI Group, Bordeaux. *PARI/GP, version 2.3.2*, 2005. <http://pari.math.u-bordeaux.fr/>.
- [42] T. Pheidas. An effort to prove that the existential theory of  $\mathbb{Q}$  is undecidable. *Contemporary Mathematics*, 270:237–252, 2000.
- [43] B. Poonen. Hilbert’s tenth problem and Mazur’s conjecture for large subrings of  $\mathbb{Q}$ . *J. Amer. Math. Soc.* 16(4):981-990, 2003.
- [44] R. Shipsey. *Elliptic divisibility sequences*. PhD thesis, Goldsmiths College (University of London), 2000.
- [45] C. L. Siegel. Über einige Anwendungen Diophantischer Approximationen. *Abh. Preussischen Akademie der Wissenschaften*, 1929.
- [46] S. Siksek. On the Diophantine equation  $x^2 = y^p + 2^k z^p$ . *Journal de Theorie des Nombres de Bordeaux*, 15:839–846, 2003.
- [47] J. H. Silverman. A quantitative version of Siegel’s theorem: Integral points on elliptic curves and catalan curves. *J. Reine Angew. Math.* 378:60-100, 1987.
- [48] J. H. Silverman. Wieferich’s criterion and the abc-conjecture. *J. Number Theory*, 30(2):226–237, 1988.
- [49] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Mathematics of Computation*, 55(192):723–743, 1990.
- [50] J. H. Silverman and N. Stephens. The sign of an elliptic divisibility sequence. *Ramanujan Math. Soc.* 21(1):1-17, 2006.

- [51] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1997. Corrected reprint of the 1986 original.
- [52] Marco Streng. Elliptic divisibility sequences with complex multiplication. Master's thesis, Universiteit Utrecht, 2006.
- [53] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris*, 273:238–241, 1971.
- [54] Morgan Ward. Memoir on elliptic divisibility sequences. *American Journal of Mathematics*, 70(1):31–74, 1948.
- [55] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Math.* 141:443-551, 1995.