On the Primality Conjecture for Certain Elliptic Divisibility Sequences

Ouamporn Phuksuwan

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

December 2009

Acknowledgements

I would like to gratefully thank Prof. Graham Everest and Dr Shaun Stevens, my supervisors, for giving me the support, encouragement, and valuable guidance.

I would like to thank Office of the Higher Education Commission, Thailand for supporting by grant fund which enabled me to study abroad. I would also like to thank Office of the Civil Service Commission and Office of Educational Affairs for help and support.

Special thanks go to Patrick Ingram for helpful suggestions on his many applications. Thanks also go to Valéry Mahé for his advice on Magma, to Jonathan, Sawian, Anthony, Matthew, and all other Math postgrads for their help in various ways, and to all members at School of Mathematics, UEA for their help and for making here an excellent place to work.

I would also like to thank Saksit, Amorn, Sujittra, Chaunjit, Pattama, Sayan and all Thai students at UEA who have made my years here enjoyable time.

I would like to give special thanks to my family for their love and support.

Abstract

On an elliptic curve of the form

$$C : U^3 + V^3 = m,$$

with a cube-free integer m, we study an integer sequence arising from the multiples of a rational point of infinite order. Given such a rational point R, say, under chord and tangent additions, write, for $n \in \mathbb{N}$,

$$\underbrace{R + ... + R}_{n \ terms} =: nR = \left(\frac{U_n}{W_n}, \frac{V_n}{W_n} \right),$$

where $U_n, V_n, W_n \in \mathbb{Z}$ such that $\gcd(U_n V_n, W_n) = 1$.

This thesis is devoted to investigating some properties of the sequence (W_n) of the denominators. This is a divisibility sequence; that is, $W_m \mid W_n$ whenever $m \mid n$. Our task here is to examine a conjecture on the number of prime terms in (W_n), well known as the Primality conjecture. We will prove that there is a uniform lower bound on n beyond such that all terms W_n have at least two distinct prime factors. In some cases, the bound is as low as $n = 2$.

Contents

Chapter 1

Introduction

The topic of prime appearance in elliptic divisibility sequences (see below and Section 4.3 for more details) was suggested by Chudnovsky and Chudnovsky in [6]. They considered the likelihood of primes in such sequences, hoping that elliptic divisibility sequences might be a source of large primes. The following examples are quoted from their paper to support this idea. To state them precisely, we shall introduce the following notations: Given an elliptic curve in short Weierstrass form

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

with $a, b \in \mathbb{Z}$, and a non-torsion point $P \in E(\mathbb{Q})$, for any $n \in \mathbb{N}$, we can write, by the shape of the equation of E,

$$nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3} \right),$$

where $A_n, B_n, C_n \in \mathbb{Z}$ with $\gcd(A_n C_n, B_n) = 1$. The integer sequence (B_n) is usually known as an *elliptic divisibility sequence* associated to E and P.

Example 1.0.1.

$$E : y^2 = x^3 + 26,\ P = [-1, 5]$$

The term B_{29} is a prime with 285 decimal digits.

$$E : y^2 = x^3 + 15,\ P = [1, 4]$$

The term B_{41} is a prime with 509 decimal digits.

The Chudnovskys examined the possibilities for prime values of the sequences (B_n) when n ran out to 100. Einsiedler, Everest and Ward extended these computations by letting n run out to 500 in [9] and found that there are no more primes. More recent examples of large primes are given below:
1. (Bríd Ní Fhlathuín, 1999)

$$E : y^2 + y = x^3 - x,\ P = [0, 0]$$

The term B_{409} is a prime with 1857 decimal digits.
2. (Everest, 2006) With the same sequence, the term B_{1291} is a prime with 18498 decimal digits.
3. (Everest, 2007)

$$E : y^2 + xy + y = x^3 + x^2 - 125615x + 61201397,\ P = [7107, 594946]$$

The term B_{3719} is a prime with 26774 decimal digits.

In [9], Einsiedler, Everest and Ward considered prime appearance in elliptic divisibility sequences and gave a suggestion from a heuristic argument and some calculations that for fixed E and P the elliptic divisibility sequences should contain only finitely many prime terms. More explicitly, Everest,

Miller and Stephens [11], have proved, using a strong form of Siegel's Theorem, the finiteness of prime terms in the sequences under a certain additional hypothesis on the generating point of the sequence. This hypothesis is concerned with an isogeny (see Section 4.5) between two elliptic curves.

Theorem 1.0.2. (THEOREM 1.3, [11]) *Let $\sigma : E \to E'$ be an isogeny. Suppose $Q \in E'(\mathbb{Q})$ is the image of a rational point on E under σ, and write $nQ = \left(\frac{a_n}{b_n^2}, \frac{c_n}{b_n^3}\right)$. Then the terms b_n are primes for only finitely many n.*

In this article, they studied, moreover, the same question for a twist of the affine cubic Fermat's curve,

$$C : U^3 + V^3 = m,$$

with a non-zero integer m. They showed again using Siegel's Theorem that there are only finitely many rational points on C that have prime power denominators.

Our purpose here is to examine the problem of prime appearance for divisibility sequences obtained from the multiples of rational points on C. Given a non-torsion point $R \in C(\mathbb{Q})$, write, in lowest terms,

$$nR = \left(\frac{U_n}{W_n}, \frac{V_n}{W_n}\right).$$

We aim to provide a uniform lower bound beyond which all terms W_n have at least two coprime divisors.

In Section 5.1, we will prove an affirmative answer under the extra hypothesis as in Theorem 1.0.2 on an elliptic curve of the form

$$E : Y^2 = X^3 - 432m^2.$$

This curve corresponds to the curve C under a bi-rational transformation, given by

$$X = \frac{2^2 3m}{U+V}, \quad Y = \frac{2^2 3^2 m(U-V)}{U+V},$$

$$U = \frac{2^2 3^2 m + Y}{6X}, \quad V = \frac{2^2 3^2 m - Y}{6X}.$$

Consequently, we have

$$\left(\frac{U_n}{W_n}, \frac{V_n}{W_n}\right) = nR = \left(\frac{2^2 3^2 m B_n^3 + C_n}{6A_n B_n}, \frac{2^2 3^2 m B_n^3 - C_n}{6A_n B_n}\right),$$

where $nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right)$ are written in lowest terms.

Our first main result states the following (see the proof in Theorem 5.1.2, Ch. 5).

Theorem 1.0.3. *Let C be an elliptic curve as defined above with $m \in \mathbb{Z}$ cube-free, and $R \in C(\mathbb{Q})$ a non-torsion point. Suppose $P \in E(\mathbb{Q})$ corresponds to R by the bi-rational transformation. Under the assumption that P is the image of a rational point under an isogeny, W_n is divisible by at least two distinct primes for all $n > 2$.*

The second part of this thesis is motivated by the idea to eliminating the isogeny condition from the first result. Consider both coordinates of nR again, we have

$$\frac{U_n}{W_n} = \frac{2^2 3^2 m B_n^3 + C_n}{6A_n B_n}$$

$$\frac{V_n}{W_n} = \frac{2^2 3^2 m B_n^3 - C_n}{6A_n B_n}.$$

As we will show in the proof of Theorem 1.0.3, any cancellation of the fractions on the right-hand side is coprime to B_n. Our idea is that once we have that:

(i) there exists a uniform bound on the index n such that $B_n > 1$; in other words, nP are integral for only finitely many n, and

(ii) $6A_n$ can escape from any cancellation,

and we will also get the uniform bound as in (i) beyond which W_n is composite.

Siegel [25] provided a classical theorem about the finiteness of the number of integral points on an elliptic curve. This means in particular that the number of integral multiples of an integral point is finite. We want to use explicit formulations of that fact in (i). More history about integral points on elliptic curves follows. Lang pursued the idea of Siegel and conjectured that the number of S-integral points on a quasi-minimal form of an elliptic curve over a number field K should be bounded solely in terms of the rank of the Mordell-Weil group $E(K)$ (see [19], p.140). Hindry and Silverman (Theorem 9.1, [14]) proved a uniform analogue of this version of Lang's conjecture provided that the Szpiro ratio of an elliptic curve E defined over a number field K, defined by

$$\sigma_{E/K} = \frac{\log \mathrm{Norm}(\Delta)}{\log \mathrm{Norm}(N)}$$

where Δ and N represent the discriminant and the conductor of the curve E, respectively, is bounded. Furthermore, Silverman [26] asserted for an elliptic curve with integral j-invariant - or with at most a fixed number of primes dividing the denominator of the j-invariant - a uniform bound for the number

of S-integral points exists without the restriction on the Szpiro ratio.

Recently, Ingram (Theorem 1, [15]) made the idea above more precise. He not only proved that the number of integral multiples of a non-torsion point, say P, is finite, but also provided a bound on the size of the second largest index n such that nP is integral in terms of some quantity $M(P) = \text{lcm}(r(P), p)$, where p is a prime and $r(P)$ is the order of the point P in the quotient $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ of finite index. In particular, Theorem 2 of [15] gives an explicit result for the family of congruent number curves,

$$E_N : y^2 = x^3 - N^2x,$$

where N is a square-free integer. Using Ingram's techniques yields similar results for the Mordell curve E, as shown in Section 5.2. Subsequently, we will obtain the second main result without the isogeny condition, however, it does require some restrictions on P and m.

Theorem 1.0.4. *Let R be a non-torsion rational point on $C : U^3 + V^3 = m$ corresponding to a non-torsion rational point P on $E : Y^2 = X^3 - 432m^2$. Write, in lowest terms, $nR = \left(\frac{U_n}{W_n}, \frac{V_n}{W_n}\right)$. Suppose that*

$gcd(A_1, m) = 1$ if $P = \left(\frac{A_1}{B_1^2}, \frac{C_1}{B_1^3}\right)$ is non-integral, or

$gcd(A_1, 3m) = 1$ and $2P, 3P$ are non-integral if $P = (A_1, C_1)$ is integral.

Then there is at most one value of $n > 1$ such that W_n is prime unless either

$m \equiv \pm 2$ mod 9 and m has a prime factor congruent to 1 mod 6, or

$m \equiv 0$ mod 9 and m has a prime factor congruent to 1 mod 6,

in such cases, the result holds for all $m > 3739071625384$.

1.1 Chapter Layout

In Chapters 2 and 3, we collect basic algebraic and geometric concepts that are required for introducing the definition and properties of elliptic curves in Chapter 4. Moreover, Chapter 2 also consists some facts used to prove the results in Chapter 5.

The definitions of the keywords such as elliptic curves, elliptic divisibility sequences, isogenies, and related topics used for the proofs of main theorems can be found in Chapter 4.

Chapter 5 consists of the proofs of Theorems 1.0.3 and 1.0.4, and a series of Lemmas.

1.2 Future works

It can be concluded from above that the question on the prime appearance in (W_n) has been answered under the isogeny assumption in the first main Theorem. The second result answered this question without the isogeny condition, but with restrictions on the integer m and the point P.

For our future plans, we aim to study the following open problems:

(1) refine the result in the second main theorem by minimizing the bound of m and then proving the result for every case of m,

(2) study the possibility to prove the uniform Primality conjecture on (W_n) in general without any restriction,

(3) prove a result on the number of semi-primes (numbers with only two prime factors) in (W_n) instead.

Chapter 2

Preliminaries

This chapter gives a short introduction of basic materials that are needed for the sequel. We start by giving the definition of Diophantine equations and some results on their integral solutions.

2.1 Diophantine equations

A Diophantine equation is a polynomial equation whose coefficients are integers or rational numbers. It is interesting to consider the rational or integral solutions of such an equation. The problem of providing an algorithm to solve given a Diophantine equation, or even, finding all solutions if they exist, has a long history. In the 2nd ICM (Paris 1900), Hilbert posed his 23 mathematical problems. The 10th of these questions asked about the existence of an algorithm determining whether a Diophantine equation in any number of unknowns with integral coefficients is solvable in integers or not. This has been answered by Davis, Putman, Robinson and Matiyasevič (1950-1970):

no such algorithm exists for integral solutions. However, this problem is unsolved for rational solutions.

The following theorem gives an answer to the question on the number of integral solutions for certain class of Diophantine equations.

Theorem 2.1.1. (Siegel's Theorem) *Suppose $F \in \mathbb{Z}[X, Y]$ is a cubic polynomial which is non-singular. Then the equation*

$$F(X, Y) = 0$$

has at most a finite number of solutions with $x, y \in \mathbb{Z}$.

Being non-singular means there is no point $(a, b) \in \mathbb{C}^2$ such that

$$F(a, b) = 0, \frac{\partial F}{\partial x}(a, b) = 0, \frac{\partial F}{\partial y}(a, b) = 0.$$

A simple case of Siegel's Theorem is given below.

Proposition 2.1.2. *All integral solutions of*

$$x^3 + y^3 = m,$$

with $m \in \mathbb{Z} \setminus \{0\}$, satisfy $|x|, |y| \leq 2\sqrt{\frac{m}{3}}$.

Proof. Factorizing the left-hand side gives

$$(x + y)(x^2 - xy + y^2) = x^3 + y^3 = m,$$

so that $(x^2 - xy + y^2) \mid m$. Hence

$$m \geq |x^2 - xy + y^2| = \left| \left(x - \frac{y}{2}\right)^2 + \frac{3y^2}{4} \right|.$$

Since both $\left(x-\frac{y}{2}\right)^2$, $\frac{3y^2}{4} \geq 0$, it follows that $\frac{3y^2}{4} \leq |m|$, so $|y| \leq 2\sqrt{\frac{|m|}{3}}$. Similarly, we have $\left|\left(y-\frac{x}{2}\right)^2+\frac{3x^2}{4}\right| \leq |m|$. This implies $|x| \leq 2\sqrt{\frac{|m|}{3}}$. □

Contrary to Siegel's result, a well-known Diophantine equation, named the *Pythagoreon equation*,

$$x^2+y^2=z^2,$$

produces infinitely many positive integral solutions (see Theorem 5.5, [23]).

Next we will present a special type of Diophantine equation. Given a homogeneous, irreducible polynomial $F(X,Y) \in \mathbb{Z}[X,Y]$ of degree $n \geq 3$, and a fixed $k \in \mathbb{Z}$, the Diophantine equation

$$F(X,Y)=k \tag{2.1}$$

is called a *Thue equation*, named after A. Thue, who proved the famous Theorem on the integral solutions of this equation in 1909 [32]:

Theorem 2.1.3. *The number of integral solutions to the equation (2.1) is finite.*

Unfortunately, Thue's proof is ineffective in the sense that it does not yield an effective method for finding the explicit solutions. Baker improved this by providing an upper bound for the size of solutions of Thue equations in [1]. However, this bound is too large to apply in special cases. Later, Bombieri and Schmidt [4] gave a better bound for the primitive solutions $(x,y) \in \mathbb{Z}^2$ (i.e. x and y are coprime). They showed that there exists an absolute constant c such that for all $n \geq c$, a Thue equation has at most $215 \cdot n^{1+\omega(k)}$

primitive solutions, where (x, y) and $(-x, -y)$ are regarded as the same, and $\omega(k)$ denotes the number of prime factors of k. Other improved results may be obtained by others for certain Thue equations. For example: the equation

$$x^4 - 4x^2y^2 + y^4 = -47$$

has been solved by Stroeker and Tzanakis [30]. They showed that only integral solutions of this equation are given by $(x, y) = (\pm 2, \pm 3)$, and $(\pm 3, \pm 2)$. Bilu and Hanrot [3] provided a method to solve some Thue equations of high degrees in practicable time. They showed the finiteness of all solutions of certain concrete Thue equations of degrees 19 and 33.

2.2 Divisibility sequences

In this section, we give the definition of divisibility sequences.

An integer sequence (A_n) is called a *divisibility sequence* if

$$A_m \mid A_n \quad \text{whenever} \quad m \mid n.$$

Example 2.2.1. Examples of divisibility sequences:
(1) The Fibonacci sequence (F_n) is given by

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...$$

Each term of the Fibonacci sequence is obtained by adding the two previous terms together; that is,

$$F_n = F_{n-1} + F_{n-2},$$

where $n \geq 3$ and $F_1 = F_2 = 1$. It can be proved by induction on $k = \frac{n}{m}$, for any integers $m \mid n$ that this sequence satisfies the divisibility property. Indeed, it satisfies the stronger property (see [36]),

$$\gcd(F_r, F_s) = F_{\gcd(r,s)}.$$

(2) The Mersenne sequence (M_n) is of the form

$$M_n = 2^n - 1.$$

It can be proved that (M_n) also satisfies the strong divisibility property,

$$\gcd(M_r, M_s) = M_{\gcd(r,s)}.$$

(3) The Lucas sequence (U_n) is defined by

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

where α and β are conjugate quadratic integers; that is, they are roots of an irreducible polynomial of the form $x^2 + Ax + B$ with $A, B \in \mathbb{Z}$. Theorem VI of [5] says that the sequence (U_n) satisfies the strong divisibility property.

We can see that the Fibonacci sequence satisfies a linear recurrence relation. Moreover, other divisibility sequences in Example 2.2.1 also satisfy a linear recurrence relation. The Mersenne sequence satisfies the relation

$$M_{n+2} = 3M_{n+1} - 2M_n, \text{ for all } n > 1,$$

and the general Lucas sequence satisfies the relation

$$U_{n+2} = (\alpha + \beta)U_{n+1} - \alpha\beta U_n, \text{ for all } n > 1.$$

Furthermore, there are the divisibility sequences that satisfy a non-linear recurrence relation. An important example is an elliptic divisibility sequence. The details will be explained in section 4.3.

2.3 Fundamental facts

This section consists of a summary of definitions and results, which are necessary for the proofs in the sequel.

2.3.1 Resultants of polynomials

Let us start by considering an example of a system of two polynomials in one variable:

$$f(x) = 3x^2 - 5x + 2,$$
$$g(x) = x^3 - 2x^2 + 2x - 1.$$

We want to find a necessary and sufficient condition for the existence of a common solution of the system.

$$\begin{aligned} f(x) &= 0 \\ g(x) &= 0. \end{aligned} \tag{2.2}$$

If $f(x)$ and $g(x)$ have a common solution in $\mathbb{C}$, they must have a common linear factor, say $D(x)$. Let

$$F(x) = \frac{f(x)}{D(x)} \text{ and } G(x) = \frac{g(x)}{D(x)}.$$

Then

$$F(x) = -A_1 x - A_0$$
$$G(x) = B_2 x^2 + B_1 x + B_0$$

for some $A_i, B_i \in \mathbb{Z}$. Note that the signs in $F(x)$ are chosen for suitability later. Since

$$\frac{f(x)}{F(x)} = \frac{g(x)}{G(x)} = D(x)$$

implies

$$f(x)G(x) = g(x)F(x),$$

we must have

$$(3x^2 - 5x + 2)(B_2x^2 + B_1x + B_0) - (x^3 - 2x^2 + 2x - 1)(-A_1x - A_0) = 0.$$

Comparing the coefficients gives a system of linear equations in 3+2 variables: B_2, B_1, B_0, A_1, A_0 as follows

$$\begin{array}{rcrcrcrcrcl}
 & 3B_2 & & & & + & A_1 & & & = 0 \\
- & 5B_2 & + & 3B_1 & & - & 2A_1 & + & A_0 & = 0 \\
 & 2B_2 & - & 5B_1 & + 3B_0 & + & 2A_1 & - & 2A_0 & = 0 \\
 & & & 2B_1 & - 5B_0 & - & A_1 & + & 2A_0 & = 0 \\
 & & & & 2B_0 & & & - & A_0 & = 0.
\end{array}$$

In order for the system (2.2) to have a common solution, the corresponding linear system must have a non-trivial solution. This happens if and only if the relevant coefficient matrix is non-invertible; that is its determinant equals to zero:

$$\begin{vmatrix}
3 & 0 & 0 & 1 & 0 \\
-5 & 3 & 0 & -2 & 1 \\
2 & -5 & 3 & 2 & -2 \\
0 & 2 & -5 & -1 & 2 \\
0 & 0 & 2 & 0 & -1
\end{vmatrix} = 0.$$

This means the determinant of its transpose matrix does also equal to zero,

$$\begin{vmatrix} 3 & -5 & 2 & 0 & 0 \\ 0 & 3 & -5 & 2 & 0 \\ 0 & 0 & 3 & -5 & 2 \\ 1 & -2 & 2 & -1 & 0 \\ 0 & 1 & -2 & 2 & -1 \end{vmatrix} = 0.$$

This idea leads to the definition of the *resultant* in a polynomial ring.

Definition 2.3.1. Given any pair of polynomials in one variable:

$$f(x) = \sum_{k=0}^{n} a_k x^k \qquad \text{and} \qquad g(x) = \sum_{k=0}^{m} b_k x^k,$$

where a_i, b_j are elements in a field k, the *(Sylvester) resultant* of f and g, denoted by $R(f, g)$, is defined as the determinant

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & \cdots & a_1 & a_0 & & & \\ & a_n & \cdots & a_2 & a_1 & a_0 & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & & & \\ & b_m & \cdots & b_2 & b_1 & b_0 & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & b_m & b_{m-1} & \cdots & b_1 & b_0 \end{vmatrix}.$$

where the blank spaces are equal to zeros.

Theorem 2.3.2. *Given $f(x)$ and $g(x)$ as above, then the system*

$$\begin{aligned} f(x) &= 0 \\ g(x) &= 0 \end{aligned}$$

has a common solution if and only if $R(f,g) = 0$.

Proof. See Proposition 8, Ch.3, [7]. □

For a polynomial system in two variables, we can regard it as a system of polynomials in one variable whose coefficients are the polynomials in another variable. For example:

Example 2.3.3. Let

$$\begin{aligned} f(x,y) &= xy^2 - xy - x - 1, \\ g(x,y) &= x^2 + xy. \end{aligned}$$

Rearranging them to be polynomials in x with coefficients as polynomials in y, we get

$$\begin{aligned} f(x,y) &= (y^2 - y - 1)x - 1, \\ g(x,y) &= x^2 + xy, \end{aligned}$$

then the *resultant of* f *and* g *with respect to* x, denoted by $R_x(f,g)$, is

$$R_x(f,g) = \begin{vmatrix} y^2 - y - 1 & -1 & 0 \\ 0 & y^2 - y - 1 & -1 \\ 1 & y & 0 \end{vmatrix} = y^3 - y^2 - y + 1 = (y+1)(y-1)^2.$$

On the other hand, if we consider $f(x,y)$ and $g(x,y)$ as polynomials in y with coefficients as polynomials in x, then the *resultant of* f *and* g *with*

respect to y is

$$R_y(f,g) = \begin{vmatrix} x & -x & -x-1 \\ x^2 & x & 0 \\ 0 & x^2 & x \end{vmatrix} = x^5 - x^3 = x^3(x^2-1).$$

Moreover, the resultant can be expressed as a product of the zeros of f and g.

Theorem 2.3.4. *Given*

$$f(x) = a_n \prod_{i=1}^{n} (x - x_i) \qquad \textit{and} \qquad g(x) = b_m \prod_{j=1}^{m} (x - y_j),$$

then

$$R(f,g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j).$$

The proof can be found in [33]. From this, it is obvious that $R(f,g) = 0$ if and only if $f(x)$ and $g(x)$ have a common solution. The elementary properties of the resultant follows from Theorem 2.3.4 above.

Proposition 2.3.5. *With $f(x)$ and $g(x)$ as defined in 2.3.4,*

(i) $R(f,g) = (-1)^{mn} R(g,f)$ *(the symmetry property),*

(ii) $R(f,gh) = R(f,g)R(f,h)$ *(the multiplicative property).*

Theorem 2.3.6. *For any pair of polynomials $f(x)$ and $g(x)$ of degrees m and n, respectively, there exist polynomials $p, q \in k[x]$ of degrees $m-1$ and $n-1$, respectively, whose coefficients are integer polynomials in the coefficients of f and g, such that*

$$R(f,g) = pf + qg.$$

Proof. See Proposition 9, Ch.3, [7] □

Theorem 2.3.6 assures us that the greatest common divisor of f and g must divide their resultant. We will use this fact several times in the proof of our results.

2.3.2 Newton polygons of polynomials

In this part we will explore a tool that helps us to extract information about the roots of a given polynomial. The construction of such tool requires the fundamental concepts of p-adic fields.

Fix a prime number p. For each $x \in \mathbb{Q} \setminus \{0\}$, write

$$x = p^n \frac{a}{b}, \qquad \text{with } \gcd(ab, p) = 1.$$

Define the *p-adic valuation of* x to be $v_p(x) = n$. For convenience, set $v_p(0) = +\infty$ (as 0 can be divisible by any power of p). Then for all $x, y \in \mathbb{Q}$, the valuation satisfies

$$v_p(xy) = v_p(x) + v_p(y), \text{ and } v_p(x+y) \geq \min\{v_p(x), v_p(y)\}.$$

We then define the *p-adic absolute value of* $x \in \mathbb{Q}$ to be

$$|x|_p = p^{-v_p(x)} \quad \text{with } |0|_p = 0.$$

Then $|\cdot|_p$ satisfies

(i) $|x|_p = 0$ iff $x = 0$,

(ii) $|xy|_p = |x|_p|y|_p$ for all $x, y \in \mathbb{Q}$,

(iii) $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ for all $x, y \in \mathbb{Q}$.

That is, $|\cdot|_p$ is a non-archimedean absolute value on $\mathbb{Q}$. Moreover,

(iv) $|1|_p = 1$,

(v) $|-x|_p = |x|_p$,

(vi) if $|x^n|_p = 1$, then $|x|_p = 1$ for all $x \in \mathbb{Q}$.

Notice that when x is divisible by a very large power of p, the valuation $v_p(x)$ is also large, and then the absolute value $|x|_p$ is small. So the p-adic absolute value indicates how large a power of p divides x.

Definition 2.3.7. A sequence (x_n) in a field k is called a *Cauchy sequence* if for all $\epsilon > 0$, there is N such that for all $m, n > N, |x_m - x_n| < \epsilon$.
A sequence (x_n) *converges* to $x \in k$ if for all $\epsilon > 0$, there is N such that for all $n > N, |x_x - x| < \epsilon$.

We note that every convergent sequence is a Cauchy sequence. The converse may not true in general. Any field k with the absolute value $|\cdot|$ is said to be *complete with respect to* $|\cdot|$ if every Cauchy sequence of elements in k is convergent.

Definition 2.3.8. A field K with $\|\cdot\|$ is the *completion of* k, $|\cdot|$ if

(i) there is an inclusion $\pi : k \to K$ respecting the absolute values,

(ii) the image $\pi(k)$ is dense in K,

i.e. for all $x \in K$, and $\epsilon > 0, B(x, \epsilon) \cap \pi(k) \neq \emptyset$,

(iii) $K, \|\cdot\|$ is complete.

For an example, $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the ordinary absolute value. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value is called $\mathbb{Q}_p$, and the p-adic absolute value $|\cdot|_p$ extends to $\mathbb{Q}_p$.

Definition 2.3.9. Any field k is called *algebraically closed* if every polynomial with coefficients in k has a root in k.

$\mathbb{Q}_p$ is not algebraically closed since $x^2 - p$ has no root in $\mathbb{Q}_p$, whereas $\mathbb{C}$ is algebraically closed.

Definition 2.3.10. An *extension* L of a field k is a field L containing k.

An extension L can be considered as a vector space over k. The *degree* of the extension is the dimension of L over k. If L is an extension of k, then an element $\alpha \in L$ is called *algebraic over* k if it is a root of a nonzero polynomial with coefficients in k. L is called an *algebraic extension over* k if every element in L is algebraic over k.

Definition 2.3.11. An extension $\bar{k}$ is called the *algebraic closure* of k if $\bar{k}$ is algebraically closed and every $\alpha \in \bar{k}$ is algebraic over k.

$\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ of degree 2, while $\bar{\mathbb{Q}}_p$ is the algebraic closure of $\mathbb{Q}_p$ of infinite degree.

Notice that $\bar{\mathbb{Q}}_p$ is not complete. The completion of $\bar{\mathbb{Q}}_p$ is called $\mathbb{C}_p$, which is complete respecting to the p-adic absolute value. Proposition 5.7.8 of [13] asserts that $\mathbb{C}_p$ is algebraically closed.

Now we are in position to define the Newton polygon, the tool that we mentioned above, for polynomials over $\mathbb{C}_p$. Let

$$f(X) = a_0 + a_1 X + ... + a_n X^n$$

with $a_0 \neq 0$ and $a_n \neq 0$. Consider the points in $\mathbb{R}^2$

$$(0, v_p(a_0)), (1, v_p(a_1)), (2, v_p(a_2)), ..., (n, v_p(a_n)),$$

where we omit the points with $a_i = 0$. We call these points the *Newton points*. The *Newton polygon* of $f(X)$ is the lower boundary of the convex hull

of the set of the Newton points in $\mathbb{R}^2$ by rotating a vertical line through the point $(0, v_p(a_0))$ counter-clockwise until it meets one of the point $(i, v_p(a_i))$ and then continue rotating the remaining part of that line until it reaches the point $(n, v_p(a_n))$ eventually. A vertex of the Newton polygon is a point where the slope changes. The slope of the segment joining the vertices $(i, v_p(a_i))$ and $(j, v_p(a_j))$ is $\dfrac{v_p(a_j) - v_p(a_i)}{j - i}$, and the length of the slope is $j - i$.

Example 2.3.12. Let $F(X) = 1 + 9X + \frac{1}{27}X^2 + \frac{1}{9}X^4 + 81X^5 + 9x^6$ and $p = 3$. Then the Newton points are

$$(0,0), (1,2), (2,-3), (4,-2), (5,4), (6,2).$$

The Newton polygon of $F(X)$ with $p = 3$ is

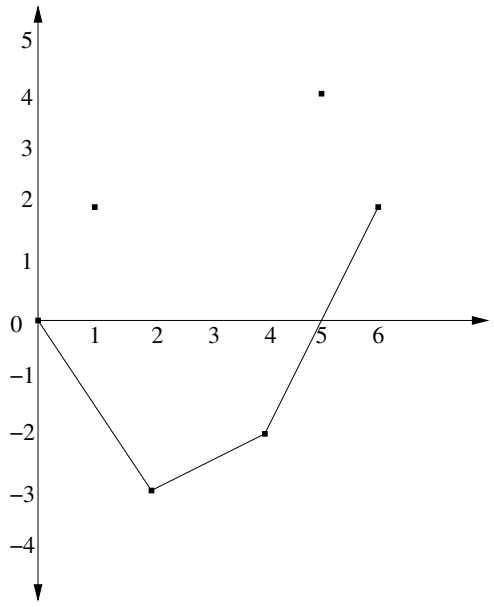

Figure 2.1: Newton Polygon of $F(X)$

It is natural to ask how the Newton polygon gives information about the roots of $f(X)$. The answer can be found in the following Theorem (see

Theorem 6.4.7 [13], for the proof).

Theorem 2.3.13. *Suppose $m_1, m_2, ..., m_r$ are the slopes of the segments of the Newton polygon with $m_1 \leq m_2 \leq \cdots \leq m_r$, and $l_1, l_2, ..., l_r$ are the corresponding lengths. Then, for each $1 \leq i \leq r$, $f(X)$ has exactly l_i roots in $\mathbb{C}_p$ (counting multiplicities) of absolute value p^{m_i}.*

Example 2.3.14. The slopes of all segments of the Newton polygon in Figure 2.3.12 are $-\frac{3}{2}, \frac{1}{2}$ and 2, respectively. It can be concluded from Theorem 2.3.13 that there are 2 roots in $\mathbb{C}_p$ of absolute value $3^{-\frac{3}{2}}$, 2 roots of absolute value $3^{\frac{1}{2}}$, and 2 roots of absolute value 3^2.

Chapter 3

Curves

As elliptic curves are also geometric objects, this chapter is devoted to give a short introduction to geometric background which are used to define elliptic curves in Chapter 4.

Throughout this chapter, k will denote an arbitrary field, k^* the set of non-zero elements of k, and $\bar{k}$ is a fixed algebraic closure of k.

3.1 Varieties

3.1.1 Affine varieties

Definition 3.1.1. *Affine n-space (over k)*, denoted by $\mathbb{A}^n(k)$, is the set of n-tuples of elements in k when n is any positive integer; that is

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

In particular, if we consider affine n-space over $\bar{k}$, then we define the set of *k-rational points* of $\mathbb{A}^n(\bar{k})$ as

$$\{(x_1, ..., x_n) \in \mathbb{A}^n(\bar{k}) : \text{all } x_i \in k\}.$$

Definition 3.1.2. Given $f_1, ..., f_s$ polynomials in $\bar{k}[x_1, ..., x_n]$, an *(affine) algebraic set defined by* $f_1, ..., f_s$, written $V(f_1, ..., f_s)$, is the set of all zeros of f_i for every i; that is

$$\{(a_1, ..., a_n) \in \mathbb{A}^n(\bar{k}) : f_i(a_1, ..., a_n) = 0, \text{ for all } 1 \leq i \leq s\}.$$

For any affine algebraic set $V \subset \mathbb{A}^n(\bar{k})$, let

$$I(V) = \{f \in \bar{k}[x_1, ..., x_n] : f(P) = 0 \text{ for all } P \in V\}.$$

Then $I(V)$ is an ideal of $\bar{k}[x_1, ..., x_n]$ (Lemma 6, Ch.1, [7]), and it is called the *ideal of* V.

By the Hilbert Basis Theorem, $I(V)$ is finitely generated. An algebraic set is said to be *defined over* k, denoted by V/k, if $I(V)$ is generated by polynomials in $k[x_1, ..., x_n]$. If V is defined over k, the set of *k-rational points of* V is the set of n-tuples in V whose coordinates are all k-rational points in $\mathbb{A}^n(\bar{k})$.

Now we have the map

$$\begin{aligned} \text{affine algebraic sets} &\longrightarrow \text{ideals} \\ V &\longrightarrow I(V). \end{aligned} \tag{3.1}$$

For any two algebraic sets $V \subset W$, $I(V) \supset I(W)$.

Conversely, given an ideal I of $\bar{k}[x_1, ..., x_n]$, define

$$V(I) = \{(a_1, ..., a_n) \in \mathbb{A}^n(\bar{k}) : f(a_1, ..., a_n) = 0 \text{ for all } f \in I\}.$$

Since I is finitely generated, write $I = \langle f_1, ..., f_s \rangle$. Note that if $f_1, ..., f_s$ and $g_1, ..., g_r$ are bases of I then $V(f_1, ..., f_s) = V(g_1, ..., g_r)$ (Proposition 4, Ch.1,

[7]). We can see that $V(I) = V(f_1, ..., f_s)$ (Proposition 9, Ch.2, [7]). Then the set $V(I)$ is an algebraic set. We now have another map

$$\begin{array}{ccc} \text{ideals} & \longrightarrow & \text{affine algebraic sets} \\ I & \longrightarrow & V(I) \end{array} \tag{3.2}$$

If $I \subset J$, then $V(I) \supset V(J)$. For any algebraic set V, $V(I(V)) = V$. The maps (3.1) and (3.2) give the relation between the geometric objects (affine algebraic sets) and the algebraic objects (ideals of $\bar{k}[x_1, ..., x_n]$).

Definition 3.1.3. An algebraic set $V \subset \mathbb{A}^n(\bar{k})$ is said to be *irreducible* if whenever $V = V_1 \cup V_2$, where V_1 and V_2 are algebraic sets, then either $V_1 = V$ or $V_2 = V$. An irreducible algebraic set is called an *affine variety*.

For any algebraic set V, V is irreducible if and only if $I(V)$ is a prime ideal (Proposition 3, Ch.4, [7]).

Remark 3.1.4. If $F \in k[x_1, ..., x_n]$ is irreducible over $\bar{k}[x_1, ..., x_n]$, then

$$I = (F) = F[x_1, ..., x_n]\bar{k}[x_1, ..., x_n]$$

is a prime ideal in $\bar{k}[x_1, ..., x_n]$, so

$$V(I) = \{P \in \mathbb{A}^n(\bar{k}) : f(P) = 0 \text{ for all } f \in I = (F)\}$$

is an (affine) variety defined over k. For example, let

$$F(X, Y) = Y^2 - X^3 - X - 1 \in \mathbb{Q}[X, Y].$$

This polynomial is irreducible over $\mathbb{C}[X, Y]$, so $I = (F)$ is a prime ideal in $\mathbb{C}[X, Y]$. Thus $V(I)$ is a variety defined over $\mathbb{Q}$. Such a variety is called an *affine plane variety* as $n = 2$.

Given a nonempty variety $V \subset \mathbb{A}^n(\bar{k})$, then $I(V)$ is a prime ideal in $\bar{k}[x_1, ..., x_n]$, so

$$\bar{k}[V] := \frac{\bar{k}[x_1, ..., x_n]}{I(V)}$$

is an integral domain. We call $\bar{k}[V]$ the *coordinate ring of V*. Let $\bar{k}(V)$ denote the quotient field of $\bar{k}[V]$. It is called the *function field of V*. Any element of $\bar{k}(V)$ is a rational function on V. For $f \in \bar{k}(V)$ and $P \in V$, we say that f is *regular (or defined) at P* if $f = g/h$ for some $g, h \in \bar{k}[V]$ and $h(P) \neq 0$. Denote $\bar{k}[V]_P$ by the set of rational functions on V that are regular at P. We can see that $\bar{k}[V]_P$ forms a subring of $\bar{k}(V)$ containing $\bar{k}[V]$:

$$\bar{k} \subset \bar{k}[V] \subset \bar{k}[V]_P \subset \bar{k}(V).$$

The ring $\bar{k}[V]_P$ is called the *local ring of V at P*.

If K a finitely generated extension of k, the *transcendence degree* of K over k is the smallest integer n such that K is algebraic over $k(x_1, ..., x_n)$ for some $x_1, ..., x_n \in K$, equivalently saying that n is the largest number of elements of K which are algebraically independent over k. The transcendence degree of $\bar{k}(V)$ over $\bar{k}$ is known as the *dimension* of V, written by $\dim(V)$.

3.1.2 Projective varieties

A *projective n-space (over* $\bar{k}$*)*, denoted by $\mathbb{P}^n(\bar{k})$, is defined geometrically to be the set of all lines through the origin in $\mathbb{A}^{n+1}(\bar{k})$. To define the line l through the point $(0, ..., 0)$ in $\mathbb{A}^{n+1}$, it suffices to know only one point of l other than $(0, ..., 0)$. If $(x_0, ..., x_n)$ is such a point then each point $(\lambda x_0, ..., \lambda x_n)$ also lies on l for $\lambda \in \bar{k}^*$. Thus any point $(x_0, ..., x_n) \neq (0, ..., 0)$ determines a unique

such line, namely $\{(\lambda x_0, ..., \lambda x_n) : \lambda \in \bar{k}\}$.

The above gives rise to the definition of $\mathbb{P}^n$ as the set of equivalent classes of points in $\mathbb{A}^{n+1} \setminus (0, ..., 0)$, where the equivalent relation is given by

$$(x_0, ..., x_n) \sim (y_0, ..., y_n)$$

if and only if there exists $\lambda \in \bar{k}^*$ such that $x_i = \lambda y_i$ for all i. The equivalent class is denoted by $[x_0, ..., x_n]$ and $x_0, ..., x_n$ are called the *homogeneous coordinates*. This means the *projective n-space* can be written as

$$\mathbb{P}^n(\bar{k}) = \{[x_0, ..., x_n] : (x_0, ..., x_n) \in \mathbb{A}^{n+1} \setminus (0, ..., 0)\}.$$

Remark 3.1.5. For $0 \leq i \leq n$, let

$$U_i = \{[x_0, ..., x_n] \in \mathbb{P}^n : x_i \neq 0\}$$

be a subset of $\mathbb{P}^n$. Then U_i is isomorphic to affine n-space $\mathbb{A}^n$ by, for example,

$$\psi_i : \mathbb{A}^n \longrightarrow U_i \subset \mathbb{P}^n,$$

$$(a_1, ..., a_n) \longmapsto [a_1, ..., a_{i-1}, 1, a_i, ..., a_n]$$

and whose inverse

$$\psi_i^{-1} : U_i \longrightarrow \mathbb{A}^n$$

is given by

$$[a_0, ..., a_n] \longmapsto \left(\frac{a_0}{a_i}, \frac{a_1}{a_i}, ..., \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, ..., \frac{a_n}{a_i}\right).$$

Note that $\mathbb{P}^n = \bigcup_{i=0}^n U_i$, so we can say that $\mathbb{P}^n$ can be decomposed into a disjoint union of $n + 1$ sets each of which looks like affine n-space.

A polynomial $f \in \bar{k}[X] = \bar{k}[x_0, ..., x_n]$ is *homogeneous of degree d* if

$$f(\lambda x_0, ..., \lambda x_n) = \lambda^d f(x_0, ..., x_n)$$

for all $\lambda \in \bar{k}$. An ideal $I \subset \bar{k}[X]$ is *homogeneous* if it is generated by homogeneous polynomials. For any homogeneous ideal I, suppose $I = \langle f_1, ..., f_s \rangle$, where $f_1, ..., f_s$ are homogeneous. Let

$$V(I) = \{P \in \mathbb{P}^n(\bar{k}) : f(P) = 0 \text{ for all } f \in I\}.$$

A *(projective) algebraic set* is any set of the form $V(I)$ for some a homogeneous ideal I. The *(homogeneous) ideal* of an algebraic set V is the set

$$I(V) = \{f \in \bar{k}[X] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}.$$

If $\bar{k}$ is an infinite field, then $I(V)$ is a homogeneous ideal in $\bar{k}[X]$ (Proposition 4, Ch.8, [7]). A projective algebraic set is called a *projective variety* if its homogeneous ideal $I(V)$ is a prime ideal in $\bar{k}[X]$.

Example 3.1.6. The polynomial $F(X, Y, Z) = Y^2Z - X^3 - XZ^2 - Z^3 \in \mathbb{Q}[X, Y, Z]$ is irreducible over $\mathbb{C}[X, Y, Z]$, so $I = (F)$ is a prime ideal in $\mathbb{C}[X, Y, Z]$. Thus $V(I)$ is a projective plane variety defined over $\mathbb{Q}$.

Let V be a projective variety. The *function field* of V, denoted by $\bar{k}(V)$, can be described as the field of rational functions g/h such that:

(i) g and h are homogeneous polynomials of the same degree,

(ii) $h \notin I(V)$,

(iii) two rational functions g/h and g'/h' are identified if $gh' - g'h \in I(V)$.

For $P \in V$ and $f \in \bar{k}(V)$, we say that f is *regular (or defined) at* P if f can be written as $f = g/h$ with $h(P) \neq 0$. Let

$$\bar{k}[V]_P = \{f \in \bar{k}(V) : f \text{ is regular at } P\}.$$

$\bar{k}[V]_P$ is a subring of $\bar{k}(V)$, and it is called the *local ring of* V *at* P.

3.2 Curves

An *(algebraic) plane curve* is a one-dimensional projective variety corresponding to a homogeneous polynomial equation

$$F(X, Y, Z) = 0.$$

The *degree* of the curve is the maximum degree of each term $X^iY^jZ^k$. For examples

the lines : $aY + bX + cZ = 0$;

the conics : $aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0$

are curves of degrees 1 and 2, respectively.

A point P on a curve C is said to be *singular* if

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Otherwise, P is *non-singular*. A curve C is *non-singular* or *smooth* if there is no singular point on C. For a smooth curve C defined by a homogeneous polynomial F, the *genus* of C is a non-negative integer defined algebraically as

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

So any line and conic have genus 0, while a smooth cubic has genus 1.

3.2.1 Maps between curves

In the statement of first main Theorem, we mentioned the isogeny as a map between elliptic curves. In this section, we give the general definition of maps between any two varieties.

Let $V_1 \subset \mathbb{P}^m$ and $V_2 \subset \mathbb{P}^n$ be projective varieties. A map ϕ from V_1 to V_2 is called a *rational map* if it is of the form

$$\phi = [f_0, ..., f_n] : V_1 \longrightarrow V_2$$
$$\phi(P) \longmapsto [f_0(P), ..., f_n(P)],$$

where $f_0, ..., f_n \in \bar{k}(V_1)$ are defined for every point $P \in V_1 \subset \mathbb{P}^m$.

Given $\phi = [f_0, ..., f_n] : V_1 \to V_2$ a rational map, we say that ϕ is *regular (or defined) at* P if there exists a function $g \in \bar{k}(V_1)$ such that gf_i is regular at P for all i and at least one $(gf_i)(P) \neq 0$. If such a g exists, let

$$\phi(P) = [(gf_0)(P), ..., (gf_n)(P)].$$

A rational map which is regular at every point of V_1 is called a *morphism*. Two varieties V_1 and V_2 are said to be *isomorphic*, written $V_1 \simeq V_2$, if there are morphisms $\phi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are identity maps on V_1 and V_2, respectively.

The following Theorems, proved in Ch.II, [28], culminate with a fundamental important definition of isogenies (see Chapter 4).

Theorem 3.2.1. *Let C_1 and C_2 be curves and $\phi : C_1 \to C_2$ a rational map. For every non-singular point $P \in C_1$, the map ϕ is regular at P. In particular, if C_1 is a smooth curve then ϕ is a morphism.*

Theorem 3.2.2. *Let $\phi : C_1 \to C_2$ be a morphism between curves. Then ϕ can be either constant or surjective.*

Chapter 4

Elliptic curves

This chapter gives the definition of elliptic curves in the first section. In the next three sections, we give an introduction to the additive law on the set of points on elliptic curves, including the definition of division polynomials and elliptic divisibility sequences. The relevant topics that we will use for the proofs in Chapter 5 are in the last five sections.

4.1 Definition

An *elliptic curve* is defined geometrically as a non-singular projective algebraic plane curve of genus 1 together with one specified base point $\mathcal{O}$. Usually, we consider the curve in an affine form. The elliptic curve E is said to be *defined over a field* k, denoted by E/k, if E is defined over k and $\mathcal{O} \in E(k)$. For most of this thesis, we will consider elliptic curves defined over $\mathbb{Q}$. One

can prove that $E/\mathbb{Q}$ is the locus of the points in x-y plane satisfying

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4.1}$$

where a_i, b_i are constants in $\mathbb{Q}$ (see Proposition 3.1(a), Ch.III, [28]). The form (4.1) will be referred to as the *Weierstrass equation of* E.

Example 4.1.1. Consider the cubic equation

$$u^3 + v^3 = 1.$$

Replacing u by $\dfrac{3x}{y}$ and v by $\dfrac{y-9}{y}$, we obtain the Weierstrass equation

$$y^2 - 9y = x^3 - 27.$$

Conversely, every smooth Weierstrass cubic curve as defined above is an elliptic curve defined over $\mathbb{Q}$ with the base point as the point at infinity $\mathcal{O} = [0, 1, 0]$ (see Proposition 3.1(c), [28]).

The equation (4.1) can be transformed further to a simpler form. As $\mathrm{char}(\mathbb{Q}) \neq 2, 3$, completing the square gives

$$(y + \frac{a_1}{2}x + \frac{a_3}{2})^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right),$$

and then replacing y by $\frac{1}{2}(y - a_1x - a_3)$ leads to

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

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

Define, moreover, the quantities as usual (see [28])

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24 b_4, \\ c_6 &= -b_2^3 + 36 b_2 b_4 - 216 b_6, \\ \Delta &= -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6, \\ j &= c_4^3 / \Delta. \end{aligned}$$

Changing (x, y) to $\left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$ yields

$$E : y^2 = x^3 - 27 c_4 x - 54 c_6.$$

The quantity Δ is called the *discriminant* of the Weierstrass equation, and j is called the *j-invariant* of the elliptic curve E. We derive the following.

Proposition 4.1.2. *Every elliptic curve defined over $\mathbb{Q}$ can be written in short Weierstrass form*

$$E : y^2 = x^3 + ax + b, \tag{4.2}$$

with $a, b \in \mathbb{Q}$.

As part of the definition of an elliptic curve, the equation (4.2) has to be non-singular; that is, the cubic polynomial on the right-hand side must have no repeated roots. This will occur if and only if the discriminant of $x^3 + ax + b$, which equals $4a^3 + 27b^2$, is not zero.

Example 4.1.3. Transforming further the Weierstrass equations obtained in Example 4.1.1, we get

$$y^2 = x^3 - \frac{27}{4}$$

by completing the square. Replaced x by $\frac{x}{2^2}$ and y by $\frac{y}{2^3}$, the equation becomes

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

Any two Weierstrass equations of elliptic curves defined over $\mathbb{Q}$ are isomorphic if they differ only by change of variables (fixing the point at infinity) of the form

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

where $u, r, s, t \in \mathbb{Q}, u \neq 0$. Substituting these to equation (4.1), we can see that the change of coordinates preserves the j-invariant, i.e. $j' = j$, while $u^{12}\Delta' = \Delta$. It can be concluded that if two elliptic curves are isomorphic over $\mathbb{Q}$ then they have the same j-invariant. The converse may not true in general. It will hold if the change of variables is defined over an algebraically closed field (see Proposition 3.7, Ch.III, [18]).

For an elliptic curve in short Weierstrass equation (4.2), the discriminant and the j-invariant are

$$\Delta = -16(4a^3 + 27b), \text{ and } j = -1728(4a)^3/\Delta.$$

The only change of variables preserving this form is

$$x = u^2 x', \text{ and } y = u^3 y',$$

with $u \in \mathbb{Q} \setminus \{0\}$.

Although the discriminant is not an invariant of an elliptic curve E, we will define following a related quantity which is invariant in the isomorphism class (over $\mathbb{Q}$).

Definition 4.1.4. A Weierstrass form of an elliptic curve defined over $\mathbb{Q}$,

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

is said to be *minimal* if $a_i \in \mathbb{Z}$ for all $1 \leq i \leq 6$, and $|\Delta| \in \mathbb{N}$ is minimal among all Weierstrass equations in the isomorphism class, respecting to the change of variables over $\mathbb{Q}$. Such Δ is called the *minimal discriminant*, which is invariant under the change of variables.

A Weierstrass form is *minimal at a prime* p if $v_p(a_i) \geq 0$ for all i, and $v_p(\Delta)$ is minimal among all such forms in the $\mathbb{Q}-$isomorphism class. It can be said that the Weierstrass form is minimal if it is minimal at all primes.

4.2 The group law

Given an elliptic curve E in short Weierstrass form (4.2), a point (x, y) on E is called a *rational point* if both coordinates are rational numbers. Let $E(\mathbb{Q})$ denote the set of all rational points on E together with the point at infinity $\mathcal{O}$.

We will now define an operation on the set $E(\mathbb{Q})$. Given $P, Q \in E(\mathbb{Q})$, the line joining P and Q (if $P = Q$, consider the tangent line at P) has to meet the curve at a third point of intersection, say R, on E, by Bezout's Theorem (see e.g. Theorem 10, §7, [7]). Define $P + Q$ to be the point obtained by reflecting the point R in the x-axis. The inverse of a point P, written $-P$, is its reflection in the x-axis. This addition law gives the following properties (see Proposition 2.2, Ch.III, [28] for the proof):

(i) If the points of intersection of E and a line L are P, Q, R (not necessarily distinct), then

$$(P+Q)+R=\mathcal{O}.$$

Given points P, Q, R on E; then

(ii) $P+\mathcal{O}=P$; that is $\mathcal{O}$ is the identity of this addition.

(iii) $P+(-P)=\mathcal{O}$.

(iii) (commutative law) $P+Q=Q+P$.

(iv) (associative law) $(P+Q)+R=P+(Q+R)$.

More explicitly, let $P=(x_1,y_1)$, and $Q=(x_2,y_2)$ be rational points on E. Then the formulas for $P+Q=(x_3,y_3)$ are given below.

If $x_1 \neq x_2$, then

$$P+Q=\left(\alpha^2-x_1-x_2,\ \alpha(x_1-x_3)-y_1\right),$$

where $\alpha=\dfrac{y_2-y_1}{x_2-x_1}$.

If $x_1=x_2$ and $y_1=y_2$, then

$$2P=P+P=\left(\alpha^2-2x_1,\ \alpha(x_1-x_3)-y_1\right),$$

where $\alpha=\dfrac{3x_1^2+a}{2y_1}$.

If $x_1=x_2$ and $y_1=-y_2$, then $Q=-P$ and $P+Q$ is the point at infinity.

With the addition law above, the structure of the set $E(\mathbb{Q})$ is known.

Theorem 4.2.1. (Mordell-Weil Theorem, [22]) *Let E denote an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group with respect to the geometric addition law above.*

Arithmetic properties of elliptic curves begin with two classical results. Siegel's Theorem (Theorem 2.1.1) says that the set of integral points on an elliptic curve is finite, and the Mordell-Weil Theorem tells more that the

group of rational points on an elliptic curve is finitely generated.

For any $n \in \mathbb{Z}$, the addition formulas above can generate the multiples of a rational point P on E by setting

$$\begin{aligned} nP &= \underbrace{P + ... + P}_{n \ terms} \text{ for } n > 0, \\ 0P &= \mathcal{O}, \\ nP &= (-n)(-P) \text{ for } n < 0. \end{aligned}$$

We say that P is a *torsion point* if there exists $n \in \mathbb{N}$ such that $nP = \mathcal{O}$, and the *order* of a torsion point is the smallest n such that $nP = \mathcal{O}$; otherwise if there are no such n, P is called a *non-torsion point.* The *n-torsion subgroup of E*, denoted by $E[n]$, $n \neq 0$, is the set of points of order dividing n in E,

$$E[n] = \{P \in E : nP = \mathcal{O}\}.$$

The *torsion subgroup of E*, written E_{tors}, is the set of all points of finite order; that is

$$E_{\text{tors}} = \bigcup_{n=1}^{\infty} E[n].$$

Denote by $E_{\text{tors}}(\mathbb{Q})$ the set of torsion points in $E(\mathbb{Q})$.

A consequence of the Mordell-Weil Theorem is that the abelian group $E(\mathbb{Q})$ of an elliptic curve $E/\mathbb{Q}$ can be written as

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

where the number r is a non-negative integer, called the *rank* of the elliptic curve.

4.2.1 Division polynomials

The multiplication of P by an integer can be described by rational functions as follows. Given E an elliptic curve defined over $\mathbb{Q}$ in short Weierstrass form,

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

with $a, b \in \mathbb{Q}$, suppose $P = (x, y) \in E(\mathbb{Q})$ is a non-torsion point. Then

$$nP = \left(\frac{\phi_n(x,y)}{\psi_n^2(x,y)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)} \right).$$

We call ψ_n the *division polynomials* associated to E and P. The division polynomials satisfy the following identities

$$\begin{aligned} \phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \\ 4y\omega_n &= \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2, \end{aligned}$$

and satisfy the following recursion

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2. \tag{4.3}$$

The division polynomials can be calculated inductively as in [28] by the following recursions:

$$
\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1, \\
\psi_2 &= 2y, \\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2, \\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3), \\
\psi_{2k+1} &= \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3, \text{ for } k \geq 2, \\
\psi_{2k}\psi_2 &= \psi_k(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2), \text{ for } k \geq 3 \\
\psi_{-k} &= -\psi_k, \text{ for } k < 0.
\end{aligned}
$$

Then ψ_n (respectively, $y\psi_n$) is a polynomial in $\mathbb{Z}[a, b, x, y^2]$ when n is odd (respectively, n is even). Replacing y^2 by $x^3 + ax + b$, we may regard them as polynomials in $\mathbb{Z}[a, b, x]$, as is ψ_n^2. It can be easily proved by induction that

$$
\begin{aligned}
\psi_n^2 &= n^2 x^{n^2-1} + \text{lower order terms}, \\
\phi_n &= x^{n^2} + \text{lower order terms}.
\end{aligned}
$$

Remark 4.2.2. If we restrict our attention to an elliptic curve of the form

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

then it can be proved by a straightforward induction that the resultant between ϕ_n and ψ_n^2 can be written in the form

$$R(\phi_n, \psi_n^2) = (432B)^d,$$

where $d = \frac{1}{6}n^2(n^2 - 1)$. Furthermore, $\psi_n,\ y^{-1}\psi_n,\ x^{-1}\psi_n$, and $(xy)^{-1}\psi_n$ are binary forms in x^3 and B (over $\mathbb{Z}$) of degrees $\frac{n^2-1}{6}$, $\frac{n^2-4}{6}$, $\frac{n^2-3}{6}$, and $\frac{n^2-6}{6}$ when $3 \nmid n$ odd, $3 \nmid n$ even, $3 \mid n$ odd, and $3 \mid n$ even, respectively.

4.3 Elliptic divisibility sequences

In this section, we give the definition of an elliptic divisibility sequence in two ways, and indicate the connection between each type of elliptic divisibility sequences and the division polynomials ψ_n.

4.3.1 EDS - from elliptic curves

The first one comes from the defining equation of an elliptic curve. Given an elliptic curve E in short Weierstrass form,

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

with $a, b \in \mathbb{Z}$, let $P \in E(\mathbb{Q})$ be non-torsion. The shape of the equation forces the expression of the point P to be in the form

$$P = \left(\frac{A}{B^2}, \frac{C}{B^3} \right),$$

where $A, B, C \in \mathbb{Z}$ such that $\gcd(AC, B) = 1$, and without loss of generality, we may take $B > 0$. For any $n \in \mathbb{N}$, write

$$nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3} \right),$$

in lowest terms. Lemma 3.12 of [17] proved the following property of the sequence (B_n).

Theorem 4.3.1. *If p is a prime divisor of B_n, then*

$$ord_p(B_{nk}) = ord_p(B_n) + ord_p(k).$$

A direct consequence of this Theorem is that $B_m \mid B_n$ whenever $m \mid n$. This means (B_n) is a divisibility sequence. It is natural to call it an *elliptic divisibility sequence*, abbreviated *EDS*, as it is derived from an elliptic curve. Indeed, (B_n) satisfies the strong divisibility property,

$$\gcd(B_m, B_m) = B_{\gcd(m,n)}.$$

Returning to the division polynomials in section 4.2.1, we now have

$$\frac{A_n}{B_n^2} = X(nP) = \frac{\phi_n(P)}{\psi_n^2(P)}.$$

In general, $|\psi_n(P)|$ may not be equal to B_n, as $\gcd(\phi_n(P), \psi_n^2(P))$ may not be equal to 1, but it always true that $B_n \mid |\psi_n(P)|$. However, the extent of the cancellation can be controlled by Lemma 3 of [15] as follows:

Lemma 4.3.2. *Let $E/\mathbb{Q}$ be an elliptic curve and $P \in E(\mathbb{Q})$ be a non-torsion point. Let $\psi_n(P)$, and B_n be as defined above. Then for $n \geq 1$,*

$$\log B_n \leq \log |\psi_n(P)| \leq \log B_n + n^2 M^2 \log |\Delta(E)|,$$

where $M = M(P)$ is the quantity as defined on page 6.

4.3.2 EDS - from Morgan Ward's definition

In fact, the term elliptic divisibility sequence was initially used by Morgan Ward (see [34]). In his sense, an integer sequence $(h_n)_{n\geq 0}$ is an elliptic divisibility sequence if it satisfies the recurrence relation

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \tag{4.4}$$

for all $m \geq n \geq 1$. We will call this sequence a *Ward-type elliptic divisibility sequence, or Ward-type EDS*, when we refer to it. The recurrence relation (4.4) gives rise to two relations. Taking $m = n + 1$ in (4.4) gives the first relation, while taking $m = n + 2$ and then replacing n by $n - 1$ gives the second one,

$$h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3 \tag{4.5}$$

and

$$h_{2n}h_n = h_{n+2}h_nh_{n-1}^3 - h_nh_{n-2}h_{n+1}^2. \tag{4.6}$$

According to Ward's paper, a solution $h = (h_n)$ of (4.4) is said to be *proper* if $h_0 = 0, h_1 = 1$, and $h_2h_3 \neq 0$. Theorem 4.1 of [34] says that a proper solution will be a Ward-type EDS if and only if h_2, h_3 and h_4 are all integral with $h_2 \mid h_4$ and the relations (4.5) and (4.6) are satisfied for all n. Thus we can compute all other terms in the sequence (h_n) from the initial values $h_0, ..., h_4$, making the sequence uniquely determined by these 5 values.

There is a close connection between Ward-type EDS and the division polynomials ψ_n. From the definition of the division polynomials, ψ_n is a Ward-type EDS. Conversely, Ward also proved in [34] that if (h_n) is a given Ward-type EDS, then there is an elliptic curve $E/\mathbb{Q} : y^2 = x^3 + ax + b$ and a non-torsion point $P \in E(\mathbb{Q})$ such that

$$\psi_n(P) = h_n,$$

where ψ_n is the division polynomial associated to E and P.

In the next five secttions, we will explain the relavant topics that will be used in some parts of the proof of our results in Chapter 5.

4.4 Reduction modulo p

This topic will be used in the proof of Theorem 5.2.18, page 95.

Given a prime p and a rational number x, write

$$x = p^n \frac{a}{b}, \text{ where } \gcd(ab, p) = 1 \text{ and } n \geq 0,$$

define

$$r_p(x) = \begin{cases} ab^{-1} \pmod{p} & \text{if } n = 0, \\ 0 & \text{if } n > 0. \end{cases}$$

Then $r_p(x) \in \mathbb{F}_p$. This map gives a ring homomorphism

$$\{x \in \mathbb{Z} : |x|_p \leq 1\} \longrightarrow \mathbb{F}_p.$$

Extending this concept to an elliptic curve defined over $\mathbb{Q}$, we may change variables by $(x, y) \to (x/u^2, y/u^3)$ so that all coefficients of E are integers, and the terms y^2 and x^3 have coefficient 1. We pass from E to a curve $\bar{E}$ by reducing the coefficients of E modulo p. That is

$$\bar{E} : y^2 + r_p(a_1)xy + r_p(a_3)y = x^3 + r_p(a_2)x^2 + r_p(a_4)x + r_p(a_6)$$

when E is in the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. This induces a reduction map

$$E(\mathbb{Q}) \longrightarrow \bar{E}(\mathbb{F}_p),$$

which is a group homomorphism. We call $\bar{E}$ the *reduction of E modulo p*. The curve $\bar{E}$ may possibly be singular. Denote by $\bar{E}_{ns}$ the non-singular part of $\bar{E}$, i.e. the set of all non-singular points of $\bar{E}$. $\bar{E}_{ns}$ is isomorphic to an abelian group (see Theorems 2.30 and 2.31, [35]).

Note that if one starts with an elliptic curve E in minimal form, then $\bar{E}$ is unique up to the change of variables as in section 4.1. We say that E has *good reduction modulo p* if $\bar{E}$ is non-singular, i.e. $\bar{E}_{ns} = \bar{E}$, and p is called a *prime of good reduction.* One can see from the formulæ

$$\bar{\Delta} \equiv \Delta \bmod p,$$

where $\bar{\Delta}$ and Δ are the discriminants of $\bar{E}$ and E, respectively, that $\bar{E}$ is non-singular if and only if $p \nmid \Delta$. Otherwise, if $\bar{E}$ is singular, we say E has *bad reduction modulo p*

Example 4.4.1. Consider $E : y^2 = x^3 + 6x^2 - 315x$, which is a minimal curve. Then

$$\begin{aligned} E &\rightarrow \bar{E} : y^2 = x^2(x+1) \bmod 2, \\ E &\rightarrow \bar{E} : y^2 = x^3 \bmod 3, \\ E &\rightarrow \bar{E} : y^2 = x^2(x+1) \bmod 5, \\ E &\rightarrow \bar{E} : y^2 = x^2(x+6) \bmod 7, \end{aligned}$$

so E has bad reduction modulo $2, 3, 5$, and 7, and has good reduction at other primes.

4.5 Isogenies

Here, we give the definition of an isogeny, which is an important ingredient in the statement of the first main Theorem.

Let E and E' be two elliptic curves which are defined over $\mathbb{Q}$. An *isogeny* between E and E' is a non-trivial homomorphism,

$$\phi : E \rightarrow E',$$

defined by rational functions on the coordinates of the points, which takes the zero of E to the zero of E'. The degree of the underlying rational functions that define the isogeny is the *degree* of the isogeny. The curves E and E' are said to be *m-isogenous* if there is an isogeny of degree m between them. One basic example of an isogeny is the multiplication by m, given by $P \mapsto mP$ for $P \in E(\mathbb{Q})$, and the degree is m^2. Note that an isogeny of degree 1 is an isomorphism; that is, a change of variables.

Example 4.5.1. (1) An isogeny of degree 1 (isomorphism) between two elliptic curves

$$E : y^2 + y = x^3 \quad \text{and} \quad E' : y^2 = x^3 + 11664$$

defined by

$$(x, y) \longmapsto (2^2 3^3 x, 2^2 3^3 (2y + 1)).$$

(2) An isogeny of degree 3 between two elliptic curves

$$E : y^2 = x^3 + 16m^2 \quad \text{and} \quad E' : y^2 = x^3 - 432m^2$$

defined by

$$(x, y) \longmapsto (x + \frac{64m^2}{x^2}, \frac{y(y + 12m)(y - 12m)}{(y + 4m)(y - 4m)}).$$

An important property of every isogeny $\phi : E \to E'$ of degree m is that there exists a *dual isogeny*

$$\phi^* : E' \to E$$

such that the composite homomorphisms $\phi\phi^*$ and $\phi^*\phi$ are multiplications by m on E and E' respectively.

4.6 Heights on elliptic curves

In this section, we will introduce the notions of the Weil height and the canonical height, which are an essential in the proof of Theorem 5.1.1, page 56.

Let $\frac{p}{q} \neq 0$ be a rational number with $\gcd(p, q) = 1$. Define

$$H\left(\frac{p}{q}\right) = \max\{|p|, |q|\},$$

and

$$h\left(\frac{p}{q}\right) = \log H\left(\frac{p}{q}\right).$$

The function h is called the *(logarithmic) height function*. For any given constant c, there are only finitely many rational numbers r with $h(r) \leq c$. This concept can be extended to rational points on elliptic curves defined over $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve in short Weierstrass form

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

By a change of variables, we may assume that $a, b \in \mathbb{Z}$. Given $P = (x, y) \in E(\mathbb{Q})$, define

$$h(P) = h(x) \text{ and } h(\mathcal{O}) = 0.$$

The height function on $E(\mathbb{Q})$, usually called the *Weil height*, satisfies the duplication formula

$$h(2P) = 4h(P) + O(1),$$

where the implied constant depends only on E but not on P. However, there exists a function $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ that has better properties. This function is called the *canonical height* defined by

$$\hat{h}(P) = \lim_{N\to\infty} \frac{h([2^N]P)}{4^N}.$$

Theorem 7.12 [12] asserts that the limit on the right-hand side always exists. The canonical height satisfies the following properties, taken from Theorem 7.13, [12], Theorem 9.3, Ch.VIII, [28], and Lemma 3.1, [29]:

(1) $\hat{h}(P) \geq 0$ for all $P \in E(\mathbb{Q})$, with equality iff P has finite order.

(2) Given a constant c, there are only finitely many rational points P with $\hat{h}(P) \leq c$.

(3) $\hat{h}(nP) = n^2\hat{h}(P)$ for all $n \in \mathbb{Z}$ and $P \in E(\mathbb{Q})$.

(4) (parallelogram law)

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

for all $P, Q \in E(\mathbb{Q})$.

(5) Suppose ϕ is an isogeny of degree d. Then for all P,

$$\hat{h}(\phi(P)) = d\hat{h}(P).$$

Silverman (Remark 1.2, [27]) gives an explicit upper and lower bound for the difference between the Weil height and the canonical height.

Theorem 4.6.1. *Given an elliptic curve in short Weierstrass form,*

$$E/\mathbb{Q} : y^2 = x^3 + ax + b,$$

then

$$-\tfrac{1}{6}h(j) - \tfrac{1}{6}h(\Delta) - 2.14 \leq h(Q) - \hat{h}(Q) \leq \tfrac{1}{4}h(j) + \tfrac{1}{6}h(\Delta) + 1.946.$$

where $\Delta = -16(4a^3 + 27b^2)$ *and* $j = -(48)a^3/\Delta$.

Note that Silverman's heights are twice our heights so we have divided his formulæ by 2. For the Mordell curve of the form $E : Y^2 = X^3 - 432m^2$, better lower bounds of the canonical height are presented in [10] and [16].

Definition 4.6.2. The condition (†) is that every prime divisor of m, which is greater than 3, is congruent to 5 modulo 6.

Theorem 4.6.3. (Lemma 4.3, [10]) *Let $P \in E(\mathbb{Q})$ be a non-torsion point. Then*

$$\hat{h}(P) \geq \frac{1}{27}\log m - 0.0562,$$

unless $m \equiv \pm 2$ mod 9 and m does not satisfy (†), in which case

$$\hat{h}(P) \geq \frac{1}{27}\log m - 0.1173.$$

Theorem 4.6.4. (Proposition 1, [16]) *Given $P \in E(\mathbb{Q})\backslash\{\mathcal{O}\}$ with $m > 2$ cube-free,*

$$\hat{h}(P) \geq \begin{cases} \frac{1}{27}\log\frac{m}{2} + \frac{1}{12}\log 3 & \text{if } m \equiv \pm 1, \pm 3, \pm 4 \ (\text{mod } 9), \\ \frac{1}{12}\log\frac{m}{2} + \frac{3}{16}\log 3 & \text{if } m \equiv \pm 2 \ (\text{mod } 9), \text{ and } m \text{ satisfies } (\dagger), \\ \frac{1}{108}\log\frac{m}{2} + \frac{1}{48}\log 3 & \text{if } m \equiv \pm 2 \ (\text{mod } 9), \\ & \text{and } m \text{ does not satisfy } (\dagger), \\ \frac{1}{3}\log\frac{m}{2} - \frac{1}{4}\log 3 & \text{if } m \equiv 0 \ (\text{mod } 9), \text{ and } m \text{ satisfies } (\dagger), \\ \frac{1}{27}\log\frac{m}{2} - \frac{1}{36}\log 3 & \text{if } m \equiv 0 \ (\text{mod } 9), \\ & \text{and } m \text{ does not satisfy } (\dagger), \end{cases} \tag{4.7}$$

Moreover, A consequence of Corollary 2 of [16] also provides the lower bound of the canonical height for integral points on the curve E as follows:

$$\hat{h}(P) \leq \frac{1}{2}\log(X(P)) + \frac{1}{3}\log 3. \tag{4.8}$$

4.7 Elliptic functions

In this section, we will give a definition of an elliptic function over $\mathbb{C}$ and also explore its properties. This topic helps us to prove the non-integrality of the multiples of integral points on the Mordell curve $E : Y^2 = X^3 - 432m^2$ in Theorem 5.2.5, page 71.

Given two complex numbers ω_1, ω_2, which are linearly independent over $\mathbb{R}$, then

$$\Lambda = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}$$

is called a *lattice*, the ω_i are called the *periods* of the lattice, and the region

$$\Pi = \{\alpha_1\omega_1 + \alpha_2\omega_2 : 0 \leq \alpha_i < 1, i = 1, 2\}$$

is called the *fundamental parallelogram* for Λ. We focus on the torus $\mathbb{C}/\Lambda$. A function on $\mathbb{C}/\Lambda$ can be considered as a function on $\mathbb{C}$ such that

$$f(z + u) = f(z)$$

for all $z \in \mathbb{C}$ and $u \in \Lambda$. Equivalently,

$$f(z + \omega_i) = f(z)$$

for all $z \in \mathbb{C}$. Such function is called a *doubly periodic function*. We then define an *elliptic function* to be a meromorphic doubly periodic function.

An important example of elliptic functions is known as the Weierstrass $\wp$-function defined by

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

The following properties of $\wp(z)$ are quoted from Theorem 3.1, Ch.VI, [28].

(1) The sum defining $\wp(z)$ converges absolutely and uniformly on every compact subset of $\mathbb{C} - \Lambda$.

(2) $\wp(z)$ is meromorphic in $\mathbb{C}$ and has a double pole at each $u \in \Lambda$.

(3) $\wp(-z) = \wp(z)$.

(4) $\wp(z+u) = \wp(z)$ for all $u \in \Lambda$.

(5) every doubly periodic function is a rational function of $\wp$ and its derivative $\wp'$.

Given the Weierstrass $\wp$-function for a lattice Λ, then

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

where $G_{2k} = \sum_{\substack{u \in \Lambda \\ u \neq 0}} u^{-2k}$. This series converges absolutely for all $k > 1$. If we let

$$g_2 = 60G_4 \text{ and } g_3 = 140G_6,$$

then the point $(\wp(z), \wp'(z))$ lies on the curve

$$y^2 = 4x^3 - g_2 x - g_3.$$

Proposition 3.6 [28] asserts that the discriminant $\Delta = g_2^3 - 27g_3^2$ is non-zero.

We now conclude from above that a complex torus yields an elliptic curve. It can be said that a torus $\mathbb{C}/\Lambda$ is isomorphic to the complex points on an

elliptic curve. In other words, let Λ be a lattice and $E : y^2 = 4x^3 - g_2x - g_3$; then

$$\begin{aligned} \Phi : \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \\ z + \Lambda &\longmapsto \left(\wp(z), \frac{1}{2}\wp'(z)\right), \text{ for } z \notin \Lambda \\ 0 + \Lambda &\longmapsto \infty, \end{aligned}$$

is a group isomorphism (Proposition 3.6, [28]).

4.8 Elliptic logarithms

To prove Theorem 5.2.5, in section 5.2, we require an upper bound and a lower bound on a linear form in elliptic logarithms (see page 75 for more details). In this section, we just give an introduction to the basic concept of an elliptic logarithm.

From Section 4.7, we have the isomorphism

$$\Phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}).$$

For any $P \in E(\mathbb{Q})$, write $\Phi(P) = u$ for some $u \in \mathbb{C}/\Lambda$. Let

$$\begin{aligned} \Psi : E(\mathbb{C}) &\longrightarrow \mathbb{C} \\ \Psi(P) &= u \end{aligned}$$

be the map inverse to Φ. We call u an *elliptic logarithm of* P. If u is chosen in a fundamental parallelogram of the period lattice of E, it is the *principal value* of the elliptic logarithm of P.

Fix a basis $\{P_1, ..., P_r\}$ for the torsion-free part of $E(\mathbb{Q})$, then we can write

$$P = q_1 P_1 + \cdots + q_r P_r + T$$

for some integers $q_1, ..., q_r$ and a torsion point T. Applying the map Ψ to above yields

$$\Psi(P) \equiv q_1 \Psi(P_1) + \cdots + q_r \Psi(P_r) + \Psi(T) \pmod{\Lambda},$$

so that if $\{\omega_1, \omega_2\}$ is a fixed basis of Λ, then we obtain a linear form in elliptic logarithms $\Psi(P_i)$ as

$$L(P) := \Psi(P) = q_1 \Psi(P_1) + \cdots + q_r \Psi(P_r) + \Psi(T) + n_1\omega_1 + n_2\omega_2,$$

for some integers n_1, and n_2.

Chapter 5

The Results

In this chapter, we will give the proofs of our main Theorems about prime appearance in divisibility sequences derived from an elliptic curve of the form

$$C : U^3 + V^3 = m, \tag{5.1}$$

where m is a nonzero integer.

Remark 5.0.1. The curves

$$C_1 : U^3 + V^3 = m_1 \text{ and } C_2 : U^3 + V^3 = m_2$$

are isomorphic (over $\mathbb{Q}$) if m_1/m_2 is a cube, so from now on, we will assume that $m > 0$ is a cube-free integer. This assumption implies U and V should be coprime and $UV \neq 0$. Furthermore, we can assume that $m > 2$ as the curves $U^3 + V^3 = m$, when $m = 1, 2$, have no points of infinite order.

Given $R \in C(\mathbb{Q})$, write, in lowest terms,

$$nR = \left(\frac{U_n}{W_n}, \frac{V_n}{W_n} \right).$$

The sequence (W_n) is a divisibility sequence. The divisibility property (see [10]) follows using the formal group of an elliptic curve as in Ch.VII of [28]. Moreover, the sequence (W_n) is a source of infinitely many prime numbers in the sense that the term W_n always has a primitive divisor (i.e. a divisor of W_n that is coprime to every nonzero term W_m with $0 \leq m < n$), for all $n > 1$, proved by Everest, Ingram, and Stevens in [10]:

Theorem 5.0.2. (THEOREM 1.1, [10]) *With C and (W_n) defined as above, for all $n > 1$, W_n has a primitive divisor.*

Our principal aim is to study the stronger property of (W_n); that is, we will find a uniform bound on the index n such that W_n is a prime. This indicates that the number of prime terms of (W_n) is finite, so a strong form of the uniform Primality conjecture will be given.

The proofs rely on some results on the elliptic divisibility sequence obtained from the Mordell curve

$$E : Y^2 = X^3 - 432m^2, \tag{5.2}$$

where $P \in E(\mathbb{Q})$ corresponds to $R \in C(\mathbb{Q})$ under the bi-rational transformation given by

$$\begin{aligned} X &= \frac{2^2 3m}{U+V}, \quad Y = \frac{2^2 3^2 m(U-V)}{U+V}, \\ U &= \frac{2^2 3^2 m + Y}{6X}, \quad V = \frac{2^2 3^2 m - Y}{6X}. \end{aligned} \tag{5.3}$$

Consequently, we have

$$\left(\frac{U_n}{W_n}, \frac{V_n}{W_n}\right) = nR = \left(\frac{2^2 3^2 m B_n^3 + C_n}{6A_n B_n}, \frac{2^2 3^2 m B_n^3 - C_n}{6A_n B_n}\right),$$

where $nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right)$ and $\gcd(A_n C_n, B_n) = 1$.

In Section 5.1, we will show that, under some hypothesis on a rational point P, there is an absolute constant N_0 such that $B_n > 2^{\frac{1}{3}} 3^{\frac{1}{2}} m^{\frac{1}{6}}$ for every $n > N_0$. Based on this result, we can bound uniformly the size of the index n such that W_n is not a prime power. The hypothesis as mentioned above is concerned with a 3-isogeny σ between the curve E and the elliptic curve of the form

$$E' : y^2 = x^3 + 16m^2, \tag{5.4}$$

given by

$$X = \sigma(x) = x + \frac{64m^2}{x^2},$$

and

$$Y = \sigma(y) = \frac{y(y + 12m)(y - 12m)}{(y + 4m)(y - 4m)}.$$

Section 5.2 will present the proof of the second main result without the isogeny condition above. To prove this, we will look at the non-integrality of the multiples of P instead, and find a uniform bound N_1 for which $B_n > 1$ when $n > N_1$ with at most one exception. Subsequently, we will get a uniform bound for the size of the second largest n such that W_n is not a prime power.

5.1 Primality Conjecture (with isogeny condition)

Lemma 5.1.1. *Let P and E be as above and suppose P is the image of a rational point on E' under the isogeny σ. Then $B_n > 2^{\frac{1}{3}}3^{\frac{1}{2}}m^{\frac{1}{6}}$ for all $n > 22$.*

Note The condition in the statement of Lemma is not infrequently met. For example, the values $m = 6, 7, 9, 12, 15, 20, 33, 34, 42, 69, 70, 75, 78, 84, 90, 105$ all yield rank-1 curves whose generators satisfy the condition stated. The following table shows a generator of E, say P, which is mapped from a generator of E', say P', under the isogeny σ.

m	P	P'
6	[28,80]	[24, 120]
7	[57,405]	[56,420]
9	[73,595]	[72, 612]
12	[52, 280]	[16, 80]
15	[49, 143]	[40, 260]
20	[84, 648]	[-16, 48]
33	[97, 665]	[88, 836]
34	[273, 4455]	[-16, 120]

m	P	P'
42	[172, 2080]	[168, 2184]
69	[553, 12925]	[552, 12972]
70	[156, 1296]	[140, 1680]
75	[601, 14651]	[600, 14700]
78	[217, 2755]	[208, 3016]
84	[148, 440]	[112, 1232]
90	[364, 6688]	[360, 6840]
105	[169, 253]	[120, 1380]

Proof of Lemma 5.1.1. Let $P \in E(\mathbb{Q})$ such that $\sigma(P') = P$, for some $P' \in E'(\mathbb{Q})$. Write

$$x_n := x(nP') = \frac{a_n}{b_n^2},$$

with $\gcd(a_n, b_n) = 1$; then

$$\frac{A_n}{B_n^2} = X(nP) = x_n + \frac{64m^2}{x_n^2} = \frac{a_n^3 + 64m^2b_n^6}{a_n^2b_n^2}. \tag{5.5}$$

We claim first that $B_n > 2^{\frac{1}{3}}3^{\frac{1}{2}}m^{\frac{1}{6}}$, provided $\max\{|a_n|, b_n^2\} > 2^{\frac{10}{3}}3^{\frac{1}{2}}m^{\frac{7}{6}}$. Consider the fraction on the right-hand side of (5.5), let $d = p^r$ be a common factor of $(a_n^3 + 64m^2b_n^6)$ and $a_n^2b_n^2$, where p is a prime and $r \in \mathbb{N}$ is the highest order of p dividing both terms. Since $\gcd(a_n, b_n) = 1$, either $d \mid a_n^2$ or $d \mid b_n^2$. If the latter occurs, then $d \mid (a_n^3 + 64m^2b_n^6)$ implies $d \mid a_n^3$, which is impossible as a_n and b_n are coprime. Thus d can only come from the term a_n^2, so that $d \mid a_n^3$. We have now that

$$d \mid (a_n^3 + 64m^2b_n^6),\ d \mid a_n^3, \text{ and } d \nmid b_n^6,$$

so $p^r = d \mid 64m^2$. Hence the greatest common divisor of numerator and denominator of the fraction on the right-hand side of (5.5), say g, has to divide $64m^2$ as well. If $|a_n| > 2^{\frac{10}{3}}3^{\frac{1}{2}}m^{\frac{7}{6}}$, then

$$B_n^2 = \frac{a_n^2b_n^2}{g} \geq \frac{a_n^2b_n^2}{64m^2} > 2^{\frac{2}{3}}3^1m^{\frac{1}{3}}.$$

Therefore $B_n > 2^{\frac{1}{3}}3^{\frac{1}{2}}m^{\frac{1}{6}}$. On the other hand, if $b_n^2 > 2^{\frac{10}{3}}3^{\frac{1}{2}}m^{\frac{7}{6}}$, then

$$B_n^2 \geq b_n^2 > 2^{\frac{10}{3}}3^{\frac{1}{2}}m^{\frac{7}{6}}$$

which plainly yields $B_n > 2^{\frac{1}{3}}3^{\frac{1}{2}}m^{\frac{1}{6}}$ with room to spare.

Next recall the difference between the Weil height and the canonical height as in Theorem 4.6.1, stated here again for convenience,

$$-\frac{1}{6}h(j) - \frac{1}{6}h(\Delta) - 2.14 \leq h(Q) - \hat{h}(Q) \leq \frac{1}{4}h(j) + \frac{1}{6}h(\Delta) + 1.946. \quad (5.6)$$

Write $h = \hat{h}(P)$ and $h' = \hat{h}(P')$; then

$$h = \hat{h}(P) = \hat{h}(\sigma(P')) = 3\hat{h}(P') = 3h'$$

as σ is a 3-isogeny and by Property (5) of the canonical heights in Section 4.6. Applying the estimate (5.6) to the curve E' with $\Delta = -16^3 3^3 m^4$, $j = 0$, and $Q = nP'$, we obtain

$$\log \max\left\{|a_n|, b_n^2\right\} = h(nP') > h'n^2 - \frac{2}{3}\log m - \frac{1}{2}\log 48 - 2.14. \qquad (5.7)$$

Moreover, the height bound in Theorem 4.6.3 makes

$$h' = \frac{h}{3} > \frac{1}{81}\log m - 0.039. \qquad (5.8)$$

for all $m \geq 0$. Then (5.7) becomes

$$\log \max\left\{|a_n|, b_n^2\right\} > \left(\frac{1}{81}\log m - 0.039\right) n^2 - \frac{2}{3}\log m - \frac{1}{2}\log 48 - 2.14.$$

We aim to find the necessary condition that makes $|a_n| > 2^{\frac{10}{3}} 3^{\frac{1}{2}} m^{\frac{7}{6}}$ assuming firstly that $|a_n| > b_n^2$. Thus the overall effect require is that

$$\left(\frac{1}{81}\log m - 0.039\right) n^2 - \frac{2}{3}\log m - \frac{1}{2}\log 48 - 2.14 > \log(2^{\frac{10}{3}} 3^{\frac{1}{2}} m^{\frac{7}{6}}). \qquad (5.9)$$

With a manipulation, (5.9) will be guaranteed for $n > 12$, but for all sufficiently large m.

However, we need to verify the statement of Lemma 5.1.1 for all m, even though we have to adjust the bound of n to be greater than 12. With some calculations, we can see from (5.9) that if $m > 353$, then $n > 22$. For the smaller values $m \leq 353$, we will study further all curves that have rank greater than 0, in Appendix A, to obtain the exact bound. Thus it can be concluded that for all m, $B_n > 2^{\frac{1}{3}} 3^{\frac{1}{2}} m^{\frac{1}{6}}$ if $n > 22$.

If $b_n^2 > |a_n|$, we still want to find such condition to force $b_n^2 > 2^{\frac{10}{3}} 3^{\frac{1}{2}} m^{\frac{7}{6}}$ and the resulting argument is the same. □

We are now in a position to prove main Theorem by using the result from Lemma 5.1.1 as a part of the proof.

Theorem 5.1.2. (Main Theorem I) *Let C be an elliptic curve as in (5.1) and $R \in C(\mathbb{Q})$ a non-torsion point. Suppose $P \in E(\mathbb{Q})$ corresponds to R by the bi-rational transformation (5.3). Under the assumption that P is the image of a rational point under σ, W_n is divisible by at least two distinct primes for all $n > 2$.*

Proof. The proof consists of two parts. The first one is a direct consequence of Lemma 5.1.1 which will be used to show that the term W_n possesses at least two coprime factors for all $n > 22$. In the second part, we prove this for every $n \leq 22$ case by case.

From the bi-rational transformation (5.3), we have

$$\frac{U_n}{W_n} = \frac{2^2 3^2 m B_n^3 + C_n}{6 A_n B_n}, \tag{5.10}$$

and also

$$\frac{V_n}{W_n} = \frac{2^2 3^2 m B_n^3 - C_n}{6 A_n B_n}, \tag{5.11}$$

where $nR = \left(\frac{U_n}{W_n}, \frac{V_n}{W_n}\right)$ and $nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right)$ are all written in lowest terms.

Firstly, we consider the fractions on the right-hand side of (5.10). Let $d = p^r$ be a common factor of $(2^2 3^2 m B_n^3 + C_n)$ and $6 A_n B_n$ with p a prime number and $r \in \mathbb{N}$ the highest order of p dividing both terms. If $d' := \gcd(d, B_n) \neq 1$,

then $d' \mid d \mid (2^2 3^2 m B_n^3 + C_n)$ implies $d' \mid C_n$, which contradicts the fact that B_n and C_n are coprime. Thus $\gcd(d, B_n) = 1$, so that d comes from the term $6A_n$. Notice, moreover, that any cancellation of the right-hand side of (5.10) and (5.11) is the same. This is because they have the same denominators, and the left-hand sides of both equations are in lowest terms. Hence d has to divide both $(2^2 3^2 m B_n^3 + C_n)$ and $(2^2 3^2 m B_n^3 - C_n)$, so that $d \mid 72m$. Thus the greatest common divisor of the fraction on the right-hand side of (5.10), say g, also divides $72m$.

As $g \mid 6A_n$ and, especially,

$$G := \frac{g}{\gcd(g, 6)} \mid A_n,$$

we need to ensure $\dfrac{A_n}{G} > 1$ to guarantee that $\dfrac{A_n}{G}$ and B_n both contribute non-trivial coprime factors to W_n. Analyzing all possibilities of $\gcd(g, 6)$, we get the following conclusions.

(i) If $\gcd(g, 6) = 6$, then

$$G = \frac{g}{\gcd(g, 6)} = \frac{g}{6} \mid 12m,$$

so in this case it is enough to prove that $A_n > 12m$ to make $\dfrac{A_n}{G} > 1$.

(ii) If $\gcd(g, 6) = 3$, then $G = \dfrac{g}{3} \mid 24m$, so in this case $A_n > 24m$ is required.

(iii) If $\gcd(g, 6) = 2$, then $G = \dfrac{g}{2} \mid 36m$, so in this case $A_n > 36m$ is required.

(iv) If $\gcd(g, 6) = 1$, then $G = g \mid 72m$, so in this case $A_n > 72m$ is required. Indeed, we need not treat the last case because W_n always contains 6 as a divisor, even though $\dfrac{A_n}{G} = 1$. This means W_n has 2 and 3 as

two coprime factors. Hence we require overall $A_n > 36m$ to make sure that $\frac{A_n}{G} > 1$. Lemma 5.1.1 and the equation

$$C_n^2 = A_n^3 - 2^4 3^3 m^2 B_n^6,$$

imply

$$A_n^3 \ > \ 432m^2B_n^6 \ > \ 2^4 3^3 m^2 (2^{\frac{1}{3}} 3^{\frac{1}{2}} m^{\frac{1}{6}})^6 \ > \ 2^6 3^6 m^3,$$

for all $n > 22$, so that $A_n > 36m$. This means W_n has at least two coprime divisors for all $n > 22$.

Secondly, we will check the terms W_n for each $n \leq 22$ to produce a sharp lower bound on n. Since the sequence (W_n) satisfies the divisibility property, it suffices to consider when n are all primes less than 22 and we group such primes, other than 2 and 3, as $n \equiv 1 \pmod 3$ and $n \equiv 2 \pmod 3$.

Suppose $R = (u, v) \in C(\mathbb{Q})$ is an integral point of infinite order (in the case of rational points, we will see below that the proof can be generalized from the case of integral points).

In **case** $n = 2$, the point $2R$ can be expressed in the form

$$2R = \left(\frac{-2vu^3 - v^4}{u^3 - v^3}, \frac{u^4 + 2v^3u}{u^3 - v^3} \right).$$

Suppose $u - v = 1$. Then

$$u^3 - v^3 = (u - v)(u^2 + uv + v^2) = 3u^2 - 3u + 1.$$

Applying the Bateman-Horn conjecture [2] to the polynomial

$$f(u) := 3u^2 - 3u + 1$$

suggests that $f(u)$ is prime for infinitely many positive integers u. It seems likely that W_2 is not composite. This leads us to study other powers of 2. Consider the case when $n = 4$. Write

$$4R = \left(\frac{U_4}{W_4}, \frac{V_4}{W_4}\right) = \left(\frac{f_4(u,v)}{g_4(u,v)}, \frac{f_4'(u,v)}{g_4(u,v)}\right),$$

where

$$\frac{f_4(u,v)}{g_4(u,v)} = \frac{-u^{16} + 8v^3u^{13} + 32v^6u^{10} + 28v^9u^7 + 10v^{12}u^4 + 4v^{15}u}{-u^{15} - 13v^3u^{12} - 10v^6u^9 + 10v^9u^6 + 13v^{12}u^3 + v^{15}},$$

and

$$\frac{f_4'(u,v)}{g_4(u,v)} = \frac{v^{16} - 8u^3v^{13} - 32u^6v^{10} - 28u^9v^7 - 10u^{12}v^4 - 4u^{15}v}{-u^{15} - 13v^3u^{12} - 10v^6u^9 + 10v^9u^6 + 13v^{12}u^3 + v^{15}}.$$

We may consider the second coordinate, and factorize $g_4(u,v)$ as

$$\begin{aligned}
g_{4,1}(u,v) &:= v - u \\
g_{4,2}(u,v) &:= u^2 + uv + v^2 \equiv (v-u)^2 \pmod 3 \\
g_{4,3}(u,v) &:= u^4 + 2u^3v + 2uv^3 + v^4 \equiv (v-u)^4 \pmod 3 \\
g_{4,4}(u,v) &:= u^8 - 2u^7v + 4u^6v^2 + 4u^5v^3 - 5u^4v^4 + 4u^3v^5 + 4u^2v^6 - 2uv^7 + v^8 \\
&\equiv (v-u)^8 \pmod 3.
\end{aligned}$$

We claim that at least two of these factors can avoid being cancelled by the numerator $f_4'(u,v)$. Choosing to consider $g_{4,3}$ and $g_{4,4}$, we can see that the resultants between them and f_4' with respect to u and v are

$$R_u(f_4', g_{4,3}) = 3^{16}v^{64} \quad \text{and} \quad R_v(f_4', g_{4,3}) = 3^{16}u^{64},$$

respectively, and also

$$R_u(f_4', g_{4,4}) = 3^{32}v^{128} \quad \text{and} \quad R_v(f_4', g_{4,3}) = 3^{32}u^{128}.$$

As u and v are coprime,

$$\gcd(f_4'(u,v), g_{4,3}(u,v)) \mid 3^{16} \quad \text{and} \quad \gcd(f_4'(u,v), g_{4,4}(u,v)) \mid 3^{32}.$$

Next we will show that both $g_{4,3}(u,v)$ and $g_{4,4}(u,v)$ are not equal any power of 3. Suppose, for a contradiction, that $g_{4,3}(u,v) = 3^k$ for some $k > 1$. Then

$$(v-u)^4 \equiv g_{4,3}(u,v) \equiv 0 \pmod 3.$$

Hence $u \equiv v \pmod 3$, so $u^3 \equiv v^3 \pmod{3^2}$. Replacing this in the expression of $g_{4,3}(u,v)$, we get

$$0 \equiv u^4 + 2u^3v + 2u^4 + u^3v \equiv 3u^3(u+v) \pmod{3^2}.$$

Then $3 \mid u$ or $3 \mid (u+v)$. Since $u \equiv v \pmod 3$, the former implies $3 \mid v$, and the latter implies $3 \mid u$ and $3 \mid v$ which are contradictions as $\gcd(u,v) = 1$. Thus the possibilities of $k's$ such that $g_{4,3}(u,v) = 3^k$ are only 0 and 1. Calculating by PARI/GP [31] shows that the only solutions (u,v) of the equation $g_{4,3}(u,v) = 1$ are $(0,\pm 1), (\pm 1, 0)$, contradicting Remark 5.0.1; and there are no solutions to $g_{4,3}(u,v) = 3$.

A similar argument will be applied for the second factor $g_{4,4}(u,v)$. Suppose $g_{4,4}(u,v) = 3^k$ for some $k > 2$. As $(v-u)^8 \equiv g_{4,4}(u,v) \equiv 0 \pmod 3$, we have $u \equiv v \pmod 3$, so that

$$u^3 \equiv v^3 \pmod{3^3},\ 10u^3 \equiv v^3 \pmod{3^3},\ \text{or}\ 19u^3 \equiv v^3 \pmod{3^3}.$$

Replacing each of these in the expression of $g_{4,4}$, we find that there are no solutions to $g_{4,4}(u,v) = 3^k$ when $k > 2$. Thus it remains to solve the equations $g_{4,4}(u,v) = 3^k$ when $0 \le k \le 2$. By computing with GP, the only solutions to $g_{4,4}(u,v) = 1$ are $(0,\pm 1), (\pm 1, 0), (-1,1), (1,-1)$, which is impossible; there are no solutions to $g_{4,4}(u,v) = 3$; and the solutions to $g_{4,4}(u,v) = 9$ are $(-1,-1), (1,1)$ only.

We will prove moreover that the multiple $g_{4,3}(u,v)g_{4,4}(u,v)$ can not be a prime power. As above, $g_{4,3}$ and $g_{4,4}$ are not powers of 3, so write

$$g_{4,3}(u,v) = 3^m p_1^{m_1} \cdots p_r^{m_r} \text{ and } g_{4,4}(u,v) = 3^n q_1^{n_1} \cdots q_s^{n_s},$$

where $p_i's$ and $q_j's$ are primes, other than 3. Considering the resultant between $g_{4,3}$ and $g_{4,4}$, we get $\gcd(g_{4,3}(u,v), g_{4,4}(u,v)) \mid 3^{10}$. Thus there is at least one prime p_i which is not equal to any prime q_j. This implies W_4 is not a prime power.

Case $n = 3$. The expression of $3R$ can be written as

$$3R = \left(\frac{u^9 + 6u^6v^3 + 3u^3v^6 - v^9}{3uv(u^6 + u^3v^3 + v^6)}, \frac{-u^9 + 3u^6v^3 + 6u^3v^6 + v^9}{3uv(u^6 + u^3v^3 + v^6)} \right).$$

For convenience, let

$$f_3(u,v) = -u^9 + 3u^6v^3 + 6u^3v^6 + v^9 \text{ and } g_3(u,v) = u^6 + u^3v^3 + v^6.$$

By the theory of resultants, we obtain

$$\gcd(f_3(u,v), g_3(u,v)) \mid 3^9.$$

To complete the proof in this case, we have to prove that the denominator $g_3(u,v)$ is not a power of 3. Suppose not, that is $g_3(u,v) = 3^k$ for some $k > 1$. Then $(u-v)^6 \equiv g_3(u,v) \equiv 0 \pmod 3$. Thus $u^3 \equiv v^3 \pmod{3^2}$, and hence

$$0 \equiv u^6 + u^3v^3 + v^6 \equiv 3u^6 \pmod{3^2},$$

so $3 \mid u$. This implies $3 \mid v$ which is impossible. For the remaining cases, the only solutions to $g_3(u,v) = 1$ are given by $(u,v) = (0, \pm 1), (\pm 1, 0), (-1, 1), (1, -1)$, and the only solutions to $g_3(u,v) = 3$ are $(-1,-1), (1,1)$. Since $\gcd(u,v) = 1$ and u and v are coprime to both $f_3(u,v)$ and $g_3(u,v)$, W_3 possesses at least two coprime divisors.

Case $n \equiv 1 \pmod 3$. The proof in this case proceeds exactly in the same way as in the case $n = 4$, by the following steps.

(i) Write

$$nR = \left(\frac{U_n}{W_n}, \frac{V_n}{W_n}\right) = \left(\frac{f_n(u,v)}{g_n(u,v)}, \frac{f'_n(u,v)}{g_n(u,v)}\right),$$

and factor the denominator $g_n(u,v)$ as $g_{n,1}(u,v), g_{n,2}(u,v), ..., g_{n,k}(u,v)$, all of which are homogeneous in u and v. By the theory of resultants, we have found fortunately that for each n, $\gcd(f'_n(u,v), g_{n,i}(u,v))$ divides a power of 3 for every $i = 1, ..., k$.

(ii) Pick two factors of g_n, say $g_{n,i}(u,v)$ and $g_{n,j}(u,v)$, which can be proved that both of them can not be any power of 3 by using the following facts:

$$g_{n,i}(u,v) \equiv (u-v)^{\text{degree}(g_{n,i})} \pmod 3,$$
$$g_{n,j}(u,v) \equiv (u-v)^{\text{degree}(g_{n,j})} \pmod 3.$$

(iii) Show that the multiple $g_{n,i}g_{n,j}$ is not a prime power, which is sufficient to prove that the resultant between $g_{n,i}$ and $g_{n,j}$ is a power of 3.

Case $n \equiv 2 \pmod 3$. In this case, the situation is much more complicated. For all n, $f'_n(u,v)$ and $g_n(u,v)$ also behave like previous case in the steps (i) and (iii). However, it is slightly different in step (ii). We need to employ some facts about the Newton polygon on 3-adic fields to know about the 3-adic valuation of $g_{n,i}$. We will show how to do this for $n = 5$ (for other n, the proofs will proceed in the same way). We have

$$g_{5,1}(u,v) = u^8 - 2u^7v - 2u^6v^2 + u^5v^3 - 5u^4v^4 + u^3v^5 - 2u^2v^6 - 2uv^7 + v^8,$$

and

$g_{5,2}(u,v) = u^{16}+2u^{15}v+6u^{14}v^2-2u^{13}v^3+11u^{12}v^4+21u^{11}v^5-11u^{10}v^6-u^9v^7+27u^8v^8-u^7v^9-11u^6v^{10}+21u^5v^{11}+11u^4v^{12}-2u^3v^{13}+6u^2v^{14}+2uv^{15}+v^{16}$.

As $g_{5,i}$ are homogeneous in u and v, we may replace $U := \frac{u}{v}$ in the expressions, and then get corresponding polynomials in terms of U. We will find the Newton polygons for $g_{5,i}(1+X)$ instead, and explore their roots, where

$$g_{5,1}(1+X) = X^8+6X^7+12X^6+3X^5-30X^4-63X^3-63X^2-36X-9,$$

and

$g_{5,2}(1+X) = X^{16}+18X^{15}+156X^{14}+852X^{13}+3261X^{12}+9279X^{11}+20394X^{10}+35496X^9+49617X^8+55971X^7+50814X^6+36774X^5+20871X^4+9072X^3+2916X^2+648X+81$.

The Newton polygons for $g_{5,1}$ and $g_{5,2}$ with $p=3$, as shown in Figure 5.1 and 5.2 below, reveal that the slope of the only segment of each polygon is $-\frac{1}{4}$. By Theorem 2.3.13, all roots of $g_{5,i}(1+X)$ (also for all of $g_{11,i}(1+X)$ and $g_{17,i}(1+X)$) have the 3-adic absolute values $3^{-\frac{1}{4}}$. Hence any root of $g_{5,i}(U)$ is in the form

$$1 + \text{a 3-adic number of absolute value } 3^{-\frac{1}{4}}.$$

If α is a root of $g_{5,i}(U)$, then

$$|U-\alpha|_3 = \max\{|U|_3, |\alpha|_3\} \geq 3^{-\frac{1}{4}},$$

so that

$$|g_{5,i}(U)|_3 = \prod_{\alpha}|U-\alpha|_3 \geq (3^{-\frac{1}{4}})^{\deg(g_{5,i})},$$

where α ranges over all roots of $g_{5,i}(U)$. Thus the 3-adic valuation of $g_{5,i}(U)$ is at most $\frac{\deg(g_{5,i})}{4}$. It remains to solve the equations $g_{5,i}(u,v) = 3^k$ with

$0 \leq k \leq \dfrac{\deg(g_{5,i})}{4}$. We find that the only solutions to $g_{5,1}(u,v) = 3^0$ are $(0, \pm 1), (\pm 1, 0)$, which contradicts the facts from Remark 5.0.1, and no solution to $g_{5,1}(u,v) = 3^k$ for other k. Similarly, the only solutions to $g_{5,2}(u,v) = 1$ are $(0, \pm 1), (\pm 1, 0), (-1, 1), (1, -1)$; the solutions to $g_{5,2}(u,v) = 3^4$ are $(-1, -1), (1, 1)$; and no solution to $g_{5,2}(u,v) = 3^k$ for other k.

That is the proof of Theorem 5.1.2 when we consider only in the case of integral points. In case of rational points, we write $R = \left(\dfrac{u_0}{w_0}, \dfrac{v_0}{w_0}\right) \in C(\mathbb{Q})$ in lowest terms. The condition that m is cube-free implies u_0 ane v_0 are coprime. Replacing u and v in the expressions of nR in previous cases by $\dfrac{u_0}{w_0}$, and $\dfrac{v_0}{w_0}$, respectively, we obtain

$$nR = \left(\frac{f_n(u_0, v_0)}{w_0 g_n(u_0, v_0)}, \frac{f'_n(u_0, v_0)}{w_0 g_n(u_0, v_0)}\right),$$

and then proceed the proof for $f_n(u_0, v_0)$ and $g_n(u_0, v_0)$, so the conclusion follows. □

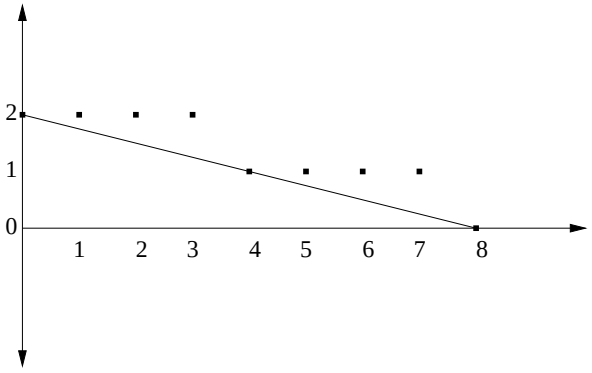

Figure 5.1: Newton polygon of $g_{5,1}(1 + X)$

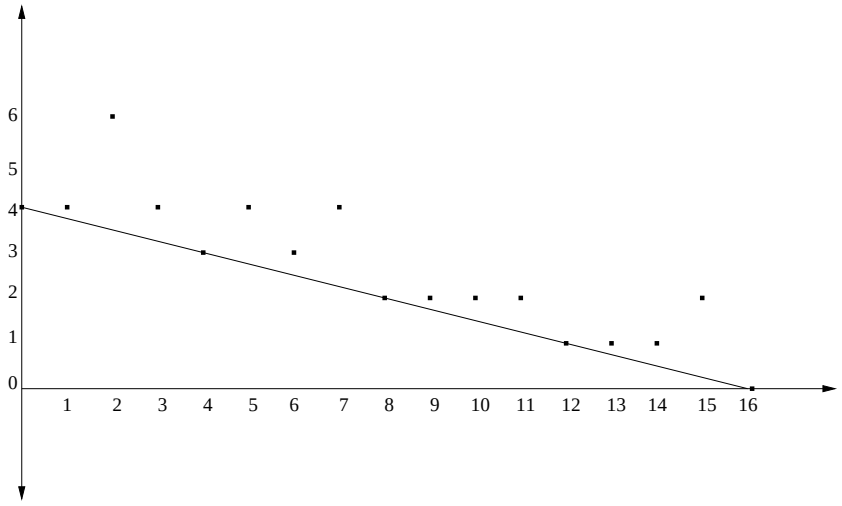

Figure 5.2: Newton polygon of $g_{5,2}(1+X)$

5.2 Primality Conjecture (without isogeny condition)

As we have seen, applying the isogeny condition entails Lemma 5.1.1, and subsequently Theorem 5.1.2. In this section, we will explore the possibilities when this hypothesis is not assumed.

The connections between the curves

$$C : U^3 + V^3 = m \quad \text{and} \quad E_m : Y^2 = X^3 - 432m^2$$

is given via the bi-rational transformation (5.3) and we have

$$\frac{U_n}{W_n} = \frac{2^2 3^2 m B_n^3 + C_n}{6 A_n B_n}.$$

Since any cancellation of the right-hand side comes from $6A_n$ only and $\gcd(A_n, B_n) = 1$, it implies that W_n has at least two coprime factors if we can prove that B_n is always greater than 1, and $6A_n$ can avoid being

cancelled eventually.

In the first part, we aim to prove that $B_n > 1$ for all $n > N_1$, where N_1 is a uniform constant. One application of Ingram's result in [15] is follows:

Proposition 5.2.1. *There exists an absolute constant N_1 (independent of m) such that $B_n > 1$ for all $n > N_1$, except for at most one value of n.*

Proof. From Theorem 1 of [15], with the notations used there, there is an absolute constant C such that $B_n > 1$ for all $n > CM(P)^{16}$, except for at most one value of n, where the quantity $M(P)$ is related to the Tamagawa number. Since the Mordell curve E_m has integral j-invariant, along the same lines as in [15], E_m always has $M(P) \leq 12$. Hence an absolute bound for the indices n such that $B_n > 1$ exists. □

The key point of this section is to make the bound for the indices n such that $B_n > 1$ explicit by following the proof of Theorem 2 of [15], which is a special, but stronger, case of Theorem 1 of [15] for the congruent number curves. Unfortunately, our result may not cover every P and m. Unlike the results of the congruent number curves shown in [15], $2P$ and $3P$ may be integral on our curve E_m, e.g. when $m = 7$ with $P = [84, 756]$, then

$$2P = [28, 28], 3P = [57, -405], \text{and } 4P = [1708, -70588].$$

However, the following Lemma guarantees that for any other prime multipliers $3 < q \leq 13$, qP can not be integral. Note that any multiple of a non-integral point is also non-integral. Thus we will initially focus on an integral point P.

Lemma 5.2.2. *Given an integral point of infinite order $P = (x, y) \in E_m(\mathbb{Q})$ such that gcd$(x, m) = 1$, the points $5P$, $7P$, $11P$, and $13P$ are all non-integral.*

Proof. Write

$$nP = \frac{\phi_n(P)}{\psi_n^2(P)} = \frac{\phi_n(x^3, m^2)}{\psi_n^2(x^3, m^2)}.$$

The idea of the proof is that we will compute the resultants of $\phi_n(x^3, m^2)$ and $\psi_n(x^3, m^2)$, which are of the form $2^A 3^B m^C$ with $A, B, C \in \mathbb{N}$. The condition $\gcd(x, m) = 1$ implies that the common factors of ϕ_n and ψ_n have to divide $2^A 3^B$. Thus our task is to solve the Thue equations

$$\psi_n(x^3, m^2) = \pm 2^a 3^b,$$

where $0 \leq a \leq A$ and $0 \leq b \leq B$. In Appendix B, we will show that the possible values of a and b can be reduced to minimize the number of such equations. Thus we will deal finally with only a small finite number of Thue equations, and then solve them using PARI/GP [31] and MAGMA [20].

For $n = 5$, and 11, we will apply this argument directly, while for $n = 7$, and 13, the general technique is the same, but the details differ slightly. The process to establish all the possible values of a and b as well as all solutions of the equations can be found in Appendix B. □

However, to prove the non-integrality of the multiples of an integral point on E_m, we need the fact that $2P$ and $3P$ are non-integral.

Definition 5.2.3. The condition $(*)$ is that for an integral point $P \in E_m(\mathbb{Q})$,

$$2P, 3P \text{ are non-integral and } \gcd(X(P), 3m) = 1$$

From now on, we will work on this kind of integral point only.

Remark 5.2.4. If nP is integral, then n cannot be divisible by $2, 3, 5, 7, 11$, and 13, by the condition $(*)$ and Lemma 5.2.2; that is $n \geq 17$.

Here is the result on the integrality of the multiples of P:

Theorem 5.2.5. *Let $P \in E_m(\mathbb{Q})$ be an integral point of infinite order such that $gcd(X(P), 3m) = 1$. Suppose $2P$, $3P$ are non-integral. Then there is at most one value of $n > 1$ such that nP is integral, except when either*

$m \equiv \pm 2$ mod 9 and m has a prime factor congruent to 1 mod 6, or

$m \equiv 0$ mod 9 and m has a prime factor congruent to 1 mod 6,

in such cases, the result always holds for all $m >$ 3739071625384.

The proof of Theorem 5.2.5 relies upon the height bounds in Theorem 4.6.4, repeated here again,

$$\hat{h}(P) \geq \begin{cases} \frac{1}{27}\log\frac{m}{2} + \frac{1}{12}\log 3 & \text{if } m \equiv \pm 1, \pm 3, \pm 4 \pmod 9, \\ \frac{1}{12}\log\frac{m}{2} + \frac{3}{16}\log 3 & \text{if } m \equiv \pm 2 \pmod 9, \text{ and } m \text{ satisfies } (\dagger), \\ \frac{1}{108}\log\frac{m}{2} + \frac{1}{48}\log 3 & \text{if } m \equiv \pm 2 \pmod 9, \\ & \text{and } m \text{ does not satisfy } (\dagger), \\ \frac{1}{3}\log\frac{m}{2} - \frac{1}{4}\log 3 & \text{if } m \equiv 0 \pmod 9, \text{ and } m \text{ satisfies } (\dagger), \\ \frac{1}{27}\log\frac{m}{2} - \frac{1}{36}\log 3 & \text{if } m \equiv 0 \pmod 9, \\ & \text{and } m \text{ does not satisfy } (\dagger), \end{cases} \tag{5.12}$$

where the condition $(\dagger)$ as on page 48 means that every prime divisor of m, which is greater than 3, is congruent to 5 modulo 6. We will refer to the cases on the right-hand side of (5.12) as Cases I-V in the sequel. We can

divide the proof into four main steps.

Step 1: *Bounding the indices n such that nP is integral in terms of m*: Suppose nP is integral, $n \geq 2$. Then

$$n \leq \begin{cases} \max\{4.608 \times 10^{28},\ 2.653 \times 10^{24}(\log m)^{\frac{5}{2}}\} \\ \max\{4.608 \times 10^{28},\ 1.769 \times 10^{24}(\log m)^{\frac{5}{2}}\} \\ \max\{1.253 \times 10^{29},\ 5.305 \times 10^{24}(\log m)^{\frac{5}{2}}\} \\ \max\{4.608 \times 10^{28},\ 2.652 \times 10^{24}(\log m)^{\frac{5}{2}}\} \\ \max\{4.608 \times 10^{28},\ 3.535 \times 10^{24}(\log m)^{\frac{5}{2}}\}, \end{cases}$$

for Cases I-V, respectively.

In order to prove these, we need to use David's lower bound, in [8], on linear forms in elliptic logarithms. On the other hand, we will provide an upper bound on the linear forms in elliptic logarithms in Lemma 5.2.10 below. Gathering these two bounds gives us the bounds on n depending only on m, as desired.

Step 2: *Exploring the relationship between two large multipliers of an integral point*: Suppose n_1P and n_2P are integral with $2 \leq n_1 < n_2$. Then

$$\log n_2 \geq \begin{cases} \frac{n_1^2}{27}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} \\ \frac{n_1^2}{12}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} \\ \frac{n_1^2}{108}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} \\ \frac{n_1^2}{27}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} - \frac{1}{3}\log 3 - \frac{3}{2}\log 2 \\ \frac{n_1^2}{48}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} - \frac{1}{3}\log 3 - \frac{3}{2}\log 2, \end{cases}$$

where ω_1 is the real period of E_1.

Step 3: *Finding an explicit upper bound on m.*

In this step, we will combine two steps above and Lemma 5.2.2 by substituting n_1 and n_2 in the estimates from step 2 by

$$n_1 \geq 17, \text{ and}$$
$$n_2 \leq \text{the bounds in step 1.}$$

With some calculations, we obtain

$$\begin{aligned}
&\text{Case I:} && m \leq 628,\\
&\text{Case II:} && m \leq 16,\\
&\text{Case III:} && m \leq 3739071625384,\\
&\text{Case IV:} && m \leq 719,\\
&\text{Case V:} && m \leq 161993.
\end{aligned}$$

Step 4: *Computing all integral points on E_m which satisfy the condition $(*)$ when $m \leq 719$.* We will discuss about this step in Appendix C.

Remark 5.2.6. To explain how these four steps imply the proof of Theorem 5.2, we suppose first that there are at least two multipliers, $n_1, n_2 > 1$, of P such that n_iP is integral (note that we omit the case when there is at most one n such that nP is integral). Step 1 implies that if nP is integral; that is $B_n = 1$, then n can be bounded above by some terms of m. In step 3, we can see that m is bounded above exactly by an absolute constant, say C. This means n is bounded by C as well. The remaining thing to do is to check all integral points on the curves $E_m : Y^2 = X^3 - 432m^2$ when $m \leq C$. In the cases III and IV, the bound of m is too large, so we will omit to work on these cases.

To follow the whole proof easier, we will separate to prove each step in the following subsections.

5.2.1 Proof of Step 1

The proof of step 1 requires firstly an upper bound for the canonical heights of integral points, which follows directly from the next Lemma.

Lemma 5.2.7. *Suppose nP is integral, $n \geq 2$. Then $|X(P)| \leq 6n^2 m^{\frac{2}{3}}$.*

Proof. Postpone to the end of section. □

Suppose nP is integral, for some $n \geq 2$. Combining (4.8) and Lemma 5.2.7 yields

$$\hat{h}(P) \leq \tfrac{1}{2}\log(X(P)) + \tfrac{1}{3}\log 3 \leq \tfrac{1}{2}\log(6n^2 m^{\frac{2}{3}}) + \tfrac{1}{3}\log 3,$$

so that

$$\hat{h}(P) \leq \log n + \frac{1}{3}\log m + \frac{1}{2}\log 2 + \frac{5}{6}\log 3 \tag{5.13}$$

Secondly, the proof of step 1 also requires an upper bound and a lower bound for linear forms in elliptic logarithms. Given an elliptic curve in short Weierstrass form

$$E/\mathbb{Q} : y^2 = f(x),$$

and $Q \in E(\mathbb{Q})$. Let ω be the real period of E. Consider the linear form

$$L_{n,k}(z, \omega) = nz + k\omega,$$

where z is chosen to be the principal value of the elliptic logarithm of Q, and k is chosen to make $L_{n,k}(z, \omega)$ the principal value of nQ. Lemma 10 of [15]

is a special case of Theorem 2.1 of [8], giving us an explicit lower bound on the value of such linear form.

Lemma 5.2.8. (Lemma 10, [15]) *Given an elliptic curve $E/\mathbb{Q}$, let ω and ω' be the real and complex periods of E, chosen such that $\tau = \omega'/\omega$ is in the fundamental region*

$$\left\{z \in \mathbb{C} : |z| \geq 1,\ Im(z) > 0,\ and\ |Re(z)| \leq \tfrac{1}{2}\right\}$$

of the action of $SL_2(\mathbb{Z})$ on the upper half plane. Given a non-torsion integral point P, let z be the principal value of the elliptic logarithm of P, and let k be chosen such that $L_{n,k}(z,\omega) = nz + k\omega$ is the principal value of the elliptic logarithm of nP. Let B, V_1 and V_2 be positive real numbers chosen such that

$$\begin{aligned} \log(V_2) &\geq \max\left\{h(E), \frac{3\pi}{Im(\tau)}\right\}, \\ \log(V_1) &\geq \max\left\{2\hat{h}(P), h(E), \frac{3\pi|z|^2}{|\omega|^2 Im(\tau)}, \log(V_2)\right\}, \end{aligned}$$

and

$$\log(B) \geq \max\{eh(E), \log|n|, \log|k|, \log(V_1)\}.$$

Then either $L_{n,k}(z,\omega) = 0$, or else

$$\log|L_{n,k}(z,\omega)| \geq -C(\log B + 1)(\log\log B + h(E) + 1)^3 \log V_1 \log V_2,$$

where C is taken to be 4×10^{41} and e is approximately 2.718281828.

Note that $L_{n,k}$ is non-vanishing if P is non-torsion.

Here, we will prove that for the Mordell curve E_m, if nP is an integral point, then $L_{n,k}(z,\omega_m)$ is very small. The proof relies upon the estimate from Lemma 8 of [15], which is as follows.

Lemma 5.2.9. *Let $P \in E_m(\mathbb{Q})$ be such that*

$$X(P) \geq 2\max\{|x_T| : T \in E[2] \setminus \{\mathcal{O}\}\}.$$

If z is the principal value of the elliptic logarithm of P, then

$$-\frac{3}{2}\log 2 \leq \log|z| + \frac{1}{2}\log|x_P| \leq \frac{3}{2}\log 2.$$

Lemma 5.2.10. *Suppose nP is integral, $n \geq 2$. Let z be the principal value of the elliptic logarithm of P, and ω_m be the real period of E_m. Choose k such that $L_{n,k} = nz + k\omega_m$ is the principal value of the elliptic logarithm of nP. Then*

$$\log|L_{n,k}(z,\omega_m)| \leq \begin{cases} -\frac{n^2}{27}\log m \\ -\frac{n^2}{12}\log m \\ -\frac{n^2}{108}\log m \\ -\frac{n^2}{27}\log m + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -\frac{n^2}{48}\log m + \frac{3}{2}\log 2 + \frac{1}{3}\log 3. \end{cases} \tag{5.14}$$

Proof. By Lemma 5.2.9, we have that if

$$X_{nP} \geq 2\max\{|x_T| : T \in E[2] \setminus \{\mathcal{O}\}\},$$

then

$$\log|L_{n,k}(z,\omega_m)| \leq \frac{3}{2}\log 2 - \frac{1}{2}\log|X_{nP}|. \tag{5.15}$$

We can see that $2\max\{|x_T| : T \in E[2] \setminus \{\mathcal{O}\}\} < 24m$, so we will show firstly that X_{nP} is greater than $24m$, and then we can employ the estimate (5.15) to prove the bound (5.14).

Suppose $X_{nP} \leq 24m$. Then, from (5.12) and (4.8),

$$\frac{1}{2}\log(24m) + \frac{1}{3}\log 3 > \hat{h}(nP) \geq \begin{cases} n^2\left(\frac{1}{27}\log\frac{m}{2} + \frac{1}{12}\log 3\right) \\ n^2\left(\frac{1}{12}\log\frac{m}{2} + \frac{3}{16}\log 3\right) \\ n^2\left(\frac{1}{108}\log\frac{m}{2} + \frac{1}{48}\log 3\right) \\ n^2\left(\frac{1}{3}\log\frac{m}{2} - \frac{1}{4}\log 3\right) \\ n^2\left(\frac{1}{27}\log\frac{m}{2} - \frac{1}{36}\log 3\right). \end{cases}$$

Note that from Remark 5.2.4, the assumption $n \geq 2$ can change to $n \geq 17$. We may assume $m \geq 6$ for Cases I-III as there are no non-torsion points on E when $m \leq 5$, and assume $m \geq 9$ for Cases IV-V as $m \equiv 0 \pmod 9$. Then $n \leq 4, 3, 9, 3$, and 11, respectively, contradicting the fact that $n \geq 17$. Thus $X_{nP} > 24m$, allowing us to deduce (5.15), so that

$$\begin{aligned} \log|L_{n,k}(z,\omega_m)| &\leq -\tfrac{1}{2}\log|X_{nP}| + \tfrac{3}{2}\log 2 && \text{by (5.15)} \\ &\leq -\hat{h}(nP) + \tfrac{1}{3}\log 3 + \tfrac{3}{2}\log 2 && \text{by (4.8)} \\ &\leq \begin{cases} -n^2\left(\frac{1}{27}\log\frac{m}{2} + \frac{1}{12}\log 3\right) + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -n^2\left(\frac{1}{12}\log\frac{m}{2} + \frac{3}{16}\log 3\right) + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -n^2\left(\frac{1}{108}\log\frac{m}{2} + \frac{1}{48}\log 3\right) + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -n^2\left(\frac{1}{3}\log\frac{m}{2} - \frac{1}{4}\log 3\right) + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -n^2\left(\frac{1}{27}\log\frac{m}{2} - \frac{1}{36}\log 3\right) + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \end{cases} \\ & && \text{by (5.12).} \end{aligned}$$

The different signs in Cases IV and V make for a different consideration. Notice that

$$\tfrac{1}{3}\log\tfrac{m}{2} - \tfrac{1}{4}\log 3 \geq \tfrac{1}{27}\log m, \text{ for } m \geq 6$$
$$\tfrac{1}{27}\log\tfrac{m}{2} - \tfrac{1}{36}\log 3 \geq \tfrac{1}{48}\log m, \text{ for } m \geq 33$$

(the cases $m < 33$ will be checked in Appendix C). Hence

$$\log|L_{n,k}| \leq \begin{cases} -\frac{n^2}{27}\log m - n^2\left(-\frac{1}{27}\log 2 + \frac{1}{12}\log 3\right) + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -\frac{n^2}{12}\log m - n^2\left(-\frac{1}{12}\log 2 + \frac{3}{16}\log 3\right) + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -\frac{n^2}{108}\log m - n^2\left(-\frac{1}{108}\log 2 + \frac{1}{48}\log 3\right) + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -\frac{n^2}{27}\log m + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -\frac{n^2}{48}\log m + \frac{3}{2}\log 2 + \frac{1}{3}\log 3. \end{cases}$$

We can see that in Cases I-III, the sum of the last three terms is always negative as $n \geq 17$. Therefore the bound (5.14) follows. □

We are now in position to find an upper bound on n such that nP is integral, which can be expressed in terms of m.

Lemma 5.2.11. *Suppose nP is integral, $n \geq 2$. Then*

$$n \leq \begin{cases} \max\{4.608 \times 10^{28},\ 2.653 \times 10^{24}(\log m)^{\frac{5}{2}}\} \\ \max\{4.608 \times 10^{28},\ 1.769 \times 10^{24}(\log m)^{\frac{5}{2}}\} \\ \max\{1.253 \times 10^{29},\ 5.305 \times 10^{24}(\log m)^{\frac{5}{2}}\} \\ \max\{4.608 \times 10^{28},\ 1.816 \times 10^{24}(\log m)^{\frac{5}{2}}\} \\ \max\{4.608 \times 10^{28},\ 2.421 \times 10^{24}(\log m)^{\frac{5}{2}}\}. \end{cases}$$

Proof. With the same notations used in Lemma 5.2.8, we have

$$\log|L_{n,k}| \geq -C(\log B + 1)(\log\log B + h(E) + 1)^3 \log V_1 \log V_2, \qquad (5.16)$$

where $C = 4 \times 10^{41}$. For the curve E_m, $\tau = \dfrac{1+\sqrt{3}i}{2}$. As $m \geq 6$,

$$h(E_m) = \log(4 \cdot 432m^2) > 11.038 > \frac{3\pi}{\mathrm{Im}(\tau)}.$$

We set

$$\log V_2 = h(E_m) = 2\log m + 6\log 2 + 3\log 3.$$

By (5.13) and the fact that $|z| \leq \dfrac{\omega_m}{2}$, we may take

$$\log V_1 = 3\log\max\{n, m\} + 6\log 2 + 3\log 3.$$

As $|nz + k\omega_m| \leq \dfrac{\omega_m}{2}$, we have $|k| < n$, and so we may take

$$\log(B) = 3e\log\max\{n, m\} + 6e\log 2 + 3e\log 3.$$

Substituting all of them into (5.16) and then combining with (5.14), we get

$$\left.\begin{array}{r} \frac{n^2}{27}\log m \\ \frac{n^2}{12}\log m \\ \frac{n^2}{108}\log m \\ \frac{n^2}{27}\log m - \frac{3}{2}\log 2 - \frac{1}{3}\log 3 \\ \frac{n^2}{48}\log m - \frac{3}{2}\log 2 - \frac{1}{3}\log 3 \end{array}\right\} \leq C(\log B + 1)(\log\log B + h(E_m) + 1)^3 \cdot \log V_1 \log V_2.$$

We separate our consideration in two cases. First, assuming that $n > m$, and using the estimate $\log(\log n + 2\log 2 + \log 3) < \log n$ for all $n \geq 6$, we obtain

$$n^2 \leq F(\log n), \tag{5.17}$$

where

$$F(x) = C'\left(x + 2\log 2 + \log 3 + \tfrac{1}{3e}\right)\left(x + 2\log 2 + \tfrac{4}{3}\log 3 + \tfrac{2}{3}\right)^3 (x + 2\log 2 + \log 3)\left(3\log 2 + \tfrac{3}{2}\log 3 + x\right),$$

for Cases I - III, and

$$F(x) = C'\{2^1 3^5 e\left(x + 2\log 2 + \log 3 + \tfrac{1}{3e}\right)\left(x + 2\log 2 + \tfrac{4}{3}\log 3 + \tfrac{2}{3}\right)^3$$

$$(x + 2\log 2 + \log 3)\left(3\log 2 + \tfrac{3}{2}\log 3 + x\right) + \tfrac{3}{2}\log 2 + \tfrac{1}{3}\log 3\},$$

for Cases IV and V.

The constant C' varies in each case as $\dfrac{2^1 3^8 eC}{\log 6}$, $\dfrac{2^3 3^6 eC}{\log 6}$, $\dfrac{2^3 3^8 eC}{\log 6}$, $\dfrac{27}{\log 9}$, and $\dfrac{48}{\log 9}$, respectively.

We know that (5.17) bounds n, but we require some tool to refine it.

Claim 5.2.12. (Claim 23, [15]) Let $F(x) \in \mathbb{R}[x]$ be a polynomial of degree d. Suppose that for some $W > 0$ and every $0 \leq k \leq d$,

$$W^2 > 2^{-k} F^{(k)}(\log W),$$

where $F^{(k)}$ denote the kth derivative of F. Then $x^2 > F(\log x)$ for all $x \geq W$.

It can be checked that if

$$W = \begin{cases} 4.608 \times 10^{28}, \\ 4.608 \times 10^{28}, \\ 1.253 \times 10^{29}, \\ 4.608 \times 10^{28}, \\ 4.608 \times 10^{28}, \end{cases}$$

then $W^2 > 2^{-k} F^{(k)}(\log W)$ for all $0 \leq k \leq 6$. Hence Claim 5.2.12 implies particularly that $x^2 > F(\log x)$ for all $x \geq W$. Therefore the bound (5.17) implies that

$$\begin{aligned} n &< 4.608 \times 10^{28}, \\ n &< 4.608 \times 10^{28}, \\ n &< 1.253 \times 10^{29}, \\ n &< 4.608 \times 10^{28}, \\ n &< 4.608 \times 10^{28}, \end{aligned}$$

for Cases I-V, respectively.

On the other hand, if $n < m$, then by the estimate

$$\log(\log m + 2\log 2 + \log 3) < \log m$$

again, we get

$$n^2 \leq C'' \log(m)^5 G(\log m),$$

where

$$G(x) = \{(x + 2\log 2 + \log 3 + 1)\left(x + 2\log 2 + \tfrac{4}{3}\log 3 + \tfrac{2}{3}\right)^3$$
$$(x + 2\log 2 + \log 3)\left(2\log 2 + \tfrac{3}{2}\log 3 + x\right)\}/x^6,$$

for Cases I-III, so that

$$G(\log m) \leq 493 \text{ for all } m \geq 6,$$

and

$$G(x) = \{2 \cdot 3^5 \cdot e \cdot C\,(x + 2\log 2 + \log 3 + 1)\left(x + 2\log 2 + \tfrac{4}{3}\log 3 + \tfrac{2}{3}\right)^3$$
$$(x + 2\log 2 + \log 3)\left(2\log 2 + \tfrac{3}{2}\log 3 + x\right) + \tfrac{3}{2}\log 2 + \tfrac{1}{3}\log 3\}/x^6,$$

for Cases IV-V, so that

$$G(\log m) \leq 1.221 \times 10^{47} \text{ for all } m \geq 9.$$

The constants C'' are $2^1 3^8 eC, 2^3 3^6 eC, 2^3 3^8 eC, 27$, and 48, respectively. Hence

$$n < 2.653 \times 10^{24} (\log m)^{\frac{5}{2}},$$
$$n < 1.769 \times 10^{24} (\log m)^{\frac{5}{2}},$$
$$n < 5.305 \times 10^{24} (\log m)^{\frac{5}{2}},$$
$$n < 1.816 \times 10^{24} (\log m)^{\frac{5}{2}},$$
$$n < 2.421 \times 10^{24} (\log m)^{\frac{5}{2}},$$

□

Next, we will show the proof of Lemma 5.2.7, which relies on the following two claims.

Claim 5.2.13. Given $Q \in E[n] \setminus \{\mathcal{O}\}$, we have $|X(Q)| \leq 3n^2 m^{\frac{2}{3}}$.

Proof of Lemma 5.2.13. Appealing to the isomorphism

$$\begin{aligned} E_m(\mathbb{C}) &\longrightarrow E_1(\mathbb{C}) \\ (X, Y) &\longmapsto (Xm^{-\frac{2}{3}}, Ym^{-1}), \end{aligned}$$

it suffices to prove the claim for $m = 1$, which we do by using another isomorphism deduced from the study of elliptic functions. Let $\Lambda = \omega_1 \mathbb{Z}[\omega]$ be the period lattice of E_1, where $\omega = \dfrac{1+\sqrt{-3}}{2}$, and ω_1 is the real period of E_1. Note that $0.88 < \omega_1 < 0.89$, computed with PARI/GP. Consider the Weierstrass $\wp$-function associated to E_1

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

and we have

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow E_1(\mathbb{C}) \\ z &\longmapsto \left(\wp(z), \frac{1}{2}\wp'(z) \right) \end{aligned}$$

is an isomorphism. Then $|\wp(z)| = |z|^{-2} + O(1)$ near $z = 0$, and we will prove the claim by making this explicit. We may choose a representative $z = \alpha_1\omega_1 + \alpha_2\omega_2$, where $\omega_2 = \omega_1\omega$, of any class in $\mathbb{C}/\Lambda$ such that $|\alpha_i| \leq \dfrac{1}{2}$, then z is in the region

$$\Lambda_0 = \left\{ z \in \mathbb{C} : |\mathrm{Re}(z)| \leq \frac{3}{4}\omega_1 \text{ and } |\mathrm{Im}(z)| \leq \frac{\sqrt{3}}{4}\omega_1 \right\}.$$

Claim I.1: $|u-z| \geq \dfrac{\sqrt{3}}{4}|u|$, *for all* $u \in \Lambda$.

Proof. If $|u| \geq \sqrt{3}|\omega_1|$, then $|z| \leq \dfrac{|u|}{2}$, so that

$$|u-z| \geq |\,|u|-|z|\,| = |u|-|z| \geq |u|-\frac{|u|}{2} = \frac{|u|}{2} > \frac{\sqrt{3}}{4}|u|.$$

The lattice points left to consider are all points u such that $|u| < \sqrt{3}|\omega_1|$. There are only 6 such lattice points: ω_1, ω_2, $\omega_2-\omega_1$, $-\omega_1$, $-\omega_2$, $\omega_1-\omega_2$. In fact, it suffices to consider just 3 points, $u = \omega_1$, ω_2, and $\omega_2-\omega_1$, because of the symmetry of the lattice. Each one satisfies $|u| = |\omega_1|$. Consider the distance between u and the corresponding closest point $z = \alpha_1\omega_1 + \alpha_2\omega_2$ in Λ_0.

(i) If $u = \omega_1$, then $z = \dfrac{\omega_1}{2} + \dfrac{\omega_2}{4}$, and

$$\begin{aligned} |u-z|^2 = \left|\frac{\omega_1}{2} - \frac{\omega_2}{4}\right|^2 &= \left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)\left(-\frac{1}{4}\right) + \left(-\frac{1}{4}\right)^2\right)|\omega_1|^2 \\ &= \frac{3}{16}|\omega_1|^2 = \left(\frac{\sqrt{3}}{4}|u|\right)^2. \end{aligned}$$

(ii) If $u = \omega_2$, then $z = \dfrac{\omega_1}{4} + \dfrac{\omega_2}{2}$, and

$$|u-z|^2 = \left|-\frac{\omega_1}{4} + \frac{\omega_2}{2}\right|^2 = \frac{3}{16}|\omega_1|^2 = \left(\frac{\sqrt{3}}{4}|u|\right)^2.$$

(iii) If $u = -\omega_1 + \omega_2$, then $z = -\dfrac{\omega_1}{2} + \dfrac{\omega_2}{2}$, and

$$|u-z|^2 = \left|-\frac{\omega_1}{2} + \frac{\omega_2}{2}\right|^2 = \frac{1}{4}|\omega_1|^2 = \left(\frac{|u|}{2}\right)^2 \geq \left(\frac{\sqrt{3}}{4}|u|\right)^2.$$

This completes the proof of Claim I.1. □

Now, by Claim I.1,

$$\begin{aligned}\left|\sum_{\substack{u\in\Lambda\\u\neq 0}}\left(\frac{1}{(u-z)^2}-\frac{1}{u^2}\right)\right| &= \left|\sum_{\substack{u\in\Lambda\\u\neq 0}}\frac{u^2-(u-z)^2}{u^2(u-z)^2}\right| \\ &\leq \left|\sum_{\substack{u\in\Lambda\\u\neq 0}}\frac{2uz}{u^2(u-z)^2}\right| + \left|\sum_{\substack{u\in\Lambda\\u\neq 0}}\frac{z^2}{u^2(u-z)^2}\right| \\ &\leq 2|z|\sum_{\substack{u\in\Lambda\\u\neq 0}}\frac{16}{3|u|^3}+|z|^2\sum_{\substack{u\in\Lambda\\u\neq 0}}\frac{16}{3|u|^4}.\end{aligned}$$

For $\sigma > 1$, let

$$F(\sigma) := \sum_{\substack{u\in\Lambda\\u\neq 0}}|u|^{-2\sigma}.$$

Then

$$|\wp(z)| \leq |z|^{-2} + \frac{32}{3}F(3/2)|z| + \frac{16}{3}F(2)|z|^2.$$

Next we will determine upper bounds for $F(3/2)$ and $F(2)$. Note that

$$F(\sigma) = \sum_{\substack{u\in\Lambda\\u\neq 0}}|u|^{-2\sigma} = 6\sum_{\substack{u\in\Lambda_1\\u\neq 0}}|u|^{-2\sigma} = 6\sum_{\alpha>0,\beta\geq 0}|\alpha\omega_1+\beta\omega_2|^{-2\sigma},$$

where

$$\Lambda_1 = \left\{u\in\Lambda : |u|>0, \text{and } 0\leq \arg(u) < \frac{\pi}{3}\right\},$$

and $\arg(u)$ is the principal argument of u. Since

$$|\alpha\omega_1+\beta\omega_2|^2 = (\alpha\omega_1+\beta\omega_2)(\alpha\omega_1+\beta\bar{\omega_2}) = \omega_1^2(\alpha^2+\alpha\beta+\beta^2),$$

we have

$$\begin{aligned}\frac{\omega_1^{2\sigma}}{6}F(\sigma) &= \sum_{\alpha>0,\beta\geq 0}\frac{1}{(\alpha^2+\alpha\beta+\beta^2)^\sigma} = \sum_{\alpha>0,\beta>0}\frac{1}{(\alpha^2+\alpha\beta+\beta^2)^\sigma}+\zeta(2\sigma)\\ &= 3^{-\sigma}+\sum_{\substack{\alpha,\beta\geq 0\\(\alpha,\beta)\neq(0,0)}}\frac{1}{((\alpha+1)^2+(\alpha+1)(\beta+1)+(\beta+1)^2)^\sigma}+\zeta(2\sigma).\end{aligned}$$

If we denote by S the region

$$S=\big\{(x,y)\in\mathbb{R}^2 : x^2+y^2\geq 1, \text{ and } 0\leq y<x\sqrt{3}\big\},$$

then

$$\begin{aligned}&\sum_{\substack{\alpha,\beta\geq 0\\(\alpha,\beta)\neq(0,0)}}\frac{1}{((\alpha+1)^2+(\alpha+1)(\beta+1)+(\beta+1)^2)^\sigma}\\ &\qquad\leq \frac{2}{\sqrt{3}}\iint_S\frac{1}{(x^2+xy+y^2)^\sigma}dxdy\\ &\qquad\leq \frac{2}{\sqrt{3}}\int_0^{\frac{\pi}{3}}\int_1^\infty (r^2+r^2\sin\theta\cos\theta)^{-\sigma}rdrd\theta.\end{aligned}$$

Calculating the last integral values by Maple [21] leads

$$F(3/2)\leq 17.539 \text{ and } F(2)\leq 15.832,$$

and hence

$$\begin{aligned}|\wp(z)| &\leq |z|^{-2}+\frac{32}{3}F(3/2)|z|+\frac{16}{3}F(2)|z|^2\\ &\leq |z|^{-2}+\frac{32}{3}(17.539)\frac{\sqrt{3}}{2}(0.89)+\frac{16}{3}(15.832)\frac{3}{4}(0.89)^2\\ &\leq |z|^{-2}+194.359,\end{aligned}$$

as $|z|\leq\frac{\sqrt{3}}{2}|\omega_1|$. If $z\in\mathbb{C}/\Lambda$ is a point of order dividing n (other that $\mathcal{O}$), then $|z|\geq\frac{|\omega_1|}{n}$, so that

$$|\wp(z)| \leq \frac{n^2}{(0.89)^2} + 194.359 \leq 3n^2,$$

for all $n \geq 11$. For the cases $n \leq 10$, we can check all explicit torsion points of order n in $E_1(\mathbb{C})$, and then the proof of Lemma is completed. □

Claim 5.2.14. Suppose nP is an integral point, and $h_n = \psi_n(P)$. Then

$$|h_n| \leq 2^{n^2-1}.$$

Proof. To give a bound for h_n, we will consider the order to which all primes divide h_n. Suppose there exists a prime p other than 2 and 3 such that $p \mid h_n = \psi_n(P)$. Then p also divides $\phi_n(P)$ as nP is integral, and hence p has to divide the resultant of ϕ_n and ψ_n, which equals $(432B)^d$, where $B = -432m^2$ and $d = \frac{1}{6}n^2(n^2-1)$, by Remark 4.2.2. As $p \neq 2, 3$, $p \mid m$. Since $\phi_n(P)$ is a monic binary form in x^3 and B, it forces $p \mid x$, contradicting the assumption that x and m are coprime. Thus no such p exists. It now remains to think about when $p = 2$ or 3.

Refering to Remark 4.2.2 again, we have

$$\psi_n(P) = \psi_n(x, m) = nx^{\frac{n^2-1}{2}} + \cdots,$$

is also a binary form in x^3 and $B = -432m^2$. Since $\gcd(x, 3) = 1$ and $3 \nmid n$, h_n is not divisible by 3, so $\mathrm{ord}_3(h_n) = 0$.

For $p = 2$, we have either $2 \mid x$ or $2 \nmid x$. With the same reasons as above, the latter would imply $\mathrm{ord}_2(h_n) = 0$. Otherwise, from the initial values of h_n, we observe that

$$\mathrm{ord}_2(h_n) \begin{cases} = n^2 - 1 & \text{if } 3 \nmid n \\ \geq n^2 - 1 & \text{if } 3 \mid n. \end{cases}$$

To verify these by induction for all n, we will use the formulas (4.5) and (4.6), as detailed in Appendix B. Therefore the conclusion of Claim II arises. □

Proof of Lemma 5.2.7. Suppose for a contradiction that $|X(P)| > 6n^2m^{\frac{2}{3}}$. If $Q \in E[n] \setminus \{\mathcal{O}\}$, then, by Claim 5.2.13,

$$|X(P) - X(Q)| > \frac{X(P)}{2}.$$

Thus

$$|h_n| \geq \left(\frac{X(P)}{2}\right)^{\frac{n^2-1}{2}},$$

as $h_n^2 = n^2 \prod_{Q \in E[n]\setminus\{\mathcal{O}\}} |X(P) - X(Q)|$ and $E[n] \setminus \{\mathcal{O}\}$ consists of $n^2 - 1$ points. On the other hand, by Claim 5.2.14,

$$|h_n| \leq 2^{n^2-1}.$$

So that

$$2^3 \geq X(P) \geq 6n^2m^{\frac{2}{3}},$$

and hence $n < 1$ as $m \geq 6$, which is impossible. Thereby $|X(P)| \leq 6n^2m^{\frac{2}{3}}$.

□

5.2.2 Proof of Step 2

We now come to step 2 of the proof of Lemma 5.1.1 to construct a relation between n_1 and n_2 when n_1P and n_2P are integral points. The first two claims below are essential to help us get there.

Claim 5.2.15. Suppose nP is an integral point, $n \geq 2$. Then n is prime.

Claim 5.2.16. Suppose nP is integral, and denote z and $nz + k\omega_m$ the principal values of the elliptic logarithms of P and nP, respectively. If $k = 0$, then $n = 1$.

We postpone the proofs of these two claims to the end of this section.

Lemma 5.2.17. *Suppose n_1P and n_2P are integral with $2 \leq n_1 < n_2$. Then*

$$\log n_2 \geq \begin{cases} \frac{n_1^2}{27}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} \\ \frac{n_1^2}{12}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} \\ \frac{n_1^2}{108}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} \\ \frac{n_1^2}{27}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} - \frac{3}{2}\log 2 - \frac{1}{3}\log 3 \\ \frac{n_1^2}{48}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2} - \frac{3}{2}\log 2 - \frac{1}{3}\log 3, \end{cases} \tag{5.18}$$

where ω_1 is the real period of E_1.

Proof. By the triangle inequality and Lemma 5.2.10, we have

$$\begin{aligned} m^{-\frac{1}{3}}\omega_1 &\leq \omega_m|n_2k_1 - n_1k_2| \\ &\leq n_2|n_1z + k_1\omega_m| + n_1|n_2z + k_2\omega_m| \\ &\leq \begin{cases} n_2m^{-\frac{n_1^2}{27}} + n_1m^{-\frac{n_2^2}{27}} \\ n_2m^{-\frac{n_1^2}{12}} + n_1m^{-\frac{n_2^2}{12}} \\ n_2m^{-\frac{n_1^2}{108}} + n_1m^{-\frac{n_2^2}{27}} \\ n_2m^{-\frac{n_1^2}{27}}e^{\frac{5}{2}\log 2 + \frac{4}{3}\log 3} + n_1m^{-\frac{n_2^2}{48}}e^{\frac{3}{2}\log 2 + \frac{1}{3}\log 3} \\ n_2m^{-\frac{n_1^2}{48}}e^{\frac{5}{2}\log 2 + \frac{4}{3}\log 3} + n_1m^{-\frac{n_2^2}{48}}e^{\frac{3}{2}\log 2 + \frac{1}{3}\log 3} \end{cases} \end{aligned} \tag{5.19}$$

The inequality on the left-hand side requires $|n_2k_1 - n_1k_2| \neq 0$: suppose that $n_2k_1 = n_1k_2$. From Claim 5.20, we know that n_1 and n_2 are prime. This implies $k_1 \neq 0$, by Claim 5.2.16. Thus either $n_1 = n_2$ or $n_1 \mid |k_1|$. If the latter

occurs, then $n_1 \leq |k_1|$. Following as in the proof of Proposition 13 [15], we have

$$2|k_1| \leq \frac{2}{\omega_m}(|n_1 z + k_1\omega_m| + |n_1 z|) \leq n_1 + 1,$$

as $|z| \leq \frac{\omega_m}{2}$ and $|n_1 z + k_1\omega_m| \leq \frac{\omega_m}{2}$. This induces

$$2n_1 \leq 2|k_1| \leq n_1 + 1,$$

which is impossible as $n_1 \geq 2$. Thus $n_1 = n_2$.

We will give details of the proof for Case I only (the same process will be applied for Cases II-V). The estimate (5.19) gives

$$\frac{m^{-\frac{1}{3}}\omega_1}{2} \leq n_2 m^{-\frac{n_1^2}{27}} \quad \text{or} \quad \frac{m^{-\frac{1}{27}}\omega_1}{2} \leq n_1 m^{-\frac{n_2^2}{27}}$$

In the latter case,

$$\frac{\omega_1}{2} \leq n_1 m^{-\frac{n_2^2}{27}+\frac{1}{3}} < n_2 m^{-\frac{n_2^2}{27}+\frac{1}{3}}.$$

Taking the logarithm gives $n_2 \leq 7$, a contradiction. Hence

$$m^{-\frac{1}{3}}\frac{\omega_1}{2} \leq n_2 m^{-\frac{n_1^2}{27}},$$

so that

$$\log n_2 \geq \frac{n_1^2}{27}\log m - \frac{1}{3}\log m + \log\frac{\omega_1}{2}.$$

□

Proof of Claim 5.2.14. Suppose n is composite and let q be the smallest prime dividing n. Write $a = \frac{n}{q}$; then $nP = q(aP)$ with $q \leq a$. Then the estimates (5.13) and (5.12) imply

$$\log q + \frac{1}{3}\log m + \frac{1}{2}\log 2 + \frac{5}{6}\log 3 \;\geq \hat{h}(aP) = a^2\hat{h}(P)$$

$$\geq \begin{cases} a^2\left(\frac{1}{27}\log\frac{m}{2} + \frac{1}{12}\log 3\right) \\ a^2\left(\frac{1}{12}\log\frac{m}{2} + \frac{3}{16}\log 3\right) \\ a^2\left(\frac{1}{108}\log\frac{m}{2} + \frac{1}{48}\log 3\right) \\ a^2\left(\frac{1}{3}\log\frac{m}{2} - \frac{1}{4}\log 3\right) \\ a^2\left(\frac{1}{27}\log\frac{m}{2} - \frac{1}{36}\log 3\right) \end{cases}$$

$$\geq \begin{cases} q^2\left(\frac{1}{27}\log\frac{m}{2} + \frac{1}{12}\log 3\right) \\ q^2\left(\frac{1}{12}\log\frac{m}{2} + \frac{3}{16}\log 3\right) \\ q^2\left(\frac{1}{108}\log\frac{m}{2} + \frac{1}{48}\log 3\right) \\ q^2\left(\frac{1}{3}\log\frac{m}{2} - \frac{1}{4}\log 3\right) \\ q^2\left(\frac{1}{27}\log\frac{m}{2} - \frac{1}{36}\log 3\right). \end{cases}$$

Again assuming $m \geq 6$ in Cases I-III, and $m \geq 9$ in Cases IV-V, then

$$q^2 \leq \begin{cases} 7.56\log q + 14.06 \\ 3.36\log q + 6.25 \\ 30.25\log q + 56.25 \\ 7.98\log q + 15.92 \\ 39.7\log q + 79.18. \end{cases} \tag{5.20}$$

Lemma 6 of [15] says that for any positive real numbers a, b, if

$$f(x) = x^2 - a\log x - b,$$

then $f(x) \geq 0$ for $x \geq \max\{e, a+b\}$. Applying to (5.20), we get

$$q \leq 21.62,\ 9.61,\ 86.5,\ 23.9, \text{ and } 118.88.$$

Indeed, $q \leq 5, 3, 11, 5$, and 13, respectively, by checking the smaller values q. These lead to contradictions as n cannot divisible by any prime less than 17. $\square$

Proof of Claim 5.2.15. From the proofs of Claim 25 and Lemma 12 of [15], the elliptic logarithm z satisfies

$$-\log|z| = -\log\left|\frac{1}{2}\int_{X(P)}^{\infty}\frac{dt}{\sqrt{t^3-432m^2}}\right|$$

$$\leq \frac{3}{2}\log 2 + \frac{1}{2}\log\max\{|X(P)|, 24m\}. \tag{5.21}$$

Moreover, by (5.14), we have

$$\log n + \log|z| = \log|nz| \leq \begin{cases} -\frac{n^2}{27}\log m \\ -\frac{n^2}{12}\log m \\ -\frac{n^2}{108}\log m \\ -\frac{n^2}{27}\log m + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \\ -\frac{n^2}{48}\log m + \frac{3}{2}\log 2 + \frac{1}{3}\log 3 \end{cases}$$

as $k = 0$. If $|X(P)| \geq 24m$, then the estimate (5.21) and Lemma 5.2.7 give

$$\begin{aligned} -\log|z| - \log n &\leq \tfrac{3}{2}\log 2 + \tfrac{1}{2}\log(|X(P)|) - \log n \\ &\leq \tfrac{3}{2}\log 2 + \tfrac{1}{2}\log 6 + \log n + \tfrac{1}{3}\log m - \log n \\ &\leq 2\log 2 + \tfrac{1}{2}\log 3 + \tfrac{1}{3}\log m. \end{aligned}$$

Then

$$\left.\begin{aligned} \tfrac{n^2}{27}\log m \\ \tfrac{n^2}{12}\log m \\ \tfrac{n^2}{108}\log m \\ \tfrac{n^2}{27}\log m - \tfrac{3}{2}\log 2 - \tfrac{1}{3}\log 3 \\ \tfrac{n^2}{48}\log m - \tfrac{3}{2}\log 2 - \tfrac{1}{3}\log 3 \end{aligned}\right\} \begin{aligned} &\leq -\log|z| - \log n \\ &\leq 2\log 2 + \tfrac{1}{2}\log 3 + \tfrac{1}{3}\log m. \end{aligned}$$

So that $n \leq 6, 4, 12, 7,$ and 9, respectively.

On the other hand, if $|X(P)| < 24m$, then

$$\left.\begin{aligned} \tfrac{n^2}{27}\log m \\ \tfrac{n^2}{12}\log m \\ \tfrac{n^2}{108}\log m \\ \tfrac{n^2}{27}\log m - \tfrac{3}{2}\log 2 - \tfrac{1}{3}\log 3 \\ \tfrac{n^2}{48}\log m - \tfrac{3}{2}\log 2 - \tfrac{1}{3}\log 3 \end{aligned}\right\} \begin{aligned} &\leq -\log|z| - \log n \\ &\leq \frac{3}{2}\log 2 + \frac{1}{2}\log 24m - \log n, \end{aligned}$$

which give $n \leq 5, 3, 8, 6,$ and 8, respectively. But n cannot divisible by $2, 3, 5,$ and 7, so $n = 1$. □

5.2.3 Proof of Step 3

We arrive now at the step in finding an explicit bound on m in each case by substituting n_1 and n_2 in the estimate (5.18) from step 2 by

$$\begin{aligned} &n_1 \geq 17, \text{ and} \\ &n_2 \leq \text{the bounds in step 1.} \end{aligned}$$

Case I: If $n_2 \leq 4.608 \times 10^{28}$ and $n_1 \geq 17$, then substituting them into the estimate (5.18), we get

$$\log 4.608 + 28 \log 10 \geq \log n_2 \geq \frac{280}{27} \log m + \log \frac{\omega_1}{2},$$

With a manipulation, $m \leq 628$.

On the other hand, if $n_2 \leq 2.653 \times 10^{24} (\log m)^{\frac{5}{2}}$ and $n_1 \geq 17$, then, by (5.18) again,

$$\log 2.653 + 24 \log 10 + \frac{5}{2} \log \log m \geq \log n_2 \geq \frac{280}{27} \log m + \log \frac{\omega_1}{2},$$

so that

$$\frac{280}{27} \log m - \frac{5}{2} \log \log m \leq 24 \log 10 + \log 2.653 - \log \frac{\omega_1}{2}.$$

Then $m \leq 376$. Thus, in this case, $m \leq 628$.

Case II: If $n_2 \leq 4.608 \times 10^{28}$ and $n_1 \geq 17$, then

$$\log 4.608 + 28 \log 10 \geq \log n_2 \geq \frac{95}{4} \log m + \log \frac{\omega_1}{2},$$

so $m \leq 16$. If $n_2 \leq 1.769 \times 10^{24} (\log m)^{\frac{5}{2}}$ and $n_1 \geq 17$, then

$$\frac{95}{4} \log m - \frac{5}{2} \log \log m \leq 24 \log 10 + \log 1.769 - \log \frac{\omega_1}{2},$$

so $m \leq 11$. Thus, in this case, $m \leq 16$.

Case III: If $n_2 \leq 1.253 \times 10^{29}$ and $n_1 \geq 17$, then

$$\log 1.253 + 29 \log 10 \geq \log n_2 \geq \frac{253}{108} \log m + \log \frac{\omega_1}{2},$$

so $m \leq 3739071625384$. If $n_2 \leq 5.305 \times 10^{24} (\log m)^{\frac{5}{2}}$ and $n_1 \geq 17$, then

$$\frac{253}{108} \log m - \frac{5}{2} \log \log m \leq 24 \log 10 + \log 5.305 - \log \frac{\omega_1}{2},$$

so $m \leq 1794187182553$. Thus, in this case, $m \leq 3739071625384$.

Case IV: If $n_2 \leq 4.608 \times 10^{28}$ and $n_1 \geq 17$, then

$$\log 4.608 + 28 \log 10 \geq \log n_2 \geq \frac{280}{27} \log m + \log \frac{\omega_1}{2} - \frac{3}{2} \log 2 - \frac{1}{3} \log 3,$$

so $m \leq 719$. If $n_2 \leq 1.816 \times 10^{24} (\log m)^{\frac{5}{2}}$ and $n_1 \geq 17$, then

$$\frac{280}{27} \log m - \frac{5}{2} \log \log m \leq 24 \log 10 + \log 1.816 - \log \frac{\omega_1}{2} + \frac{3}{2} \log 2 + \frac{1}{3} \log 3,$$

so $m \leq 417$. Thus, in this case, $m \leq 719$.

Case V: If $n_2 \leq 4.608 \times 10^{28}$ and $n_1 \geq 17$, then

$$\log 4.608 + 28 \log 10 \geq \log n_2 \geq \frac{273}{48} \log m + \log \frac{\omega_1}{2} - \frac{3}{2} \log 2 - \frac{1}{3} \log 3,$$

so $m \leq 161993$. If $n_2 \leq 2.421 \times 10^{24} (\log m)^{\frac{5}{2}}$ and $n_1 \geq 17$, then

$$\frac{273}{48} \log m - \frac{5}{2} \log \log m \leq 24 \log 10 + \log 2.421 - \log \frac{\omega_1}{2} + \frac{3}{2} \log 2 + \frac{1}{3} \log 3,$$

so $m \leq 83262$. Thus, in this case, $m \leq 161993$.

In Cases III and V, we get massive bounds on m, so we will not work on these Cases anymore. For other Cases, we will deal with the curves E_m with small values $m \leq 719$ in Appendix C, and then the proof of Theorem 5.2.5 will be completed.

We now come to the final part of this section. Given a non-torsion point $R \in C(\mathbb{Q})$, suppose P is a non-torsion rational point on E corresponding to R by the bi-rational transformation (5.3). This gives

$$\frac{U_n}{W_n} = \frac{2^2 3^2 m B_n^3 + C_n}{6 A_n B_n}.$$

From the proof of Theorem 5.1.2, we have that the greatest common divisor g of the numerator and the denominator of the right-hand side comes from the term $6A_n$ only; that is, $g \nmid B_n$, and $g \mid 72m$.

If R corresponds to a non-integral point $P = \left(\frac{A_1}{B_1^2}, \frac{C_1}{B_1^3}\right)$, then $B_n > 1$ for all $n \geq 1$. In this situation, proving that $\frac{6A_n}{g} > 1$ requires the condition that $\gcd(A_1, m) = 1$.

If R corresponds to an integral point $P = (A_1, C_1)$, then, by Theorem 5.1.1, $B_n > 1$ for at most one exception under the assumption that $\gcd(A_1, 3m) = 1$, and $2P$, $3P$ are non-integral.

We can conclude the precise statement of the second main result as follows:

Theorem 5.2.18. (Main Theorem II) *Given C an elliptic curve as in (5.1) with $m \in \mathbb{Z}$ cube-free, let R be a rational point on C corresponding to a rational point P on E. Write, in lowest terms, $nR = \left(\frac{U_n}{W_n}, \frac{V_n}{W_n}\right)$. Suppose that*

$gcd(A_1, m) = 1$ if $P = \left(\frac{A_1}{B_1^2}, \frac{C_1}{B_1^3}\right)$ is non-integral, or

$gcd(X(P), 3m) = 1$ and $2P, 3P$ are non-integral if P is integral.

Then there is at most one value of $n > 1$ such that W_n is a prime power unless

$m \equiv \pm 2$ mod 9 and m has a prime factor congruent to 1 mod 6, or

$m \equiv 0$ mod 9 and m has a prime factor congruent to 1 mod 6,

in which cases, the result holds for $m >$ 3739071625384.

Remark 5.2.19. If $\gcd(A_1, m) = 1$, then $\gcd(A_n, m) = 1$ for all n.

Proof. Let p be arbitrary prime number. We aim to show that

$$\mathrm{ord}_p(\gcd(A_n, m)) = 0.$$

It is obvious when $p \nmid m$. Otherwise, suppose $p \mid m$. Reducing

$$E : Y^2 = X^3 - 2^4 3^3 m^2$$

modulo p yields

$$\bar{E} : y^2 = x^3,$$

which is singular at $(0, 0)$. Let $P = \left(\frac{A_1}{B_1^2}, \frac{C_1}{B_1^3}\right) \in E(\mathbb{Q})$. Since $\gcd(A_1, m) = 1$ and $p \mid m$, so that $p \nmid A_1$. Then P maps to some point $\bar{P}$ on $\bar{E}$, other than $(0, 0)$, i.e. P maps to a non-singular point $\bar{P}$ on $\bar{E}$. We have the following facts:

(i) $\bar{E}_{ns}$ is a group, and

(ii) the reduction mod p map is a homomorphism.

Thus the point $nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right)$ maps to $n(\bar{P})$ on $\bar{E}_{ns}$. This means $p \nmid A_n$; that is $\mathrm{ord}_p(\gcd(A_n, m)) = 0$. □

Proof of Main Theorem II. After we can prove that B_n is guaranteed to be greater than 1, for at most one exception, it remains to show that $6A_n$ can avoid being cancelled. For convenience, write

$$G = \frac{g}{\gcd(g, 6)},$$

where g is as above; then $G \mid g \mid 72m$ and $G \mid A_n$. This means our goal is equivalent to showing that the term $\frac{A_n}{G}$ is greater than 1. Since $G \mid A_n$ and $\gcd(A_n, m) = 1$, it follows that $\gcd(G, m) = 1$, so $G \mid 72 = 2^3 3^2$. Notice that the condition $\gcd(A_n, m) = 1$ and the defining equation of E,

$$C_n^2 = A_n^3 - 432 m^2 B_n^6, \tag{5.22}$$

imply $\mathrm{ord}_3(A_n) \leq 1$ for all n. Hence $G \mid 24$. It now requires $A_n > 24$ to complete the proof. As $m \geq 6$, we have, by the equation (5.22),

$$A_n^3 > 2^4 3^3 m^2 > 2^4 3^3 6^2,$$

and hence $A_n > 24$, as desired. □

Appendix A

Computation I

In order to complete the proof of Lemma 5.1.1, it remains to check the statement for all cube-free integers m up to 353, as mentioned in the end of the proof. In this part, we deal with the particular computations to find a uniform bound, N_0, on the indices n such that $B_n > 2^{\frac{1}{3}}3^{\frac{1}{2}}m^{\frac{1}{6}}$ for such m. We start by computing ranks and generators of $E : Y^2 = X^3 - 432m^2$ by MAGMA [20] and PARI/GP [31]. We consider the curves of rank greater than 0 only. For rank-1 curves, we test the elliptic divisibility sequence (B_n) arising from the generator for $n = 1, ..., 22$. A special treatment is required for the curves of rank 2. There are two parts needed to find the bound N_0. We begin by finding the finite set of pairs (i, j), $i, j \in \mathbb{Z}$, such that the canonical height of each point $iP + jQ$ is less than 40, where P and Q represent the generators. Then we compute the elliptic divisibility sequence (B_n) arising from each point $iP + jQ$, for $n = 1, ..., 22$. Now we get a bound, say N_0', for the indices n from the points of canonical height less than 40. To treat all cases, when $h > 40$, we return to the proof of Lemma 5.1.1 again.

Replacing the estimate (5.8) by

$$h' > \frac{h}{3} > \frac{40}{3},$$

leading to

$$\frac{40}{3}n^2 - \frac{2}{3}\log m - \frac{1}{2}\log 48 - 2.14 > 2^{\frac{10}{3}}3^{\frac{1}{2}}m^{\frac{7}{6}}.$$

Taking specific values for m such that E_m has rank-2 gives another bound, say N_0'', for the indices n. Comparing N_0' and N_0'', let

$$N_0 = \min\{N_0', N_0''\}.$$

The following tables show the uniform bound N_0 for all curves of rank 1 and 2 (there are no curves of higher rank appearing).

Note that when $m = 337$, the curve requires a special tool, because we could not find its generator and rank using Magma. This problem was solved by using the SAGE online programme [24].

m	N_0
6	1
7	1
9	1
12	1
13	0
15	1
17	0
20	2
22	1
26	1
28	1
31	0
33	1
34	1
35	1
42	1
43	0
49	0
50	1
51	0
53	0
58	1
61	0
62	0
63	1
67	0
68	0
69	1

m	N_0
70	1
71	0
75	1
78	1
79	0
84	1
85	1
87	0
89	0
90	1
92	1
94	0
97	0
98	0
103	0
105	1
106	1
107	0
114	1
115	0
117	0
123	0
130	0
133	0
134	0
139	0
140	1
141	0

m	N_0
142	0
143	0
151	0
156	1
157	0
159	0
161	0
164	0
166	0
169	0
170	1
171	0
172	0
177	0
178	0
179	0
180	1
186	0
187	1
195	1
197	0
198	1
202	0
205	1
206	0
211	0
212	0
213	0

m	N_0
214	0
215	1
222	0
223	0
228	0
229	0
231	1
233	0
236	1
238	1
241	0
244	0
247	0
249	0
251	0
258	1
259	0
265	0
267	1
274	0
275	0
277	0
278	0
279	0
284	0
285	1
286	1
287	0

m	N_0
289	0
294	1
295	1
301	0
303	1
305	0
306	1
308	1
310	0
313	0
314	0
316	0
319	0
321	0
322	1
323	0
325	0
330	1
331	0
333	0
337	0
339	0
341	0
346	0
349	0

Table A.1: Rank-1 Curves

m	N_0
19	1
30	1
37	0
65	1
86	1
91	0
110	1
124	1
126	1
127	0
132	1

m	N_0
153	1
163	0
182	1
183	1
201	1
203	1
209	1
210	1
217	1
218	1
219	1

m	N_0
246	1
254	1
271	0
273	1
282	1
309	0
335	1
342	1
345	1
348	1

Table A.2: Rank-2 Curves

Appendix B

Proofs of Claim 5.2.14 and Lemma 5.2.2

The purpose of this chapter is to complete the proofs of Claim 5.2.14 (p. 86) and Lemma 5.2.2 (p. 74).

Claim 5.2.7: Suppose nP is an integral point, and $h_n = \psi_n(P)$. Then

$$|h_n| \leq 2^{n^2-1}.$$

The first part will verify the expressions for $\mathrm{ord}_2(h_n)$ in Claim II of Lemma 5.2.7. Remind that in this Lemma, we suppose $P = (x, y)$ is an integral point such that $2P$ ans $3P$ are non-integral, and $\gcd(x, 3m) = 1$. We claim that when $2 \mid x$,

$$\mathrm{ord}_2(h_n) \begin{cases} = n^2 - 1 & \text{if } 3 \nmid n \\ \geq n^2 - 1 & \text{if } 3 \mid n. \end{cases}$$

For n **odd**, write $n = 2k + 1$. We can divide all possibilities of n and k as follows.

If $3 \mid n$, then

(i) $k \equiv 1 \pmod 3$ and k is odd,

(ii) $k \equiv 1 \pmod 3$ and k is even,

If $3 \nmid n$, then

(iii) $k \equiv 0 \pmod 3$ and k is odd,

(iv) $k \equiv 0 \pmod 3$ and k is even,

(v) $k \equiv -1 \pmod 3$ and k is odd,

(vi) $k \equiv -1 \pmod 3$ and k is even.

Then we use the formula (4.5),

$$h_n = h_{k+2}h_k^3 - h_{k-1}h_{k+1}^3,$$

to prove our claim.

For n **even**, write $n = 2k$. Then we use the formula (4.6),

$$h_2 h_n = h_k(h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2),$$

instead for this case. All possibilities of n and k are described as follows.

If $3 \mid n$, then $3 \mid k$ with

(vii) k is odd,

(viii) k is even.

If $3 \nmid n$, then $3 \nmid k$, so

(ix) $k \equiv 1 \pmod 3$ and k is odd,

(x) $k \equiv 1 \pmod 3$ and k is even,

(xi) $k \equiv -1 \pmod 3$ and k is odd,

(xii) $k \equiv -1 \pmod 3$ and k is even.

Note that since we consider $\mathrm{ord}_2(h_n)$ when $2 \mid x$ and $\gcd(x, m) = 1$, from the equation

$$y^2 = x^3 - 432m^2,$$

it follows that $\mathrm{ord}_2(y) = 2$ and $\mathrm{ord}_2(x) \geq 2$.

Case (i): $k \equiv 1 \pmod 3$ and k is odd imply $3 \mid k+2$ odd, $3 \mid k-1$ even, $3 \nmid k+1$ even, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_k^3) &= \mathrm{ord}_2(h_{k+2}) + 3\mathrm{ord}_2(h_k) \\ &\geq (k+2)^2 - 1 + 3(k^2-1) \\ &= 4k^2 + 4k, \end{aligned}$$

and

$$\begin{aligned} \mathrm{ord}_2(h_{k-1}h_{k+1}^3) &= \mathrm{ord}_2(h_{k-1}) + 3\mathrm{ord}_2(h_{k+1}) \\ &\geq (k-1)^2 - 3 + \mathrm{ord}_2(y) + 3((k+1)^2 - 3 + \mathrm{ord}_2(y)) \\ &= 4k^2 + 4k - 8 + 4\mathrm{ord}_2(y) = 4k^2 + 4k, \end{aligned}$$

as $\mathrm{ord}_2(y) = 2$. Then

$$\mathrm{ord}_2(h_n) \geq 4k^2 + 4k = (2k+1)^2 - 1 = n^2 - 1.$$

Case (ii): $k \equiv 1 \pmod 3$ and k is even imply $3 \mid k+2$ even, $3 \mid k-1$ odd, $3 \nmid k+1$ odd, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_k^3) &\geq (k+2)^2 - 3 + \mathrm{ord}_2(y) + 3(k^2 - 3 + \mathrm{ord}_2(y)) \\ &= 4k^2 + 4k - 8 + 4\mathrm{ord}_2(y) = 4k^2 + 4k, \end{aligned}$$

and

$$\begin{aligned} \mathrm{ord}_2(h_{k-1}h_{k+1}^3) &\geq (k-1)^2 - 1 + 3((k+1)^2 - 1)) \\ &= 4k^2 + 4k. \end{aligned}$$

Then

$$\mathrm{ord}_2(h_n) \geq 4k^2 + 4k = (2k+1)^2 - 1 = n^2 - 1.$$

Case (iii): $k \equiv 0 \pmod 3$ and k is odd imply $3 \nmid k+2$ odd, $3 \nmid k-1$ even, $3 \nmid k+1$ even, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_k^3) &\geq (k+2)^2 - 1 + 3(k^2-1) \\ &= 4k^2 + 4k, \end{aligned}$$

and

$$\begin{aligned} \mathrm{ord}_2(h_{k-1}h_{k+1}^3) &= (k-1)^2 - 3 + \mathrm{ord}_2(y) + 3((k+1)^2 - 3 + \mathrm{ord}_2(y)) \\ &= 4k^2 + 4k - 8 + 4\mathrm{ord}_2(y) = 4k^2 + 4k, \end{aligned}$$

Then

$$\mathrm{ord}_2(h_n) = 4k^2 + 4k = n^2 - 1.$$

Case (iv): $k \equiv 0 \pmod 3$ and k is even imply $3 \nmid k+2$ even, $3 \nmid k-1$ odd, $3 \nmid k+1$ odd, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_k^3) &\geq (k+2)^2 - 3 + \mathrm{ord}_2(y) + 3(k^2 - 3 + \mathrm{ord}_2(y)) \\ &= 4k^2 + 4k - 8 + 4\mathrm{ord}_2(y) = 4k^2 + 4k, \end{aligned}$$

and

$$\begin{aligned} \mathrm{ord}_2(h_{k-1}h_{k+1}^3) &= (k-1)^2 - 1 + 3((k+1)^2 - 1)) \\ &= 4k^2 + 4k. \end{aligned}$$

Then

$$\mathrm{ord}_2(h_n) = 4k^2 + 4k = n^2 - 1.$$

Case (v): $k \equiv -1 \pmod 3$ and k is odd imply $3 \nmid k+2$ odd, $3 \nmid k-1$ even, $3 \mid k+1$ even, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_k^3) &= (k+2)^2 - 1 + 3(k^2-1) \\ &= 4k^2 + 4k, \end{aligned}$$

and

$$\begin{aligned} \mathrm{ord}_2(h_{k-1}h_{k+1}^3) &\geq (k-1)^2 - 3 + \mathrm{ord}_2(y) + 3((k+1)^2 - 3 + \mathrm{ord}_2(y)) \\ &= 4k^2 + 4k - 8 + 4\mathrm{ord}_2(y) = 4k^2 + 4k, \end{aligned}$$

Then

$$\mathrm{ord}_2(h_n) = 4k^2 + 4k = n^2 - 1.$$

Case (vi): $k \equiv -1 \pmod 3$ and k is even imply $3 \nmid k+2$ even, $3 \nmid k-1$ odd, $3 \mid k+1$ odd, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_k^3) &= (k+2)^2 - 3 + \mathrm{ord}_2(y) + 3(k^2 - 3 + \mathrm{ord}_2(y)) \\ &= 4k^2 + 4k - 8 + 4\mathrm{ord}_2(y) = 4k^2 + 4k, \end{aligned}$$

and

$$\begin{aligned} \mathrm{ord}_2(h_{k-1}h_{k+1}^3) &\geq (k-1)^2 - 1 + 3((k+1)^2 - 1)) \\ &= 4k^2 + 4k. \end{aligned}$$

Then

$$\mathrm{ord}_2(h_n) \geq 4k^2 + 4k = n^2 - 1.$$

Case (vii): $k \equiv 0 \pmod 3$ and k is odd imply $3 \nmid k+2$ odd, $3 \nmid k-2$ odd, $3 \nmid k-1$ even, $3 \nmid k+1$ even, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_{k-1}^2) &= \mathrm{ord}_2(h_{k+2}) + 2\mathrm{ord}_2(h_{k-1}) \\ &= (k+2)^2 - 1 + 2(k - 1^2 - 3 + \mathrm{ord}_2(y)) \\ &= 3k^2 - 1 + 2\mathrm{ord}_2(y), \end{aligned}$$

and

$$\begin{aligned} \mathrm{ord}_2(h_{k-2}h_{k+1}^2) &= \mathrm{ord}_2(h_{k-2}) + 2\mathrm{ord}_2(h_{k+1}) \\ &= (k-2)^2 - 1 + 2((k+1)^2 - 3 + \mathrm{ord}_2(y)) \\ &= 3k^2 - 1 + 2\mathrm{ord}_2(y), \end{aligned}$$

Then

$$\begin{aligned} \mathrm{ord}_2(h_n) &= \mathrm{ord}_2(h_k) - \mathrm{ord}_2(h_2) + \mathrm{ord}_2(h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2) \\ &\geq k^2 - 1 - 1 - \mathrm{ord}_2(y) + 3k^2 - 1 + 2\mathrm{ord}_2(y) \\ &= 4k^2 - 3 + \mathrm{ord}_2(y) = n^2 - 3 + \mathrm{ord}_2(y) = n^2 - 1 \end{aligned}$$

as $\mathrm{ord}_2(y) = 2$.

Case (viii): $k \equiv 0 \pmod 3$ and k is even imply $3 \nmid k+2$ even, $3 \nmid k-2$ even, $3 \nmid k-1$ odd, $3 \nmid k+1$ odd, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_{k-1}^2) &= (k+2)^2 - 3 + \mathrm{ord}_2(y) + 2(k - 1^2 - 1) \\ &= 3k^2 + 1 + \mathrm{ord}_2(y), \end{aligned}$$

and

$$\begin{aligned}\mathrm{ord}_2(h_{k-2}h_{k+1}^2) &= (k-2)^2 - 3 + \mathrm{ord}_2(y) + 2((k+1)^2 - 1) \\ &= 3k^2 + 1 + \mathrm{ord}_2(y),\end{aligned}$$

Then

$$\begin{aligned}\mathrm{ord}_2(h_n) &= \mathrm{ord}_2(h_k) - \mathrm{ord}_2(h_2) + \mathrm{ord}_2(h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2) \\ &\geq k^2 - 3 + \mathrm{ord}_2(y) - 1 - \mathrm{ord}_2(y) + 3k^2 + 1 + \mathrm{ord}_2(y) \\ &= 4k^2 - 3 + \mathrm{ord}_2(y) = n^2 - 3 + \mathrm{ord}_2(y) = n^2 - 1.\end{aligned}$$

Case (ix): $k \equiv 1 \pmod 3$ and k is odd imply $3 \mid k+2$ odd, $3 \nmid k-2$ odd, $3 \mid k-1$ even, $3 \nmid k+1$ even, so

$$\begin{aligned}\mathrm{ord}_2(h_{k+2}h_{k-1}^2) &\geq (k+2)^2 - 1 + 2(k - 1^2 - 3 + \mathrm{ord}_2(y)) \\ &= 3k^2 - 1 + 2\mathrm{ord}_2(y),\end{aligned}$$

and

$$\begin{aligned}\mathrm{ord}_2(h_{k-2}h_{k+1}^2) &= (k-2)^2 - 1 + 2((k+1)^2 - 3 + \mathrm{ord}_2(y)) \\ &= 3k^2 - 1 + 2\mathrm{ord}_2(y),\end{aligned}$$

Then

$$\begin{aligned}\mathrm{ord}_2(h_n) &= \mathrm{ord}_2(h_k) - \mathrm{ord}_2(h_2) + \mathrm{ord}_2(h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2) \\ &= k^2 - 1 - 1 - \mathrm{ord}_2(y) + 3k^2 - 1 + 2\mathrm{ord}_2(y) \\ &= 4k^2 - 3 + \mathrm{ord}_2(y) = n^2 - 3 + \mathrm{ord}_2(y) = n^2 - 1.\end{aligned}$$

Case (x): $k \equiv 1 \pmod 3$ and k is even imply $3 \mid k+2$ even, $3 \nmid k-2$ even, $3 \mid k-1$ odd, $3 \nmid k+1$ odd, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_{k-1}^2) &\geq (k+2)^2 - 3 + \mathrm{ord}_2(y) + 2(k - 1^2 - 1) \\ &= 3k^2 + 1 + \mathrm{ord}_2(y), \end{aligned}$$

and

$$\begin{aligned} \mathrm{ord}_2(h_{k-2}h_{k+1}^2) &= (k-2)^2 - 3 + \mathrm{ord}_2(y) + 2((k+1)^2 - 1) \\ &= 3k^2 + 1 + \mathrm{ord}_2(y), \end{aligned}$$

Then

$$\begin{aligned} \mathrm{ord}_2(h_n) &= \mathrm{ord}_2(h_k) - \mathrm{ord}_2(h_2) + \mathrm{ord}_2(h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2) \\ &= k^2 - 3 + \mathrm{ord}_2(y) - 1 - \mathrm{ord}_2(y) + 3k^2 + 1 + \mathrm{ord}_2(y) \\ &= 4k^2 - 3 + \mathrm{ord}_2(y) = n^2 - 3 + \mathrm{ord}_2(y) = n^2 - 1. \end{aligned}$$

Case (xi): $k \equiv -1 \pmod 3$ and k is odd imply $3 \nmid k+2$ odd, $3 \mid k-2$ odd, $3 \nmid k-1$ even, $3 \mid k+1$ even, so

$$\begin{aligned} \mathrm{ord}_2(h_{k+2}h_{k-1}^2) &= (k+2)^2 - 1 + 2((k-1)^2 - 3 + \mathrm{ord}_2(y)) \\ &= 3k^2 - 1 + 2\mathrm{ord}_2(y), \end{aligned}$$

and

$$\begin{aligned} \mathrm{ord}_2(h_{k-2}h_{k+1}^2) &\geq (k-2)^2 - 1 + 2((k+1)^2 - 3 + \mathrm{ord}_2(y)) \\ &= 3k^2 - 1 + 2\mathrm{ord}_2(y), \end{aligned}$$

Then

$$\begin{aligned}\mathrm{ord}_2(h_n) &= \mathrm{ord}_2(h_k) - \mathrm{ord}_2(h_2) + \mathrm{ord}_2(h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2)\\ &= k^2 - 1 - 1 - \mathrm{ord}_2(y) + 3k^2 - 1 + 2\mathrm{ord}_2(y)\\ &= 4k^2 - 3 + \mathrm{ord}_2(y) = n^2 - 3 + \mathrm{ord}_2(y) = n^2 - 1.\end{aligned}$$

Case (xii): $k \equiv -1 \pmod 3$ and k is even imply $3 \nmid k+2$ even, $3 \mid k-2$ even, $3 \nmid k-1$ odd, $3 \mid k+1$ odd, so

$$\begin{aligned}\mathrm{ord}_2(h_{k+2}h_{k-1}^2) &= (k+2)^2 - 3 + \mathrm{ord}_2(y) + 2(k - 1^2 - 1)\\ &= 3k^2 + 1 + \mathrm{ord}_2(y),\end{aligned}$$

and

$$\begin{aligned}\mathrm{ord}_2(h_{k-2}h_{k+1}^2) &\geq (k-2)^2 - 3 + \mathrm{ord}_2(y) + 2((k+1)^2 - 1)\\ &= 3k^2 + 1 + \mathrm{ord}_2(y),\end{aligned}$$

Then

$$\begin{aligned}\mathrm{ord}_2(h_n) &= \mathrm{ord}_2(h_k) - \mathrm{ord}_2(h_2) + \mathrm{ord}_2(h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2)\\ &= k^2 - 3 + \mathrm{ord}_2(y) - 1 - \mathrm{ord}_2(y) + 3k^2 + 1 + \mathrm{ord}_2(y)\\ &= 4k^2 - 3 + \mathrm{ord}_2(y) = n^2 - 3 + \mathrm{ord}_2(y) = n^2 - 1.\end{aligned}$$

Next, we will show the rest of the proof of Lemma 5.2.2 (p. 74). **Lemma 5.2.2:** Given an integral point of infinite order $P = (x, y) \in E_m(\mathbb{Q})$ such that $\gcd(x, m) = 1$, the points $5P$, $7P$, $11P$, and $13P$ are all non-integral.

We will give details of the proof of Lemma 5.2.2 for $\psi_5(x, m)$ only. Note that for $n = 7, 13$, $\psi_n(x, m)$ can be factorized. So we choose one of their

factors, and then proceed the same argument.

Definition B.0.20. We define an *admissible solution* of the equation

$$\psi_n(x, m) = c$$

is a solution (x, m) satisfying the properties:

(i) $m \geq 6 \in \mathbb{Z}$, cube-free,

(ii) $x, y \in \mathbb{Q}$ and $xy \neq 0$, where $y^2 = x^3 - 432m^2$.

Consider the resultant between $\phi_5(x, m)$ and $\psi_5(x, m)$, which is

$$2^{600}3^{450}m^{200}.$$

From the assumption that $\gcd(x, m) = 1$, we have that any common factor of ϕ_5 and ψ_5 has to divide $2^{600}3^{450}$. So the result will be completed after we can show that the solutions of the following equations

$$\psi_5(x, m) = 5x^{12} - 164160m^2x^9 - 44789760m^4x^6 + 128994508800m^6x^3 - 8916100448256m^8 = 2^a3^b,$$

for $0 \leq a \leq 600$ and $0 \leq b \leq 450$, are all not admissible solutions.

Firstly, we will simplify all possible values of the exponents a. Let $f(x, m) := \psi_5(x, m)$. We could have $a = 0$.

Suppose $a > 0$. Then $2 \mid x$, write $x = 2x_1$, so

$$f(x, m) = 2^{12}f_1(x_1, m),$$

where $f_1(x_1, m) = 5x_1^{12} - 20520m^2x_1^9 - 699840m^4x_1^6 + 251942400m^6x_1^3 - 2176782336m^8$. This implies that a could be 12.

Suppose $a > 12$. Then $2 \mid x_1$, write $x_1 = 2x_2$, and

$$f_1(x_1, m) = 2^{12}f_2(x_2, m),$$

where $f_2(x_2, m) = 5x_2^{12} - 2565m^2x_2^9 - 10935m^4x_2^6 + 492075m^6x_2^3 - 531441m^8$. So $a = 12 + 12 = 24$.

Suppose $a > 24$. Then $2 \mid x_2$ and $2 \mid m$, which is impossible as $\gcd(x, m) = 1$. Thus we could have $a = 0, 12, 24$.

The argument to simplify the values of b is slightly different. We begin by giving $f(x, m) = \psi_5(x, m)$ again. Suppose $b > 0$. Since $\gcd(x, m) = 1$, we omit the case $3 \mid x$ and $3 \mid m$. If $3 \nmid x$ and $3 \mid m$, then $3 \nmid \psi_5(x, m)$, from the expression of ψ_5.

Now suppose $3 \mid x$ and $3 \nmid m$, then replacing $x = 3x_1$ to $\psi_5(x, m)$ implies

$$f(x, m) = 3^{12} f_1(x_1, m)$$

with $f_1(x_1, m) = 5x_1^{12} - 6080m^2x_1^9 - 61440m^4x_1^6 + 6553600m^6x_1^3 - 16777216m^8$. Then we have $b = 12$. Suppose $b > 12$. Substituting $r := \dfrac{x_1^3}{m^2}$ in $f_1(x_1, m)$ gives a non-monic polynomial in r,

$$F(r) = 5r^4 - 6080r^3 - 61440r^2 + 6553600r - 16777216.$$

We can check that

(i) $F(r) \equiv 2r^4 + r^3 + r + 2 \pmod 3$,

(ii) all roots of $F(r) = 0$ are $1 \pmod 3$ only.

Thus if $F(r)$ is divisible by 3, then $r = 1 + 3s$ for some $s \in \mathbb{Z}$. We find that

$$\begin{aligned} F(1 + 3s) &= 405s^4 - 163620s^3 - 716850s^2 + 19237500s - 10291131 \\ &= 3^4 G(s), \end{aligned}$$

where $G(s) = 5s^4 - 2020s^3 - 8850s^2 + 237500s - 127051$, so that $b = 12 + 4 = 16$. Repeating this approach again for $G(s)$, we get

(i) $G(s) \equiv 2s^4 + 2s^3 + 2s + 2 \pmod 3$,

(ii) all roots of $G(s)$ are 2 (mod 3) only.

If $G(s)$ is divisible by 3, then $s = 2 + 3t$ for some $t \in \mathbb{Z}$, and

$$G(2+3t) = 405t^4 - 53460t^3 - 187650t^2 + 534060t + 296469 = 3^2 H(t),$$

where $H(t) = 45t^4 - 5940t^3 - 20850t^2 + 59340t + 32941$. Then $b = 16 + 2 = 18$. We can check that $H(t)$ is never divisible by 3 at all. Thus we can summarize all possible values of b as $0, 12, 16, 18$.

Finally, we will solve a finite number of equations of the form

$$\psi_5(x, m) = \pm 2^a 3^b,$$

with a, b as above. Since $\psi_5(x, m)$ is homogeneous in x^3 and m^2, we replace $X = x^3$ and $M = m^2$ in $\psi_5(x, m)$. Then the equations become Thue equations. The following tables show all solutions (X, M) of Thue equations obtained by computing with PARI/GP and MAGMA. We can see that all solutions lead to non-admissible solutions. Note that the symbol [ ] in the tables means there is no solutions in those cases.

For other n, the expressions for $\psi_n(x, m)$, or $\psi_{n'}(x, m)$, a factor of $\psi_n(x, m)$, are given below.

$\psi_{7'}(x, m) = x^{18} - 2^6 3^4 47^1 m^2 x^{15} - 2^{12} 3^7 11^2 m^4 x^{12} + 2^{20} 3^9 13^1 37^1 m^6 x^9 -$
$2^{24} 3^{13} 13^1 19^1 m^8 x^6 + 2^{34} 3^{16} m^{10} x^3 + 2^{36} 3^{18} m^{12}.$

$\psi_{11}(x, m) = 11x^{60} - 2^6 3^3 11^1 2111^1 m^2 x^{57} - 2^{12} 3^6 11^1 17^1 31^1 199^1 m^4 x^{54} +$
$2^{18} 3^{10} 11^1 587^1 3203^1 m^6 x^{51} + 2^{25} 3^{13} 7^1 11^1 43^1 3329^1 m^8 x^{48} +$
$2^{30} 3^{16} 11^1 5477^1 8831^1 m^{10} x^{45} - 2^{36} 3^{19} 11^2 449^1 52639^1 m^{12} x^{42} +$
$2^{42} 3^{22} 11^2 13113091^1 m^{14} x^{39} - 2^{48} 3^{25} 11^2 61487^1 m^{16} x^{36} -$

$$2^{56}3^{27}11^{1}53^{1}3453997^{1}m^{18}x^{33} + 2^{60}3^{30}11^{2}157^{1}557747^{1}m^{20}x^{30} -$$

$$2^{66}3^{33}11^{1}17^{1}433^{1}60139^{1}m^{22}x^{27} + 2^{72}3^{37}7^{1}11^{1}17^{2}73^{1}227^{1}m^{24}x^{24} -$$

$$2^{78}3^{40}5^{1}11^{1}13^{1}88523^{1}m^{26}x^{21} + 2^{85}3^{43}11^{1}131^{1}6869^{1}m^{28}x^{18} -$$

$$2^{90}3^{46}11^{1}527069^{1}m^{30}x^{15} + 2^{96}3^{49}11^{1}89^{1}773^{1}m^{32}x^{12} -$$

$$2^{102}3^{52}11^{2}283^{1}m^{34}x^{9} + 2^{108}3^{54}5^{1}11^{2}m^{36}x^{6} + 2^{115}3^{57}11^{2}m^{38}x^{3} - 2^{120}3^{60}m^{40}.$$

$$\psi_{13'}(x,m) = x^{72} - 2^{8}3^{4}479^{1}m^{2}x^{69} - 2^{13}3^{7}133073^{1}m^{4}x^{66} +$$

$$2^{20}3^{9}281^{1}99233^{1}m^{6}x^{63} + 2^{25}3^{13}131^{1}872033^{1}m^{8}x^{60} +$$

$$2^{30}3^{16}11^{1}11353^{1}60149^{1}m^{10}x^{57} - 2^{36}3^{18}151^{1}881^{1}1977817^{1}m^{12}x^{54} -$$

$$2^{42}3^{23}5^{1}2789^{1}3214811^{1}m^{14}x^{51} + 2^{52}3^{26}12824767049^{1}m^{16}x^{48} -$$

$$2^{58}3^{27}19^{1}61^{1}101^{1}701413^{1}m^{18}x^{45} + 2^{62}3^{31}53^{1}709001219^{1}m^{20}x^{42} -$$

$$2^{76}3^{34}43^{1}191^{1}11261^{1}m^{22}x^{39} + 2^{72}3^{36}43^{1}113^{1}4421^{1}27127^{1}m^{24}x^{36} -$$

$$2^{79}3^{40}43^{1}83^{1}24921151^{1}m^{26}x^{33} + 2^{84}3^{43}7^{1}23^{1}43^{1}317^{1}32803^{1}m^{28}x^{30} -$$

$$2^{92}3^{45}53^{1}203389231^{1}m^{30}x^{27} + 2^{97}3^{50}199806241^{1}m^{32}x^{24} +$$

$$2^{102}3^{53}37^{1}47^{1}40361^{1}m^{34}x^{21} - 2^{108}3^{54}5^{1}11^{1}7527977^{1}m^{36}x^{18} +$$

$$2^{115}3^{58}337^{1}45317^{1}m^{38}x^{15} - 2^{120}3^{61}2088139^{1}m^{40}x^{12} -$$

$$2^{128}3^{63}5^{1}4621^{1}m^{42}x^{9} - 2^{132}3^{67}5749^{1}m^{44}x^{6} +$$

$$2^{139}3^{70}59^{1}m^{46}x^{3} + 2^{144}3^{72}m^{48}.$$

$b\backslash a$	0	12	24
0	[ ]	[ ]	[ ]
12	[ ]	[ ]	[ ]
16	[ ]	[ ]	[ ]
18	[ ]	[ ]	[-8640, -4] [17280, -1] [-17280, 1] [8640, 4]

Table B.1: $\psi_5 = 2^a 3^b$

$b\backslash a$	0	12	24
0	[ ]	[ ]	[ ]
12	[ ]	[ ]	[0, -1] [0, 1]
16	[ ]	[ ]	[0, -3] [8640, -2] [-8640, -1] [8640, 1] [-8640, 2] [0, 3]
18	[ ]	[ ]	[ ]

Table B.2: $\psi_5 = -2^a 3^b$

$b\backslash a$	0	18	36
0	[1, 0] [-1, 0]	[8, 0] [-8, 0]	[64, 0] [-64, 0]
18	[27, 0] [-27, 0]	[216, 0] [-216, 0]	[1728, 0] [-1728, 0] [0, -1] [0, 1]
24	[81, 0] [-81, 0]	[648, 0] [-648, 0]	[5184, 0] [-5184, 0] [0, -3] [-1728, -1] [1728, 1] [0, 3]
27	[ ]	[ ]	[ ]

Table B.3: $\psi_{7'} = 2^a 3^b$

$b\backslash a$	0	18	36
0	[ ]	[ ]	[ ]
18	[ ]	[ ]	[ ]
24	[ ]	[ ]	[ ]
27	[ ]	[ ]	[-1728, -4] [3456, -1] [-3456, 1] [1728, 4]

Table B.4: $\psi_{7'} = -2^a 3^b$

$b\backslash a$	0	60	120
0	[ ]	[ ]	[ ]
60	[ ]	[ ]	[ ]
80	[ ]	[ ]	[ ]
90	[ ]	[ ]	[ ]

Table B.5: $\psi_{11} = 2^a 3^b$

$b\backslash a$	0	60	120
0	[ ]	[ ]	[ ]
60	[ ]	[ ]	[0, -1] [0, 1]
80	[ ]	[ ]	[0, -3] [-297, -1] [297, 1] [0, 3]
90	[ ]	[ ]	[-297, -4] [594, -1] [-594, 1] [297, 4]

Table B.6: $\psi_{11} = -2^a 3^b$

$b\backslash a$	0	72	144
0	[1, 0] [-1, 0]	[1, 0] [-1, 0]	[1, 0] [-1, 0]
72	[27, 0] [-27, 0]	[27, 0] [-27, 0]	[0, 1] [0, -1] [27, 0] [-27, 0]
96	[81, 0] [-81, 0]	[81, 0] [-81, 0]	[81, 0] [-81, 0] [0, -3] [-27, -1] [27, 1] [0, 3]
108	[ ]	[ ]	[-27, -4] [54, -1] [-54, 1] [27, 4]

Table B.7: $\psi_{13'} = 2^a 3^b$

$b\backslash a$	0	72	144
0	[ ]	[ ]	[ ]
72	[ ]	[ ]	[ ]
96	[ ]	[ ]	[ ]
108	[ ]	[ ]	[ ]

Table B.8: $\psi_{13'} = -2^a 3^b$

Appendix C

Computation II

In this chapter, we compute all non-torsion integral points on the curves $E : Y^2 = X^3 - 432m^2$ with $6 \leq m \leq 719$, cube-free which satisfy

(i) $(X(P), 3m) = 1$, and

(ii) $2P$ and $3P$ are non-integral.

The following table presents all such integral points. We can see that all curves with m in this table contain only one point. Thus the result of Theorem 5.2.5 is true for these curves.

m	Integral Points
9	[73, 595]
15	[49, 143]
30	[241, 3689]
33	[97, 665]
69	[553, 12925]
75	[601, 14651]
78	[217, -2755]
105	[169, 253]
114	[313, 5005]
132	[1057, -34255]
195	[1561, 61541]
210	[361, -5291]
273	[337, -2465]
282	[2257, 107065]
285	[481, 8729]

m	Integral Points
294	[2353, -113975]
345	[409, 4123]
348	[937, -27755]
357	[457, 6355]
399	[3193, -180235]
420	[1129, 36917]
429	[433, 1295]
435	[721, 17119]
450	[481, 4879]
555	[1489, 56287]
609	[673, 12025]
639	[5113, 365365]
645	[1729, 70633]
651	[793, -17765]
657	[5257, 380915]

Bibliography

[1] A. Baker. Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms. *Philos. Trans. Roy. Soc. London Ser. A*, 263:173–191, 1967/1968.

[2] Paul T. Bateman and Roger A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[3] Yuri Bilu and Guillaume Hanrot. Solving Thue equations of high degree. *J. Number Theory*, 60(2):373–392, 1996.

[4] E. Bombieri and W. M. Schmidt. On Thue's equation. *Invent. Math.*, 88(1):69–81, 1987.

[5] R. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15(1-4):30–48, 1913/14.

[6] 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(4):385–434, 1986.

[7] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[8] Sinnou David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, (62):iv+143, 1995.

[9] Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in elliptic divisibility sequences. *LMS J. Comput. Math.*, 4:1–13 (electronic), 2001.

[10] Graham Everest, Patrick Ingram, and Shaun Stevens. Primitive divisors on twists of Fermat's cubic. *LMS J. Comput. Math.*, 12:54–81, 2009.

[11] Graham Everest, Victor Miller, and Nelson Stephens. Primes generated by elliptic curves. *Proc. Amer. Math. Soc.*, 132(4):955–963 (electronic), 2004.

[12] Graham Everest and Thomas Ward. *An introduction to number theory*, volume 232 of *Graduate Texts in Mathematics*. Springer-Verlag London Ltd., London, 2005.

[13] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[14] M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988.

[15] Patrick Ingram. Multiples of integral points on elliptic curves. *J. Number Theory*, 129(1):182–208, 2009.

[16] Tomasz Jedrzejak. Height estimates on cubic twists of the Fermat elliptic curve. *Bull. Austral. Math. Soc.*, 72(2):177–186, 2005.

[17] Helen King. *Prime appearance in elliptic divisibility sequences*. PhD thesis, School of Mathematics, University of East Anglia, 2005.

[18] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[19] Serge Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1978.

[20] *MAGMA, Version V2.14-16*. University of Sydney. `http://magma.maths.usyd.edu.au/magma/`.

[21] *MAPLE, Version 9.5*. Waterloo. `http://www.maplesoft.com`.

[22] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Cambr. Phil. Soc. Proc.*, 21:179–192, 1922.

[23] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons Inc., New York, fifth edition, 1991.

[24] *SAGE Notebook V4.1.1*. `http://www.sagemath.org/`.

[25] C. L. Siegel. The integral solutions of the equation $y^2 = ax^n + bx^{n-1} \cdots k$. *J. London Math. Soc.*, 1:66–68, 1926.

[26] Joseph 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.

[27] Joseph H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

[28] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[29] Macro Streng. Elliptic divisibility sequences with complex multiplication. Master's thesis, Universiteit Utrecht, 2006.

[30] R. J. Stroeker and N. Tzanakis. On the application of Skolem's p-adic method to the solution of Thue equations. *J. Number Theory*, 29(2):166–195, 1988.

[31] The PARI Group, Bordeaux. *PARI/GP, Version 2.3.2*, 2005. `http://pari.math.u-bordeaux.fr/`.

[32] A. Thue. Über annäherungswerte algebraischer zahlen. *J. Reine Angew. Math.*, 135, 1909.

[33] B. L. van der Waerden. *Modern Algebra. Vol. I.* Frederick Ungar Publishing Co., New York, N. Y., 1949. Translated from the second revised

German edition by Fred Blum, With revisions and additions by the author.

[34] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.

[35] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

[36] W. A. Webb and E. A. Parberry. Divisibility properties of Fibonacci polynomials. *Fibonacci Quart.*, 7(5):457–463, 1969.