THE SIGNS IN AN ELLIPTIC NET

MANOJ KUMAR
Bachelor of Science, Panjab University, Chandigarh, 2005
Master of Science, Panjab University, Chandigarh, 2007

A Thesis
Submitted to the School of Graduate Studies
of the University of Lethbridge
in Partial Fulfillment of the
Requirements for the Degree

MASTER OF SCIENCE

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

THE SIGNS IN AN ELLIPTIC NET

MANOJ KUMAR

Approved:

Signature *Date*

Co-Supervisor: Dr. Soroosh Yazdani

Co-Supervisor: Dr. Amir Akbary

Committee Member: Dr. Habiba Kadiri

Committee Member: Dr. Pascal Ghazalian

Chair, Thesis Examination Committee: Dr. Hadi Kharaghani

Dedication

For my parents

Abstract

Let A be a finitely-generated free abelian group, and let R be an integral domain. An *elliptic net* is a map $W : A \longrightarrow R$ with $W(0) = 0$, such that for all $p, q, r, s \in A$,

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\quad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\quad + W(r+p+s)W(r-p)W(q+s)W(q) = 0. \end{aligned}$$

Let E be an elliptic curve defined over a field K. Let $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ be an n-tuple of points in $E(K)$, the group of K-rational points on E. An important example of an elliptic net is $\Psi(\mathbf{P}; E)$, the elliptic net associated to E and P.

In this thesis the following results are proved:

1. For an elliptic curve E defined over $\mathbb{R}$ and $\mathbf{P} = (P_1, P_2, \ldots, P_n)$, an n-tuple of linear independent points in $E(\mathbb{R})^n$, let $\Psi(\mathbf{P}; E)$ be the elliptic net associated to E and $\mathbf{P}$. For $\mathbf{v} = (v_1, v_2, \ldots v_n) \in \mathbb{Z}^n$ we give an explicit formula for the sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$, the value of $\Psi(\mathbf{P}; E)$ at $\mathbf{v}$.

2. For any non-singular, non-degenerate elliptic net $W : \mathbb{Z}^n \longrightarrow \mathbb{R}$ and $\mathbf{v} = (v_1, v_2, \ldots v_n) \in \mathbb{Z}^n$ we give a formula to compute the sign of $W(\mathbf{v})$ up to the sign of a quadratic form.

3. For a rank one elliptic net we prove that the distribution of the signs is uniform.

4. For an elliptic curve E defined over $\mathbb{Q}$ and an n-tuple of linear independent points $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ in $E(\mathbb{Q})^n$. For every prime ℓ let $P_i \pmod{\ell}$ is non-

singular for each $1 \leq i \leq n$. If $(D_{\mathbf{v}\cdot P})$ is the elliptic denominator net associated to E and $\mathbf{P}$ (defined in 5.2), we give a way to assign signs to the net $(D_{\mathbf{v}\cdot P})$ such that it becomes an elliptic net.

Acknowledgments

I would like to thank everyone that helped me during my two years of study in Lethbridge. First of all I thank my supervisors Dr. Soroosh Yazdani and Dr. Amir Akbary. I am specially thankful to Dr. Soroosh Yazdani for giving me the opportunity to work with him. I would also like to say a special thank you to Dr. Amir Akbary for all the time spent guiding me throughout this thesis. I want to thank my committee members, Dr. Habiba Kadiri and Dr. Pascal Ghazalian for serving as my committee members. I would also like to thank Dr. Hadi Kharaghani for serving as Chair of my examination committee.

There are some special people that I want to thank. I am grateful to Allysa Lumley who made me feel not like an outsider and Jeff Bleaney for all the loud discussions we had. The other friends that helped me succeed and made me not to miss my home are Fariha Naz, Sara Sasani, Adela Gherga, Jayati Law, Ram Dahal, Mohammad Akbari, Farzad Aryan, Jim Parks, and Adam Felix. All of these people were there to support me when I needed throughout my stay at Lethbridge. I would also like to thank my friends in India who guided me all the way through my life, Preetinder Singh, Pankaj Narula, Naveen Garg, Ajay Chhabra, Shiv Parsad, Jay Pee, and Amit Kaura.

A very warm and special thanks to my family. I cannot express how grateful I am to my mother, father, brothers Pankaj and Neeraj, and my sister Suman for all the sacrifices that they have made on my behalf. I would also like to express my love for my nieces Kashish, Radha, Anushka and nephew Aditya for cheering me up during my studies.

Contents

List of Tables

List of Figures

Chapter 1

Introduction and Statement of the Results

1.1 Introduction

An *elliptic divisibility sequence* (W_n) is a sequence of integers satisfying the non-linear recurrence

$$W_{m+n}W_{m-n} = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 \tag{1.1}$$

for all $m \geq n \geq 1$ and such that $W_n | W_m$ whenever $n|m$.

In 1948, M. Ward [14] introduced this concept of an elliptic divisibility sequence and studied arithmetic properties of such sequences. He also studied the relation of elliptic divisibility sequences with elliptic curves and elliptic functions. The following are some examples of an elliptic divisibility sequences.

Example 1.1.1. $W_n = (0)$ and $W_n = (n)$ are trivial examples of elliptic divisibility sequences. Some other examples are:

1. $W_n = (n/3)$, where (n/p) is the Legendre symbol.

2. $(W_n) = 1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -23, 29, 59, 129, -314, -65, 1529, -3689, \ldots$

3. $(W_n) = 1, 1, 2, 1, -7, -16, -57, -113, 670, 3983, 23647, 140576, -833503, -14871471$
$$-147165662, -2273917871, 11396432249, \ldots$$

A fundamental fact in Ward's investigation was the connection of sequences satisfying (1.1) with elliptic curves and elliptic functions. For example elliptic divisibility sequences in parts 2 and 3 in the above example are related to the elliptic curves given by $y^2+y=x^3-x$ and $y^2+xy+y=x^3+x^2-416x+3009$ respectively. The relation is given via elliptic functions and is described in detail in Chapter 3. This was Ward's fundamental result in his memoir. More precisely Ward proved the following theorem.

Theorem 1.1.2 (Ward). *Let (W_n) be a non-singular, non-degenerate elliptic divisibility sequence. Then there is a lattice $\Lambda \subset \mathbb{C}$ and a complex number $z \in \mathbb{C}$ such that*

$$W_n = \frac{\sigma(nz;\Lambda)}{\sigma(z;\Lambda)^{n^2}} \quad for\ all\ n \geq 1. \tag{1.2}$$

The function $\sigma(z)$ in the above theorem is the Weierstrass σ-function defined in Section 2.2.2. See Definitions 2.2.1, 3.1.2, and 3.2.5 for the other relevant definitions.

Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$ be a non-torsion point, where $E(\mathbb{Q})$ is the group of $\mathbb{Q}$-rational points on E. Then for each $n \geq 1$ we can write

$$nP = \left(\frac{A_{nP}}{D_{nP}^2},\ \frac{B_{nP}}{D_{nP}^3}\right),$$

(see Proposition 5.2.1).

The sequence (D_{nP}) is called the *elliptic denominator sequence* associated to E and P. The construction of elliptic denominator sequences via rational points on elliptic curves gives rise to a sequence of positive integers, whereas the recurrence (1.1) yields a sequence of signed integers. It can be proved that (D_{nP}) is a divisibility sequence. Moreover, Shipsey [8] showed that if the signs are chosen correctly then (D_{nP}) can be made into an elliptic divisibility sequence. Thus it is interesting to know about the behavior of the signs of an elliptic divisibility sequence. In [11] Silverman and Stephens answered the question about the behavior of signs in an elliptic divisibility sequence and they gave a formula for the signs of the terms of an elliptic divisibility

sequence. In order to state their theorem we need the following definition.

Definition 1.1.3. Let x be any real number. Then the *Parity* of x is defined as

$$\text{Sign}(x) = (-1)^{\text{Parity}(x)} \qquad \text{with Parity}(x) \in \mathbb{Z}/2\mathbb{Z}.$$

Observe that, $\text{Sign}(x) = 1$ if and only if $\text{Parity}(x) \equiv 0 \pmod 2$ and $\text{Sign}(x) = -1$ if and only if $\text{Parity}(x) \equiv 1 \pmod 2$.

Theorem 1.1.4 (Silverman-Stephens). *Let (W_n) be an non-singular, non-degenerate elliptic divisibility sequence. Then possibly after replacing (W_n) by the related sequence $((-1)^{n-1}W_n)$, there is an irrational number $\beta \in \mathbb{R}$ so that the parity of W_n is given by one of the following formulas:*

$$\text{Parity}(W_n) = \lfloor n\beta \rfloor \qquad for\ all\ \ n.$$

$$\text{Parity}(W_n) = \begin{cases} \lfloor n\beta \rfloor + n/2 & if\ n\ is\ even, \\ (n-1)/2 & if\ n\ is\ odd, \end{cases}$$

where $\lfloor . \rfloor$ denotes the greatest integer function.

The number β in the above theorem can be calculated explicitly using the elliptic curve associated to (W_n) (see [11, Appendix A] for details on elliptic curves related to (W_n)).

In 2008 K. Stange in her Ph.D. thesis [12] gave a higher-dimensional analogue of elliptic divisibility sequences called *elliptic nets*. Thus generalizes the recurrence (1.1) to the following recurrence relation

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\qquad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\qquad\qquad + W(r+p+s)W(r-p)W(q+s)W(q) = 0, \end{aligned}$$

where $W : A \longrightarrow R$ is a map from a finitely generated free abelian group A to an integral domain R. She also generalized the concept of *division polynomials* to *net polynomials* and using them she proved that under certain conditions there is a one to one correspondence between elliptic nets and elliptic curves. In other words, there exists a bijection which takes an elliptic net of rank n to the tuple of an elliptic curve and n-points on it (See Section 3.5).

In this thesis, we generalize Theorem 1.1.4 to elliptic nets. More precisely, we give a formula to compute the signs of the values of the net polynomials. Furthermore, under some conditions we give a formula to compute the signs in an elliptic net up to the sign of a *quadratic form*. We introduce some of the results proved in this thesis in the next section.

1.2 Statements of the Results

The first result of this thesis gives a formula to compute the sign of any term of an elliptic net $\Psi(\mathbf{P}; E)$ associated to an elliptic curve E and a collection of points $\mathbf{P}$ on it (see Definition 3.4.4).

Theorem 1.2.1. *Let E be an elliptic curve defined over $\mathbb{R}$ and $\Lambda \subset \mathbb{C}$ be its corresponding lattice. Let $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ be an n-tuple consisting of n linearly independent points in $E(\mathbb{R})$, and $u_i \longmapsto P_i$ be the corresponding real numbers under the isomorphism $E(\mathbb{R}) \cong \mathbb{R}/q^{\mathbb{Z}}$. For $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$ let $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ be the value of the $\mathbf{v}$-th net polynomial at $\mathbf{P}$. Then there are n irrational numbers $\beta_1, \beta_2, \ldots, \beta_n$, which are $\mathbb{Q}$-linearly independent, given by the rules in the following table*

so that, possibly after replacing $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ with $(-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \le i < j \le n} v_i v_j - 1} \Psi_{\mathbf{v}}(\mathbf{P}; E)$, the

q	β_i
$0 < q < 1$	$\log_q \lvert u_i \rvert$
$-1 < q < 0$	$\frac{1}{2}\log_{\lvert q \rvert} u_i$

Table 1.1: Explicit expressions for β_i

parity of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ *is given by one of the following formulas:*

$$\text{Parity}(\Psi_{\mathbf{v}}(\mathbf{P}; E)) \equiv \left\lfloor \sum_{i=1}^{n} v_i \beta_i \right\rfloor + \sum_{1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \pmod 2, \tag{1.3}$$

$$\text{Parity}(\Psi_{\mathbf{v}}(\mathbf{P}; E)) \equiv \begin{cases} \displaystyle\sum_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \\ \displaystyle + \Big\lfloor \sum_{i=1}^{n} v_i \beta_i \Big\rfloor + \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \displaystyle\sum_{i=1}^{k} v_i \text{ is even,} \\ \displaystyle\sum_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \\ \displaystyle + \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \displaystyle\sum_{i=1}^{k} v_i \text{ is odd,} \end{cases} \tag{1.4}$$

In the above theorem for a fixed elliptic curve E each irrational number β_i corresponds to the point P_i in $E(\mathbb{R})$ and can be computed explicitly.

The next theorem gives a formula for the signs in any general non-singular, non-degenerate elliptic net up to the sign of a *quadratic form* (see Definition 3.3.7).

Theorem 1.2.2. *Let* $W : \mathbb{Z}^n \longrightarrow \mathbb{R}$ *be a non-singular, non-degenerate elliptic net. Then possibly after replacing* $W(\mathbf{v})$ *with* $f(\mathbf{v})W(\mathbf{v})$ *for a quadratic form* $f : \mathbb{Z}^n \longrightarrow \mathbb{R}^*$ *there are* n *irrational numbers* $\beta_1, \beta_2, \cdots, \beta_n$ *given by the rule in the Table 1.1 and can be calculated using an elliptic curve associated to* W *and points on it. Then the*

parity of $W(\mathbf{v})$ *is given by one of the following formulas:*

$$\text{Parity}[W(\mathbf{v})] \equiv \left\lfloor \sum_{i=1}^{n} v_i\beta_i \right\rfloor \pmod 2.$$

$$\text{Parity}[W(\mathbf{v})] \equiv \begin{cases} \left\lfloor \sum_{i=1}^{n} v_i\beta_i \right\rfloor + \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \sum_{i=1}^{k} v_i \text{ is even} \\ \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \sum_{i=1}^{k} v_i \text{ is odd .} \end{cases}$$

The next two results are regarding the applications of our main theorems introduced above. The first application is regarding the distribution of signs in an elliptic net.

Theorem 1.2.3. *Let* $W : \mathbb{Z} \longrightarrow \mathbb{R}$ *be an elliptic sequence. Then the sequence* $(\text{Sign}[W(n)])$*, of signs of the terms of an elliptic sequence, is uniformly distributed.*

The next proposition gives a way to assign signs to each terms of an elliptic denominator net so that it results in an elliptic net.

Proposition 1.2.4. *Let* $E/\mathbb{Q}$ *be an elliptic curve. Let* $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ *be an* n*-tuple of linear independent points in* $E(\mathbb{Q})$*. Let* ℓ *be a prime so that* $P_i \pmod \ell$ *is non-singular for* $1 \leq i \leq n$*. Define a map* $W(\mathbf{v}) : \mathbb{Z}^n \longrightarrow \mathbb{Q}$ *as*

$$W(\mathbf{v}) = (-1)^{Parity[\Psi_{\mathbf{v}}(\mathbf{P};E)]} D_{\mathbf{v}\cdot P},$$

where $\Psi(\mathbf{P}; E)$ *is the elliptic net associated to* E *and a collection of points* $\mathbf{P}$*. Then* $W(\mathbf{v})$ *is an elliptic net.*

The structure of the thesis is as follows.

In chapter 2 we give necessary background required to read this thesis. First two sections deal with the theory of elliptic curves and elliptic functions. Third section is devoted to the study of division polynomials. The last two sections of this chapter

describe the product expansions and the geometry of elliptic curves defined over field of real numbers.

In chapter 3 we define the concept of elliptic sequences and their generalizations to elliptic nets. We also give details on elliptic divisibility sequences and state Silverman-Stephens' result regarding the sign of an elliptic divisibility sequence. This chapter also deals with the constructions of net polynomials. Finally in the last section we study the relationship between elliptic nets and elliptic curves.

In chapter 4 we state and prove the main results of this thesis. Our first main result, Theorem 1.2.1, is regarding the signs in an elliptic net associated to an elliptic curve and a collection of points on it. The second main result, Theorem 1.2.2, is related to the signs in any non-singular, non-degenerate elliptic net. These theorems generalize the result of Silverman-Stephens about the behavior of signs in an elliptic divisibility sequence to the case of elliptic nets. Some examples illustrating the various cases of the main theorem are also given in this chapter.

Finally in chapter 5 we give some applications to the results obtained in Chapter 4. First application, Theorem 1.2.3, is related to the distribution of the signs in an elliptic net of rank 1. We prove that the signs in an elliptic net of rank 1 are uniformly distributed. The second application, Proposition 1.2.4, is regarding the elliptic denominator net. We give a way to assign signs to terms of an elliptic denominator net such that it becomes an elliptic net.

Chapter 2

Preliminaries

This chapter describes the background on elliptic curves and elliptic functions. To know more on elliptic curves see [9] and [10]. Details on elliptic functions can be found in [5]. We start with the section on *elliptic curves*.

2.1 Elliptic Curves

An *elliptic curve* defined over a field K, is a non-singular cubic curve in two variables x and y of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. There is a specified point $\mathcal{O} = [0 : 1 : 0]$ called point at infinity. We denote an elliptic curve over K with E/K. Equation (2.1) is known as the *generalized Weierstrass equation* of an elliptic curve. Geometrically the term non-singular means that the graph of the curve has no cusp or self-intersection. When working with the elliptic curve defined over a field of characteristic $\neq 2, 3$, there is a simpler form of (2.1). If characteristic of underlying field is not equal to 2, we can divide by 2 and complete the square as follows

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right),$$

which we can write as

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6',$$

where $y_1 = y + a_1x/2 + a_3/2$ and a_2', a_4', a_6' are constants. Further if the characteristic of the field is not 3, then by letting $x_1 = x + a_2'/3$ we get $y_1^2 = x_1^3 + Ax_1 + B$, or equivalently

$$y^2 = x^3 + Ax + B, \tag{2.2}$$

for some constants A and B. Equation (2.2) is know as the *Weierstrass equation* of an elliptic curve. Since E is non-singular, the cubic $x^3 + Ax + B$ does not have any repeated roots, or equivalently, the discriminant of the Weierstrass equation (2.2) given by $\Delta = -16(4A^3 + 27B^2)$ is non-zero.

Definition 2.1.1. Let E/K be an elliptic curve given by $f(x, y) = 0$, where $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$. Let P be any point on the curve $f(x, y) = 0$. We say that the P is a *singular point* if

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

If P is not a singular point we call it *non-singular*.

Any elliptic curve can be equipped with a group law. The next section describes this fact in detail.

2.1.1 The Group law for Elliptic Curves

Let E be an elliptic curve defined over a field K. Then

$$E(K) = \{(x, y) \in K \times K \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

denotes the set of K-rational points on E. It is possible to define a group operation on $E(K)$. We define the *composition law* $\oplus$ on $E(K)$ as follows:

Let $P, Q \in E(K)$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to $E(K)$ at P), and let R be the third point of intersection of L with $E(K)$. Let L' be the line through R and $\mathcal{O}$. Then L' intersects $E(K)$ at $R, \mathcal{O}$, and a third point. Denote that third point by $P \oplus Q$.

The next proposition give some properties of the above composition law under which $E(K)$ will be an abelian group.

Proposition 2.1.2. *Let P, Q, and R be in $E(K)$ and let $\mathcal{O}$ be the point at infinity. Then the above described composition law $\oplus$ on $E(K)$ has following properties.*

(a) If a line L intersects E at the points P, Q, R (not necessarily distinct), then $(P \oplus Q) \oplus R = \mathcal{O}$.

(b) $P \oplus \mathcal{O} = P$.

(c) For every P in $E(K)$, there is a point, denoted by $\ominus P$ in $E(K)$ such that $P \oplus (\ominus P) = \mathcal{O}$.

(d) $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

(e) $P \oplus Q = Q \oplus P$

Thus $(E(K), \oplus)$ is an abelian group.

Proof. See [9, Chapter III, Proposition 2.2]. □

The composition law is given geometrically in Figure 2.1.

For the purpose of this thesis we are mostly interested in elliptic curves defined over the fields $\mathbb{C}$ or $\mathbb{R}$. Since an elliptic curve over $\mathbb{R}$ can also be viewed as an elliptic curve over $\mathbb{C}$, so for most parts we will be restricting our attention to the elliptic curves defined over $\mathbb{C}$. In the case that $K = \mathbb{C}$, the group of $\mathbb{C}$-rational points, denoted by $E(\mathbb{C})$ has a simple structure. In order to study elliptic curves over complex numbers we need to introduce some topics form the theory of *elliptic functions*.

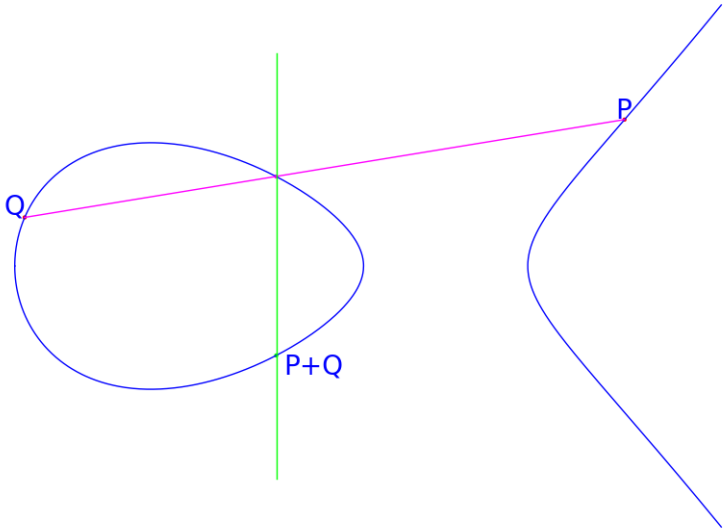

Figure 2.1: Addition of points on an elliptic curve

2.2 Elliptic Functions

In order to define elliptic functions we need the following definitions. We start with the concept of a *lattice.*

Definition 2.2.1. A *lattice* Λ is a discrete subgroup of $\mathbb{C}$ generated by ω_1 and ω_2. That is

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\},$$

where $\omega_1, \omega_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent. $[\omega_1, \omega_2]$ is called a basis for Λ.

Definition 2.2.2. A function f of a complex variable is called *doubly periodic* (with respect to Λ) if

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

for all $z \in \mathbb{C}$ and $\omega \in \Lambda$.

Equivalently, we say that a function f is doubly periodic if and only if

$$f(z + \omega_1) = f(z + \omega_2) = f(z)$$

for $\mathbb{R}$-linearly independent $\omega_1, \omega_2 \in \mathbb{C}$ and $z \in \mathbb{C}$.

Definition 2.2.3. A function f (with respect to Λ) is called an *elliptic function* if it has the following two properties:

(a) f is doubly periodic.

(b) f is meromorphic (i.e., its singularities are only poles).

Definition 2.2.4. A *fundamental parallelogram* for Λ is a set of the form

$$\mathcal{F} = \{t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 < 1\},$$

where ω_1, ω_2 are basis elements of Λ.

A different choice of basis for Λ will give a different fundamental parallelogram. Any elliptic function f is completely determined by its values on a fundamental parallelogram. Next we will describe some properties of elliptic functions that we will be using in this thesis. We start with the following theorem.

Theorem 2.2.5. *Any elliptic function with no poles (or no zeros) is a constant function.*

Proof. Let f be an elliptic function with no poles. Then f is holomorphic. Let $\mathcal{F}$ be a fundamental parallelogram for a lattice Λ. Then by periodicity of f we have that

$$\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in\overline{\mathcal{F}}} |f(z)|,$$

where $\overline{\mathcal{F}}$ is the closure of $\mathcal{F}$. Since f is holomorphic and $\overline{\mathcal{F}}$ is compact, so $|f(z)|$ is bounded on $\overline{\mathcal{F}}$. Thus $|f(z)|$ is bounded on complex plane. Hence by Liouville's theorem (see [7, Theorem 8.27]) f is constant. Note that if f has no zeros then $1/f$ has no poles. Hence by the same argument $1/f$ is constant, which means f is constant. □

The following is an immediate corollary of the above theorem.

Corollary 2.2.6. *Two elliptic functions differ by a constant multiple if and only if they have same zeros and poles.*

Proof. Let f and g be two elliptic functions with the same zeros and poles. Then the ratio f/g has no zeros or poles. Hence by the previous theorem f/g is a constant.

□

Theorem 2.2.7. *The number of zeros of an elliptic function in any fundamental parallelogram is equal to the number of its poles, each counted with multiplicity.*

Proof. See [1, Chapter 1, Theorem 1.8]. □

Definition 2.2.8. The *order* of an elliptic function is the number of poles (counted with multiplicity) it has in a fundamental parallelogram.

Constant functions are trivial examples of elliptic functions. Any non-constant elliptic function will have order at least 2 (see [1, Chapter 1, Theorem 1.7]). The most important example of a non-constant elliptic function is the Weierstrass $\wp$-function, which we will describe next.

2.2.1 Weierstrass $\wp$-function

Definition 2.2.9. For a given lattice Λ the *Weierstrass $\wp$-function* is defined by

$$\wp(z) = \wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ w\neq 0}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right]. \tag{2.3}$$

In (2.3) the series converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$ (see [9, Chapter 6, Theorem 3.1]). Thus it defines a meromorphic function on $\mathbb{C}$ having a double pole at each lattice point with residue 0 and no other poles. Note that

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

as the above sum is over all the non-zero lattice points. Thus the Weierstrass $\wp$-function is an even function. Next we observe that since the series for $\wp(z)$ is uniformly convergent on compact subsets of $\mathbb{C} \setminus \Lambda$, we can differentiate (2.3) term by term. Differentiating (2.3) with respect to z yields

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}. \tag{2.4}$$

Note that $\wp'(z)$ is a meromorphic function with poles of order 3 at each lattice points. Moreover, since $\wp'(-z) = -\wp'(z)$, we see that $\wp'(z)$ is an odd function.

Next we show that $\wp$ and $\wp'$ are elliptic functions. In (2.4) since ω runs over all the lattice points we see that $\wp'(z+\omega) = \wp'(z)$ for all $\omega \in \Lambda$. This shows that $\wp'(z)$ is an elliptic function. Integrating equation $\wp'(z+\omega) = \wp'(z)$ yields

$$\wp(z+\omega) = \wp(z) + C \tag{2.5}$$

where C is a constant which may depends on ω. By setting $z = -\omega/2$ in (2.5), and using the fact that $\wp(z)$ is even we get that $C = 0$. Thus $\wp(z+\omega) = \wp(z)$ for all $\omega \in \Lambda$. Hence $\wp(z)$ is an elliptic function.

The addition and multiplication of two elliptic functions are elliptic functions. In other words the collection of all elliptic functions forms a field. More precisely we have the following important result.

Theorem 2.2.10. *The collection of elliptic functions (with respect to Λ) forms a field generated by $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$.*

Proof. See [4, Theorem 2.1]. □

The above theorem says that every non-constant elliptic function can be written as a rational expression in terms of $\wp(z)$ and $\wp'(z)$. There is an algebraic relation between the functions $\wp(z)$ and $\wp'(z)$. To establish this relation we need the power

series expansions for $\wp(z)$ and $\wp'(z)$. We start with the following definition.

Definition 2.2.11. The *Eisenstein series* of weight k for Λ is defined as

$$G_k(\Lambda) = \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{\omega^k}. \tag{2.6}$$

It can be shown that G_k is absolutely convergent for $k > 2$ (see [1, Chapter 1, Lemma 1]). Moreover, from (2.6) we can see that $G_k = 0$ for all odd values of k. The Eisenstein series appear in the differential equation satisfied by the Weierstrass $\wp$-function, which also gives the relation between $\wp$-function and elliptic curves. More precisely we have the following assertion.

Theorem 2.2.12. *Let $\Lambda \subset \mathbb{C}$ be a lattice and $\wp(z)$ be the Weierstrass function. We have the following assertions:*

(a) The Laurent expansion around $z = 0$ for $\wp(z)$ is

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(\Lambda) z^{2n}, \tag{2.7}$$

where G_k is the Eisenstein series of weight k.

(b) The function $\wp(z)$ satisfies the differential equation

$$(\wp'(z))^2 = 4\wp^3(z) - g_2(\Lambda)\wp(z) - g_3(\Lambda), \tag{2.8}$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

Proof. (a) For $\omega \in \Lambda$, consider the disk $0 < |z| < |\omega|$. We have

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

Expanding $(1 - z/w)^{-2}$ in the latter equation yields

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ w\neq 0}} \frac{1}{\omega^2} \sum_{n=1}^{\infty} \frac{(n+1)z^n}{\omega^n} \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n G_{n+2}(\Lambda).\end{aligned}$$

Observing that $G_k = 0$ whenever k is odd, we have

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(\Lambda) z^{2n}.$$

(b) First of all note that first few terms of the expansion of $\wp(z)$ in part (a) can be written as

$$\wp(z) = z^{-2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + 7G_8(\Lambda)z^6 \cdots . \tag{2.9}$$

From here we have that

$$4\wp(z)^3 = 4z^{-6} + 36G_4(\Lambda)z^{-2} + 60G_6(\Lambda) + \cdots . \tag{2.10}$$

Next by differentiating (2.9) with respect to z and squaring we get

$$\wp'(z)^2 = 4z^{-6} - 24G_4(\Lambda)z^{-2} - 80G_4(\Lambda) + \cdots . \tag{2.11}$$

Define a function

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda). \tag{2.12}$$

Using equations (2.9), (2.10), and (2.11) in (2.12) we see that the function $f(z)$ has no constant terms and no terms with negative powers of z. Thus $f(z)$ has

no poles and therefore it is holomorphic. On the other hand by Theorem 2.2.10 $f(z)$ is an elliptic function. Thus by using Theorem 2.2.5 it must be a constant. Letting $z = 0$ in (2.12) yields $f(0) = 0$, hence f is identically zero. Thus we get the desired result.

□

The above theorem shows that the point $(\wp(z), \wp'(z))$ lies on the curve defined by the equation

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda), \tag{2.13}$$

and as long as the discriminant $\Delta = 16(g_2^3 - 27g_3^2)$ of the cubic on the right-hand side of equation (2.13) is non-zero, (2.13) defines an elliptic curve over $\mathbb{C}$. We will show that Δ is indeed not zero. In order to do this we need the following lemma.

Lemma 2.2.13. *A complex number u, such that $u \not\equiv 0 \pmod{\Lambda}$, is a zero of $\wp'(z)$ if and only if $u \equiv -u \pmod{\Lambda}$.*

Proof. Let u be a complex number such that $2u \equiv 0 \pmod{\Lambda}$ but $u \not\equiv 0 \pmod{\Lambda}$. Observe that for a lattice $\Lambda = [\omega_1, \omega_2]$, the points

$$\frac{\omega_1}{2}, \frac{\omega_2}{2}, \text{ and } \frac{\omega_3}{2},$$

where $\omega_3 = \omega_1 + \omega_2$, are the only points in a fundamental parallelogram with the above property (i.e., $u \notin \Lambda$ but $2u \in \Lambda$). Next using the facts that $\wp'$ is odd and periodic we see that

$$\wp'(u) = \wp'(2u - u) = \wp'(-u) = -\wp'(u)$$
$$2\wp'(u) = 0 \implies \wp'(u) = 0.$$

Since $\wp'(z)$ is an elliptic function of order 3, it has only three zeros in $\mathcal{F}$, a fundamental parallelogram. Hence the lemma. □

We will now prove our claim about non-vanishing of the discriminant Δ.

Proposition 2.2.14. *The discriminant* $\Delta = 16(g_2^3 - 27g_3^2)$ *of the cubic equation* $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ *is non-zero.*

Proof. Let $\Lambda = [\omega_1, \omega_2]$ be a lattice, then from Lemma 2.2.13 we know that

$$\frac{\omega_1}{2}, \frac{\omega_2}{2}, \text{ and } \frac{\omega_3}{2}$$

are the only zeros of $\wp'(z)$, where $\omega_3 = \omega_1 + \omega_2$. Hence we see that

$$\wp\left(\frac{\omega_1}{2}\right), \wp\left(\frac{\omega_2}{2}\right), \text{ and } \wp\left(\frac{\omega_3}{2}\right)$$

are the roots of the equation (2.8). In order to prove that $\Delta \neq 0$ we need to show that all three roots are distinct. For $i = 1, 2$, and 3 define a function

$$P_i(z) = \wp(z) - \wp\left(\frac{\omega_i}{2}\right).$$

Then $P_i(z)$ is an elliptic function of order 2 (its poles are the poles of $\wp(z)$), thus by Theorem 2.2.7, $P_i(z)$ has exactly 2 zeros. Moreover, since $P_i(\omega_i/2) = P_i'(\omega_i/2) = 0$ we have that $\omega_i/2$ is a zero of order 2 of $P_i(z)$ and there is no other zero of $P_i(z)$. Therefore $P_i(z) \neq P_j(z)$ for $i \neq j$ or equivalently $\wp(\omega_i/2) \neq \wp(\omega_j/2)$ for $i \neq j$. Thus all the roots of (2.8) are distinct. Hence $\Delta = 16(g_2^3 - 27g_3^2) \neq 0$. □

The above proposition implies that (2.13) is an equation of an elliptic curve. Since the functions $\wp(z)$ and $\wp'(z)$ depend only on the points $z \pmod{\Lambda}$ then the map $z \longmapsto (\wp(z), \wp'(z))$ define a function from $\mathbb{C}/\Lambda$ to $E_\Lambda(\mathbb{C})$. More precisely this map is a complex analytic isomorphism which maps the points of $\mathbb{C}/\Lambda$ to the points in $E_\Lambda(\mathbb{C})$. In fact we have the following very important theorem.

Theorem 2.2.15 (**Uniformization Theorem**). *Let $E/\mathbb{C}$ be an elliptic curve given by $E : y^2 = x^3 + ax + b$. Then there is a unique lattice $\Lambda \subset \mathbb{C}$ such that*

$$g_2(\Lambda) = 60G_4 = -4a \quad \textit{and} \quad g_3(\Lambda) = 140G_6(\Lambda) = -4b.$$

The map

$$\begin{aligned} \varphi : \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \\ z &\longmapsto \left(\wp(z), \frac{1}{2}\wp'(z)\right) \\ 0 &\longmapsto \mathcal{O} \end{aligned}$$

is a complex analytic isomorphism.

Proof. See [10, Chapter I Corollary 4.3]. □

In other words, to every elliptic curve over $\mathbb{C}$ we can associate a lattice Λ and conversely every lattice Λ gives rise to an elliptic curve $E/\mathbb{C}$. The group law on $E(\mathbb{C})$ corresponds to the usual addition in $\mathbb{C}/\Lambda$.

Next we define another very important function in the theory of elliptic functions.

2.2.2 Weierstrass σ-function

Definition 2.2.16. The *Weierstrass σ-function* (associated to a lattice Λ) is defined as

$$\sigma(z) = \sigma(z;\Lambda) := z \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2}, \tag{2.14}$$

where z is a complex variable.

The Weierstrass σ-function is of much importance to us because an elliptic divisibility sequence can be parametrized using it. Therefore we will study the properties of Weierstrass σ-function in detail. We start with the following proposition.

Proposition 2.2.17. *Let $\Lambda \subset \mathbb{C}$ be a fixed lattice. Let $\sigma(z)$ be the corresponding Weierstrass σ-function. Then the following statements holds.*

(a) The infinite product (2.14) *for $\sigma(z)$ defines a holomorphic function on $\mathbb{C}$. The function $\sigma(z)$ has simple zeros at each lattice point and no other zeros.*

(b) For all $z \in \mathbb{C} \setminus \Lambda$ we have

$$\frac{d^2}{dz^2} \log \sigma(z) = -\wp(z).$$

(c) For all $z \in \mathbb{C}$ and for every $\omega \in \Lambda$ there are constants $a, b \in \mathbb{C}$, depending on ω, such that

$$\sigma(z + \omega) = e^{az+b}\sigma(z). \tag{2.15}$$

(d) The function $\sigma(z)$ is an odd function (i.e., $\sigma(-z) = -\sigma(z)$).

Proof. (a) See [9, Chapter 6, Lemma 3.3].

(b) Taking logarithm in (2.14) yields

$$\log \sigma(z) = \log z + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left[\log\left(1 - \frac{z}{\omega}\right) + \frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2 \right].$$

Using (a) we can differentiate the above series, twice with respect to z, to get

$$\frac{d}{dz} \log \sigma(z) = \frac{1}{z} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left[\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right]. \tag{2.16}$$

Differentiating again with respect to z yields

$$\frac{d^2}{dz^2} \log \sigma(z) = -\frac{1}{z^2} - \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left[\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right] = -\wp(z). \tag{2.17}$$

(c) Using the fact that $\wp(z)$ is periodic, from part (b) we have

$$\frac{d^2}{dz^2}\log\sigma(z+\omega) = -\wp(z+\omega) = -\wp(z) = \frac{d^2}{dz^2}\log\sigma(z).$$

Integrating, last equation, twice with respect to z yields

$$\log\sigma(z+\omega) = \log\sigma(z) + az + b,$$

where a and b are constants. The result follows by exponentiating the above equation.

(d) We have

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

The above expression is equal to $-\sigma(z)$, since the product is taken over all the non-zero lattice points.

□

We continue by introducing another important function form the theory of elliptic functions.

Definition 2.2.18. The *Weierstrass ζ-function* for lattice Λ is defined as

$$\zeta(z) = \zeta(z;\Lambda) := \frac{1}{z} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\left[\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right], \tag{2.18}$$

where z is a complex variable.

The following proposition describes the main properties of the Weierstrass ζ-function.

Proposition 2.2.19. *(a) The series defining $\zeta(z)$ is absolutely and uniformly convergent on the compact subsets of $\mathbb{C}\setminus\Lambda$.*

(b) The function $\zeta(z)$ defines a meromorphic function on $\mathbb{C}$ with simple poles at each point of lattice Λ and no other poles.

Proof. See [10, Proposition 5.1]. □

From (2.16) and (2.17) we see that there is a relation between Weierstrass's functions $\wp(z), \sigma(z)$, and $\zeta(z)$. The next proposition describes these relations. Moreover, we introduce an another function called Weierstrass's η-function.

Proposition 2.2.20. *Let $\wp(z), \sigma(z)$, and $\zeta(z)$ be the Weierstrass's functions as defined earlier,*

(a) We have

$$(i)\ \ \frac{d}{dz}\log\sigma(z) = \zeta(z), \qquad (ii)\ \ \frac{d}{dz}\zeta(z) = -\wp(z), \qquad (iii)\ \ \zeta(-z) = -\zeta(z)$$

(b) For all $z \in \mathbb{C}$ and for all $\omega \in \Lambda$ there exists a function of ω, denoted by $\eta(\omega)$, satisfying

$$\zeta(z+\omega) = \zeta(z) + \eta(\omega). \tag{2.19}$$

(c) The map $\eta : \Lambda \longrightarrow \mathbb{C}$ has the following properties:

(i) It is a homomorphism form Λ into $\mathbb{C}$.

(ii) If $\omega \in \Lambda$ and $\omega \notin 2\Lambda$, then $\eta(\omega)$ is given by the formula

$$\eta(\omega) = 2\zeta(\omega/2). \tag{2.20}$$

(iii) Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice with $[\omega_1, \omega_2]$ satisfying $\Im(\omega_1/\omega_2) > 0$. Then

$$\omega_1\eta(\omega_2) - \omega_2\eta(\omega_1) = 2\pi i. \tag{2.21}$$

Proof. (a) Part (i) and (ii) can be seen from (2.16) and (2.16). Part (iii) is a c consequence of the definition of $\zeta(z)$.

(b) From part (a) we have that

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

By integrating both sides of the above equation respect to z we get that

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

where $\eta(w)$ depends only on ω.

(c) Let $\eta : \Lambda \longrightarrow \mathbb{C}$ be the function as introduced above. Then

(i) Let $\omega_1, \omega_2 \in \Lambda$, then

$$\begin{aligned}\eta(\omega_1+\omega_2) - \eta(\omega_1) &= \zeta(z+\omega_1+\omega_2) - \zeta(z) - \zeta(z+\omega_1) + \zeta(z)\\ &= \zeta(z+\omega_1+\omega_2) - \zeta(z+\omega_1)\\ &= \eta(\omega_2).\end{aligned}$$

(ii) Note that $\omega \notin 2\Lambda$ is equivalent to $\omega/2 \notin \Lambda$ and by Proposition 2.2.19(b) the function $\zeta(z)$ is holomorphic for all the points not in the lattice. Therefore by setting $z = -\omega/2$ in (2.19) and using the fact that ζ is an odd function we get the result.

(iii) See [10, Proposition 5.2(d)].

□

The function η introduced in (2.19) is called the *quasi-period homomorphism* for Λ. We are now in a position to prove a transformation property for the Weierstrass σ-function. We know that the function $\sigma(z)$ is not elliptic because it does not have any poles. From (2.15) it is clear that $\sigma(z)$ is also not periodic. However it satisfies a transformation formula given by the next proposition.

Proposition 2.2.21. *Let $\Lambda \subset \mathbb{C}$ be a lattice and $\sigma(z)$ be the Weierstrass σ- function, then for all $z \in \mathbb{C}$ and $\omega \in \Lambda$,*

$$\sigma(z+\omega;\Lambda) = \lambda(\omega)e^{\eta(\omega)(z+\frac{1}{2}\omega)}\sigma(z;\Lambda), \tag{2.22}$$

where $\eta : \Lambda \longrightarrow \mathbb{C}$ is the quasi-period homomorphism for Λ, and $\lambda : \Lambda \longrightarrow \{\pm 1\}$ is given by

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

Proof. Using parts (a) and (b) of Proposition 2.2.20 we can write

$$\begin{aligned} \zeta(z+\omega) &= \zeta(z) + \eta(\omega) \\ \frac{d}{dz}\log\sigma(z+\omega) &= \frac{d}{dz}\log\sigma(z) + \eta(\omega). \end{aligned}$$

Integrating and taking exponential we get

$$\sigma(z+\omega;\Lambda) = Ce^{\eta(\omega)z}\sigma(z;\Lambda),$$

where C is a constant which may depend upon ω. We consider two cases. First, if $\omega \notin 2\Lambda$ or equivalently $\omega/2 \notin \Lambda$, then $\sigma(z)$ does not vanish at $\pm\omega/2$. Hence by setting $z = -\omega/2$ we get

$$\sigma\left(\frac{\omega}{2};\Lambda\right) = Ce^{-\frac{1}{2}\eta(\omega)\omega}\sigma\left(-\frac{\omega}{2};\Lambda\right).$$

Since $\sigma(z)$ is an odd function we have that

$$C = -e^{\frac{1}{2}\eta(\omega)\omega}.$$

Second, if $\omega \in 2\Lambda$ or equivalently $\omega/2 \in \Lambda$, then $\sigma(z)$ has a simple zero at $\pm\omega/2$.

Employing L'Hôpital's rule yields

$$Ce^{-\frac{1}{2}\eta(\omega)\omega} = \lim_{z\to-\omega/2} \frac{\sigma(z+\omega;\Lambda)}{\sigma(z;\Lambda)} = \lim_{z\to-\omega/2} \frac{\sigma'(-\omega/2;\Lambda)}{\sigma'(-\omega/2;\Lambda)} = 1. \tag{2.23}$$

Here we have used the fact that $\sigma'(z)$ is even. Hence (2.23) we find that

$$C = e^{\frac{1}{2}\eta(\omega)\omega}.$$

Combining the two cases finishes our proof. □

We have already mentioned that the Weierstrass σ-function is of much interest for us because elliptic divisibility sequences can be parametrized by the Weierstrass σ-function. In order to establish that relation we need the concept of *division polynomials*. In the theory of elliptic divisibility sequences division polynomials play a significant role because the terms of an elliptic divisibility sequence can be realized as the values of division polynomials. Moreover, division polynomials can be written as rational functions in terms of the σ-function.

2.3 Division Polynomials

Division polynomials can be formulated in two different ways. One way is analytic and uses the Weierstrass $\wp$-function. The other is algebraic, in which for any generic point (x, y) the multiple $n(x, y)$ can be expressed as rational functions in x and y, and the denominators of these rational functions give rise to division polynomials. Here we will define division polynomials analytically using elliptic functions and later in this section we give algebraic formulation of them. We start with the following definitions.

Definition 2.3.1. Let $E/\mathbb{C}$ be an elliptic curve. For each $n \in \mathbb{Z}$ define *multiplication*

by n map

$$[n] : E(\mathbb{C}) \longrightarrow E(\mathbb{C})$$

as follows. If $n > 0$ and $P \in E(\mathbb{C})$, we have

$$[n]P = \underbrace{P + P + \cdots + P}_{n\text{-times}}.$$

If $n < 0$ then $[n]P = [-n](-P)$. We also define $[0]P = \mathcal{O}$.

Definition 2.3.2. Let n be an integer and P be a point in $E(\mathbb{C})$. Then P is called an *n-torsion* point if $[n]P = \mathcal{O}$.

Definition 2.3.3. Let $E/\mathbb{C}$ be an elliptic curve and $n \in \mathbb{Z} \setminus \{0\}$. The set of n-torsion points, denoted by $E[n]$, is defined as

$$E[n] = \{P \in E(\mathbb{C}) \mid [n]P = \mathcal{O}\}.$$

The set $E[n]$ is a subgroup of $E(\mathbb{C})$. Henceforth we will write nP for $[n]P$.

In order to define division polynomials we will start by employing the Weierstrass $\wp$-function to construct a certain elliptic function. The next proposition shows the existence of such elliptic function $f_n(z)$ that can be written as polynomials in terms of $\wp(z)$ and $\wp'(z)$, for a complex variable z.

Proposition 2.3.4. *There exists an elliptic function f_n, for each integer $n \geq 1$, such that*

$$f_n(z)^2 = n^2 \prod_{\substack{u \in (\mathbb{C}/\Lambda)[n] \\ u \neq 0}} (\wp(z) - \wp(u)), \tag{2.24}$$

where $(\mathbb{C}/\Lambda)[n]$ is the subgroup of elements $u \in \mathbb{C}/\Lambda$ such that $nu \equiv 0 \mod \Lambda$. Furthermore

(a) $f_n = n\wp^{(n^2-1)/2} + \ldots$ if n is odd.

(b) $f_n = \dfrac{n}{2}\wp'\wp^{(n^2-4)/2} + \dots$ *if* n *is even.*

(c) In all cases, the expansion of f_n *at* $z = 0$ *is of the form*

$$f_n(z) = \frac{(-1)^{n+1}n}{z^{n^2-1}} + \cdots . \tag{2.25}$$

Proof. See [4, Chapter II, Section 1]. □

In the next proposition we describe another relation between $\wp(z)$ and $f_n(z)$.

Proposition 2.3.5. *We have*

$$\wp(z) - \wp(nz) = \frac{f_{n+1}(z)f_{n-1}(z)}{f_n^2(z)}. \tag{2.26}$$

Proof. First of all recall that Weierstrass $\wp$-function has a double pole at each lattice point and no other pole. Next observe that for $z \not\equiv 0 \pmod{\Lambda}$ (i.e., z is not a lattice point) the function

$$\wp(z) - \wp(nz)$$

has the following properties:

(i) It has n^2 double poles located at the n-torsion points of $\mathbb{C}/\Lambda$, which exactly are the zeros of $f_n^2(z)$ with the multiplicity 2.

(ii) It has $2n^2$ simple zeros at z such that $z \equiv \pm nz \pmod{\Lambda}$. These are points z such that

$$(n+1)z \equiv 0 \pmod{\Lambda} \quad \text{and} \quad (n-1)z \equiv 0 \pmod{\Lambda},$$

which are the zeros of the functions $f_{n+1}(z)$ and $f_{n-1}(z)$. Hence, by Theorem 2.2.10, the function

$$\frac{f_n^2(z)(\wp(nz) - \wp(z))}{f_{n+1}(z)f_{n-1}(z)} \tag{2.27}$$

is elliptic and has no zeros or poles other than 0 in $\mathbb{C}/\Lambda$. Thus by Theorem 2.2.5 it is a constant. To evaluate the constant observe that using (2.7) and (2.25) the expansion of (2.27) at 0 is given by

$$\frac{n^2(-n^2+1)/n^2}{(n+1)(n-1)} = -1.$$

Hence the result follows. □

The next proposition establishes a fundamental identity for $f_n(z)$.

Proposition 2.3.6. *For $m > n$, we have*

$$f_{m+n}f_{m-n} = f_{m+1}f_{m-1}f_n^2 - f_{n+1}f_{n-1}f_m^2. \tag{2.28}$$

Proof. From (2.26) we have

$$\wp(z) - \wp(nz) = \frac{f_{n+1}(z)f_{n-1}(z)}{f_n^2(z)}$$

and

$$\wp(z) - \wp(mz) = \frac{f_{m+1}(z)f_{m-1}(z)}{f_m^2(z)}.$$

Subtracting the above two identities yields

$$\wp(mz) - \wp(nz) = \frac{f_{m+1}(z)f_{m-1}(z)f_n^2(z) - f_{n+1}(z)f_{n-1}(z)f_m^2(z)}{f_m^2(z)f_n^2(z)}. \tag{2.29}$$

Observe that the function $\wp(mz) - \wp(nz)$ has a zero at those points such that

$$mz \equiv \pm nz \not\equiv 0 \pmod{\Lambda}.$$

For such a point note that

$$m\wp'(mz) - n\wp'(nz) \neq 0,$$

so a point $(m \pm n)z \equiv 0 \pmod{\Lambda}$ is a simple zero of the function $\wp(mz) - \wp(nz)$. Since $mz \equiv \pm nz \not\equiv 0 \pmod{\Lambda}$, therefore $f_m(z)$ and $f_n(z)$ can not have zeros at $(m \pm n)z \equiv 0 \pmod{\Lambda}$. Hence these points are the zeros of

$$f_{m+1}(z)f_{m-1}(z)f_n^2(z) - f_{n+1}(z)f_{n-1}(z)f_m^2(z). \tag{2.30}$$

On the other hand $(m \pm n)z \equiv 0 \pmod{\Lambda}$ are zeros of

$$f_{m+n}(z)f_{m-n}(z). \tag{2.31}$$

Furthermore, note that (2.30) and (2.31) are polynomial in $\wp$ so they have poles only at lattice points. Hence (2.30) and (2.31) are constant multiple of each other. The expansion for the quotient of (2.30) over (2.31) gives 1 as the constant. Thus Theorem 2.2.5 yields the desired result. □

Note that (2.28) is the same recurrence relation as in the definition of an elliptic divisibility sequence.

Definition 2.3.7. For all $n \geq 1$, we define the function $\psi_n : E(\mathbb{C}) \to \mathbb{C}$ by the relation

$$\psi_n(x, y) = f_n(z), \quad \text{where } x = \wp(z) \text{ and } y = \frac{1}{2}\wp'(z).$$

The function ψ_n is called the n-th *division polynomial* associated to E and a generic point (x, y).

The map $(x, y) \longmapsto \big(\wp(z), \frac{1}{2}\wp'(z)\big)$ is well defined by using Theorem 2.2.15.

Division polynomials are closely related to torsion points. A point P is an n-torsion point of $E(\mathbb{C})$ if and only if the n-th division polynomial associated to E vanishes at P. We are specifically interested in points which are not sent to the identity element (infinity) of $E(\mathbb{C})$ by any integer. Such points are called *non-torsion* points.

In the next section we give algebraic formulas for division polynomials.

2.3.1 Algebraic Formulation of Division Polynomials

The expressions obtained in the previous section about division polynomials are all in terms of the Weierstrass $\wp$-function and its derivative $\wp'$. However using Theorem 2.2.15 (Uniformization Theorem) we can give the algebraic formulation of the division Polynomials. Let E be an elliptic curve given by the equation $E : y^2 = x^3 + ax + b$. Let $\wp(z;\Lambda)$ be the Weierstrass $\wp$-function. Then by Theorem 2.2.15 we may let

$$x = \wp(z), \quad y = \frac{1}{2}\wp'(z), \quad a = -\frac{1}{4}g_2(\Lambda), \quad b = -\frac{1}{4}g_2(\Lambda).$$

It can be shown that the division polynomials ψ_n can be constructed algebraically using initial values

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2),
\end{aligned}$$

and to calculate rest of terms inductively as

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \qquad \text{for } n \geq 2, \tag{2.32}$$

$$\psi_{2n}\psi_2 = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \qquad \text{for } n \geq 3. \tag{2.33}$$

The division polynomials have several interesting properties. The next theorem summarizes the main properties of division polynomials.

Theorem 2.3.8. *Let $P = (x, y)$ be a point on the elliptic curve $y^2 = x^3 + ax + b$, and let n be a positive integer. Then*

(a)

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

where

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1},$$

and

$$\omega_n = (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).$$

(b) The expressions $\phi_n, \psi_n, y^{-1}\omega_n$ (for n odd), and $\phi_n, (2y)^{-1}\psi_n, \omega_n$ (for n even) are polynomials in $\mathbb{Z}[a,b,x,y^2]$. Hence, replacing y^2 with x^3+ax+b, they are polynomials in $\mathbb{Z}[a,b,x]$.

(c) For all $m > n > r$, ψ_n satisfies

$$\psi_{m+n}\psi_{m-n}\psi_r^2 = \psi_{m+r}\psi_{m-r}\psi_n^2 - \psi_{n+r}\psi_{n-r}\psi_m^2.$$

Proof. See [4, Theorem 2.1]. □

Theorem 2.3.9. *Let $E/\mathbb{C}$ be an elliptic curve and let ψ_n be the n-th division polynomial. Considered as a function on $\mathbb{C}/\Lambda$,*

$$\psi_n\left(\wp(z), \frac{1}{2}\wp'(z)\right) = f_n(z) = (-1)^{n+1}\frac{\sigma(nz;\Lambda)}{\sigma(z;\Lambda)^{n^2}}.$$

Proof. First of all observe that using (2.22) we have

$$\begin{aligned}\frac{\sigma(nz+n\omega;\Lambda)}{\sigma(z+\omega;\Lambda)^{n^2}} &= \frac{\lambda(n\omega)e^{\eta(n\omega)(nz+\frac{1}{2}n\omega)}\sigma(nz;\Lambda)}{(\lambda(\omega)e^{\eta(\omega)(z+\frac{1}{2}\omega)}\sigma(z;\Lambda))^{n^2}} \\ &= \frac{\lambda(n\omega)\sigma(nz;\Lambda)}{\lambda(\omega)^{n^2}\sigma(z\Lambda)^{n^2}}.\end{aligned}$$

If $\omega,\ n\omega \notin 2\Lambda$, then we see that n is odd, so $\lambda(\omega)^{n^2} = \lambda(n\omega) = -1$. If $\omega \notin 2\Lambda$ but $n\omega \in 2\Lambda$, then n must be even, and so $\lambda(\omega)^{n^2} = \lambda(n\omega) = 1$. Finally, if $\omega \in 2\Lambda$, then

$n\omega \in 2\Lambda$, and $\lambda(\omega) = \lambda(n\omega) = 1$. Thus in all cases we have

$$\frac{\lambda(n\omega)}{\lambda(\omega)^{n^2}} = 1$$

. In conclusion

$$\frac{\sigma(nz + n\omega; \Lambda)}{\sigma(z + \omega; \Lambda)^{n^2}} = \frac{\sigma(nz; \Lambda)}{\sigma(z; \Lambda)^{n^2}}.$$

This means that $\sigma(nz; \Lambda)/\sigma(z; \Lambda)^{n^2}$ is an elliptic function. From (2.24) we have that

$$f_n(z)^2 = n^2 \prod_{\substack{u \in (\mathbb{C}/\Lambda)[n] \\ u \neq 0}} (\wp(z) - \wp(u)),$$

where $(\mathbb{C}/\Lambda)[n]$ is the subgroup of elements $u \in \mathbb{C}/\Lambda$ such that $nu \equiv 0 \bmod \Lambda$. We will compare the zeros and poles of $f_n(z)$ and $\sigma(nz; \Lambda)/\sigma(z; \Lambda)^{n^2}$. The function $f_n(z)$ has zero at $0 \neq u \in (\mathbb{C}/\Lambda)[n]$. There are $n^2 - 1$ such points. In other words z is zero of $f_n(z)$ for $nz \in \Lambda$, which are precisely the zeros of $\sigma(nz; \Lambda)/\sigma(z; \Lambda)^{n^2}$. Since $\sigma(z; \Lambda)$ does not have any poles so the only poles for the function $\sigma(nz; \Lambda)/\sigma(z; \Lambda)^{n^2}$ are the zeros of the denominator, which are the points $z \in \Lambda$. Each $z \in \Lambda$ is a pole of order $n^2 - 1$ for $f_n(z)$. Hence using Corollary 2.2.6 we see that

$$f_n(z) = C \frac{\sigma(nz; \Lambda)}{\sigma(z; \Lambda)^{n^2}}.$$

Using equations (2.14) and (2.25)

$$\frac{(-1)^{n+1} n}{z^{n^2-1}} + \cdots = C \frac{nz \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(1 - \frac{nz}{\omega}\right) e^{\frac{nz}{\omega} + \frac{1}{2}\left(\frac{nz}{\omega}\right)^2}}{z^{n^2} \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right)^{n^2} e^{\frac{n^2 z}{\omega} + \frac{1}{2}\left(\frac{nz}{\omega}\right)^2}}.$$

After simplification we get

$$(-1)^{n+1} = C \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(1 - \frac{nz}{\omega}\right) \left(1 - \frac{z}{\omega}\right)^{-n^2} e^{\frac{nz}{\omega} - \frac{n^2 z}{\omega}}$$

. Taking $z \to 0$ we get that $C = (-1)^{n+1}$, which proves the result.

□

2.4 q-Expansions

In this section we describe *q-product expansions or q-expansions* of some elliptic functions. The q-expansion of the Weierstrass σ-function was a major tool in the proof of Silverman-Stephens' theorem for the sign of terms of an elliptic divisibility sequence. The q- expansions will also play an important role in the proof of the main theorem of this thesis. Study of q-expansions will also lead us to another uniformization for elliptic curves which we will describe in this section. We start with the following definition.

Definition 2.4.1. Two lattices Λ_1 and Λ_2 are called *homothetic* if there exists $\alpha \in \mathbb{C}^*$ such that

$$\Lambda_1 = \alpha \Lambda_2.$$

Proposition 2.4.2. *Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be any lattice. Then Λ is homothetic to the lattice $\Lambda_\tau = \tau\mathbb{Z} + \mathbb{Z}$ (generated by τ and 1) where τ is in the upper half plane $\mathcal{H} = \{z \in \mathbb{Z} \mid \Im(z) > 0\}$.*

Proof. Since for any lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ the complex numbers ω_1 and ω_2 are linearly independent over $\mathbb{R}$. One of the numbers ω_1/ω_2 or ω_2/ω_1 will be in the upper half plane. Without loss of generality we assume that the number ω_1/ω_2 is in the

upper half plane. Let $\tau = \omega_1/\omega_2 \in \mathcal{H}$ and define

$$\Lambda_\tau = \tau\mathbb{Z} + \mathbb{Z}$$

be the lattice generated by τ and 1. Then the lattices Λ and Λ_τ are homothetic since

$$\Lambda_\tau = \frac{1}{\omega_2}\Lambda.$$

□

Definition 2.4.3. A lattice is called *normalized* if one of its generators in 1.

Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be any lattice such that $\Im(\omega_1/\omega_2) > 0$. Let $\Lambda_\tau = \tau\mathbb{Z} + \mathbb{Z}$ be a normalized lattice, where $\tau = \omega_1/\omega_2$. Then the multiplication map $z \longmapsto \omega_2 z$ from $\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda_\tau$ is an isomorphism and carries field of elliptic functions for Λ isomorphically to the filed of elliptic functions for Λ_τ. Let $\wp(z;\Lambda_\tau)$ and $\sigma(z;\Lambda_\tau)$ be the Weierstrass functions for lattice Λ_τ. From now on for simplicity we will denote $\wp(z;\Lambda_\tau)$ by $\wp(z,\tau)$ and $\sigma(z;\Lambda_\tau)$ by $\sigma(z,\tau)$. We observe that the functions $\wp$ and σ can be considered as functions of two variables $(z,\tau) \in \mathbb{Z} \times \mathbb{H}$.

Since $1 \in \Lambda_\tau$ and $\wp(z)$ is periodic we see that $\wp$-function satisfies the relation

$$\wp(z+1,\tau) = \wp(z,\tau).$$

Thus we can expand $\wp$ as a Fourier series in the variable $u = \mathrm{e}^{2\pi i z}$. Furthermore, observe that since $(\tau+1)\mathbb{Z}+\mathbb{Z} = \tau\mathbb{Z}+\mathbb{Z}$ we have $\Lambda_{\tau+1} = \Lambda_\tau$, thus $\wp$-function satisfies

$$\wp(z,\tau+1) = \wp(z,\tau).$$

Consequently, as a function of τ, the function $\wp$ has a Fourier expansion in terms of a variable $q = \mathrm{e}^{2\pi i\tau}$ as well. More precisely, let

$$u = e^{2\pi i z} \qquad \text{and} \qquad q = e^{2\pi i\tau}$$

and let

$$q^{\mathbb{Z}} = \{q^k \mid k \in \mathbb{Z}\}$$

be the cyclic subgroup generated by q of the multiplicative group $\mathbb{C}^*$. Observe that since $\tau \in \mathcal{H}$ we have $|q| < 1$. Observe that under the exponential map $z \longmapsto e^{2\pi iz}$ form $\mathbb{C} \longrightarrow \mathbb{C}^*$ with kernel $\mathbb{Z}$, the lattice Λ_τ is mapped to infinite cyclic group $q^{\mathbb{Z}}$. Thus there is a complex analytic isomorphism

$$\begin{aligned} \mathbb{C}/\Lambda_\tau &\xrightarrow{\sim} \mathbb{C}^*/q^{\mathbb{Z}} \\ z &\longmapsto e^{2\pi iz}. \end{aligned}$$

Using this isomorphism, the next two theorems give the formula for the $\wp$-function and σ-function in terms of variables u and q in $\mathbb{C}^*/q^{\mathbb{Z}}$.

Theorem 2.4.4. *Let $u = e^{2\pi iz}$ and $q = e^{2\pi i\tau}$.*

(a) Then for $\wp$ we have

$$\frac{1}{(2\pi i)^2}\wp(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1}\frac{q^n}{(1-q^n)^2} + \frac{1}{12}. \tag{2.34}$$

(b) For $\wp'$ we have

$$\frac{1}{(2\pi i)^3}\wp'(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u(1+q^n u)}{(1-q^n u)^3}. \tag{2.35}$$

Proof. See [10, Chapter 1, Theorem 6.2]. □

Theorem 2.4.5. *The q-product expansion for the σ-function is given by*

$$\sigma(u,q) = -\frac{1}{2\pi i}e^{\frac{1}{2}\eta z^2 - \pi iz}(1-u)\prod_{m\geq 1}\frac{(1-q^m u)(1-q^m u^{-1})}{(1-q^m)^2}.$$

Proof. See [10, Chapter I, Theorem 6.4]. □

Theorem 2.4.4 can be used to describe another uniformization for elliptic curves over $\mathbb{C}$. Let $E/\mathbb{C}$ be an elliptic curve corresponding to a normalized lattice $\Lambda_\tau = \tau\mathbb{Z}+\mathbb{Z}$. From Theorem 2.2.15 we know that $C/\Lambda_\tau \cong E(\mathbb{C})$, thus have that $\mathbb{C}^*/q^{\mathbb{Z}} \cong E(\mathbb{C})$. More precisely, there is an isomorphism

$$\begin{aligned} \mathbb{C}^*/q^{\mathbb{Z}} &\xrightarrow{\sim} E(\mathbb{C}) \\ u &\longmapsto (\wp(u,q), \wp'(u,q)), \end{aligned}$$

where the power series expansions of $\wp(u,q)$ and $\wp'(u,q)$ are given by (2.34) and (2.35).

2.5 Geometry of $E(\mathbb{R})$

In this section, we will study some elementary facts for an elliptic curve E defined over $\mathbb{R}$. Since an elliptic curve defined over $\mathbb{R}$ can be viewed as an elliptic curve defined over $\mathbb{C}$, we can use the isomorphism $E(\mathbb{C}) \cong \mathbb{C}^*/q^{\mathbb{Z}}$ to classify elliptic curves over $\mathbb{R}$.

For any $q = e^{2\pi i\tau}$ let E_q be the elliptic curve defined as

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q),$$

where $a_4(q)$ and $a_6(q)$ are the power series given by

$$\begin{aligned} a_4(q) &= -5\sum_{n\geq 1}\frac{n^3q^n}{1-q^n} \\ a_6(q) &= -\frac{5}{12}\sum_{n\geq 1}\frac{n^3q^n}{1-q^n} - \frac{7}{12}\sum_{n\geq 1}\frac{n^5q^n}{1-q^n}. \end{aligned}$$

Let

$$\phi : \mathbb{C}^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(\mathbb{C}) \tag{2.36}$$

$$u \longmapsto (X(u,q), Y(u,q)) \tag{2.37}$$

be the $\mathbb{C}$-analytic isomorphism, where

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2},$$
$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^2} + \sum_{n\geq 1} \frac{q^n}{(1-q^n)^2}.$$

(See [10, Chapter 5, Theorem 1.1] for a proof).

Then the following theorem will play a very important role in our investigation.

Theorem 2.5.1. *Let $E/\mathbb{R}$ be an elliptic curve. Then the following assertions hold.*

(a) There is a unique $q \in \mathbb{R}$ with $0 < |q| < 1$ such that

$$E \cong_{/\mathbb{R}} E_q$$

(i.e., E is $\mathbb{R}$-isomorphic to E_q.)

(b) The composition of the isomorphism in part (a) with the isomorphism ϕ defined in (2.36)*, yields an isomorphism*

$$\psi : \mathbb{C}^*/q^{\mathbb{Z}} \xrightarrow{\sim} E(\mathbb{C})$$

which commutes with complex conjugation. Thus ψ is defined over $\mathbb{R}$ and moreover,

$$\psi : \mathbb{R}^*/q^{\mathbb{Z}} \xrightarrow{\sim} E(\mathbb{R})$$

is an $\mathbb{R}$-analytic isomorphism.

Proof. See [10, Chapter V, Theorem 2.3]. □

We are interested in describing the shape of the group of the $\mathbb{R}$-rational points $E(\mathbb{R})$.

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

$$E : y^2 = x^3 + ax + b. \tag{2.38}$$

The geometry of $E(\mathbb{R})$ depends upon the roots of the cubic equation $x^3 + ax + b = 0$. Recall form Section that E is non-singular if and only if the cubic $x^3 + ax + b$ does not have any repeated roots, or equivalently, the discriminant $\Delta(E) = -(4a^3 + 27b^2)$ is non-zero. If the cubic $x^3 + ax + b$ has three real roots (i.e., $\Delta(E) > 0$) then E is disconnected and will have two components. On the other hand if cubic $x^3 + ax + b$ has only one real root (i.e., $\Delta(E) < 0$) then E is connected. Figure 2.2 represents the connected elliptic curve $y^2 = x^3 - x + 1$ with $\Delta = -368$. The disconnected elliptic curve $y^2 = x^3 - x$ with two components and $\Delta = 64$ is shown in Figure 2.3. We will be using the following definition in later part of this thesis.

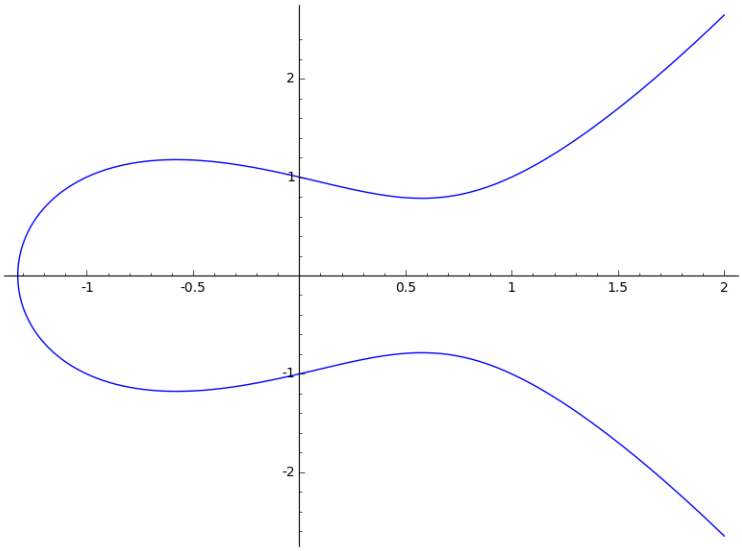

Figure 2.2: Elliptic Curve given by $y^2 = x^3 - x + 1$

Next proposition summarizes the geometry of $E(\mathbb{R})$ and its relation with $q = e^{2\pi i\tau}$ defined in Section 2.4.

Proposition 2.5.2. *Let $E/\mathbb{R}$ be an elliptic curve given by* (2.38)*. Let $\Delta(E)$ be the*

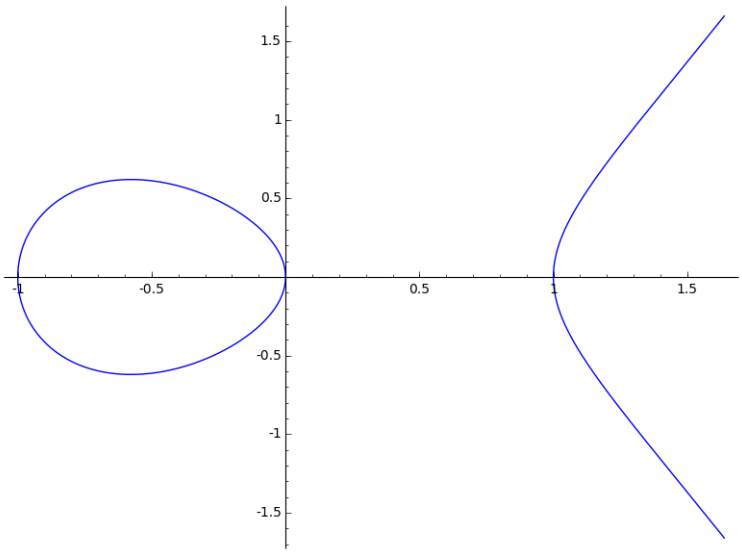

Figure 2.3: Elliptic Curve given by $y^2 = x^3 - x$

discriminant of Weierstrass equation of $E/\mathbb{R}$. *Then there is an isomorphism of real Lie groups*

$$E(\mathbb{R}) \cong \begin{cases} \mathbb{R}/\mathbb{Z} & \text{if } \Delta(E) < 0 \\ (\mathbb{R}/\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) & \text{if } \Delta(E) > 0. \end{cases}$$

Proof. From Theorem 2.5.1 we have that for any elliptic curve $E/\mathbb{R}$ there is a unique $q \in \mathbb{R}$ with $0 < |q| < 1$ and an elliptic curve E_q such that $E \cong_{\mathbb{R}} E_q$. Then using Jacobi's product formula (see [10, Chapter I, Theorem 8.1]) we have

$$u^{12}\Delta(E) = \Delta(E_q) = q\prod_{n\geq 1}(1-q^n)^{24}$$

for some $u \in \mathbb{R}$. Hence

$$\text{Sign } \Delta(E) = \text{Sign } \Delta(E_q) = \text{Sign } q.$$

By [10, Chapter V, Theorem 2.3(b)] there is an isomorphism

$$E(\mathbb{R}) \cong E_q(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}.$$

Thus using the following isomorphisms result follows:

$$\mathbb{R}^*/q^{\mathbb{Z}} \longrightarrow \mathbb{R}/\mathbb{Z};\ u \longmapsto \frac{1}{2}\left(\frac{\log|u|}{\log|q|} - \operatorname{sign}(u) + 1\right) \pmod{\mathbb{Z}} \quad \text{if } q < 0,$$
$$\mathbb{R}^*/q^{\mathbb{Z}} \longrightarrow (\mathbb{R}/\mathbb{Z}) \times \{\pm 1\};\ u \longmapsto \left(\frac{\log|u|}{\log q} \pmod{\mathbb{Z}},\ \operatorname{sign}(u)\right) \text{ if } q > 0.$$

□

Chapter 3

Elliptic Sequences and Elliptic Nets

3.1 Elliptic Sequences

Definition 3.1.1. An *elliptic sequence* over an integral domain R is any sequence (W_n), with $W_n \in R$, satisfying the homogeneous recurrence relation

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2, \qquad m > n > 0. \tag{3.1}$$

Moreover, we can extend an elliptic sequence (W_n) backwards by setting $W_0 = 0$ and $W_{-n} = -W_n$ over R.

Definition 3.1.2. We say that an elliptic sequence is *non-degenerate* if $W_1W_2W_3 \neq 0$. Furthermore, if $W_1 = 1$. we call it a *normalized* elliptic sequence.

We give some examples of elliptic sequences.

Example 3.1.3. $W_n = (0)$ and $W_n = (n)$ are trivial examples of elliptic sequences. Some other examples are

1. $W_n = (n/3)$, where (n/p) is the Legendre symbol.
2. $W_n = (-8/n)$, where (d/n) is the Kronecker symbol.
3. $W_n = \psi_n(P)$, where $\psi_n(P)$ is the value of n-th division polynomial evaluated at P for an elliptic curve E/K and point $P \in E(K)$ (see Section 2.3).

Note that, if (W_n) is an elliptic sequence over a field K, then the sequences (aW_n) and $(b^{n^2}W_n)$ are also elliptic sequences for a and b in K. Furthermore, observe that if (W_n) is an elliptic sequence over R then the sequence (W_n/W_1) is a normalized elliptic sequence over K, where K is the field of fractions of R.

The next proposition shows that certain elliptic sequences can be completely determined by their four initial terms.

Proposition 3.1.4. *Let (W_n) be an elliptic sequence over R with $W_1W_2 \neq 0$. Then W_n satisfies the following two recurrences*

$$W_{2n+1}W_1^3 = W_{n+2}W_n^3 - W_{n-1}W_{n+1}^3 \qquad n \geq 1, \tag{3.2}$$

$$W_{2n}W_2W_1^2 = W_n(W_{n+2}W_{n-1}^2 - W_{n-2}W_{n+1}^2) \qquad n \geq 2. \tag{3.3}$$

Moreover, (W_n) is completely determined by initial values W_1, W_2, W_3, and W_4.

Proof. First observe that by replacing m by $n+1$ in (3.1) we obtain the recurrence (3.2). Second, if we replace m with $n+1$ and n with $n-1$ in (3.1), the resultant recurrence is (3.3). If $W_1W_2 \neq 0$ then the fact that (W_n) is completely determined by initial values W_1, W_2, W_3, and W_4 can be seen by using induction on recurrences (3.2) and (3.3). □

In the above proposition we saw that if a sequence (W_n) satisfy (3.1) it will also satisfy (3.2) and (3.3). The converse of the above fact is also true. In other words, it can also be shown that for a sequence (W_n) to be an elliptic sequence it is enough to show that W_n satisfy (3.2) and (3.3) (see [9, Chapter III, Exercise 3.34]).

In the case when $R = \mathbb{Z}$, an elliptic sequence, with an additional condition of divisibility has many interesting properties. This leads to the concept of an *elliptic divisibility sequence*. The next section is devoted to the study of elliptic divisibility sequences.

3.2 Elliptic Divisibility Sequences

In [14] gave a complete description of elliptic divisibility sequences. In this section we describe some of his results. We start with some definitions.

Definition 3.2.1. An integer sequence (D_n) is called a *divisibility sequence* if $D_m|D_n$ whenever $m|n$.

Definition 3.2.2. An integer elliptic sequence (W_n) is called an *elliptic divisibility sequence* if it is also a divisibility sequence.

As in the case of elliptic sequences an elliptic divisibility sequence is completely determined by its initial values W_1, W_2, W_3, and W_4. In other words, given any integers W_1, W_2, W_3, and W_4 (under certain conditions) we can create an elliptic divisibility sequence. More precisely we have the following theorem

Theorem 3.2.3. *Let (W_n) be a sequence with $W_0 = 0, W_1 = 1$ and $W_2, W_3 \neq 0$ such that (W_n) is a solution of the recurrence*

$$W_{m+n}W_{m-n} = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2, \qquad m \geq n \geq 1. \tag{3.4}$$

Then (W_n) is an elliptic divisibility sequence if and only if W_2, W_3, and W_4 are integers and $W_2|W_4$.

Proof. See [14, Theorem 4.1]. □

It is known that a generic elliptic divisibility sequence can be realized as values of division polynomials. This important fact was proved by Ward [14] in 1948. In order to state Ward's result we need the following definition.

Definition 3.2.4. The Discriminant of an elliptic divisibility sequence (W_n) is defined

by

$$\begin{aligned}\mathrm{Disc}(W_n) = W_4W_2^{15} - W_3^3W_2^{12} + 3W_4^2W_2^{10} - 20W_4W_3^3W_2^7 \\ + 3W_4^3W_2^5 + 16W_3^6W_2^4 + 8W_4^2W_3^3W_2^2 + W_4^4. \quad (3.5)\end{aligned}$$

Definition 3.2.5. An elliptic divisibility sequence (W_n) is said to be *non-singular* if

$$\mathrm{Disc}(W_n) \neq 0.$$

We are ready to describe Ward's structure theorem for elliptic divisibility sequences. The theorem, under certain conditions, says that the values of elliptic divisibility sequences can be written in terms of the values of elliptic functions.

Theorem 3.2.6 (Ward). *Let (W_n) be a non-singular, non-degenerate elliptic divisibility sequence. Then there is a lattice $\Lambda \subset \mathbb{C}$ and a complex number $z \in \mathbb{C}$ such that*

$$W_n = \frac{\sigma(nz;\Lambda)}{\sigma(z;\Lambda)^{n^2}} \quad for\ all\ n \geq 1, \tag{3.6}$$

where $\sigma(z;\Lambda)$ is the Weierstrass σ-function associated to the lattice Λ. Further, the Eisenstein series $g_2(\Lambda)$ and $g_3(\Lambda)$ associated to the lattice Λ and the Weierstrass values $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$ associated to the point z on the elliptic curve $\mathbb{C}/\Lambda$ are in the field $\mathbb{Q}(W_2, W_3, W_4)$. In other words $g_2(\Lambda), g_3(\Lambda), \wp(z;\Lambda), \wp'(z;\Lambda)$ are all defined over the same field as the terms of the sequence (W_n).

Proof. See [14, Theorem 12.1 and 19.1]. □

The expression for $\mathrm{Disc}(W_n)$ is related to the discriminant of the elliptic curve which is associated with the sequence (W_n)

In [11], by employing Theorem 2.4.5 and Theorem 3.2.6, Silverman and Stephens proved the following result regarding the sign of an elliptic divisibility sequence.

Theorem 3.2.7 (Silverman-Stephens). *Let (W_n) be a non-singular, non-degenerate elliptic divisibility sequence. Then possibly after replacing (W_n) by the related sequence $((-1)^{n-1}W_n)$, there is an irrational number $\beta \in \mathbb{R}$ given by*

q	$E(\mathbb{R})$	P	u	Formula	β
$0 < q < 1$	Disconnected	Identity component	$u > 0$	(3.7)	$\log_q u = \log_q \lvert u \rvert$
	Disconnected	Nondentity component	$u < 0$	(3.8)	$\log_q \lvert u \rvert$
$-1 < q < 0$	Connected			(3.7)	$\frac{1}{2}\log_{\lvert q \rvert} u$

Table 3.1: Explicit expressions for β

so that the sign of W_n is given by one of the following formulas:

$$\mathrm{Sign}(W_n) = (-1)^{\lfloor n\beta \rfloor} \qquad for\ all\ \ n. \tag{3.7}$$

$$\mathrm{Sign}(W_n) = \begin{cases} (-1)^{\lfloor n\beta \rfloor + n/2} & if\ n\ is\ even, \\ (-1)^{(n-1)/2} & if\ n\ is\ odd, \end{cases} \tag{3.8}$$

where $\lfloor . \rfloor$ denotes the greatest integer function.

Silverman-Stephens, using Theorem 3.2.6, associated an elliptic curve over $\mathbb{R}$ and a point P in $E(\mathbb{R})$ an to elliptic divisibility sequence (W_n). Then the quantity q in the above Table 3.1 is related to a fixed $\mathbb{R}$-isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$. The number $u \in \mathbb{R}^*$ corresponds to a point P in $E(\mathbb{R})$ under the same isomorphism described above. Furthermore, u is normalized to satisfy $q < |u| < 1$ if $q > 0$ and $q^2 < u < 1$ if $q < 0$.

Proof. Let (W_n) be a nonsingular elliptic divisibility sequence, the using Theorem

3.2.6 choose a lattice Λ and complex number z so that

$$W_n = \frac{\sigma(nz, \Lambda)}{\sigma(z, \Lambda)^{n^2}}. \tag{3.9}$$

For the lattice Λ, let E be the associated elliptic curve

$$E : Y^2 = 4X^3 - g_2(L)X - g_3(L) \tag{3.10}$$

and $P = \big(\wp(z, \Lambda), \wp'(z, \Lambda)\big)$ the associated point on E. Theorem 3.2.6 implies that the curve E is defined over $\mathbb{Q}$ (i.e., $g_2(L), g_3(L) \in \mathbb{Q}$) and that $P \in E(\mathbb{Q})$. In particular, E and P are defined over $\mathbb{R}$. Then [9, Theorem 2.3(b), Chapter V] says that there exists a unique $q \in \mathbb{R}^*$ with $0 < |q| < 1$ such that there is an $\mathbb{R}$-isomorphism

$$\psi : \mathbb{R}^*/q^{\mathbb{Z}} \xrightarrow{\sim} E(\mathbb{R}). \tag{3.11}$$

so the fact that $P \in E(\mathbb{R})$ implies that $\psi^{-1}(P) \in \mathbb{R}^*/q^{\mathbb{Z}}$. Let $u \in \mathbb{R}^*$ be a representative for $\psi^{-1}(P)$. Write $u = e^{2\pi i z}$ with (say) $z \in i\mathbb{R}$ if $u > 0$ and $z \in \frac{1}{2} + i\mathbb{R}$ if $u < 0$. Then the σ-function on $\mathbb{C}^*/q^{\mathbb{Z}}$ given by the Theorem 2.4.5 is

$$\sigma(u, q) = -\frac{1}{2\pi i} e^{\frac{1}{2}\eta z^2 - \pi i z}\theta(u, q) \quad \text{with}$$
$$\theta(u, q) = (1 - u)\prod_{m \geq 1} \frac{(1 - q^m u)(1 - q^m u^{-1})}{(1 - q^m)^2} \tag{3.12}$$

were η is a quasi-period homomorphism defined for lattice Λ, and it disappears when we substitute (3.12) into (3.9). It is important to observe that the σ- function in formula (3.9) and the σ-function defined by the formula (3.12) may only be constant multiples of one another, since $\sigma(z, \Lambda)$ has weight one (i.e., $\sigma(cz, c\Lambda) = c\sigma(z, \Lambda)$).

Hence substituting (3.12) into (3.9), yields

$$W_n = \gamma^{n^2-1} u^{(n^2-n)/2} \frac{\theta(u^n, q)}{\theta(u, q)^{n^2}} \tag{3.13}$$

for some $\gamma \in \mathbb{C}^*$. However, since u, q, and W_n are all in $\mathbb{R}$, taking $n = 2$ and $n = 3$ shows that $\gamma^3 \in \mathbb{R}$ and $\gamma^8 \in \mathbb{R}$, so $\gamma \in \mathbb{R}^*$.

Next observe that since $n^2 - 1 \equiv n - 1 \pmod 2$ for all $n \in \mathbb{Z}$, the effect of a negative γ is simply to replace an elliptic divisibility sequence (W_n) with the equivalent sequence $((-1)^{n-1}W_n)$. Hence without loss of generality, we may assume that $\gamma > 0$.

Furthermore, since the factor $(1-q^m)^2$ always positive it does not contribute to the sign of (3.13). Hence we may discard the $(1 - q^m)^2$ factors appearing in the product expansion (3.12) for $\theta(u, q)$. We now consider several cases, depending on the sign of q and u.

Case I: $0 < q < 1$ **and** $u > 0$

Geometrically, this is the case that $\mathbb{R}^*/q^{\mathbb{Z}}$ has two components and the point $P = \psi(u)$ is on the identity component. The value of the right-hand side of (3.13) is invariant under $u \to q^{\pm 1}u$, so we may choose u to satisfy $q < u < 1$ (See Lemma 4.1.3). Then

$$1 - u > 0 \qquad \text{and} \qquad 1 - q^m u^{\pm 1} > 0 \quad \text{for all } m \geq 1,$$

so $\theta(u, q) \geq 0$. Doing a similar analysis for $\theta(u^n, q)$ implies that

$$1 - q^m u^n > 0 \qquad \text{for all } m \geq 1.$$

Next we have

$$1 - q^m u^{-n} < 0 \iff u^n < q^m \iff n \log_q u > m.$$

Hence there are $\lfloor n \log_q(u) \rfloor$ negative signs. This proves that

$$\text{Parity}(W_n) \equiv \text{Parity}(\theta(u^n, q)) \equiv \lfloor n\beta \rfloor \pmod 2,$$

where $\beta = \log_q u$.

Case II: $0 < q < 1$ **and** $u < 0$

Geometrically, we are again in the case that $\mathbb{R}^*/q^{\mathbb{Z}}$ has two components, and the point u is on the nonidentity component. We may choose u to satisfy $q < |u| < 1$, and then as in Case I, we see that $\theta(u, q) > 0$ and that all factors $1 - q^m u^n$ are positive. Further, since $u < 0$ and $q > 0$, it is clear that $1 - q^m u^{-n} > 0$ for all odd values of n. Thus if n is odd, we also have $\theta(u^n, q) > 0$.

For the case when n is even we have

$$1 - q^m u^{-n} < 0 \iff |u|^n < q^m \iff n \log_q |u| > m.$$

Hence there are $\lfloor n \log_q |u| \rfloor$ negative signs, so

$$\text{Parity}(\theta(u^n, q)) \equiv \lfloor n\beta \rfloor \pmod 2 \qquad \text{when } n \text{ is even},$$

with $\beta = \log_q |u|$.

Finally, since $u < 0$, we observe that

$$\text{Parity}\left[u^{(n^2-n)/2}\right] \equiv \frac{n^2 - n}{2} \equiv \begin{cases} n/2 \pmod 2 & \text{if } n \text{ is even}, \\ (n-1)/2 \pmod 2 & \text{if } n \text{ is odd}. \end{cases}$$

Case III: $q < 0$

Geometrically, this is the case that the curve $\mathbb{R}^*/q^{\mathbb{Z}}$ is connected. Using Lemma 4.1.3

we may assume that

$$u > 0 \qquad \text{and} \qquad q^2 < u < 1.$$

For above choice of u, we have

$$1 - q^m u^{\pm 1} > 1 - |q|^{m-2} \geq 0 \qquad \text{for } m \geq 2,$$

However, when $m = 1$, it is also positive, since $q < 0$ and $u > 0$. Hence $\theta(u, q) > 0$.

Next we examine the factors of $\theta(u^n, q)$. Since $|q| < 1$ and $u < 1$, the factors $1 - q^m u^n$ are positive. Further, the factors $1 - q^m u^{-n}$ with m odd are also positive, since $q < 0$ and $u > 0$. Suppose now that m is even. Then

$$1 - q^m u^{-n} < 0 \iff u^n < |q|^m \iff n \log_{|q|} u > m.$$

Thus we get one negative factor in $\theta(u^n, q)$ for each even integer smaller than $n \log_{|q|}(u)$, so

$$\text{Parity}(W_n) \equiv \text{Parity}(\theta(u^n, q)) \equiv \lfloor n\beta \rfloor \pmod 2, \tag{3.14}$$

where $\beta = \frac{1}{2} \log_{|q|} u$. □

Example 3.2.8. Consider the elliptic divisibility sequence

$$1,\ 1,\ -5,\ -16,\ 109,\ 735,\ -9529,\ -103904,\ 3464585,\ 28525409,\ -5987285341,$$
$$160484333520, 53055650250901, -6621577642502849, \ldots$$

This is the elliptic divisibility sequence associated to the elliptic curve $y^2 + xy = x^3 - x$ defined over $\mathbb{Q}$ and point $P = (-1, 1) \in E(\mathbb{Q})$. Then there is an $\mathbb{R}$-isomorphism

$E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ where $P \longleftrightarrow u$ with explicit values

$$q = 0.00129253745290950573653818145 51\ldots,$$
$$u = -0.54050181433028242974505191985\ldots.$$

Observe that q is positive, thus $E(\mathbb{R})$ is disconnected. Using Theorem 3.2.7 the sign of W_n is given by

$$\text{Parity}(W_n) \equiv \begin{cases} \lfloor n\beta \rfloor + \dfrac{n}{2} + 1 & \text{if } n \text{ is even,} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd,} \end{cases}$$

with explicit value $\beta = 0.092503923753913072607717383131\ldots$.

3.3 Elliptic Nets

This section is devoted to the theory of elliptic nets. Elliptic nets are higher dimensional analogue of elliptic sequences. In 2008, K. Stange in her Ph.D. thesis [12] introduced the concept of an elliptic net. We start by giving the definition of an elliptic net.

Definition 3.3.1. Let A be a finitely-generated free abelian group, and let R be an integral domain. An *elliptic net* is a map $W : A \longrightarrow R$ with $W(0) = 0$, and such that for all $p, q, r, s \in A$,

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\quad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\quad + W(r+p+s)W(r-p)W(q+s)W(q) = 0. \end{aligned} \tag{3.15}$$

We also define the *rank* of an elliptic net to be the rank of the free abelian group A.

Example 3.3.2. The following are some examples of elliptic nets.

(1) The zero map $W : \mathbb{Z}^n \longrightarrow R$ defined as $W(\mathbf{v}) = 0$ for all $\mathbf{v} \in \mathbb{Z}^n$. This map is called the *zero net*.

(2) The identity map $W : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined as $W(v) = v$ for all $v \in \mathbb{Z}$ is a rank 1 elliptic net.

(3) The map $W : \mathbb{Z} \longrightarrow \mathbb{Z}$ given by $W(n) = \left(\frac{n}{3}\right)$, the Legendre symbol of n modulo 3, is an elliptic net of rank 1. The fact that $W(n)$ is an elliptic net can be verified by observing that at least one of $p,\ q,\ r,\ p-q,\ q-r$, and $r-p$ is divisible by 3.

(4) The next example is the most important class of elliptic nets.

Let $E : y^2 + xy = x^3 - x^2 + 4x - 4$ be an elliptic curve over $\mathbb{Q}$. Let $P = (1, 0)$ and $Q = (2, 2)$ be two points in $E(\mathbb{Q})$. Then the following table is an example of a rank 2 elliptic net $W(m, n)$ derived from the values of net polynomials associated to curve E and points P and Q (for definition of net polynomials and the fact that they satisfy recurrence (3.15) see Definition 3.4.1 and Theorem 3.4.2).

			$\vdots$			
	-193904640	239163904	171823616	-583063552	-3544041984	
	-1013696	74944	805824	396224	-17965504	
	-4656	-3392	3952	24560	-76032	
$\cdots$	20	-92	-84	764	6364	$\cdots$
	6	-2	-16	2	1194	
	1	1	-3	-25	227	
	0	1	1	-28	-309	
			$\vdots$			

In the above array, the bottom-left corner represents the value $W(0, 0)$, and the top-right corner is the value $W(4, 6)$. The dots show that the table is just a portion

of the elliptic net. The row and column containing zero in the table are elliptic nets of rank 1. In other words the row and column having zero in the table are elliptic sequences.

Next proposition summarizes some basic properties of elliptic nets which we will be using in this thesis.

Proposition 3.3.3. *Let $W : A \longrightarrow R$ be an elliptic net, then*

(a) For any $v \in A$, we have $W(-v) = -W(v)$ (i.e., W is an odd function).

(b) Let $B \subset A$ be any subgroup of A, then the restriction map $W|_B : B \longrightarrow R$ is an elliptic net.

(c) Let I be an integral domain and $\pi : R \longrightarrow S$ be any homomorphism of integral domains, then the composition $\pi \circ W : A \longrightarrow S$ is an elliptic net.

Proof. (a) If $W(-v) = -W(v) = 0$ for all $v \in A$, then there is nothing to prove. Assume that one of $W(v)$ or $W(-v)$ is non-zero, without loss of generality we may assume that $W(v) \neq 0$. Then by letting $p = q = v$ and $r = s = 0$ in (3.15) and using the fact that $W(0) = 0$ we have

$$W(v)^3[W(v) + W(-v)] = 0.$$

Since R is an integral domain and $W(v) \neq 0$, we see that $W(-v) = -W(v)$.

The proofs of (b) and (c) are straightforward and can be seen easily by verifying that $W|_B$ and $\pi \circ W$ satisfy the recurrence (3.15).

□

Proposition 3.3.4. *The values of a rank 1 elliptic net can be realized as an elliptic sequence.*

Proof. Let $A = \mathbb{Z}$ in the definition of the elliptic net and set $p = m,\ q = n,\ r = 1$, and $s = 0$ in (3.15), then using the fact that W is an odd function we see that $(W(n))$ satisfies (3.4). In other words the values of rank 1 elliptic net form an elliptic sequence. □

The above proposition shows that elliptic nets can be considered as generalization of elliptic sequences.

We give the following definitions in order to have a better understanding of elliptic nets. These definitions generalize the concepts of normalized and non-degenerate elliptic sequence to elliptic nets.

Definition 3.3.5. Let $W : \mathbb{Z}^n \longrightarrow R$ be an elliptic net. Let $\mathcal{B} = \{\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}\}$ be the standard basis of $\mathbb{Z}^n$. We say that W is *non-degenerate* if $W(\mathbf{e_i}),\ W(\mathbf{2e_i}) \neq 0$ for all $1 \leq i \leq n$, and $W(\mathbf{e_i} \pm \mathbf{e_j}) \neq 0$ for $1 \leq i, j \leq n,\ i \neq j$. For the case of $n = 1$ we need an additional condition that $W(\mathbf{3e_i}) \neq 0$. If any of the above conditions is not satisfied we say that W is *degenerate*.

Definition 3.3.6. Let $W : \mathbb{Z}^n \longrightarrow R$ be an elliptic net. Then we say that W is *normalized* if $W(\mathbf{e_i}) = 1$ for all $1 \leq i \leq n$ and $W(\mathbf{e_i} + \mathbf{e_j}) = 1$ for all $1 \leq i < j \leq n$.

Next we will describe an equivalence relation among elliptic nets. In order to do this, we recall some facts about *quadratic forms* on abelian groups. We start with the following definition.

Definition 3.3.7. Let B and C be two abelian groups under addition. A *quadratic form* is a function $f : B \longrightarrow C$ such that

$$f(a+b+c) - f(a+b) - f(b+c) - f(a+c) + f(a) + f(b) + f(c) = 0 \qquad (3.16)$$

for all $a, b, c \in B$.

For purpose of this thesis we are interested in the case when $B = \mathbb{Z}^n$ under addition while the group C is the multiplicative group of real numbers. In this case we can rewrite (3.16) as follows

$$f(a+b+c)f(a+b)^{-1}f(b+c)^{-1}f(c+a)^{-1}f(a)f(b)f(c) = 1. \tag{3.17}$$

Example 3.3.8. Let K be a field. These are some examples of quadratic forms:

(1) Let $a_i, b_{ij} \in K$. Then the function $f : \mathbb{Z}^n \longrightarrow K$ defined by

$$f(v_1, v_2, \ldots, v_n) = \sum_{i=1}^{n} a_i v_i^2 + \sum_{1 \leq i < \leq jn} b_{ij} v_i v_j$$

is a quadratic form on $\mathbb{Z}^n$ with values in K.

(2) Let $p_i, q_{ij} \in K^*$. Then the function $g : \mathbb{Z}^n \longrightarrow K^*$ defined by

$$g(v_1, v_2, \ldots, v_n) = \prod_{i=1}^{n} p_i^{v_i^2} \prod_{1 \leq i < \leq jn} q_{ij}^{v_i v_j}$$

is a quadratic form on $\mathbb{Z}^n$ with values in K^*.

Lemma 3.3.9. *Let $f : \mathbb{Z}^n \longrightarrow C$ be a quadratic form, where C is a group under addition. Let $B = \{\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}\}$ be the standard basis of $\mathbb{Z}^n$. Suppose that the values of f at the basis vectors $\mathbf{e_i}$ and $\mathbf{e_i} + \mathbf{e_j}$ are known. Then we can find the value of f at any $\mathbf{v} \in \mathbb{Z}^n$.*

Proof. It is known that a quadratic form $f : \mathbb{Z}^n \longrightarrow C$ satisfies

$$f\left(\sum_{i=1}^{n} v_i \mathbf{e_i}\right) = \sum_{i=1}^{n} \left(2v_i^2 - \sum_{i=1}^{n} v_i v_j\right) f(\mathbf{e_i}) + \sum_{1 \leq i < j \leq n} v_i v_j f(\mathbf{e_i} + \mathbf{e_j}),$$

(See [13, Lemma 4.5]). Since the values of $\mathbf{e_i}$ and $\mathbf{e_i} + \mathbf{e_j}$ are known, the result follows from the above identity. □

Next proposition gives a way to create a new elliptic net out of a known elliptic net.

Proposition 3.3.10. *Let $W : A \longrightarrow R$ be an elliptic net. Let $f : A \longrightarrow R^*$ be a quadratic form. Then the map $W^f : A \longrightarrow R$ defined by*

$$W^f(v) = f(v)W(v)$$

is an elliptic net.

Proof. See [13, Theorem 6.1]. □

Definition 3.3.11. Let $W : A \longrightarrow R$ and $W' : A \longrightarrow R$ be two elliptic nets. Let $f : A \longrightarrow R^*$ be a quadratic form such that

$$W(v) = f(v)W'(v).$$

Then we say that the elliptic nets W and W' are *scale equivalent*.

The relation of being scale equivalent is an equivalence relation. Note that given any non-degenerate elliptic net $W : \mathbb{Z}^n \longrightarrow R$ we have only one scale equivalent normalized elliptic net associated to W. More precisely we have the following proposition.

Proposition 3.3.12. *Let $W : \mathbb{Z}^n \longrightarrow R$ be a non-degenerate elliptic net. Then there is exactly one scaling W^f which is normalized.*

Proof. Let $\mathcal{B} = \{\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}\}$ be the standard basis for $\mathbb{Z}^n$. Define

$$\begin{aligned} A_{ii} &= W(\mathbf{e_i})^{-1}, \qquad \text{for } 1 \leq i \leq n, \\ A_{ij} &= \frac{W(\mathbf{e_i})W(\mathbf{e_j})}{W(\mathbf{e_i} + \mathbf{e_j})} \qquad \text{for } 1 \leq i < j \leq n, \\ f(\mathbf{v}) &= \prod_{1 \leq i \leq j \leq n} A_{ij}^{v_i v_j}. \end{aligned}$$

Then $W^f = f(\mathbf{v})W$ is a normalized, non-degenerate elliptic net.

To prove the uniqueness let f and g be two scalings such that W^f and W^g are normalized. Then we have

$$f(\mathbf{e_i})W(\mathbf{e_i}) = g(\mathbf{e_i})W(\mathbf{e_i}) = 1 \qquad \text{for } 1 \leq i \leq n.$$

Since W is non-degenerate we have that $W(\mathbf{e_i}) = 1$. Thus we see that $(f-g)(\mathbf{e_i}) = 0$ for all $1 \leq i \leq n$. Similarly, we have that $(f-g)(\mathbf{e_i} + \mathbf{e_j}) = 0$ for all $1 \leq i < j \leq n$. Using Lemma 3.3.9 we get that $(f-g)(\mathbf{v}) = 0$ or equivalently $f(\mathbf{v}) = g(\mathbf{v})$.

□

3.4 Net Polynomials

As we saw in Section 2.3, division polynomials can be used to construct elliptic divisibility sequences. Here we describe a generalization of division polynomials, the so called *net polynomials,* and show that the values of these polynomials generate elliptic nets. We start with the following definition.

Definition 3.4.1. Let $\Lambda \subset \mathbb{C}$ be a fixed lattice corresponding to an elliptic curve $E/\mathbb{C}$. For an n-tuple $\mathbf{v} = (v_1, v_2, ..., v_n) \in \mathbb{Z}^n$, define a function $\Omega_{\mathbf{v}}$ (with respect to Λ) on $\mathbb{C}^n$ in variable $\mathbf{z} = (z_1, z_2, ..., z_n)$ as follows:

$$\Omega_{\mathbf{v}}(\mathbf{z};\Lambda) = (-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1\leq i<j\leq n} v_i v_j - 1} \frac{\sigma(v_1 z_1 + v_2 z_2 + ... + v_n z_n;\Lambda)}{\prod_{i=1}^{n} \sigma(z_i;\Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1\leq i<j\leq n} \sigma(z_i + z_j;\Lambda)^{v_i v_j}} \tag{3.18}$$

where $\sigma(z;\Lambda)$ is the Weierstrass σ-function defined in Section 2.2.2.

In special case of $n = 1$, for each $v \in \mathbb{Z}$, we have

$$\Omega_v(z;\Lambda) = (-1)^{v^2-1} \frac{\sigma(vz,\Lambda)}{\sigma(z,\Lambda)^{v^2}} = \psi_v(\wp(z), \frac{1}{2}\wp'(z)),$$

where $\psi_v(x, y)$ is the v-th division polynomial defined in Section 2.3. See Theorem 2.3.9.

In the case $n = 2$, for each pair $(v_1, v_2) \in \mathbb{Z} \times \mathbb{Z}$, the function $\Omega_{(v_1,v_2)}$ on $\mathbb{C} \times \mathbb{C}$ in variables z_1 and z_2 is

$$\Omega_{(v_1,v_2)}((z_1, z_2); \Lambda) = \frac{\sigma(v_1 z_1 + v_2 z_2; \Lambda)}{\sigma(z_1; \Lambda)^{v_1^2 - v_1 v_2} \sigma(z_1 + z_2; \Lambda)^{v_1 v_2} \sigma(z_2; \Lambda)^{v_2^2 - v_1 v_2}}.$$

We can show that $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ satisfies (3.15). Thus we have the following theorem.

Theorem 3.4.2 (Stange). *Let $\Lambda \subset \mathbb{C}$ be a fixed lattice corresponding to an elliptic curve $E/\mathbb{C}$. Then for a fixed $\mathbf{z} \in \mathbb{C}^n$, the function*

$$\begin{aligned} \Omega(\mathbf{z}; \Lambda) : \mathbb{Z}^n &\longrightarrow \mathbb{C} \\ \mathbf{v} &\longmapsto \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) \end{aligned}$$

is an elliptic net.

Proof. See [13, Theorem 3.7]. □

There is a close relation between the rational function $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ and elliptic functions. In fact we can show that $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ is itself an elliptic function with respect to each variable z_i. More precisely we have the following proposition.

Proposition 3.4.3. *Let E be an elliptic curve and Λ be its corresponding lattice. Then the rational functions $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ are elliptic functions in each variable.*

Proof. Let $\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{C}$ and let $\omega_1 \in \Lambda$. Without loss of generality we will show that $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ is elliptic in the variable z_1. Let $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ and $\mathbf{w} = (\omega_1, 0, \ldots, 0) \in \mathbb{C}^n$. Using (2.22), we have

$$\frac{\Omega_{\mathbf{v}}(\mathbf{z} + \mathbf{w}; \Lambda)}{\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)} = \frac{\lambda(v_1 \omega_1)}{\lambda(\omega_1)^{v_1^2}}$$

If $\omega_1,\ v_1\omega_1 \notin 2\Lambda$, then we see that v_1 is odd, so $\lambda(\omega_1)^{v_1^2} = \lambda(v_1\omega_1) = -1$. If $\omega_1 \notin 2\Lambda$ but $v_1\omega_1 \in 2\Lambda$, then v_1 must be even, and so $\lambda(\omega_1)^{v_1^2} = \lambda(v_1\omega_1) = 1$. Finally, if $\omega \in 2\Lambda$, then $v_1\omega \in 2\Lambda$, and $\lambda(\omega_1) = \lambda(v_1\omega_1) = 1$. Therefore we have

$$\frac{\lambda(v_1\omega_1)}{\lambda(\omega_1)^{v_1^2}} = 1$$

in each case. Thus $\Omega_{\mathbf{v}}$ is invariant under adding a period to the variable z_1. Similarly $\Omega_{\mathbf{v}}$ is elliptic in each variable. □

Definition 3.4.4. Let E be an elliptic curve defined over $\mathbb{C}$, and let Λ be its corresponding lattice. Let $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ be an n-tuple consisting of n points in $E(\mathbb{C})$ such that $P_i \neq \mathcal{O}$ for each i and $P_i \pm P_j \neq \mathcal{O}$ for $1 \leq i < j \leq n$. Let $\mathbf{z} = (z_1, z_2, ..., z_n)$ in $\mathbb{C}^n$ be such that each z_i corresponds to P_i under the isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. Then the function

$$\begin{aligned} \Psi(\mathbf{P}; E) : \mathbb{Z}^n &\longrightarrow \mathbb{C} \\ \mathbf{v} &\longmapsto \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) \end{aligned}$$

is an elliptic net with values in $\mathbb{C}$. We call $\Psi(\mathbf{P}; E)$ the *elliptic net associated to E (over $\mathbb{C}$) and $\mathbf{P}$*.

Note that in the above definition we have an elliptic curve over $\mathbb{C}$ and the associated elliptic net $\Psi(\mathbf{P}; E)$ have values in $\mathbb{C}$ as well. However for the purpose of this thesis we are only interested in elliptic nets with values in $\mathbb{R}$. Next we show that if E is defined over $\mathbb{R}$ and $\mathbf{P} \in E(\mathbb{R})^n$ then $\Psi(\mathbf{P}; E)$ takes values in $\mathbb{R}$.

Let E be an elliptic curve defined over $\mathbb{R}$ with the Weierstrass equation $f(x, y) = 0$, where

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \ ;\ a_i \in \mathbb{R}. \tag{3.19}$$

Let $\mathcal{S}^{\text{univ}} = \mathbb{Z}[\alpha_1, \alpha_3, \alpha_3, \alpha_4, \alpha_6]$ be the polynomial ring over $\mathbb{Z}$ in variables α_i. For any

positive integer n let

$$\mathcal{R}_n^{\text{univ}} = \mathcal{S}^{\text{univ}}[x_i, y_i]_{1\le i\le n}[(x_i - x_j)^{-1}]_{1\le i<j\le n}/\langle f^{\text{univ}}(x_i, y_i)\rangle_{1\le i\le n},$$

where $f^{\text{univ}}(x, y) = y^2 + \alpha_1 xy + \alpha_3 y - x^3 - \alpha_2 x^2 - \alpha_4 x - \alpha_6$. Then for every elliptic curve $E/\mathbb{R}$ defined by the polynomial (3.19) and point $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ in $E(\mathbb{R})^n$ such that $P_i \neq \mathcal{O}$ for each i and $P_i \pm P_j \neq \mathcal{O}$ for $1 \le i < j \le n$, we can find a morphism

$$\pi = \pi_{\mathbf{P};E} : \mathcal{R}_n^{\text{univ}} \longrightarrow \mathbb{R}$$

so that $\pi(\alpha_i) = a_i$, and $(\pi(x_i), \pi(y_i)) = P_i$. Then we have the following theorem.

Theorem 3.4.5 (Stange). *For each $\mathbf{v} \in \mathbb{Z}^n$, there is a $\Psi_{\mathbf{v}}^{univ} \in \mathcal{R}^{univ}$ so that the map $\Psi^{univ} : \mathbf{v} \longmapsto \Psi_{\mathbf{v}}^{univ}$ is an elliptic net, and for any elliptic curve $E/\mathbb{C}$ and $\mathbf{P} \in E(\mathbb{C})^n$ with $P_i \neq \mathcal{O}$ for each i and $P_i \pm P_j \neq \mathcal{O}$ for $1 \le i < j \le n$, we have*

$$\pi_{\mathbf{P};E} \circ \Psi^{univ} = \Psi(\mathbf{P}; E).$$

Proof. See [13, Section 4]. □

Let $\mathcal{R}_n^{\text{univ}}$, $\mathcal{S}^{\text{univ}}$ as before and let $E/\mathbb{R}$ be an elliptic curve. Then there exists a map $\pi_E : \mathcal{S}^{\text{univ}} \longrightarrow \mathbb{R}$, such that $\pi_E(\alpha_i) = a_i$. This induces a map

$$(\pi_E)_* : \mathcal{R}_n^{\text{univ}} \longrightarrow \mathbb{R}[x_i, y_i]_{1\le i\le n}[(x_i - x_j)^{-1}]_{1\le i<j\le n}/\langle f(x_i, y_i)\rangle_{1\le i\le n}.$$

Then by part (c) of Proposition 3.3.3, the map $\Psi = (\pi_E)_* \circ \Psi^{\text{univ}}$ defines an elliptic net with values in

$$\mathcal{R}_n = \mathbb{R}[x_i, y_i]_{1\le i\le n}[(x_i - x_j)^{-1}]_{1\le i<j\le n}/\langle f(x_i, y_i)\rangle_{1\le i\le n}.$$

We call $\Psi_{\mathbf{v}} \in \mathcal{R}_n$ the $\mathbf{v}$-*th net polynomial* associated to E. Now let $P_i \neq \mathcal{O}$ for

each i and $P_i \pm P_j \neq \mathcal{O}$ for $1 \leq i < j \leq n$, then by part (c) of Proposition 3.3.3, $\Psi(\mathbf{P}; E) : \mathbf{v} \longmapsto \Psi_{\mathbf{v}}(\mathbf{P})$ is an elliptic net with values in $\mathbb{R}$. We call $\Psi(\mathbf{P}; E)$ the elliptic net associated to E (over $\mathbb{R}$) and $\mathbf{P}$.

In the next proposition we give explicit expressions for the net polynomials for the case of $n = 1$ and 2.

Proposition 3.4.6. *Let E/K be an elliptic curve given by the generalized Weierstrass equation*

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

and let

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Let $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ be the net polynomial associated to E and point $\mathbf{P}$. Then we have the following expressions for $\Psi_{\mathbf{v}}(\mathbf{P}; E)$.

(a) For rank 1 elliptic net $\Psi_n(P; E)$ where $P = (x, y)$, we have

$$\Psi_1 = 1, \quad \Psi_2 = 2y + a_1x + a_3,$$
$$\Psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$
$$\Psi_4 = \Psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2).$$

(b) For rank 2 elliptic net $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ *where* $P_1 = (x_1, y_1)$ *and* $P_2 = (x_2, y_2)$*, we have*

$$\begin{aligned}
\Psi_{(1,0)} &= \Psi_{(0,1)} = \Psi_{(1,1)} = 1, \\
\Psi_{(1,-1)} &= x_2 - x_1, \quad \Psi_{(-1,1)} = x_1 - x_2, \\
\Psi_{(2,1)} &= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2, \\
\Psi_{(1,2)} &= x_1 + 2x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2.
\end{aligned}$$

Proof. See [13, Proposition 3.8]. □

3.5 Curve-Net Theorem

In the previous section we showed that given an elliptic curve E/K and a collection of points $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ in $E(K)^n$ we can generate an elliptic net $\Psi(\mathbf{P}; E)$ with values in K. (These elliptic nets arise as values of the net polynomials associated to elliptic curves and points on them). One can ask the following question: Given an elliptic net $W : \mathbb{Z}^n \longrightarrow K$, can we find an elliptic curve E/K and a collection of points $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ in $E(K)^n$ such that $W = \Psi(\mathbf{P}; E)$. This section deals with this question. We will show that for certain elliptic nets the answer to the above question is positive. More precisely, for certain elliptic nets $W : \mathbb{Z} \longrightarrow K$ or $W : \mathbb{Z}^2 \longrightarrow K$, we have the following two propositions that associate to W an elliptic curve E and a collection of points $\mathbf{P}$ such that $W = \Psi(\mathbf{P}; E)$.

Proposition 3.5.1 (Swart). *Let* $W : \mathbb{Z} \longrightarrow K$ *be a normalized non-degenerate elliptic net. Then there is a cubic curve* $\mathcal{C}$ *given by*

$$\mathcal{C} : \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where

$$a_1 = \frac{W(2) + W(2)^5 - 2W(2)W(3)}{W(2)^2W(3)},$$
$$a_2 = \frac{W(2)W(3)^2 + W(4) + W(2)^5 - W(2)W(3)}{W(2)^3W(3)},$$
$$a_3 = W(2), \qquad a_4 = 1, \qquad a_6 = 0,$$

such that $\Psi(P; \mathcal{C}_{ns}) = W$, *where* $P = (0, 0)$ *is non-singular point and* $\mathcal{C}_{ns}$ *is the non-singular part of* $\mathcal{C}$.

Proof. See [13, Proposition 6.3]. □

Proposition 3.5.2 (**Stange**). *Let* $W : \mathbb{Z}^2 \longrightarrow R$ *be a normalized non-degenerate elliptic net. Then there is a cubic curve* $\mathcal{C}$ *given by*

$$\mathcal{C} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where

$$a_1 = \frac{W(2,0) - W(0,2)}{W(2,1) - W(1,2)}, \qquad a_2 = 2W(2,1) - W(1,2),$$
$$a_3 = W(2,0), \quad a_4 = W(2,1)[W(2,1) - W(1,2)], \quad a_6 = 0,$$

along with the points

$$P_1 = (0, 0), \quad Q = (W(1,2) - W(2,1), 0),$$

such that $\Psi(\mathbf{P}; \mathcal{C}_{ns}) = W$, *where* $\mathbf{P} = (P, Q)$ *and* $\mathcal{C}_{ns}$ *is the non-singular part of* $\mathcal{C}$.

Proof. See [13, Proposition 6.4]. □

More generally, similar to the case of elliptic divisibility sequences, there is a relationship between elliptic nets and elliptic curves. In [13] this relationship is made

explicit using *curve-net* theorem. In order to state this theorem we need the following definitions.

Definition 3.5.3. We call a change of variables of a cubic curve in Weierstrass form to be *unihomothetic* if it is of the form

$$x' = x + r, \qquad y' = y + sx + t$$

for some r, s, and t.

Definition 3.5.4. Let $\mathcal{C}$ be a cubic curve given by $f(x, y) = 0$ defined over a field K, where

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

Let $C_{ns}(K)$ denotes the non-singular part of $\mathcal{C}$ defined over K. Then the set of points $\{P_1, P_2, \ldots, P_n\}$ on $C_{ns}(K)$ are called *appropriate* if the following holds:

(1) $P_i \neq 0$ for each i,

(2) $2P_i \neq 0$ for each i,

(3) $3P_1 \neq 0$ whenever $n = 1$ and

(4) $P_i \neq \pm P_j$ for $i \neq j$.

The next theorem establishes the relation between elliptic nets and elliptic curves.

Theorem 3.5.5 (Stange). *For each field K, there is an explicit isomorphism of sets*

$$\{\textit{scale equivalence classes of non-degenerate elliptic nets } W : \mathbb{Z}^n \to K \textit{ for some } n\ \}$$

$$\updownarrow$$

$$\{\textit{tuples } (C, P_1, P_2....P_n) \textit{ for some } n, \textit{ where } C \textit{ is a cubic curve in}$$
$$\textit{Weierstrass form over } K, \textit{ considered modulo unihomothetic}$$
$$\textit{changes of variables, and such that } \{P_i\} \in C_{ns}(K)^n \quad \textit{is appropriate } \}$$

Non-singular nets correspond to elliptic curves. The bijection takes an elliptic net of rank n to a tuple with n points. The elliptic net W associated to a tuple $(C, P_1, P_2....P_n)$ *satisfies the property that* $W(v_1, \ldots, v_n) = 0$ *if and only if* $v_1P_1 + \cdots + v_nP_n = 0$ *on the curve C.*

Proof. See [13, Theorem 7.4]. □

Chapter 4

The Signs in an Elliptic Net

In this chapter we prove the main result of this thesis which generalizes Silverman-Stephens' theorem [11, Theorem 4] for elliptic divisibility sequences to the case of elliptic nets. The first section of this chapter is devoted to developing a formula for the sign of elliptic nets arising from values of net polynomials. Some examples for various cases of the formula are also given. The second section of the chapter gives a formula for signs in non-singular, non-degenerate elliptic nets up to quadratic forms.

4.1 The Signs in the Elliptic Net $\Psi(\mathbf{P}; E)$

Let E be an elliptic curve defined over $\mathbb{R}$ and Λ be a lattice associated to it. Let $\mathbf{P} = (P_1, P_2, \ldots, P_n) \in E(\mathbb{R})^n$ be such that $P_i \neq \mathcal{O}$ for $1 \leq i \leq n$ and $P_i \pm P_j \neq \mathcal{O}$ for $1 \leq i < j \leq n$. Let

$$\begin{aligned} \Psi(P; E) : \mathbb{Z}^n &\longrightarrow \mathbb{R} \\ \mathbf{v} &\longmapsto \Psi_{\mathbf{v}}(P; E) \end{aligned}$$

be the elliptic net associated to E and P. From the construction of net polynomials over field $\mathbb{R}$ described in Section 3.4 we know that

$$\Psi_{\mathbf{v}}(P; E) = \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda),$$

where $\mathbf{z}$ is the n-tuple corresponding to $\mathbf{P}$ under the isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ and $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ is given by

$$\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) = (-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \le i < j \le n} v_i v_j - 1} \frac{\sigma(v_1 z_1 + v_2 z_2 + ... + v_n z_n; \Lambda)}{\prod_{i=1}^{n} \sigma(z_i; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le i < j \le n} \sigma(z_i + z_j; \Lambda)^{v_i v_j}}. \tag{4.1}$$

We compute the sign of $\Psi_{\mathbf{v}}(P; E)$ or equivalently $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$. We start by finding the q-expansion of $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$.

Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice with basis $[\omega_1, \omega_2]$. Let Λ_τ be the normalized lattice with basis $[\tau, 1]$, where $\tau = \omega_1/\omega_2$ is in the upper half-plane. Recall from Theorem 2.4.5 that the q-expansion for $\sigma(z; \Lambda_\tau)$ is given by

$$\sigma(z; \Lambda_\tau) = -\frac{1}{2\pi i} e^{\frac{1}{2} z^2 \eta - \pi i z} (1 - w) \prod_{m \ge 1} \frac{(1 - q^m w)(1 - q^m w^{-1})}{(1 - q^m)^2}, \tag{4.2}$$

where $w = e^{2\pi i z}$, $q = e^{2\pi i \tau}$, and η is the quasi-period homomorphism. The next proposition gives the q-expansion for the numerator in the expression for $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda_\tau)$ in (4.1).

Proposition 4.1.1. *Let* $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$ *and* $\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n$. *Let* $w_j = e^{2\pi i z_j}$ *for* $j = 1, 2, \ldots n$ *and* $q = e^{2\pi i \tau}$. *Then*

$$\sigma(\mathbf{v}\cdot\mathbf{z}; \Lambda_\tau) = -\frac{1}{2\pi i} e^{\frac{1}{2}(\mathbf{v}\cdot\mathbf{z})^2 \eta - \pi i (\mathbf{v}\cdot\mathbf{z})} \Big(1 - \prod_{j=1}^{n} w_j^{v_j}\Big) \prod_{m \ge 1} \frac{(1 - q^m \prod_{j=1}^{n} w_j^{v_j})(1 - q^m \prod_{j=1}^{n} w_j^{-v_j})}{(1 - q^m)^2}, \tag{4.3}$$

where $\mathbf{v} \cdot \mathbf{z} = v_1 z_1 + v_2 z_2 + ... + v_n z_n$.

Proof. Note that (4.2) gives the q-expansion for σ-function. The result is obtained by replacing z with $\mathbf{v} \cdot \mathbf{z} = v_1 z_1 + v_2 z_2 + + \cdots v_n z_n$ in (4.2). Observe that the map $z \longmapsto v_1 z_1 + v_2 z_2 + + \cdots v_n z_n$, corresponds to $w \longmapsto \prod_{j=1}^{n} w_j^{v_j}$. □

Next, by applying (4.3) and (4.2) in the numerator and the denominator of (4.1), we have the following explicit expression for $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda_\tau)$.

Proposition 4.1.2. *Let $\mathbf{v}, \mathbf{z}, w_i$ and q be the same as in Proposition 4.1.1. Then we have*

$$\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda_\tau) = (2\pi i)^{\sum_{j=1}^{n} v_j^2 - \sum_{1\le j<k\le n} v_j v_k - 1} \prod_{j=1}^{n} w_j^{\frac{v_j^2 - v_j}{2}} \frac{\theta\Big(\prod_{j=1}^{n} w_j^{v_j}, q\Big)}{\prod_{j=1}^{n} \theta(w_j, q)^{2v_j^2 - \sum_{k=1}^{n} v_j v_k} \prod_{1\le j<k\le n} \theta(w_j w_k, q)^{v_j v_k}},$$

where

$$\theta(w_j, q) = (1 - w_j) \prod_{m\ge 1} \frac{(1 - q^m w_j)(1 - q^m w_j^{-1})}{(1 - q^m)^2},$$
$$\theta(w_j w_k, q) = (1 - w_j w_k) \prod_{m\ge 1} \frac{(1 - q^m w_j w_k)(1 - q^m w_j^{-1} w_k^{-1})}{(1 - q^m)^2},$$

and

$$\theta\Big(\prod_{j=1}^{n} w_j^{v_j}, q\Big) = \Big(1 - \prod_{j=1}^{n} w_j^{v_j}\Big) \prod_{m\ge 1} \frac{(1 - q^m \prod_{j=1}^{n} w_j^{v_j})(1 - q^m \prod_{i=1}^{n} w_j^{-v_j})}{(1 - q^m)^2}.$$

Proof. The proof is highly computational and follows by substituting the q-expansions (4.2) and (4.3) in (4.1). The one thing to note is that the product expansion of $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda_\tau)$ is independent of η, the quasi-period homomorphism. It disappears after substituting the q-expansions and simplifying the terms. □

We also need the following elementary fact in the proof of our main result.

Lemma 4.1.3. *Let $q \in \mathbb{R}$ be such that $0 < |q| < 1$ and $u \in \mathbb{R}^+$, we have the following statements.*

(i) For $0 < q < 1$ there exists an integer k such that $0 < q < q^k u < 1$.

(ii) For $-1 < q < 0$ there exists an integer k such that $0 < q^2 < q^k u < 1$.

Proof. (i) Let $k_0 = \min\{k \in \mathbb{Z} \mid q^k u < 1\}$. Then $q^{k_0} u < 1$ and $q^{k_0-1} u > 1$. We claim that $q < q^{k_0} u < 1$. Clearly $q^{k_0} u < 1$. If $q^{k_0} u \leq q$ then $q^{k_0-1} u \leq 1$ which contradicts the minimality of k_0. So the claim holds.

(ii) If $-1 < q < 0$, then $0 < q^2 < 1$, so the result follows from part (i).

□

We also recall the concept of parity as defined in the introduction. For any real number x, the Parity of x is defined by

$$\text{Sign}(x) = (-1)^{\text{Parity}(x)} \qquad \text{with Parity}(x) \in \mathbb{Z}/2\mathbb{Z}.$$

We are only concerned about elliptic net $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ with values in $\mathbb{R}$. By Theorem 3.4.5 if is defined over $\mathbb{R}$, then we have $\Psi_{\mathbf{v}}(\mathbf{P}; E) \in \mathbb{R}$ for any $\mathbf{v} \in \mathbb{Z}^n$. So from now on we assume that our elliptic curves is defined over $\mathbb{R}$.

We are now ready to state and prove the main theorem of this section.

Theorem 4.1.4. *Let E be an elliptic curve defined over $\mathbb{R}$ and $\Lambda \subset \mathbb{C}$ be its corresponding lattice. Let $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ be an n-tuple consisting of n linearly independent points in $E(\mathbb{R})$, and $\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n$ be the corresponding n-tuple of complex numbers under the isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. Let $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$ be any n-tuple of integers. Let $\Psi_{\mathbf{v}}(\mathbf{P}; E) = \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ be the value of the $\mathbf{v}$-th net polynomial at $\mathbf{P}$. Let each $u_i \longleftrightarrow P_i$ under a fix $\mathbb{R}$-isomorphism $\mathbb{R}^*/q^{\mathbb{Z}} \cong E(\mathbb{R})$ with $q \in \mathbb{R}^*$ and $0 < |q| < 1$. Then there are n irrational numbers $\beta_1, \beta_2, \ldots, \beta_n$, which are $\mathbb{Q}$-linearly independent, given by the rules in the following table*

so that, possibly after replacing $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ with $(-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \leq i < j \leq n} v_i v_j - 1} \Psi_{\mathbf{v}}(\mathbf{P}; E)$, the

q	$E(\mathbb{R})$	P_i	u_i	β_i
$0 < q < 1$	Disconnected	Identity component	$u_i > 0$	$\log_q u_i = \log_q \lvert u_i \rvert$
	Disconnected	Nondentity component	$u_i < 0$	$\log_q \lvert u_i \rvert$
$-1 < q < 0$	Connected			$\frac{1}{2} \log_{\lvert q \rvert} u_i$

Table 4.1: Explicit expressions for β_i

parity of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ *is given by one of the following formulas:*

$$\text{Parity}(\Psi_{\mathbf{v}}(\mathbf{P}; E)) \equiv \left\lfloor \sum_{i=1}^{n} v_i \beta_i \right\rfloor + \sum_{1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \pmod 2, \tag{4.4}$$

$$\text{Parity}(\Psi_{\mathbf{v}}(\mathbf{P}; E)) \equiv \begin{cases} \displaystyle\sum_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \\ \displaystyle + \Big\lfloor \sum_{i=1}^{n} v_i \beta_i \Big\rfloor + \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \displaystyle\sum_{i=1}^{k} v_i \text{ is even,} \\ \displaystyle\sum_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \\ \displaystyle + \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \displaystyle\sum_{i=1}^{k} v_i \text{ is odd,} \end{cases} \tag{4.5}$$

where k *is a positive integer such that* $u_1, u_2, \ldots, u_k < 0$ *and* $u_{k+1}, u_{k+2}, \ldots, u_n > 0$. *Here each* u_i *is normalized to satisfy* $q^2 < u_i < 1$ *if* $q < 0$ *and* $|q| < |u_i| < 1$ *otherwise. The formula* (4.4) *is used when* $u_i > 0$ *for all* $1 \le i \le n$, *otherwise* (4.5) *is used.*

Proof. Since E is defined over $\mathbb{R}$, by Theorem 2.5.1, there is a unique real number $q \in \mathbb{R}$ with $0 < |q| < 1$ such that $E \cong_{/\mathbb{R}} E_q$. Assume that π represents the isomorphism $E \cong_{/\mathbb{R}} E_q$. Let τ be the unique complex number associated to q given in Theorem 2.5.1 such that $q = e^{2\pi i \tau}$ and let Λ_τ be the lattice generated by $[\tau, 1]$. Since $E \cong E_q$, there exists an $\alpha \in \mathbb{C}^*$ such that $\Lambda = \alpha \Lambda_\tau$. The multiplication by α carries $\mathbb{C}/\Lambda$

isomorphically to $\mathbb{C}/\Lambda_\tau$. Let z_i be the corresponding complex number to $P_i \in E(\mathbb{R})$ under the isomorphism $E(\mathbb{C}) \cong C/\Lambda$. Then z_i/α is the corresponding complex number to $\pi^{-1}(P_i) \in E_q(\mathbb{R})$ under the isomorphism $E_q(\mathbb{C}) \cong C/\Lambda_\tau$. From part (b) of Theorem 2.5.1, the map

$$\psi = \pi \ o \ \phi : \mathbb{C}^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(\mathbb{C}) \xrightarrow{\sim} E(\mathbb{C})$$

is an isomorphism, moreover the map ψ (restricted to $\mathbb{R}^*/q^{\mathbb{Z}}$)

$$\psi : \mathbb{R}^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(\mathbb{R}) \xrightarrow{\sim} E(\mathbb{R})$$

is an $\mathbb{R}$-isomorphism. Thus from construction of ψ, we can consider $u_i = e^{2\pi i z_i/\alpha}$ as a representative in $\mathbb{R}^*/q^{\mathbb{Z}}$ for $\psi^{-1}(P_i)$. Since ψ is an $\mathbb{R}$ isomorphism we have that $u_i \in \mathbb{R}^*$.

Next Let $\Psi_{\mathbf{v}}(\mathbf{P}, E) = \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ be the value of the $\mathbf{v}$-th net polynomial at $\mathbf{P}$. Then for $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$, fixed $\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n$, and Λ, we have

$$\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) = \Omega_{\mathbf{v}}(\mathbf{z}; \alpha\Lambda_\tau) = (\alpha^{-1})^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \le i < j \le n} v_i v_j - 1} \Omega_{\mathbf{v}}(\alpha^{-\mathbf{1}}\mathbf{z}; \Lambda_\tau).$$

Here we have used the fact that the σ-function is of weight one (i.e., for a non-zero $\alpha \in \mathbb{C}^*$ we have $\sigma(\alpha z; \alpha\Lambda) = \alpha\sigma(z; \Lambda)$). Now substituting the value of $\Omega_{\mathbf{v}}\left(\alpha^{-\mathbf{1}}\mathbf{z}; \Lambda_\tau\right)$ from Proposition 4.1.2 yields

$$\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) = \left(\frac{2\pi i}{\alpha}\right)^{\sum_{j=1}^{n} v_j^2 - \sum_{1 \le j < k \le n} v_j v_k - 1} \prod_{j=1}^{n} u_j^{\frac{v_j^2 - v_j}{2}} \frac{\theta\Big(\prod_{j=1}^{n} u_j^{v_j}, q\Big)}{\prod_{j=1}^{n} \theta(u_j, q)^{2v_j^2 - \sum_{k=1}^{n} v_j v_k} \prod_{1 \le j < k \le n} \theta(u_j u_k, q)^{v_j v_k}}, \tag{4.6}$$

where

$$\theta(u_j, q) = (1 - u_j) \prod_{m \geq 1} \frac{(1 - q^m u_j)(1 - q^m u_j^{-1})}{(1 - q^m)^2}, \tag{4.7}$$

$$\theta(u_j u_k, q) = (1 - u_j u_k) \prod_{m \geq 1} \frac{(1 - q^m u_j u_k)(1 - q^m u_j^{-1} u_k^{-1})}{(1 - q^m)^2}, \tag{4.8}$$

and

$$\theta\Big(\prod_{j=1}^{n} u_j^{v_j}, q\Big) = \Big(1 - \prod_{j=1}^{n} u_j^{v_j}\Big) \prod_{m \geq 1} \frac{(1 - q^m \prod_{j=1}^{n} u_j^{v_j})(1 - q^m \prod_{i=1}^{n} u_j^{-v_j})}{(1 - q^m)^2}. \tag{4.9}$$

Observe that in the above expressions u_j, and q are in $\mathbb{R}^*$. Therefore the product containing u_j and q are also in $\mathbb{R}$. Moreover, by the construction of net polynomials described in the last chapter we have $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) \in \mathbb{R}$. Hence from (4.6) we conclude that the expression $(2\pi i/\alpha)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \leq i < j \leq n} v_i v_j - 1} \in \mathbb{R}^*$. Note that this statement is true for all $\mathbf{v} \in \mathbb{Z}^n$, therefore, taking $v_1 = 1, v_2 = 2$ and $v_i = 0$ for all $3 \leq i \leq n$, we get that $(2\pi i/\alpha)^2 \in \mathbb{R}^*$. Furthermore, taking $v_1 = 2$ and $v_i = 0$ for all $2 \leq i \leq n$, shows that $(2\pi i/\alpha)^3 \in \mathbb{R}^*$. Since $(2\pi i/\alpha)^2$ and $(2\pi i/\alpha)^3 \in \mathbb{R}^*$ we have that $2\pi i/\alpha \in \mathbb{R}^*$. Hence $2\pi i/\alpha$ is either a positive real number or a negative real number. From now on, without loss of generality, we will assume that $2\pi i/\alpha > 0$. Note that if $2\pi i/\alpha < 0$ we can compute the sign of $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ by considering $(-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \leq i < j \leq n} v_i v_j - 1} \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$. Since $2\pi i \alpha^{-1} > 0$, it does not play any role in determining the sign of (4.6). Thus from (4.6) we have that the Parity$\big[\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)\big]$ in $\mathbb{Z}/2\mathbb{Z}$ is equal to

$$\begin{aligned} &\text{Parity}\left[\prod_{i=1}^{n} u_i^{(v_i^2 - v_i)/2}\right] + \text{Parity}\left[\prod_{i=1}^{n} \theta(u_i, q)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j}\right] \\ &\qquad + \text{Parity}\left[\prod_{1 \leq i < j \leq n} \theta(u_i u_j, q)^{v_i v_j}\right] + \text{Parity}\left[\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q\Big)\right]. \end{aligned} \tag{4.10}$$

We will examine each of these parities individually. However, before computing these parities we make the following observations.

(a) In studying the parities in (4.10), without loss of generality, we normalize u_i as follows:

(i) We may assume $0 < q < |u_i| < 1$, if $q > 0$.

(ii) We may assume $0 < q^2 < u_i < 1$, if $q < 0$.

The above assertions are direct consequences of Lemma 4.1.3 and the fact that the value of the right hand side of (4.6) is invariant under $u_i \longmapsto q^{\pm 1}u_i$. Thus while computing the signs in (4.6) we may focus our attention to values of $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ for these specific ranges of u_i.

(b) Our second observation is that the factor $(1-q^m)^2$ appearing in the denominators of all the expansions of θ-terms in (4.6) does not contributes to the signs in (4.6). Thus we may discard the factor $(1 - q^m)^2$ while computing the signs of $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ in (4.6).

Next we compute the parities in (4.10). We consider two cases according to the sign of q.

Case I. Assume that $0 < q < 1$.

We start by computing Parity $\left[\prod_{i=1}^{n} \theta(u_i, q)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j}\right]$ in (4.10).

As stated in our assumption we have

$$u_1,\ u_2,\ u_3,\ \ldots,\ u_k < 0 \quad \text{and} \quad u_{k+1},\ u_{k+2},\ u_{k+3},\ \ldots,\ u_n > 0.$$

First we observe that if $u_i < 0$, from (4.7), it is clear that $\theta(u_i, q) > 0$. Thus for all $1 \leq i \leq k$ we have that $\theta(u_i, q) > 0$. On the other hand if $u_i > 0$, as described above,

we may assume that $0 < q < u_i < 1$. Then for all $k+1 \leq i \leq n$ we have

$$1 - u_i > 0 \qquad \text{and} \qquad 1 - q^m u_i^{\pm 1} > 0 \quad \text{for all} \quad m \geq 1.$$

Thus from (4.7) we have $\theta(u_i, q) > 0$ for all $1 \leq i \leq n$. Hence from the above discussion we conclude that

$$\text{Parity}\left[\prod_{i=1}^{n} \theta(u_i, q)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j}\right] \equiv 0 \pmod 2. \tag{4.11}$$

Next we compute Parity $\left[\prod_{1 \leq i < j \leq n} \theta(u_i u_j, q)^{v_i v_j}\right]$ in (4.10).

From (4.8) we see that when $u_i u_j < 0$ we have $\theta(u_i u_j, q) > 0$. So while computing the signs in $\prod_{1 \leq i < j \leq n} \theta(u_i u_j, q)^{v_i v_j}$ we will only focus on $\theta(u_i u_j, q)$ with pairs (u_i, u_j) such that $u_i u_j > 0$, which is equivalent of saying that u_i and u_j should have the same parity. Hence we either have

$$0 < q < u_i < 1 \qquad \text{and} \qquad 0 < q < u_j < 1 \tag{4.12}$$

or we have

$$0 < q < |u_i| < 1 \qquad \text{and} \qquad 0 < q < |u_j| < 1. \tag{4.13}$$

First assume that (4.12) holds. Then we have $1 - u_i u_j > 0$. This along with the fact that $q^m < 1$ implies that

$$1 - q^m u_i u_j > 0 \quad \text{for all } m \geq 1.$$

Again from (4.12) we get that $0 < q^2 < u_i u_j < 1$ or equivalently $0 < q^2 u_i^{-1} u_j^{-1} < 1$ for all $1 \leq i < j \leq k$. Thus

$$1 - q^m u_i^{-1} u_j^{-1} > 0 \quad \text{for all } m \geq 2.$$

However, there is possibly one negative sign in (4.8) coming from the factor $1 - qu_i^{-1}u_j^{-1}$. Observe that

$$1 - qu_i^{-1}u_j^{-1} < 0 \iff 1 < \log_q u_i + \log_q u_j \iff \lfloor \log_q u_i + \log_q u_j \rfloor \geq 1.$$

On the other hand, since $1 - q^2u_i^{-1}u_j^{-1} > 0$ we have $\lfloor \log_q u_i + \log_q u_j \rfloor < 2$. By combining the above two inequalities for $\lfloor \log_q u_i + \log_q u_j \rfloor$ we get that

$$1 - qu_i^{-1}u_j^{-1} < 0 \iff \lfloor \log_q u_i + \log_q u_j \rfloor = 1.$$

Thus for the case when both $u_i > 0$ and $u_j > 0$ there is one negative sign in (4.8) if and only if $\lfloor \log_q u_i + \log_q u_j \rfloor = 1$. Hence

$$\begin{aligned} \text{Parity}[\theta(u_iu_j, q)^{v_iv_j}] &\equiv \text{Parity}[(-1)^{\lfloor \log_q u_i + \log_q u_j \rfloor v_iv_j}] \\ &\equiv \lfloor \log_q u_i + \log_q u_j \rfloor v_iv_j \pmod 2 \quad \text{when } u_i > 0,\ u_j > 0. \end{aligned} \tag{4.14}$$

Next, assume that (4.13) holds. With a similar argument as above, in this case we see that there is one negative sign in (4.8) if and only if $\lfloor \log_q |u_i| + \log_q |u_j| \rfloor = 1$. Thus

$$\begin{aligned} \text{Parity}[\theta(u_iu_j, q)^{v_iv_j}] &\equiv \text{Parity}[(-1)^{\lfloor \log_q |u_i| + \log_q |u_j| \rfloor v_iv_j}] \\ &\equiv \lfloor \log_q |u_i| + \log_q |u_j| \rfloor v_iv_j \pmod 2 \quad \text{when } u_i < 0,\ u_j < 0. \end{aligned} \tag{4.15}$$

We therefore, from (4.14) and (4.15), conclude that in $\prod_{1 \leq i < j \leq n} \theta(u_iu_j, q)^{v_iv_j}$ the only terms that contribute to the sign of the product are

$$\begin{aligned} &\theta(u_1u_2, q),\ \theta(u_1u_3, q), \ldots,\ \theta(u_1u_k, q),\ \theta(u_2u_3, q),\ \ldots,\ \theta(u_{k-1}u_k, q), \\ &\theta(u_{k+1}u_{k+2}, q),\ \theta(u_{k+1}u_{k+3}, q),\ \ldots,\ \theta(u_{k+1}u_n, q),\ \theta(u_{k+2}u_{k+3}, q),\ \ldots,\ \theta(u_{n-1}u_n, q). \end{aligned}$$

Thus,

$$\begin{aligned}\text{Parity}\left[\prod_{1\le i<j\le n}\theta(u_iu_j,q)^{v_iv_j}\right] &= \text{Parity}\left[\prod_{1\le i<j\le k}\theta(u_iu_j,q)^{v_iv_j}\quad\prod_{k+1\le i<j\le n}\theta(u_iu_j,q)^{v_iv_j}\right]\\ &= \text{Parity}\left[\prod_{1\le i<j\le k}\theta(u_iu_j,q)^{v_iv_j}\right]+\text{Parity}\left[\prod_{k+1\le i<j\le n}\theta(u_iu_j,q)^{v_iv_j}\right]\end{aligned}$$

$$\equiv \sum_{1\le i<j\le k}\lfloor \log_q|u_i|+\log_q|u_j|\rfloor v_iv_j+\sum_{k+1\le i<j\le n}\lfloor \log_q u_i+\log_q u_j\rfloor v_iv_j \pmod 2$$

where the last congruence is written by using (4.14) and (4.15). In conclusion

$$\text{Parity}\left[\prod_{1\le i<j\le n}\theta(u_iu_j,q)^{v_iv_j}\right] \equiv \sum_{1\le i<j\le k}\lfloor\beta_i+\beta_j\rfloor v_iv_j+\sum_{k+1\le i<j\le n}\lfloor\beta_i+\beta_j\rfloor v_iv_j \pmod 2 \tag{4.16}$$

with explicit values $\beta_i=\log_q|u_i|$ (since when $u_i>0$ we can write $u_i=|u_i|$).

Next, we will analyze the parity of $\theta\Big(\prod_{i=1}^n u_i^{v_i},q\Big)$ in (4.10).

Recall that $u_1,u_2,u_3,\ldots,u_k<0$ and $u_{k+1},u_{k+2},u_{k+3},\ldots,u_n>0$. For all $u_i<0$ we can write $u_i=(-1)|u_i|$. Thus the expansion (4.9) for $\theta\Big(\prod_{i=1}^n u_i^{v_i},q\Big)$ can be rewritten as

$$\Big(1-(-1)^{\sum_{i=1}^k v_i}\prod_{i=1}^n|u_i|^{v_i}\Big)\prod_{m\ge1}\frac{(1-q^m(-1)^{\sum_{i=1}^k v_i}\prod_{i=1}^n|u_i|^{v_i})(1-q^m(-1)^{\sum_{i=1}^k v_i}\prod_{i=1}^n|u_i|^{-v_i})}{(1-q^m)^2}.$$

Since $q>0$, it is clear from the above expression that if $\sum_{i=1}^k v_i$ is odd then $\theta\Big(\prod_{i=1}^n u_i^{v_i},q\Big)$ is positive. For the case that $\sum_{i=1}^k v_i$ is even, the factor $1-\prod_{i=1}^n|u_i|^{v_i}$ may be positive or negative depending upon the sign of v_i. Thus we further split into two cases.

Sub-case I. Assume that $1-\prod_{i=1}^n|u_i|^{v_i}>0$.

We observe that for all $m\ge1$ we have $q^m<1$, and so $1-q^m\prod_{i=1}^n|u_i|^{v_i}>0$. However,

$$1-q^m\prod_{i=1}^n|u_i|^{-v_i}<0 \quad\Longleftrightarrow\quad \prod_{i=1}^n|u_i|^{v_i}<q^m$$

$$\iff \sum_{i=1}^{n} v_i \log |u_i| < m \log q \iff m < \sum_{i=1}^{n} v_i \log_q |u_i|.$$

Hence for this case there are $\lfloor \sum_{i=1}^{n} v_i \log_q |u_i| \rfloor$ negative signs in the expression for $\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q\Big)$.

Sub-case II. Assume that $1 - \prod_{i=1}^{n} |u_i|^{v_i} < 0$.

Following a similar argument used in the Sub-case I we see that,

$$1 - q^m \prod_{i=1}^{n} |u_i|^{v_i} < 0 \quad \iff \quad m < \sum_{i=1}^{n} -v_i \log_q |u_i|.$$

Observe that since $1 - \prod_{i=1}^{n} |u_i|^{v_i} < 0$, we have $\sum_{i=1}^{n} -v_i \log_q |u_i| > 0$. Hence there are $\lfloor -\sum_{i=1}^{n} v_i \log_q |u_i| \rfloor + 1$ negative signs in expression (4.9) for $\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q\Big)$. The 1 in the above expression comes from the factor $1 - \prod_{i=1}^{n} |u_i|^{v_i}$.

Now we claim that the number $\sum_{i=1}^{n} v_i \log_q |u_i|$ is not an integer. In other words we claim that $\log_q |u_1|, \log_q |u_2|, \ldots, \log_q |u_n|$, and 1 are linearly independent over $\mathbb{Q}$. To see this suppose that there are integers $k_0, k_1, k_2, \ldots, k_n$ not all zero such that the sum $\sum_{i=1}^{n} k_i \log_q |u_i| + k_0 = 0$. Equivalently we have that $\sum_{i=1}^{n} k_i z_i = -k_0$. Note that since our lattice is normalized we have $1 \in \Lambda_\tau$ hence under the isomorphism $\mathbb{C}/\Lambda_\tau \cong E(\mathbb{C})$ all the integers are mapped to the identity element of $E(\mathbb{C})$. Thus $\sum_{i=1}^{n} k_i z_i = -k_0$ under the isomorphism $\mathbb{C}/\Lambda_\tau \cong E(\mathbb{C})$ leads to having $\sum_{i=1}^{n} k_i P_i = \mathcal{O}$. This contradicts our assumption that the points $P_1, P_2, \ldots, P_n$ are linearly independent in $E(\mathbb{R})$. Hence we have that $\log_q |u_1|, \log_q |u_2|, \ldots, \log_q |u_n|$, and 1 are linear independent over $\mathbb{Q}$. This also shows that each number $\log_q |u_i|$ is irrational. Therefore the number $\sum_{i=1}^{n} v_i \log_q |u_i|$ can not be an integer. Using this fact and the property of the greatest integer function that

$$\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0 & \text{if } x \in \mathbb{Z} \\ -1 & \text{if } x \notin \mathbb{Z} \end{cases} \tag{4.17}$$

we see that the number of negative signs in both sub-cases are same. Therefore we can combine the results from these two sub-cases to get that

$$\text{Parity}\left[\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q\Big)\right] \equiv \left\lfloor \sum_{i=1}^{n} v_i\beta_i \right\rfloor \pmod 2 \quad \text{if } \sum_{i=1}^{k} v_i \text{ is even}, \tag{4.18}$$

where $\beta_i = \log_q |u_i|$ for all $1 \le i \le n$.

Finally we deal with Parity $\left[\prod_{i=1}^{n} u_i^{(v_i^2-v_i)/2}\right]$ in (4.10).

Recall that $u_1, u_2, u_3, \ldots, u_k < 0$ and $u_{k+1}, u_{k+2}, u_{k+3} \ldots u_n > 0$. Thus we have

$$\begin{aligned}
\text{Parity}\left[\prod_{i=1}^{n} u_i^{(v_i^2-v_i)/2}\right] &= \text{Parity}\left[\prod_{i=1}^{k} u_i^{(v_i^2-v_i)/2}\right] \\
&= \text{Parity}\left[\prod_{i=1}^{k} (-1)^{(v_i^2-v_i)/2}\right] \\
&\equiv \sum_{i=1}^{k} \frac{v_i^2 - v_i}{2} \pmod 2 \qquad (4.19) \\
&\equiv \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2. \qquad (4.20)
\end{aligned}$$

Applying (4.11), (4.16), (4.18), and (4.19) in (4.10) yields

$$\text{Parity}[\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)] \equiv \begin{cases} \displaystyle\sum_{1\le i<j\le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1\le i<j\le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \\ \displaystyle + \Big\lfloor \sum_{i=1}^{n} v_i\beta_i \Big\rfloor + \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \displaystyle\sum_{i=1}^{k} v_i \text{ is even} \\ \\ \displaystyle\sum_{1\le i<j\le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1\le i<j\le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \\ \displaystyle + \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \displaystyle\sum_{i=1}^{k} v_i \text{ is odd} \end{cases}$$

which is the desired result (4.5) with the explicit values $\beta_i = \log_q |u_i|$.

Case II. Assume that $-1 < q < 0$.

First of all as described earlier we may assume that

$$u_i > 0 \qquad \text{and} \qquad q^2 < u_i < 1 \quad \text{for all } 1 \le i \le n.$$

Consequently we see that

$$\text{Parity}\left[\prod_{i=1}^{n} u_i^{(v_i^2 - v_i)/2}\right] \equiv 0 \pmod 2. \tag{4.21}$$

Next note that in the expansion of $\theta(u_i, q)$, from (4.7), for all $1 \le i \le n$, we have

$$1 - q^m u_i^{\pm 1} > 1 - |q|^{m-2} \ge 0 \qquad \text{for all } m \ge 2.$$

Therefore $1 - q^m u_i^{\pm 1} > 0$ for all m, except possibly for $m = 1$. However for $m = 1$, since $q < 0$ and $u_i > 0$ we see that $1 - q u_i^{\pm 1} > 0$ for all $1 \le i \le n$. Hence all the terms in the expansion for $\theta(u_i, q)$ in (4.7) are positive. In conclusion we have

$$\text{Parity}\left[\prod_{i=1}^{n} \theta(u_i, q)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j}\right] \equiv 0 \pmod 2. \tag{4.22}$$

In analyzing the parity of $\prod_{1 \le i < j \le n} \theta(u_i u_j, q)^{v_i v_j}$ in (4.10), first of all observe that $1 - u_i u_j > 0$ for all $1 \le i, j \le n$. Furthermore, using our normalization conditions $q^2 < u_i < 1$ and $q^2 < u_j < 1$, we have $q^4 < u_i u_j < 1$ or equivalently $1 - q^4 u_i^{\pm 1} u_j^{\pm 1} > 0$. As a consequence of this fact, in expansion of (4.8) we have that

$$1 - q^m u_i^{\pm 1} u_j^{\pm 1} > 1 - |q|^{m-4} \ge 0 \qquad \text{for all } m \ge 4.$$

So the factor $1 - q^m u_i^{\pm 1} u_j^{\pm 1}$ may be negative for $m = 1,\ 2,\ 3$. However, for the case of $m = 1$ and 3 notice that $1 - q^m u_i^{\pm 1} u_j^{\pm 1} > 0$ because $q < 0$ and $u_i > 0$ for all $1 \le i \le n$.

Moreover observe that since $u_i u_j < 1$ and $q^2 < 1$ we have $1 - q^2 u_i u_j > 0$. Hence the only possible contribution to the sign in the expansion of $\theta(u_i u_j, q)$ comes from the factor $1 - q^2 u_i^{-1} u_j^{-1}$. Thus

$$1 - q^2 u_i^{-1} u_j^{-1} < 0 \iff \log_{|q|} u_i + \log_{|q|} u_j > 2 \iff \left\lfloor \frac{1}{2} \log_{|q|} u_i + \frac{1}{2} \log_{|q|} u_j \right\rfloor \geq 1.$$

On the other hand we observe that $q^4 < u_i u_j < 1$, which implies that

$$\left\lfloor \frac{1}{2} \log_{|q|} u_i + \frac{1}{2} \log_{|q|} u_j \right\rfloor \leq 1.$$

By combining the above two inequalities for $\lfloor \frac{1}{2} \log_{|q|} u_i + \frac{1}{2} \log_{|q|} u_j \rfloor$ we conclude that there is one negative sign in the expansion of $\theta(u_i u_j, q)$ if and only if

$$\left\lfloor \frac{1}{2} \log_{|q|} u_i + \frac{1}{2} \log_{|q|} u_j \right\rfloor = 1.$$

Hence from the above discussion we have

$$\text{Parity}\left[\prod_{1 \leq i < j \leq n} \theta(u_i u_j, q)^{v_i v_j} \right] \equiv \sum_{1 \leq i < j \leq n} \lfloor \beta_i + \beta_j \rfloor \, v_i v_j \pmod 2, \tag{4.23}$$

where $\beta_i = \frac{1}{2} \log_{|q|} u_i$ for all $1 \leq i \leq n$.

Next, we examine the signs in $\theta\Big(\prod_{i=1}^n u_i^{v_i}, q \Big)$. From the expression (4.9) notice that, as in Case I, the factor $1 - \prod_{i=1}^n u_i^{v_i}$ may be positive or negative depending on the indices v_i. So we further split our analysis in two sub-cases.

Sub-case I. Assume that $1 - \prod_{i=1}^n u_i^{v_i} > 0$.

Since $|q|^m < 1$ for all $m \geq 1$ and $\prod_{i=1}^n u_i^{v_i} < 1$, we see that $1 - q^m \prod_{i=1}^n u_i^{v_i} > 0$. Further observe that, since $q < 0$, the factors $1 - q^m \prod_{i=1}^n u_i^{-v_i}$ are positive for all odd

values of m. However for the case when m is even

$$1 - q^m \prod_{i=1}^{n} u_i^{-v_i} < 0 \quad \iff \quad \prod_{i=1}^{n} u_i^{v_i} < |q|^m,$$

which is the same as

$$\sum_{i=1}^{n} v_i \log u_i < m \log |q| \iff m < \sum_{i=1}^{n} v_i \log_{|q|} u_i.$$

Thus for every positive even integer smaller than $\sum_{i=1}^{n} v_i \log_{|q|} u_i$ we get a negative sign in (4.9). Hence, in this sub-case, the total number of negative signs in the expression for $\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q\Big)$ is given by $\Big\lfloor \frac{1}{2} \sum_{i=1}^{n} v_i \log_{|q|} u_i \Big\rfloor$.

Sub-case II. Assume that $1 - \prod_{i=1}^{n} u_i^{v_i} < 0$.

Following a similar argument used in the previous sub-case we see that, there are $\Big\lfloor -\frac{1}{2} \sum_{i=1}^{n} v_i \log_{|q|} u_i \Big\rfloor + 1$ negative signs in the expression for $\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q\Big)$. The 1 in the above expression is coming from the factor $1 - \prod_{i=1}^{n} u_i^{v_i} < 0$.

Again using a similar argument as in Case I we can show that $\displaystyle\sum_{i=1}^{n} v_i \log_{|q|} u_i$ is not an integer, and as earlier using the property (4.17) of greatest integer function we can combine both sub-cases. Thus we see that in both sub-cases the total number of negative signs in $\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q\Big)$ is equal to $\Big\lfloor \frac{1}{2} \sum_{i=1}^{n} v_i \log_{|q|} u_i \Big\rfloor$. As a consequence we have that

$$\text{Parity} \left[\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q \Big) \right] \equiv \left\lfloor \frac{1}{2} \sum_{i=1}^{n} v_i \log_{|q|} u_i \right\rfloor \pmod 2. \tag{4.24}$$

In conclusion combining (4.21), (4.22), (4.23), and (4.25) yields

$$\begin{aligned}\text{Parity}[\Omega_{\mathbf{v}}(\mathbf{z};\Lambda)] &\equiv \left\lfloor \frac{1}{2}\sum_{i=1}^{n} v_i \log_{|q|} u_i \right\rfloor + \sum_{1\le i<j\le n} \left\lfloor \frac{1}{2}\log_{|q|} u_i + \frac{1}{2}\log_{|q|} u_j \right\rfloor v_i v_j \pmod 2 \\ &\equiv \left\lfloor \sum_{i=1}^{n} v_i \beta_i \right\rfloor + \sum_{1\le i<j\le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \pmod 2. \end{aligned} \tag{4.25}$$

This is the required expression (4.4) with the explicit value of $\beta_i = \frac{1}{2}\log_{|q|} u_i$ for all $1 \le i \le n$. The proof of our theorem is complete. □

Remark 4.1.5. Note that in the statement of the Theorem 4.1.4 we have assumed that $u_1, u_2, \ldots, u_k < 0$ and $u_{k+1}, u_{k+2}, u_{k+3}, \ldots, u_n > 0$ (i.e., first k elements are negative). We want to show that we are not losing any generality by having this assumption. For simplicity we explain the case when $n = 2$ and $k = 1$.

Let $u_2 < 0$ and $u_1 > 0$. Let $P_i \longleftrightarrow u_i$ be corresponding point in $E(\mathbb{R})$ under the isomorphism $E(\mathbb{R}) \cong \mathbb{R}/q^{\mathbb{Z}}$. We want to calculate sign of

$$\Psi_{(v_1,v_2)}((P_1, P_2); E). \tag{4.26}$$

Observe that since

$$v_1 P_1 + v_2 P_2 = v_2 P_2 + v_1 P_1$$

we have

$$\Psi_{(v_1,v_2)}((P_1, P_2); E) = \Psi_{(v_2,v_1)}((P_2, P_1); E)$$

Thus instead of calculating the sign of (4.26) we calculate sign of

$$\Psi_{(v_2,v_1)}((P_2, P_1); E).$$

Remark 4.1.6. We give a brief comparison for the proof of Theorem 4.1.4 and the proof of Theorem 3.2.7. The first observation is that in Theorem 3.2.7 the n is always

positive. However it can be used to calculate the sign of W_n when n is negative using relation $W_{-n} = -W_n$. For higher ranks there is a similar relation. For $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$ we have $W_{-\mathbf{v}} = -W_{\mathbf{v}}$. However we have to deal with the case when some of the v_i are positive and others are negative.

Second observation is that in proof of Theorem 3.2.7 the denominator of W_n is always positive. However in Theorem 4.1.4 the denominator of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ contains negative signs.

Finally, in Theorem 4.1.4 for the case when $0 < q < 1$ there are two possible cases depending on sign of u. However in Theorem 3.2.7 for higher rank for $0 < q < 1$ we have $u_1, u_2, \ldots, u_n$ and each may be positive or negative in any possible combination. Thus instead of splitting in to a number of possible cases we consider a general case where $u_1, u_2, \ldots, u_k > 0$ and $u_{k+1}, u_{k+2}, \ldots, u_{k+n} < 0$, where $0 \leq k \leq n$.

We now give illustrations of various cases of Theorem 4.1.4 with the help of some examples. For sake of simplicity we only give examples for rank 2 elliptic nets.

Software: All the computations were done using mathematical software `SAGE`.

Keeping the assumptions and notations used in Theorem 4.1.4, for the case $n = 2$, the sign of either $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ or $(-1)^{v_1^2+v_2^2-v_1v_2-1}\Psi_{\mathbf{v}}(\mathbf{P}; E)$, can be computed using one of the following parity formulas:

$$\text{Parity}[\Psi_{\mathbf{v}}(P; E)] \equiv \Big\lfloor v_1\beta_1 + v_2\beta_2 \Big\rfloor + \Big\lfloor \beta_1 + \beta_2 \Big\rfloor v_1v_2 \pmod 2 \tag{4.27}$$

$$\text{Parity}[\Psi_{\mathbf{v}}(P; E)] \equiv \begin{cases} \Big\lfloor v_1\beta_1 + v_2\beta_2 \Big\rfloor + \Big\lfloor \dfrac{v_1}{2} \Big\rfloor \pmod 2 & \text{if } v_1 \text{ is even,} \\ \Big\lfloor \dfrac{v_1}{2} \Big\rfloor \pmod 2 & \text{if } v_1 \text{ is odd.} \end{cases} \tag{4.28}$$

$$\text{Parity}[\Psi_{\mathbf{v}}(P;E)] \equiv \begin{cases} \left\lfloor v_1\beta_1 + v_2\beta_2 \right\rfloor + \left\lfloor \frac{v_2}{2} \right\rfloor \pmod 2 & \text{if } v_2 \text{ is even,} \\ \left\lfloor \frac{v_2}{2} \right\rfloor \pmod 2 & \text{if } v_2 \text{ is odd.} \end{cases} \tag{4.29}$$

$$\text{Parity}[\Psi_{\mathbf{v}}(P;E)] \equiv \begin{cases} \left\lfloor v_1\beta_1 + v_2\beta_2 \right\rfloor + \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 \\ \qquad + \left\lfloor \frac{v_1}{2} \right\rfloor + \left\lfloor \frac{v_2}{2} \right\rfloor \pmod 2 & \text{if } v_1 + v_2 \text{ is even,} \\ \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 + \left\lfloor \frac{v_1}{2} \right\rfloor + \left\lfloor \frac{v_2}{2} \right\rfloor \pmod 2 & \text{if } v_1 + v_2 \text{ is odd.} \end{cases} \tag{4.30}$$

Here the two irrational numbers β_1 and β_2 are given by

q	β_1	β_2
$0 < q < 1$	$\log_q \lvert u_1 \rvert$	$\log_q \lvert u_2 \rvert$
$-1 < q < 0$	$\frac{1}{2}\log_{\lvert q \rvert} u_1$	$\frac{1}{2}\log_{\lvert q \rvert} u_2$

Table 4.2: Explicit expression for β_1 and β_2

The formula (4.27) is used when $u_1 > 0$ and $u_2 > 0$ and formula (4.28) is used for the case when $u_1 < 0$ and $u_2 > 0$. We use the formula (4.29) when $u_1 > 0$ and $u_2 < 0$. Finally the formula (4.30) is used when both $u_1 < 0$ and $u_2 < 0$.

We have verified the truth of above formulas for several rank 2 elliptic net $W(v_1, v_2)$ for range of $0 \leq v_1 \leq 500$ and $0 \leq v_2 \leq 500$. Thus the results have been verified for the up to 25×10^4 terms and same for the negative indices as well.

Example 4.1.7. Let E be the elliptic curve defined over $\mathbb{R}$ given by the Weierstrass equation $y^2 + xy = x^3 - x^2 - 4x + 4$. Let $P_1 = (69/25, -32/125)$ and $P_2 = (2, -2)$ be two points in $E(\mathbb{R})$. Let $\mathbf{P} = (P_1, P_2)$. The following table presents the values of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ for $\mathbf{v} = (v_1, v_2)$ in the range $0 \leq v_1 \leq 3$ and $0 \leq v_2 \leq 5$.

			$\vdots$		
	-832	1232600000	430685595625000000	3330569636331576171875000000	
	112	-12560000	-18772893750000	12109328555378515625000000	
$\cdots$	-4	-165500	-141878687500	-1754232556789062500	$\cdots$
	-2	-150	196317500	-1270400610718750	
	1	95	152725	-181061702375	
	0	5	-3595	63803440	
			$\vdots$		

Table 4.3: Elliptic net $\Psi(\mathbf{P}; E)$ associated to elliptic curve $E : y^2+xy = x^3-x^2-4x+4$ and points $P_1 = (69/25, -32/125)$, $P_2 = (2, -2)$.

In the above array the bottom left corner represent the value $\Psi_{(0,0)}(\mathbf{P}; E)$ and the upper right corner represents $\Psi_{(3,5)}(\mathbf{P}; E)$.

There is an isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ such that $P_1 \longleftrightarrow u_1$ and $P_2 \longleftrightarrow u_2$ with the explicit values

$$q = 0.000119963294449278151298548014264366784 0\ldots\ldots,$$

$$u_1 = 0.080328571958686877796192265939926490960 8\ldots\ldots,$$

$$u_2 = 0.036009425429663267978488080494773069884 56\ldots\ldots$$

Observe that $q > 0$, thus from Proposition 2.5.2, $E(\mathbb{R})$ is disconnected having two components. The points P_1 and P_2 both are on the component having identity. Since $u_1 > 0$, and $u_2 > 0$ so using Theorem 4.1.4, the sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ can be calculated by either

$$\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] \equiv \Big\lfloor v_1\beta_1 + v_2\beta_2 \Big\rfloor + \Big\lfloor \beta_1 + \beta_2 \Big\rfloor v_1 v_2 \pmod 2 \tag{4.31}$$

or

$$\begin{aligned}\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] &\equiv \Big\lfloor v_1\beta_1 + v_2\beta_2 \Big\rfloor + \Big\lfloor \beta_1 + \beta_2 \Big\rfloor v_1 v_2 + (v_1^2 + v_2^2 - v_1 v_2 - 1) \pmod 2 \\ &\equiv \Big\lfloor v_1\beta_1 + v_2\beta_2 \Big\rfloor + \Big\lfloor \beta_1 + \beta_2 \Big\rfloor v_1 v_2 + (v_1 + v_2 + v_1 v_2 + 1) \pmod 2\end{aligned} \tag{4.32}$$

with

$$\beta_1 = 0.279302082980192795774933134397681241646 7\ldots,$$

$$\beta_2 = 0.368171798473479719398145282660133495406 4\ldots,$$

since Theorem 4.1.4 gives either sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ or $(-1)^{v_1^2+v_2^2-v_1v_2-1}\Psi_{\mathbf{v}}(\mathbf{P}; E)$. By computing the sign of $\Psi_{(2,2)}(\mathbf{P}; E)$ using (4.31) and (4.32) we conclude that in this case the parity is given by formula (4.32). Next we illustrate the truth of our formula using two special cases.

$$\begin{aligned}\text{sign}[\Psi_{(1,3)}(\mathbf{P}; E)] &= (-1)^{\text{Parity}\Psi_{(1,3)}(\mathbf{P};E)} \\ &= (-1)^{\lfloor \beta_1+3\beta_2 \rfloor + 3\lfloor \beta_1+\beta_2 \rfloor + 8} = -1\end{aligned}$$

and from the table we see that $\Psi_{(1,3)}(\mathbf{P}; E) = -150$ having negative sign and

$$\begin{aligned}\text{sign}[\Psi_{(3,4)}(\mathbf{P}; E)] &= (-1)^{\lfloor 3\beta_1+4\beta_2 \rfloor + 12\lfloor \beta_1+\beta_2 \rfloor + 20} \\ &= (-1)^{22} = 1\end{aligned}$$

and from the table we see that $\Psi_{(3,4)}(\mathbf{P}; E) = 1210932855537851562500 00$ having positive sign

Example 4.1.8. Let E be the elliptic curve defined over $\mathbb{R}$ given by the Weierstrass equation $y^2 + xy = x^3 - x^2 - 4x + 4$. Let $P_1 = (-1, 3)$ and $P_2 = (3, 2)$ be two points in $E(\mathbb{R})$ so that $\mathbf{P} = (P_1, P_2)$. The following table presents the values of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ for

$\mathbf{v} = (v_1, v_2)$ in the range $0 \leq v_1 \leq 3$ and $0 \leq v_2 \leq 6$.

		$\vdots$			
	-219900856	71486913947	48178148140103	-112925826309806338	
	-495235	58762243	3246745150	-20471103308793	
	-749	170718	-24093133	-16532329817	
$\cdots$	62	2291	-154139	-28273396	$\cdots$
	7	67	-1256	-101083	
	1	4	3	-1579	
	0	1	5	-94	
		$\vdots$			

Table 4.4: Elliptic net $\Psi(\mathbf{P}; E)$ associated to elliptic curve $E : y^2+xy = x^3-x^2-4x+4$ and points $P_1 = (-1, 3)$, $P_2 = (3, -2)$.

In the above array the bottom left corner represent the value $\Psi_{(0,0)}(\mathbf{P}; E)$ and the upper right corner represents $\Psi_{(3,6)}(\mathbf{P}; E)$.

In this case there is an isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ such that $P_1 \longleftrightarrow u_1$ and $P_2 \longleftrightarrow u_2$ with the explicit values

$$q = 0.000119963294449278151298548014264366784 0\ldots\ldots,$$

$$u_1 = -0.283422955948679072053638499724508663516\ldots\ldots,$$

$$u_2 = 0.001296678719774479631663060145895048233 38\ldots\ldots$$

Observe that q is same as in the previous example. The point P_1 is not on the identity component, however P_2 is on the component having identity. Further since $u_1 < 0$,

and $u_2 > 0$ so using Theorem 4.1.4, parity of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ is either given by

$$\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] \equiv \begin{cases} \left\lfloor v_1\beta_1 + v_2\beta_2 \right\rfloor + \left\lfloor \frac{v_1}{2} \right\rfloor \pmod 2 & \text{if } v_1 \text{ is even} \\ \left\lfloor \frac{v_1}{2} \right\rfloor \pmod 2 & \text{if } v_1 \text{ is odd} \end{cases} \tag{4.33}$$

or

$$\begin{aligned} \text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] &\equiv \begin{cases} \left\lfloor v_1\beta_1 + v_2\beta_2 \right\rfloor + \left\lfloor \frac{v_1}{2} \right\rfloor + v_1^2 + v_2^2 - v_1v_2 - 1 \pmod 2 & \text{if } v_1 \text{ is even} \\ \left\lfloor \frac{v_1}{2} \right\rfloor \pmod 2 & \text{if } v_1 \text{ is odd} \end{cases} \\ &\equiv \begin{cases} \left\lfloor v_1\beta_1 + v_2\beta_2 \right\rfloor + \left\lfloor \frac{v_1}{2} \right\rfloor + v_2 + 1 \pmod 2 & \text{if } v_1 \text{ is even} \\ \left\lfloor \frac{v_1}{2} \right\rfloor \pmod 2 & \text{if } v_1 \text{ is odd} \end{cases} \end{aligned} \tag{4.34}$$

with

$$\begin{aligned} \beta_1 &= 0.139651041490096397887466567198840620823 3\ldots, \\ \beta_2 &= 0.736343596946959438796290565320266990812 8\ldots, \end{aligned}$$

since Theorem 4.1.4 gives either sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ or $(-1)^{v_1^2+v_2^2-v_1v_2-1}\Psi_{\mathbf{v}}(\mathbf{P}; E)$. By computing the sign of $\Psi_{(2,2)}(\mathbf{P}; E)$ using (4.33) and (4.34) we conclude that in this case the parity is given by formula (4.34). Next we illustrate the truth of our formula using two special cases.

$$\begin{aligned} \text{sign}[\Psi_{(2,3)}(\mathbf{P}; E)] &= (-1)^{\text{Parity}\Psi_{(2,3)}(\mathbf{P};E)} \\ &= (-1)^{\lfloor 2\beta_1+3\beta_2 \rfloor + \lfloor 1 \rfloor + 3 + 1} = (-1)^7 = -1 \end{aligned}$$

and from the table we see that $\Psi_{(2,3)}(\mathbf{P}; E)] = -154139$ is of negative sign and

$$\begin{aligned}\text{sign}[\Psi_{(1,5)}(\mathbf{P}; E)] &= (-1)^{\text{Parity}\Psi_{(1,5)}(\mathbf{P};E)} \\ &= (-1)^{\lfloor \frac{1}{2} \rfloor} = (-1)^0 = 1\end{aligned}$$

and from the table we see that $\Psi_{(1,5)}(\mathbf{P}; E) = 58762243$ is of positive sign.

Example 4.1.9. Let E be the elliptic curve defined over $\mathbb{R}$ given by the Weierstrass equation $y^2 + y = x^3 + x^2 - 2x$. Let $P_1 = (-1, 1)$ and $P_2 = (0, -1)$ be two points in $E(\mathbb{R})$. Let $\mathbf{P} = (P_1, P_2)$. The following table presents the values of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ for $\mathbf{v} = (v_1, v_2)$ in the range $-5 \leq v_1 \leq 5$ and $-2 \leq v_2 \leq 2$.

					$\vdots$						
	535	44	-7	-1	1	-1	-4	17	151	-55	-106201	
	1187	67	1	-2	-1	1	1	-5	26	709	-19061	
$\cdots$	-3376	129	19	-3	-1	**0**	1	3	-19	-129	3376	$\cdots$
	19061	-709	-26	5	-1	-1	1	2	-1	-67	-1187	
	106201	55	-151	-17	4	1	-1	1	7	-44	-535	
					$\vdots$						

Table 4.5: Elliptic net $\Psi(\mathbf{P}; E)$ associated to elliptic curve $E : y^2 + y = x^3 + x^2 - 2x$ and points $P_1 = (-1, 1)$, $P_2 = (0, -1)$.

The above array is centered at $\Psi_{(0,0)}(\mathbf{P}; E) = 0$. The bottom left corner represent the value $\Psi_{(-5,-2)}(\mathbf{P}; E)$ and the upper right corner represents $\Psi_{(5,2)}(\mathbf{P}; E)$.

For this example we have the isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ such that $P_1 \longleftrightarrow u_1$

and $P_2 \longleftrightarrow u_2$ with the explicit values

$$q = 0.000357859761537234808182808967028562232 92\ldots\ldots,$$
$$u_1 = -0.217077183508541420345010153615522413434 1\ldots\ldots,$$
$$u_2 = -0.007762272030051816121894244150082449321 9\ldots\ldots,$$

Observe that $q > 0$, thus from Proposition 2.5.2, $E(\mathbb{R})$ is disconnected. Moreover, both the points P_1 and P_2 both are on the non-identity component. Since both $u_1 < 0$ and $u_2 < 0$ so using Theorem 4.1.4, sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ is given by either

$$\text{Parity}[\Psi_{\mathbf{v}}(P; E)] \equiv \begin{cases} \left\lfloor v_1\beta_1 + v_2\beta_2 \right\rfloor + \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 & \\ + \left\lfloor \dfrac{v_1}{2} \right\rfloor + \left\lfloor \dfrac{v_2}{2} \right\rfloor & (\text{mod } 2) \quad \text{if } v_1 + v_2 \text{ is even} \\ \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 + \left\lfloor \dfrac{v_1}{2} \right\rfloor + \left\lfloor \dfrac{v_2}{2} \right\rfloor & (\text{mod } 2) \quad \text{if } v_1 + v_2 \text{ is odd} \end{cases} \tag{4.35}$$

or

$$\text{Parity}[\Psi_{\mathbf{v}}(P; E)] \equiv \begin{cases} \left\lfloor v_1\beta_1 + v_2\beta_2 \right\rfloor + \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 & \\ + \left\lfloor \dfrac{v_1}{2} \right\rfloor + \left\lfloor \dfrac{v_2}{2} \right\rfloor + v_1 v_2 + 1 & (\text{mod } 2) \quad \text{if } v_1 + v_2 \text{ is even} \\ \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 + \left\lfloor \dfrac{v_1}{2} \right\rfloor + \left\lfloor \dfrac{v_2}{2} \right\rfloor & (\text{mod } 2) \quad \text{if } v_1 + v_2 \text{ is odd} \end{cases} \tag{4.36}$$

with

$$\beta_1 = 0.192492905113942322817376565297300099630 7\ldots\ldots,$$
$$\beta_2 = 0.612256338695947642022046474559194434493 9\ldots\ldots,$$

since Theorem 4.1.4 gives either sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ or $(-1)^{v_1^2+v_2^2-v_1v_2-1}\Psi_{\mathbf{v}}(\mathbf{P}; E)$. Note that in formula (4.36) we have used $v_1v_2 + 1$ for every $v_1 + v_2$ even instead of $v_1^2 +$

$v_2^2 - v_1 v_2 - 1$ since these two expressions are congruent modulo 2. By computing the sign of $\Psi_{(2,2)}(\mathbf{P}; E)$ using (4.35) and (4.36) we conclude that in this case the parity is given by formula (4.36). Next we illustrate the truth of our formula using two special cases.

$$\begin{aligned}\operatorname{sign}[\Psi_{(-4,-1)}(\mathbf{P}; E)] &= (-1)^{\operatorname{Parity}\Psi_{(-4,-1)}(\mathbf{P};E)} \\ &= (-1)^{\lfloor \beta_1+\beta_2 \rfloor(-4)(-1)+\lfloor \frac{-4}{2} \rfloor+\lfloor \frac{-1}{2} \rfloor} \\ &= (-1)^{-3} = -1\end{aligned}$$

and from the table we see that $\Psi_{(-4,-1)}(\mathbf{P}; E) = -709$ having negative sign and

$$\begin{aligned}\operatorname{sign}[\Psi_{(4,0)}(\mathbf{P}; E)] &= (-1)^{\operatorname{Parity}\Psi_{(4,0)}(\mathbf{P};E)} \\ &= (-1)^{\lfloor 4\beta_1 \rfloor+1} \\ &= (-1)^{1} = -1\end{aligned}$$

and from the table we see that $\Psi_{(4,0)}(\mathbf{P}; E) = -129$ having negative sign. Note that from the table it is also clear that $\Psi_{-\mathbf{v}}(\mathbf{P}; E) = -\Psi_{\mathbf{v}}(\mathbf{P}; E)$.

Example 4.1.10. Let E be the elliptic curve defined over $\mathbb{R}$ given by Weierstrass equation $y^2 = x^3 - 7x + 10$. Let $P_1 = (-2, 4)$ and $P_2 = (1, 2)$ be two linear independent points in $E(\mathbb{R})$. Let $\mathbf{P} = (P_1, P_2)$ The following table presents the values of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ for $\mathbf{v} = (v_1, v_2)$ in range $0 \leq v_1 \leq 4$ and $0 \leq v_2 \leq 6$.

			$\vdots$			
	-54525952	1086324736	81340137472	-15800157077504	-29481936481157120	
	-163840	-950272	131956736	30954979328	-31977195339776	
	-2048	-17408	280576	85124096	30585993216	
$\cdots$	32	-352	-9440	979488	449423648	$\cdots$
	4	-4	-276	-16028	8814788	
	1	3	-31	-1697	67225	
	0	1	8	-409	-65488	
			$\vdots$			

Table 4.6: Elliptic net $\Psi(\mathbf{P}; E)$ associated to elliptic curve $E : y^2 = x^3 - 7x + 10$ and points $P_1 = (-2, 4)$, $P_2 = (1, 2)$.

In the above array the bottom left corner represent the value $\Psi_{(0,0)}(\mathbf{P}; E)$ and the upper right corner represents $\Psi_{(4,6)}(\mathbf{P}; E)$.

In this case there is an isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ such that $P_1 \longleftrightarrow u_1$ and $P_2 \longleftrightarrow u_2$ with explicit values

$$q = -0.000407748982234323905766785474181754917 2\ldots\ldots,$$

$$u_1 = 0.001201936348983837429349696735400418601519\ldots\ldots,$$

$$u_2 = 0.008992979917906651664620780969726498312814\ldots\ldots$$

Observe that $q < 0$, thus from Proposition 2.5.2, $E(\mathbb{R})$ is connected. Since $u_1 > 0$ and $u_2 > 0$ so using Theorem 4.1.4, by calculating the sign of $\Psi_{(2,2)}(\mathbf{P}; E)$ we notice that the sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ in this case is given by

$$\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] \equiv \Big\lfloor v_1\beta_1 + v_2\beta_2 \Big\rfloor + \Big\lfloor \beta_1 + \beta_2 \Big\rfloor v_1 v_2 \pmod 2$$

with

$$\beta_1 = 0.430745869979239079423919719220424966824 6\ldots\ldots,$$

$$\beta_2 = 0.301819105784181111103136173897431538966 6\ldots\ldots.$$

Next we illustrate the truth of our formula using two special case examples:

$$\begin{aligned}\text{sign}[\Psi_{(2,3)}(\mathbf{P};E) &= (-1)^{\text{Parity}\Psi_{(2,3)}(\mathbf{P};E)}\\ &= (-1)^{\lfloor 2\beta_1+3\beta_2\rfloor+6\lfloor\beta_1+\beta_2\rfloor}\\ &= (-1)^1 = -1\end{aligned}$$

and from the table we see that $\Psi_{(2,3)}(\mathbf{P};E) = -9440$, having negative sign and

$$\begin{aligned}\text{sign}[\Psi_{(3,5)}(\mathbf{P};E)] &= (-1)^{\text{Parity}\Psi_{(3,5)}(\mathbf{P};E)}\\ &= (-1)^{\lfloor 3\beta_1+5\beta_2\rfloor+15\lfloor\beta_1+\beta_2\rfloor}\\ &= (-1)^2 = 1\end{aligned}$$

and from the table we see that $\Psi_{(3,5)}(\mathbf{P};E) = 30954979328$ having positive sign

Note that Theorem 4.1.4 gives the sign of an elliptic net $\Psi(\mathbf{P};E)$ associated to an elliptic curve E and a collection of points $\mathbf{P}$ on it. In the next section we show this theorem can be used for calculating the signs in any general non-singular non-degenerate elliptic net W.

4.2 The Signs in a General Elliptic Net

We can use Theorem 4.1.4 in order to find the sign of any non-singular non-degenerate elliptic net. The main observation is that non-singular non-degenerate elliptic nets W are scale equivalent to the nets $\Psi(\mathbf{P};E)$ associated elliptic curves E

and collection of points $\mathbf{P}$. More precisely, given any non-singular, non-degenerate elliptic net $W : \mathbb{Z}^n \longrightarrow K$ we can find an elliptic net E over K and an n-tuple of points $\mathbf{P} = (P_1,\ P_2, \ldots,\ P_n) \in E(K)^n$, such that

$$W(\mathbf{v}) = f(\mathbf{v})\Psi_{\mathbf{v}}(P; E)$$

for any $\mathbf{v} \in \mathbb{Z}^n$, where $f : \mathbb{Z}^n \longrightarrow K^*$ is a quadratic form. We next prove a general result regarding the sign of an elliptic net.

Theorem 4.2.1. *Let $W : \mathbb{Z}^n \longrightarrow \mathbb{R}$ be a non-singular non-degenerate elliptic net. Then possibly after replacing $W(\mathbf{v})$ with $f(\mathbf{v})W(\mathbf{v})$ for a quadratic form $f : \mathbb{Z}^n \longrightarrow \mathbb{R}^*$ there are n irrational numbers $\beta_1, \beta_2, \cdots, \beta_n$ given by Table 4.1 and can be calculated using an elliptic curve attached to W and points on it by following the similar procedure as described in Theorem 4.1.4 so that the parity of $W(\mathbf{v})$ up to parity of a quadratic form is given by one of the following formulas:*

$$\text{Parity}[W(\mathbf{v})] \equiv \left\lfloor \sum_{i=1}^{n} v_i\beta_i \right\rfloor \pmod 2. \tag{4.37}$$

$$\text{Parity}[W(\mathbf{v})] \equiv \begin{cases} \left\lfloor \sum_{i=1}^{n} v_i\beta_i \right\rfloor + \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \sum_{i=1}^{k} v_i \text{ is even} \\ \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod 2 & \text{if } \sum_{i=1}^{k} v_i \text{ is odd} \end{cases} \tag{4.38}$$

where the formula (4.37) *is used when $u_i > 0$ for all $1 \leq i \leq n$, otherwise* (4.38) *is used.*

Proof. First of all note that by Theorem 3.5.5, for a non-singular non-degenerate elliptic net $W : \mathbb{Z}^n \longrightarrow \mathbb{R}$ there exists an elliptic curve E defined over $\mathbb{R}$ and a collection $\mathbf{P} = (P_1,\ P_2, \ldots, P_n)$ of points in $E(\mathbb{R})$, such that

$$W(\mathbf{v}) = f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P}; E)$$

for any $\mathbf{v} \in \mathbb{Z}^n$. Here $f : \mathbb{Z}^n \longrightarrow \mathbb{R}^*$ is a quadratic form and $\Psi(P; E)$ is the elliptic net associated to $\mathbf{P}$ and E. Thus

$$\begin{aligned} \text{Sign}[W(\mathbf{v})] &= \text{Sign}[f(\mathbf{v})]\ \text{Sign}[\Psi_{\mathbf{v}}(P; E)] \\ &= (-1)^{\text{Parity}[f(\mathbf{v})]}\ \text{Sign}[\Psi_{\mathbf{v}}(P; E)], \end{aligned} \tag{4.39}$$

where Parity$[f(\mathbf{v})]$ is in $\mathbb{Z}/2\mathbb{Z}$.

Next, consider $g : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ defined as

$$g(\mathbf{v}) = \begin{cases} \displaystyle\sum_{1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j & \text{if } \ 0 < \ q \ < \ 1 \\ \displaystyle\sum_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j & \text{if } -1 < q < 0, \end{cases}$$

and $H : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ defined as

$$H(\mathbf{v}) = \left\lfloor \sum_{i=1}^{n} v_i \beta_i \right\rfloor \qquad \text{if } \ 0 < \ q \ < \ 1$$

$$H(\mathbf{v}) = \begin{cases} \left\lfloor \displaystyle\sum_{i=1}^{n} v_i \beta_i \right\rfloor + \displaystyle\sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor & \text{if } \ \displaystyle\sum_{i=1}^{k} v_i \text{ is even} \\ \displaystyle\sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor & \text{if } \ \displaystyle\sum_{i=1}^{k} v_i \text{ is odd} \ \text{ if } \ 0 < \ q \ < \ 1 \end{cases}$$

where q and β_i are defined in Theorem 4.1.4. Then using Theorem 4.1.4 we know that

$$\text{Sign}[\Psi_{\mathbf{v}}(P; E)] = (-1)^{g(\mathbf{v}) + H(\mathbf{v})}.$$

So we can rewrite (4.39) as follows

$$\begin{aligned} \text{Sign}[W(\mathbf{v})] &= (-1)^{\text{Parity}[f(\mathbf{v})]}\ (-1)^{g(\mathbf{v}) + H(\mathbf{v})} \\ &= (-1)^{\text{Parity}[f(\mathbf{v})] + g(\mathbf{v})}\ (-1)^{H(\mathbf{v})} \end{aligned} \tag{4.40}$$

Furthermore, note that $f(\mathbf{v})(-1)^{g(\mathbf{v})}$ is a quadratic form. So up to the sign of a quadratic form

$$\text{Sign}[W(\mathbf{v})] = (-1)^{H(\mathbf{v})}.$$

In other words,

$$\text{Parity}[W(\mathbf{v})] \equiv H(\mathbf{v}) \pmod 2.$$

□

Remark 4.2.2. We remark that in order to use Theorem 4.2.1 in applications, we need an effective version of the curve-net theorem (Theorem 3.5.5). In other words for a given non-degenerate, non-singular elliptic net we should be able to compute the corresponding curve E and the points $\mathbf{P}$ on it. For simplicity we explain concretely how we can compute the sign of any non-singular, non-degenerate elliptic net of rank 1 and 2. For higher ranks see [13].

Procedure for elliptic net of rank 1.

Let $W : \mathbb{Z} \longrightarrow \mathbb{R}$ be a non-singular, non-degenerate elliptic net. By using Proposition 3.3.12, there is a quadratic form $f(n) : \mathbb{Z} \longrightarrow \mathbb{R}$ given by

$$f(n) = W(1)^{-n^2}$$

such that $W = f(n)W'$, where W' is a normalized elliptic net. Note that since W is non-degenerate, $W(1) \neq 0$. Then from Proposition 3.5.1 there is an elliptic curve $E/\mathbb{R}$ given by

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x, \qquad \text{and point } P = (0, 0),$$

where

$$a_1 = \frac{W(2) + W(2)^5 - 2W(2)W(3)}{W(2)^2W(3)},$$
$$a_2 = \frac{W(2)W(3)^2 + W(4) + W(2)^5 - W(2)W(3)}{W(2)^3W(3)},$$
$$a_3 = W(2), \qquad a_4 = 1,$$

such that

$$\Psi_n(P; E) = W'(n) \qquad \text{for all } n \in \mathbb{Z}.$$

Thus the sign of $W(n)$ is given by

$$\begin{aligned}\text{Sign}[W(n)] &= \text{Sign}[f(n)]\text{Sign}[\Psi_n(P; E)] \\ &= \text{Sign}[W(1)^{n^2}]\text{Sign}[\Psi_n(P; E)],\end{aligned}$$

where $\text{Sign}[\Psi_n(P; E)$ can be computed by using Theorem 4.1.4. Moreover, since for any rank 1 elliptic net W, the value of $W(1)$ is known, therefore we can easily calculate the sign of any term in net W.

Procedure for elliptic net of rank 2.

Let $W : \mathbb{Z}^2 \longrightarrow \mathbb{R}$ be a non-singular, non-degenerate elliptic net. From Proposition 3.3.12 we know that for any non-degenerate elliptic net $W : \mathbb{Z}^2 \longrightarrow \mathbb{R}$, there is a quadratic form $f(m, n) : \mathbb{Z}^2 \longrightarrow \mathbb{R}$ given by

$$f(m, n) = W(1, 0)^{-m^2+mn}\ W(0, 1)^{-n^2+mn}\ W(1, 1)^{-mn}$$

such that $W = f(m, n)W'$, where W' is a normalized elliptic net. Observe that since W is non- degenerate the terms $W(1, 0), W(0, 1)$, and $W(1, 1)$ are non-zero. Then from Proposition 3.5.2 there is an elliptic curve $E/\mathbb{R}$ and a collection of points $\mathbf{P} = (P, Q)$

given by

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

where

$$a_1 = \frac{W(2,0) - W(0,2)}{W(2,1) - W(1,2)}, \qquad a_2 = 2W(2,1) - W(1,2),$$
$$a_3 = W(2,0), \quad a_4 = W(2,1)[W(2,1) - W(1,2)],$$

and

$$P = (0,0), \quad Q = (W(1,2) - W(2,1), 0),$$

such that

$$\Psi_{(m,n)}(\mathbf{P}; E) = W'(m,n) \qquad \text{for all } (m,n) \in \mathbb{Z}^2.$$

Thus the sign of $W(m,n)$ is given by

$$\begin{aligned}\text{Sign}[W(m,n)] &= \text{Sign}[f(m,n)]\text{Sign}[\Psi_{(m,n)}(\mathbf{P}; E)] \\ &= \text{Sign}[W(1,0)^{m^2+mn}\ W(0,1)^{n^2+mn}\ W(1,1)^{mn}]\text{Sign}[\Psi_{(m,n)}(\mathbf{P}; E)],\end{aligned}$$

where $\text{Sign}[\Psi_{(m,n)}(\mathbf{P}; E)]$ can be computed by using Theorem 4.1.4. Moreover, Since for any rank 2 elliptic net W, the value of $W(1,0), W(0,1)$, and $W(1,1)$ are known, therefore we can easily calculate the sign of any term in W.

Chapter 5

Applications

In this chapter we give some applications of our theorems in Chapter 4. The first application is related to the distribution of signs in an elliptic net, which will be described in Section **??** We will show that the signs in elliptic net are uniformly distributed. In Section 5.2 of this chapter we give the second application which is regarding *elliptic denominator sequences*.

5.1 Distribution of Signs in an Elliptic Sequence

In 1960, I. Niven [6] introduced the concept of uniform distribution modulo m of sequence of integers. We start with the following definition.

Definition 5.1.1. Let $A = (a_n)$ be an infinite sequence of integers. For any integers j and $m \geq 2$ denote $A(N, j, m)$ by the number of terms among $a_1, a_2, \ldots, a_N$ such that $a_i \equiv j \pmod{m}$. Then the sequence A is said to be *uniformly distributed modulo* m if

$$\lim_{N\to\infty} \frac{1}{N} A(N, j, m) = \frac{1}{m}$$

for $j = 0, 1, \ldots, m-1$.

A sequence (a_n) of integers is said to be *uniformly distributed* if (a_n) is uniformly distributed modulo m for every $m \geq 2$. We give some examples of sequences which are uniformly distributed modulo m.

1. The sequence $(a_n) = (n)$, $n \in \mathbb{Z}$ is uniformly distributed modulo m for every

$m \geq 2$.

2. An arithmetic progression $\{an + b \mid n = 1, 2, 3, \ldots\}$ is uniformly distributed modulo m if and only if $\gcd(a, m) = 1$.

We are interested in how the signs of an elliptic net of rank 1 are distributed. In order to do this we need to define what we mean when we say the sequence of signs is *uniformly distributed*.

Definition 5.1.2. We say that signs of a real sequence (a_n) is *uniformly distributed* if the parity sequence $(\text{Parity}(a_n))$ is uniformly distributed modulo 2.

We will employ the following known theorem in our investigation.

Theorem 5.1.3. *For any real number θ let $A(\theta)$ be the sequence of integers*

$$\lfloor\theta\rfloor, \lfloor 2\theta\rfloor, \lfloor 3\theta\rfloor, \ldots, \lfloor n\theta\rfloor, \ldots.$$

Then the sequence $A(\theta)$ is uniformly distributed if and only if θ is irrational or $\theta = 1/k$ for some non-zero integer k.

Proof. See [6, Theorem 3.1]. □

As a direct consequence of Theorems 4.1.4 and 5.1.3 we have the following result on distribution of signs of real elliptic sequences.

Theorem 5.1.4. *Let $W : \mathbb{Z} \longrightarrow \mathbb{R}$ be an elliptic sequence. Then the sequence* $(\text{Sign}[W(n)])$, *of signs of the terms of an elliptic sequence, is uniformly distributed.*

Proof. From Theorem 4.1.4 the sign of the n-th term of an elliptic sequence is given

by

$$\text{Sign}[W(n)] = (-1)^{\lfloor n\beta \rfloor}$$

$$\text{Sign}[W(n)] = \begin{cases} (-1)^{\lfloor n\beta \rfloor + \lfloor n/2 \rfloor} & \text{if } n \text{ is even,} \\ (-1)^{\lfloor n/2 \rfloor} & \text{if } n \text{ is odd.} \end{cases}$$

We want to show that each of the sequences $\left((-1)^{\lfloor n\beta \rfloor}\right)$, $\left((-1)^{\lfloor n\beta \rfloor + \lfloor n/2 \rfloor}\right)_{n \text{ even}}$, and $\left((-1)^{\lfloor n/2 \rfloor}\right)_{n \text{ odd}}$ is uniformly distributed. In view of Definition 5.1.2 equivalently we can show that the sequences $(\lfloor n\beta \rfloor)$, $(\lfloor n\beta \rfloor + \lfloor n/2 \rfloor)_{n \text{ even}}$, and $(\lfloor n/2 \rfloor)_{n \text{ odd}}$ are uniformly distributed modulo 2. Since β is an irrational number therefore the fact that the distribution of the sequence $(\lfloor n\beta \rfloor)$ is uniform modulo 2 follows from Theorem 5.1.3.

The sequence $(\lfloor n\beta \rfloor + \lfloor n/2 \rfloor)_{n \text{ even}}$ can be written as, with $n = 2m$,

$$(\lfloor n\beta \rfloor + \lfloor n/2 \rfloor)_{n \text{ even}} = (\lfloor 2m\beta \rfloor + \lfloor m \rfloor) = (\lfloor m(2\beta + 1) \rfloor),$$

which is uniformly distributed modulo 2 using Theorem 5.1.3. Finally the sequence $(\lfloor n/2 \rfloor)_{n \text{ odd}}$, for $n = 2m + 1$, can be written as

$$(\lfloor n/2 \rfloor)_{n \text{ odd}} = (\lfloor m + 1/2 \rfloor) = (m),$$

which is again uniformly distributed modulo 2. Hence for all the cases the sequence of (Parity(a_n)) of terms of an elliptic sequence is uniformly distributed modulo 2. □

We now move on to our second application of Theorem 4.1.4.

5.2 Connection With Denominator Net

In order to explain the second application we first introduce the concept of a *denominator net*, for that we need the following proposition.

Proposition 5.2.1. *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $a_i \in \mathbb{Z}$ be an elliptic curve defined over $\mathbb{Q}$. Then any point P in $E(\mathbb{Q})$ will be of the form*

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

where $A_P, B_P, D_P \in \mathbb{Z}$, $D_P > 0$ and $\gcd(A_P, D_P) = \gcd(B_P, D_P) = 1$.

Proof. See [3, Proposition 7.3.1]. □

Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation with integer coefficients. If $P \in E(\mathbb{Q})$ is a non-torsion point (i.e., $nP \neq \mathcal{O}$ for any n) then we have that

$$nP = \left(\frac{A_{nP}}{D_{nP}^2},\ \frac{B_{nP}}{D_{nP}^3}\right).$$

We call the sequence (D_{nP}) an *elliptic denominator sequence* associated to curve E and the point P. It can be proved that (D_{nP}) is a divisibility sequence. Many authors have extensively studied the sequence (D_{nP}). In fact, Shipsey [8] showed that there is a way to assign signs (observe that $D_{nP} > 0$ for all n) to (D_{nP}) so that it becomes an elliptic divisibility sequence. More precisely, let E be an elliptic curve given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x, \qquad a_i \in \mathbb{Z} \tag{5.1}$$

with the condition that $\gcd(a_3, a_4) = 1$. Let $P = (0, 0)$ be a point of infinite order in $E(\mathbb{Q})$. Let (D_{nP}) be the associated elliptic denominator sequence. Let (W_n) be a sequence defined by the rule given below

$$W_1 = 1, \qquad W_2 = a_3, \qquad |W_n| = D_{nP} \ \text{ for } n \geq 2.$$

Suppose we assign signs to the terms of (W_n) as follows

$$\text{Sign}(W_{n-2}W_n) = -\text{Sign}(A_{(n-1)P}) \text{ for } n \geq 3.$$

Then in [8, Section 4.4] Shipsey showed that (W_n) will be an elliptic divisibility sequence. We observe that the condition on E that $\gcd(a_3, a_4) = 1$ is equivalent to that $P = (0, 0)$ reduces to a non-singular point modulo any prime ℓ. She also showed that if a curve is not of the form (5.1) then it is always possible to transform a given curve into a curve of the form (5.1) (see [8, Chapter 5]).

The concept of elliptic denominator sequence has been generalized to higher ranks, the so called *elliptic denominator net*. If $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ is an n-tuple of linear independent points in $E(\mathbb{Q})$. Then for $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$ we can write

$$\mathbf{v} \cdot \mathbf{P} = v_1P_1 + v_2P_2 + \cdots + v_nP_n = \left(\frac{A_{\mathbf{v}\cdot P}}{D^2_{\mathbf{v}\cdot P}}, \frac{B_{\mathbf{v}\cdot P}}{D^3_{\mathbf{v}\cdot P}}\right).$$

Then $(D_{\mathbf{v}\cdot P})$ is called the elliptic denominator net associated to an elliptic curve E and a collection of points $\mathbf{P}$. There is a relation between elliptic denominator net $(D_{\mathbf{v}\cdot P})$ and the values of the $\mathbf{v}$-th net polynomial $\Psi_{\mathbf{v}}(\mathbf{P}; E)$. In order to explain this relation we will consider a scale equivalent net $\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)$ which is defined by relation

$$\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E) = F_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P}; E) \qquad \text{for all } \mathbf{v} \in \mathbb{Z}^n, \tag{5.2}$$

where $F(\mathbf{P}) : \mathbb{Z}^n \longrightarrow \mathbb{Q}^*$ is the quadratic form given by

$$F_{\mathbf{v}}(\mathbf{P}) = \prod_{1\leq i\leq j\leq n} A_{ij}^{v_iv_j}, \tag{5.3}$$

with

$$A_{ii} = D_{\mathbf{e_i}\cdot\mathbf{P}} = D_{P_i}, \quad \text{and} \quad A_{ij} = \frac{D_{P_i+P_j}}{D_{P_i}D_{P_j}} \text{ for } i \neq j.$$

Then we know form Proposition 3.3.10 that $\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)$ will be an elliptic net, which is scale equivalent to $\Psi_{\mathbf{v}}(\mathbf{P}; E)$. Furthermore, note that

$$\hat{\Psi}_{e_i}(\mathbf{P}; E) = F_{\mathbf{e_i}}(\mathbf{P})\Psi_{\mathbf{e_i}}(\mathbf{P}; E) = A_{ii} = D_{\mathbf{e_i}\cdot\mathbf{P}}$$

and

$$\hat{\Psi}_{\mathbf{e_i}+\mathbf{e_j}}(\mathbf{P}; E) = F_{\mathbf{e_i}+\mathbf{e_j}}(\mathbf{P})\Psi_{\mathbf{e_i}+\mathbf{e_j}}(\mathbf{P}; E) = A_{ii}A_{ij}A_{jj} = D_{P_i+P_j} = D_{(\mathbf{e_i}+\mathbf{e_j})\cdot\mathbf{P}}.$$

In [2], the following proposition is proved.

Proposition 5.2.2 (**Akbary-Bleaney-Yazdani**). *Let E be an elliptic curve defined over $\mathbb{Q}$ given by the Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Z}.$$

Let $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ be an n-tuple of linear independent points in $E(\mathbb{Q})$ so that each $P_i \pmod{\ell}$ is non-singular for every prime ℓ. Then we have

$$D_{\mathbf{v}\cdot P} = |\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)| \tag{5.4}$$

for all $\mathbf{v} \in \mathbb{Z}^n$.

Proof. See [2, Proposition 1.7]. □

Here as a consequence of Theorem 4.1.4 and above proposition we describe how one can assign signs to a denominator net to obtain an elliptic net.

Proposition 5.2.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ under the assumptions of Proposition 5.2.2. Define a map $W(\mathbf{v}) : \mathbb{Z}^n \longrightarrow \mathbb{Q}$ as*

$$W(\mathbf{v}) = (-1)^{Parity[\Psi_{\mathbf{v}}(\mathbf{P};E)]} D_{\mathbf{v}\cdot P}, \tag{5.5}$$

where $\Psi(\mathbf{P}; E)$ *is the elliptic net associated to* E *and a collection of points* $\mathbf{P}$*. Then* $W(\mathbf{v})$ *is an elliptic net.*

Proof. First of all observe that since all the terms of a denominator net is positive hence the quadratic form given by (5.3) is also positive. Therefore from (5.2) it follows that

$$\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] = \text{Parity}[\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)], \tag{5.6}$$

Now define a map $W(\mathbf{v}) : \mathbb{Z}^n \longrightarrow \mathbb{Q}$ such that

$$|W(\mathbf{v})| = D_{\mathbf{v}\cdot P} \qquad \text{for all } \mathbf{v} \in \mathbb{Z}^n,$$

and assign the sign to $W(\mathbf{v})$ by

$$\text{Sign}[W(\mathbf{v})] = (-1)^{\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P};E)]},$$

where the $\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)]$ is given in Theorem 4.1.4. Thus define

$$W(\mathbf{v}) = (-1)^{\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P};E)]} D_{\mathbf{v}\cdot P}. \tag{5.7}$$

Observe that using (5.4) and (5.6) we can rewrite (5.7) as follows

$$\begin{aligned} W(\mathbf{v}) &= (-1)^{\text{Parity}[\hat{\Psi}_{\mathbf{v}}(\mathbf{P};E)]} |\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)| \\ &= \text{Sign}[\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)] |\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)| \\ &= \hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E) \end{aligned}$$

which is an elliptic net by (5.2). Hence $W(\mathbf{v})$ is an elliptic net. This completes the proof of this theorem. □

Remark 5.2.4. For rank one elliptic net the above proposition gives an alternative

method different from Shipsey's in generating elliptic sequences out of elliptic denominator sequences.

Bibliography

[1] T. M. Apostol. *Modular Functions and Dirichlet Series in Number Theory.* Springer-Verlag, 1990.

[2] A. Akbary, J. Bleaney, and S. Yazdani. On Symmetries of Elliptic Nets and Valuations of Net Polynomials. *arXiv : 1408.6623*, 2014.

[3] H. Cohen. *Number Theory Volume I : Tools and Diophantine Equations.* Springer, New York, 2007.

[4] S. Lang. *Elliptic Curves: Diophantine Analysis.* Springer-Verlag, 1978.

[5] S. Lang. *Elliptic Functions.* Springer-Verlag, 1986.

[6] I. Niven. Uniform Distribution of Sequences of Integers. *Trans. Amer.Math. Soc.*, 98: 52–61, 1960.

[7] S. Ponnusamy and H. Silverman. *Complex Variables with Applications.* Birkhäuser, Boston, 2006.

[8] R. Shipsey. Elliptic Divisibility Sequences. *Ph.D. Thesis, Goldsmith's College, University of London*, 2000.

[9] J. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.

[10] J. Silverman. *Advanced Topic in the Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1994.

[11] J. Silverman and N. Stephens. The sign of an Elliptic Divisibility Sequence. *Journal of Ramanujan Mathematical Society*, 21(1):1–17, 2006.

[12] K. Stange. Elliptic Nets and Elliptic Curves. *PhD Thesis, Brown University*, 2003.

[13] K. Stange. Elliptic Nets and Elliptic Curves. *Algebra and Number Theory*, 5(2):197–229, 2011.

[14] M. Ward. Memoir on Elliptic Divisibility Sequences. *American Journal of Mathematics.*, 70:31–74, 1948.