ON SOME PROPERTIES OF ELLIPTIC NETS

JEFF BLEANEY
Bachelor of Arts and Science, University of Lethbridge, 2012
Master of Science, University of Lethbridge, 2014

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

ON SOME PROPERTIES OF ELLIPTIC NETS

JEFF BLEANEY

Approved:

Signature *Date*

Supervisor: Dr. Amir Akbary

Supervisor: Dr. Soroosh Yazdani

Committee Member: Dr. Nathan Ng

Committee Member: Dr. Peter Dibble

Chair, Thesis Examination Committee: Dr. Hadi Kharaghani

ON SOME PROPERTIES OF ELLIPTIC NETS

Jeff Bleaney
Department of Mathematics and Computer Science
University of Lethbridge
M. Sc. Thesis, 2014

Let A be a finite rank free Abelian group, and let R be an Integral domain. An elliptic net is any map $W : A \to R$, which satisfies $W(0) = 0$, and

$$\begin{aligned} W(p+q+s)W(p-q)W(r+s)W(r) + \\ W(q+r+s)W(q-r)W(p+s)W(p) + \\ W(r+p+s)W(r-p)W(q+s)W(q) = 0, \quad (1) \end{aligned}$$

for all $p, q, r, s \in A$. For our purposes, we will typically consider an elliptic net $W : A \to k$, where k denotes a residue field. Letting $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$ be a basis for A, we say that W has a unique zero-rank of apparition with respect to $\mathcal{B}$ provided that there exists a tuple of natural numbers $(\rho_1, \rho_2, \ldots, \rho_r)$, with $\rho_i > 1$ for $i \leq i \leq r$, such that

$$W(nb_i) = 0 \iff \rho_i \mid n.$$

In this thesis, the following three results are proved.

1. Let $W : A \to k$ be an elliptic net with $\mathcal{B} = \{b_1, \ldots, b_r\}$ a basis for A and let

   $$\Lambda := \{v \in A : \ W(v) = 0\}.$$

   Under the assumptions that W has unique zero-rank of apparition with respect to $\mathcal{B}$, and that $W(b_i) \neq 0$ for $1 \leq i \leq r$, we prove that the set Λ is a lattice. In other words, Λ is a rank r subgroup of A.

2. Let $W : A \to k$ be an elliptic net with unique zero-rank of apparition $(\rho_1, \ldots, \rho_r)$ for which there exists i such that $\rho_i \geq 3$. In the case that $r = 1$ we assume that

$\rho_1 \geq 4$. We also define the function

$$\begin{array}{rccc} \phi: & \Lambda \times A \setminus \Lambda & \longrightarrow & k \\ & (\lambda, p) & \longmapsto & \frac{W(\lambda+p)}{W(p)}. \end{array}$$

Then, there eixsts functions

$$\begin{array}{rccc} \chi: & \Lambda \times A & \longrightarrow & k \\ & (\lambda, p) & \longmapsto & \frac{\phi(\lambda,p+v)}{\phi(\lambda,v)}, \end{array}$$

where v is any element of $A \setminus \Lambda$, with $v + p \notin \Lambda$, and

$$\begin{array}{rccc} a: & \Lambda & \longrightarrow & k \\ & \lambda & \longmapsto & \frac{\phi(\lambda,v)}{\chi(\lambda,v)}, \end{array}$$

for any $v \in A \setminus \Lambda$, such that for all $\lambda \in \Lambda$ and $p \in A$, we have

$$W(\lambda + p) = a(\lambda)\chi(\lambda, p)W(p).$$

3. Let K be a number field with ring of integers $\mathcal{O}_K$ and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Let E/K be an elliptic curve given by

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

with $a_i \in \mathcal{O}_K$ for $i = 1, 2, 3, 4, 6$. Letting $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$, and $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$, we have

$$\mathbf{v} \cdot \mathbf{P} = v_1P_1 + v_2P_2 + \cdots + v_rP_r = \left(\frac{\Phi_{\mathbf{v}}(\mathbf{P})}{\Psi_{\mathbf{v}}(\mathbf{P})^2}, \frac{\Omega_{\mathbf{v}}(\mathbf{P})}{\Psi_{\mathbf{v}}(\mathbf{P})^3} \right),$$

where $\Phi_{\mathbf{v}}(\mathbf{P}), \Omega_{\mathbf{v}}(\mathbf{P})$, and $\Psi_{\mathbf{v}}(\mathbf{P})$ are elements of a polynomial ring. Moreover, as a function of $\mathbf{v} \in \mathbb{Z}^r$, the net polynomials $\Psi_{\mathbf{v}} := \Psi_{\mathbf{v}}(\mathbf{P})$ satisfy equation (1).

We assume that $P_i \not\equiv \mathcal{O} \pmod{\mathfrak{p}}$, for $1 \leq i \leq r$, and $P_i \pm P_j \not\equiv \mathcal{O} \pmod{\mathfrak{p}}$, for $1 \leq i < j \leq r$. We also assume that $\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) \geq 0$ for all $\mathbf{v} \in \mathbb{Z}^n$. Then the following are equivalent:

(a) There exists $1 \leq i \leq r$ such that

$$\nu_{\mathfrak{p}}(\Psi_{2\mathbf{e_i}}(\mathbf{P})) > 0 \text{ and } \nu_{\mathfrak{p}}(\Psi_{3\mathbf{e_i}}(\mathbf{P})) > 0.$$

(b) There exists $1 \leq i \leq r$ such that for all $n \geq 2$ we have $\nu_{\mathfrak{p}}(\Psi_{n\mathbf{e_i}}(\mathbf{P})) > 0$.

(c) There exists $\mathbf{v} \in \mathbb{Z}^r$ and $1 \leq i \leq r$ such that

$$\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) > 0 \text{ and } \nu_{\mathfrak{p}}(\Psi_{\mathbf{v}+\mathbf{e_i}}(\mathbf{P})) > 0.$$

(d) There exists $\mathbf{v} \in \mathbb{Z}^r$ such that

$$\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) > 0 \text{ and } \nu_{\mathfrak{p}}(\Phi_{\mathbf{v}}(\mathbf{P})) > 0.$$

(e) There exists $1 \leq i \leq r$ such that $P_i \pmod{\mathfrak{p}}$ is singular.

We also explain how elliptic nets can be used to study the class of Diophantine equations

$$Y^2 = X^3 + dZ^{12},$$

under the condition that $d \mid Z$.

Contents

Chapter 1

Introduction

1.1 Overview

An *elliptic divisibility sequence*, first introduced by Morgan Ward [10] in 1948, is an integer sequence (W_n) which satisfies the equation

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

for all $m > n > 1$. Throughout his study of elliptic divisibility sequences, Ward made the assumption that $W_1^2 = 1$. If we drop this condition, the appropriate relation to consider is given by the homogeneous equation

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2. \tag{1.2}$$

However, for simplicity, we frequently assume that $W_1 = 1$.

Example 1.1.1. We note that the sequence (0) trivially satisfies 1.1, as does the sequence (n), hence both are examples of elliptic sequences. A more interesting example is given by the sequence

$$1, 1, -2, -3, 5, 8, -13, -21, 34, 55, \ldots$$

In absolute value this is precisely the Fibonacci sequence.

Among the key results proved in [10] regarding the structure of an elliptic divisibility sequence, is the following:

Theorem 1.1.2. Ward's Symmetry Theorem Let p be any prime, with rank of

apparition $\rho > 3$. Then there exist integers a and b such that

$$W_{\rho-i} \equiv -ab^{-i}W_i \pmod{p} \text{ for } 0 \leq i \leq \rho. \tag{1.3}$$

where $\rho > 1$ is the smallest number such that $p \mid W_\rho$.

See [10, Theorem 8.1] for a proof.

The importance of Theorem 1.1.2 comes from the fact that equation (1.1) does not provide an effective means of computing arbitrary terms of an elliptic divisibility sequence. However, by using Theorem 1.1.2, and examining the relations between the terms a, and b, Ward [10, Lemma 9.1] gave an explicit formula for calculating arbitrary terms of an elliptic divisibility sequence modulo p, for certain primes p.

Theorem 1.1.3. With the notation and assumptions of Theorem 1.1.2, we have

$$W_{\rho+i} \equiv ab^iW_i \pmod{p}, \tag{1.4}$$

for all positive integers i.

We remark that we can define an equivalence relation on the set of elliptic divisibility sequences. Two elliptic divisibility sequences (W_n) and (W'_n) are said to be *equivalent* if there exist non-zero constants c_1 and c_2, such that $(W'_n) = (c_1c_2^{n^2}W_n)$. Ward [10, Theorem 25.2] was able to prove that any sequence (W_n) satisfying (1.1) is equivalent to one of the following

$$W'_n = n,\ W'_n = \frac{\sin(n\theta)}{\sin(\theta)},\ W'_n = \frac{\sigma(nu;\Lambda)}{\sigma(u;\Lambda)^{n^2}},\ W'_n = \lambda_n c^{1-n\lambda_n},$$

where $\sigma(u;\Lambda)$ denotes the Weierstrass σ-function relative to the lattice $\Lambda \subset \mathbb{C}$, for some $u \in \mathbb{C}$, (see §3.1 Definition 3.1.4), c is a non-zero constant, and λ_n is defined by

$$\lambda_n = \begin{cases} 0 \text{ if } n \not\equiv \pm 1 \bmod l \\ 1 \text{ if } n \equiv 1 \bmod l \\ -1 \text{ if } n \equiv -1 \bmod l, \end{cases}$$

for any fixed odd number $l > 1$.

Of particular interest to us, are sequences of the form $W_n = \sigma(nu;\Lambda)/\sigma(u;\Lambda)^{n^2}$. Sequences of this type are closely related to rational points on elliptic curves, and have been studied extensively for their number theoretic and cryptographic applications (see [3], [6] and [7]).

An elliptic curve E over a field K (denoted E/K) is defined by a non-singular cubic equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.5}$$

with $a_1, a_2, a_3, a_4, a_6 \in K$, together with the point at infinity $\mathcal{O}$ given in projective coordinates as $[0, 1, 0]$. If K is a number field, and E/K is an elliptic curve defined by (1.5) with $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_K$, where $\mathcal{O}_K$ denotes the ring of integers of K, we can *reduce* E modulo a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ by considering the curve $\bar{E}$ defined by

$$y^2 + [a_1]xy + [a_3]y \equiv x^3 + [a_2]x^2 + [a_4]x + [a_6] \pmod{\mathfrak{p}}.$$

If the equation defining E/K remains non-singular when reduced modulo $\mathfrak{p}$, we say that E has *good* reduction at $\mathfrak{p}$, otherwise we say that E has *bad* reduction at $\mathfrak{p}$.

We denote by $E(K)$ the set of K-rational points of E. Thus

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

We have already considered the reduction of an elliptic curve modulo a prime ideal $\mathfrak{p}$, similarly, we can consider the reduction of a point $P \in E(K)$ modulo a prime ideal $\mathfrak{p}$. We define the reduction of a point $P = (x, y) \in E(K)$ modulo $\mathfrak{p}$ to be the point

$$\bar{P} = (x + \mathfrak{p}, y + \mathfrak{p}) \in \bar{E}(\mathcal{O}_K/\mathfrak{p}).$$

Letting

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

and letting $P = (x_0, y_0)$ be a point on the curve $f(x, y) = 0$, we say that P is *singular* modulo $\mathfrak{p}$ if we have

$$\frac{\partial f}{\partial x}(x_0, y_0) \equiv \frac{\partial f}{\partial y}(x_0, y_0) \equiv 0 \pmod{\mathfrak{p}}.$$

In general, for a cubic equation E (not necessarily non-singular), defined over a field k, we can define a group structure on the set of non-singular k-rational points $E_{ns}(k) \subset E(k)$, where addition of points can be described geometrically, as seen in Figure 1.1. Under this operation $E_{ns}(K)$ is an Abelian group. For an algebraic description of the

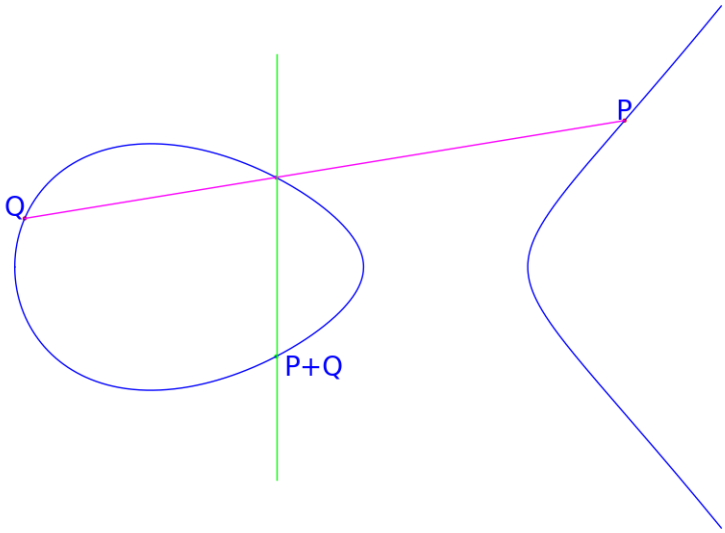

Figure 1.1: Group law for elliptic curves.

group law for elliptic curves, see [8, Chapter III.2].

The following proposition gives an explicit representation for the coordinates of K-rational points on an elliptic curve.

Proposition 1.1.4. Let R be a principal ideal domain with the field of fractions K. For an elliptic curve E/K defined by (1.5), with $a_i \in R$ for $i = 1, 2, 3, 4, 6$, and a rational point $P \in E(K)$, we have

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

for some $A_P, B_P, D_P \in R$ with $\gcd(A_P, D_P) = \gcd(B_P, D_P) = 1$.

See [2, Proposition 7.3.1] for a proof. We remark that with the notation of Proposition 1.1.4, the terms A_P, B_P and D_P are uniquely defined up to multiplication by a unit

$u \in R^*$.

A rational point P on an elliptic curve E/K with representation as in proposition 1.1.4, is said to be *integral* if $D_P \in R^*$. We say that P is *power integral* if $D_P = d^n$ for some $d \in R$, and a natural number $n > 1$, if $n = 2$, we say P is *square integral*.

For an elliptic curve E/K, with K the field of fractions of a principal ideal domain R, and a point $P \in E(K)$, we define

$$nP = \left(\frac{A_{nP}}{D_{nP}^2}, \frac{B_{nP}}{D_{nP}^3} \right), \tag{1.6}$$

where A_{nP}, B_{nP}, D_{nP} are as in Proposition 1.1.4. With this construction in mind, the *elliptic denominator sequence* (D_{nP}) is intimately related to an elliptic divisibility sequence (W_n), of the form $W_n = \sigma(nu;\Lambda)/\sigma(u;\Lambda)^{n^2}$, for some $u \in \mathbb{C}$, and $\Lambda \subset \mathbb{C}$.

For an elliptic curve E/K defined by (1.5), there exist polynomials ψ_n, ϕ_n, and $\omega_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]$ such that for all rational points $P = (x, y) \in E(K)$, we have

$$nP = \left(\frac{\phi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3} \right). \tag{1.7}$$

Moreover, we have that ϕ_n and ψ_n are relatively prime as polynomials, and the polynomials ψ_n satisfy equation (1.1). Furthermore, there exists $u \in \mathbb{C}^*$, and a lattice $\Lambda \subset \mathbb{C}$ such that

$$\psi_n(P) = -(-1)^{n^2} \frac{\sigma(nu;\Lambda)}{\sigma(u;\Lambda)^{n^2}}.$$

The polynomial ψ_n is referred to as the n^{th} *division polynomial* associated to E.

Before we can state the main theorem relating terms $\psi_n(P)$ with the terms D_{nP}, of the elliptic denominator sequence associated to P, we first introduce the necessary notation.

Let K be a number field with ring of integers $\mathcal{O}_K$, and $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$, we also fix an embeding $K \hookrightarrow \mathbb{C}$. For each $x \in K^*$, $x\mathcal{O}_K$ is a fractional ideal of $\mathcal{O}_K$, and can therefore be written uniquely as a product of prime ideals of $\mathcal{O}_K$. Thus, we have

$$x\mathcal{O}_K = I\mathfrak{p}^\alpha,$$

where I is a fractional ideal of R, with $I \cap \mathfrak{p} = \{0\}$, and α is an integer. With this

notation, we define the $\mathfrak{p}$-adic valuation, $\nu_{\mathfrak{p}}$, as

$$\nu_{\mathfrak{p}}(x) := \alpha.$$

For a number field K with the ring of integers $\mathcal{O}_K$, and a valuation $\nu_{\mathfrak{p}}$ associated to a prime ideal $\mathfrak{p}$, Ayad [1, Theorem A] proved the following theorem on the $\mathfrak{p}$-adic valuation of $\psi_n(P)$.

Theorem 1.1.5 (Ayad). Let E/K be an elliptic curve defined by (1.5), with $a_i \in \mathcal{O}_K$ for $i = 1, 2, 3, 4, 6$. Let $P \in E(K)$ be a point other than the point at infinity $\mathcal{O}$. Suppose that the reduction modulo $\mathfrak{p}$ of P is not the point at infinity. Then the following assertions are equivalent:

(a) $\nu_{\mathfrak{p}}(\psi_2(P))$ and $\nu_{\mathfrak{p}}(\psi_3(P)) > 0$.

(b) For all integers $n \geq 2$, we have $\nu_{\mathfrak{p}}(\psi_n(P)) > 0$.

(c) There exists an integer $n \geq 2$ such that $\nu_{\mathfrak{p}}(\psi_n(P))$ and $\nu_{\mathfrak{p}}(\psi_n(P)) > 0$.

(d) There exists an integer $n \geq 2$ such that $\nu_{\mathfrak{p}}(\psi_n(P))$ and $\nu_{\mathfrak{p}}(\phi_n(P)) > 0$.

(e) $P \pmod{\mathfrak{p}}$ is singular.

The next proposition employs Theorem 1.1.5 to make the connection between the representations of points nP in (1.6) and (1.7) explicit.

Proposition 1.1.6. Suppose the assumptions of Theorem 1.1.5 hold for E, P, and all primes of bad reduction $\mathfrak{p}$. Moreover suppose that $P \pmod{\mathfrak{p}}$ is non-singular for all primes of bad reduction $\mathfrak{p}$. We also assume that $\mathcal{O}_K$ is a principal ideal domain, and let (D_{nP}) be the elliptic denominator sequence associated to E and P. Then we have

$$D_{nP} = uD_P^{n^2}\psi_n(P),$$

where $u \in \mathcal{O}_K^*$ is a unit. More generally if the assumptions of Theorem 1.1.5 hold for E, P, and a prime $\mathfrak{p}$, and if $P \pmod{\mathfrak{p}}$ is non-singular, then

$$\nu_{\mathfrak{p}}(D_{nP}) = \nu_{\mathfrak{p}}(\psi_n(P)).$$

By considering the $\mathfrak{p}$-adic valuation of terms in an elliptic divisibility sequence, Reynolds [6] recently proved that under certain conditions, the corresponding elliptic denominator sequence has finitely many terms which are perfect powers. This result is useful in determining whether an elliptic curve has any power integral points. For instance, it can be shown that the elliptic curve $E : y^2 = x^3 + 11$ has no power integral points. This result relies on the fact that for the elliptic curve E, there exists a point $P \in E(\mathbb{Q})$ such that $E(\mathbb{Q}) = \langle P \rangle \oplus E_{tors}(\mathbb{Q})$.

In general, the free part of the group $E(K)$ is not necessarily generated by a single point, however the following theorem describes the structure of $E(K)$.

Theorem 1.1.7 (**Mordell-Weil**). The group $E(K)$ is finitely generated, i.e.

$$E(K) \cong \mathbb{Z}^r \oplus \mathbf{T}$$

where $\mathbf{T}$ is a finite Abelian group.

See [8, Theorem VIII.6.7] for a proof. With the notation of the preceding theorem, we call r the *rank* of E.

We remark that Reynold's result can be applied in determining if a rank 1 elliptic curve has any power integral points. In this thesis, we give a method of finding square integral points on higher rank elliptic curves. In order to do so, we need a generalization of Proposition 1.1.6 to linear combinations of points on an elliptic curve.

For a tuple of points $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$ and $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$, we define

$$\mathbf{v} \cdot \mathbf{P} = v_1 P_1 + v_2 P_2 + \cdots + v_r P_r = \left(\frac{A_{\mathbf{v}\cdot\mathbf{P}}}{D^2_{\mathbf{v}\cdot\mathbf{P}}}, \frac{B_{\mathbf{v}\cdot\mathbf{P}}}{D^3_{\mathbf{v}\cdot\mathbf{P}}} \right),$$

where $A_{\mathbf{v}\cdot\mathbf{P}}, B_{\mathbf{v}\cdot\mathbf{P}}$, and $D_{\mathbf{v}\cdot\mathbf{P}}$ are as in Proposition 1.1.4. The collection of terms $(D_{\mathbf{v}\cdot\mathbf{P}})$ is referred to as the *elliptic denominator net* associated to E and $\mathbf{P}$. We can also express the points $\mathbf{v} \cdot \mathbf{P}$ as

$$\mathbf{v} \cdot \mathbf{P} = \left(\frac{\Phi_{\mathbf{v}}(\mathbf{P})}{\Psi^2_{\mathbf{v}}(\mathbf{P})}, \frac{\Omega_{\mathbf{v}}(\mathbf{P})}{\Psi^3_{\mathbf{v}}(\mathbf{P})} \right)$$

where $\Psi_{\mathbf{v}}, \Phi_{\mathbf{v}}, \Omega_{\mathbf{v}}$ are elements of a certain polynomial ring (See §3.2 for a complete description).

In her 2008 Ph.D. thesis [9], Kate Stange showed that for a fixed tuple $\mathbf{P} \in E(K)^r$, the $\mathbf{v}^{th}$ *net polynomials* $\Psi_{\mathbf{v}} := \Psi_{\mathbf{v}}(\mathbf{P})$ satisfy the relation

$$\Psi_{\mathbf{p+q+s}}\Psi_{\mathbf{p-q}}\Psi_{\mathbf{r+s}}\Psi_{\mathbf{r}} + \Psi_{\mathbf{q+r+s}}\Psi_{\mathbf{q-r}}\Psi_{\mathbf{p+s}}\Psi_{\mathbf{p}} + \Psi_{\mathbf{r+p+s}}\Psi_{\mathbf{r-p}}\Psi_{\mathbf{q+s}}\Psi_{\mathbf{q}} = 0, \tag{1.8}$$

for all $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s} \in \mathbb{Z}^r$.

Functions satisfying the type of relation described in (1.8) were first introduced in 2008 by Stange [9], as a generalization of elliptic divisibility sequences. These type of functions are the main objects of interest of this thesis.

Definition 1.1.8. Let A be a finite rank free Abelian group and R be an integral domain. An *elliptic net* is any map $W : A \to R$ with $W(0) = 0$ satisfying

$$\begin{aligned} W(p+q+s)W(p-q)W(r+s)W(r) \\ + W(q+r+s)W(q-r)W(p+s)W(p) \\ + W(r+p+s)W(r-p)W(q+s)W(q) = 0, \end{aligned} \tag{1.9}$$

for all $p, q, r, s \in A$. We identify the *rank* of W with the rank of A.

For our purposes, we will typically consider an elliptic net $W : A \to k$, where k will denote a residue field.

We also remark that if $W : \mathbb{Z} \to R$ is an elliptic net, then setting $p = m, q = n, r = 1$, and $s = 0$ in (1.9) gives equation (1.2). In this sense elliptic nets are generalizations of elliptic divisibility sequences, which can be represented as n-dimensional arrays.

1.2 Statement of results

Here we are interested in understanding the structure of the zero-set of an elliptic net, as well as providing a generalization of Ward's symmetry theorem, which is applicable to elliptic nets. We are also interested in exploring the relation between the $\mathbf{v}^{th}$ net polynomials $\Psi_{\mathbf{v}}$, associated to an elliptic curve E/K and a tuple $\mathbf{P} \in E(K)^r$, and the elliptic denominator net $(D_{\mathbf{v}\cdot\mathbf{P}})$. We exploit this relation to study certain Diophantine equations.

Before we can state our results, we must first introduce the following concept.

Definition 1.2.1. Let $W : A \to k$ be an elliptic net. Let $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$ be a basis for A. We say that W has a unique *zero-rank of apparition* (with respect to $\mathcal{B}$) if there exists an r-tuple $(\rho_1, \rho_2, \ldots, \rho_r)$ of positive integers, with $\rho_i > 1$ for $1 \leq i \leq r$, such that the following holds:

$$W(nb_i) = 0 \iff \rho_i \mid n,$$

for all $1 \leq i \leq r$.

In Chapter 2, we prove two theorems on the structure of an elliptic net $W : A \to R$. First, we prove the following key result on the zero set of an elliptic net.

Theorem 1.2.2. Let $W : A \to k$ be an elliptic net with $\mathcal{B} = \{b_1, \ldots, b_r\}$ a basis for A. Assume that $W(b_i) \neq 0$ for $1 \leq i \leq r$ and moreover that W has a unique zero-rank of apparition. Let

$$\Lambda := \{v \in A : \ W(v) = 0\}$$

be the zero set of W. Then Λ is a lattice. In other words, Λ is a rank r subgroup of A.

We then use Theorem 1.2.2 to give a generalization of Theorem 1.1.3 which is applicable to elliptic nets. In order to state our result, we first consider the function ϕ defined as

$$\begin{array}{rccc} \phi : & \Lambda \times A \setminus \Lambda & \longrightarrow & k \\ & (\lambda, p) & \longmapsto & \frac{W(\lambda+p)}{W(p)}. \end{array}$$

Theorem 1.2.3. Let $W : A \to k$ be an elliptic net with unique zero-rank of apparition $(\rho_1, \ldots, \rho_r)$ for which there exists i such that $\rho_i \geq 3$. In the case that $r = 1$ we assume that $\rho_1 \geq 4$. Then for all $\lambda \in \Lambda$ and $p \in A$, we have

$$W(\lambda + p) = a(\lambda)\chi(\lambda, p)W(p).$$

Here, the function $\chi(\lambda, p)$ is defined as

$$\begin{array}{rccc} \chi : & \Lambda \times A & \longrightarrow & k \\ & (\lambda, p) & \longmapsto & \frac{\phi(\lambda, p+v)}{\phi(\lambda, v)}, \end{array}$$

where v is any element of $A \setminus \Lambda$ with $v + p \notin \Lambda$, and $a(\lambda)$ is defined as

$$\begin{array}{rccc} a: & \Lambda & \longrightarrow & k \\ & \lambda & \longmapsto & \frac{\phi(\lambda,v)}{\chi(\lambda,v)}, \end{array}$$

for any $v \in A \setminus \Lambda$.

We remrak that the key component of Theorem 1.2.3 is that the functions $\chi(\lambda, p)$, and $a(\lambda)$, as defined above, are independent of our choice of v.

In Chapter 3, we again make use of Theorem 1.2.2 in proving the following generalizations of Theorem 1.1.5 and Proposition 1.1.6, regarding valuations of net polynomials.

Theorem 1.2.4. Let K be a number field with ring of integers $\mathcal{O}_K$ and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$. We also let E/K be an elliptic curve given by the Weierstrass equation (1.5) with $a_i \in \mathcal{O}_K$ for $i = 1, 2, 3, 4, 6$. Let $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$ be such that P_i, for $1 \leq i \leq r$, and $P_i \pm P_j$, for $1 \leq i < j \leq r$, are not the point at infinity. Moreover assume that $P_i \not\equiv \mathcal{O} \pmod{\mathfrak{p}}$, for $1 \leq i \leq r$, and $P_i \pm P_j \not\equiv \mathcal{O} \pmod{\mathfrak{p}}$, for $1 \leq i < j \leq r$. We also assume that $\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) > 0$ for all $\mathbf{v} \in \mathbb{Z}^r$. Then the following statements are equivalent:

(a) There exists i such that

$$\nu_{\mathfrak{p}}(\Psi_{2\mathbf{e_i}}(\mathbf{P})) > 0 \text{ and } \nu_{\mathfrak{p}}(\Psi_{3\mathbf{e_i}}(\mathbf{P})) > 0.$$

(b) There exists i such that for all $n \geq 2$ we have $\nu_{\mathfrak{p}}(\Psi_{n\mathbf{e_i}}(\mathbf{P})) > 0$.

(c) There exists $\mathbf{v} \in \mathbb{Z}^r$ and i such that

$$\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) > 0 \text{ and } \nu_{\mathfrak{p}}(\Psi_{\mathbf{v}+\mathbf{e_i}}(\mathbf{P})) > 0.$$

(d) There exists $\mathbf{v} \in \mathbb{Z}^r$ such that

$$\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) > 0 \text{ and } \nu_{\mathfrak{p}}(\Phi_{\mathbf{v}}(\mathbf{P})) > 0.$$

(e) There exists i such that $P_i \pmod{\mathfrak{p}}$ is singular.

By employing Theorem 1.2.2, we also give a generalization of Proposition 1.1.6, however we must first introduce some notation. Let $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$ and $\mathbf{P} \in E(K)^r$. We define the quadratic form

$$f_{\mathbf{v}}(\mathbf{P}) := \prod_{1 \leq i \leq j \leq r} A_{ij}^{v_i v_j},$$

where $A_{ii} := D_{P_i}$ and, for $i \neq j$, $A_{ij} := D_{P_i+P_j}/D_{P_i}D_{P_j}$.

Proposition 1.2.5. Suppose that E/K, $\mathbf{P} = (P_1, P_2, \ldots, P_r)$, and $\mathfrak{p}$ satisfy the assumptions of Theorem 1.2.4. Moreover, assume that $\mathcal{O}_K$ is a principal ideal domain, and $P_i \pmod{\mathfrak{p}}$ is non-singular for all i. Then we have

$$\nu_{\mathfrak{p}}(D_{\mathbf{v}\cdot\mathbf{P}}) = \nu_{\mathfrak{p}}(f_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P})).$$

Finally, in Chapter 4, we discuss how Theorem 1.2.3, Theorem 1.2.4, and Proposition 1.2.5, can be used in determining whether the Diophantine equation

$$Y^2 = X^3 + dZ^{12} \tag{1.10}$$

has any non-trivial solutions for certain values of d, under the additional condition $d \mid Z$. A Diophantine equation is a polynomial equation in several variables, in which we restrict the solutions to integers. Since we are interested in finding integer solutions to (1.10), we can make the change of variables

$$x = \frac{X}{Z^4},\ y = \frac{Y}{Z^6}$$

and consider the elliptic curve

$$E_d : y^2 = x^3 + d.$$

Under this change of variables, an integer solution to (1.10) corresponds to a square integral point $P \in E_d(\mathbb{Q})$. Moreover, letting

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

as in Proposition 1.1.4, we see that the condition that $d \mid Z$ corresponds to $d \mid D_P$. Letting $\mathbf{P} = (P_1, P_2, \cdots P_r) \in E_d(\mathbb{Q})^r$, be a generating set for the free part of $E(\mathbb{Q})$, the preceding discussion illustrates that we can prove that (1.10) has no non-trivial solutions by showing that the elliptic denominator net $(D_{\mathbf{v}\cdot\mathbf{P}})$ contains no terms which are both perfect squares and divisible by d. We present computational results following this observation.

Chapter 2

Elliptic Nets

2.1 Elliptic divisibility sequences

2.1.1 Elliptic sequences over fields

Throughout this section we let K denote an arbitrary field.

Definition 2.1.1. An *elliptic sequence* over K is any sequence (W_n), with $W_n \in K$, satisfying the homogeneous recurrence relation

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 \text{ for all } m > n > 0. \tag{2.1}$$

An elliptic sequence is called *non-degenerate* if $W_1W_2W_3 \neq 0$.

Example 2.1.2. i) The sequences (0) and (n) are elliptic sequences.

ii) Let $W_n = (\frac{n}{3})$ where $(\frac{a}{p})$ denotes the Legendre symbol of a modulo p. Then (W_n) is an elliptic sequence.

iii) Let $W_n = (\frac{-8}{n})$ where $(\frac{a}{\cdot})$ denotes the Kronecker symbol (See [4, §12.3] for the definition of the Kronecker symbol). Then (W_n) is an elliptic sequence.

iv) For constants $u, c_1, c_2 \in \mathbb{C}$, and a lattice $\Lambda \subset \mathbb{C}$, let $W_n = c_1 c_2^{n^2} \sigma(nu;\Lambda)/\sigma(u;\Lambda)^{n^2}$, where $\sigma(u;\Lambda)$ is the Weierstrass σ-function relative to Λ (see §3.1 Definition 3.1.4). Then W_n is an elliptic sequence over $\mathbb{C}$. Letting $\Lambda = \langle \omega_1, \omega_2 \rangle$, with $\omega_1 \approx 1.6285, \omega_2 \approx 0.81427 + 1.41036i, u \approx 1.030737$, and $c_1 = c_2 = -1$, gives the sequence

$$1, 8, -153, -98864, -47036791, 244502512920, \ldots \tag{2.2}$$

This sequence is associated (in a way described in Chapter 3) to the elliptic curve $y^2 = x^3 - 11$ and the point $(3, 4)$.

We start our study of elliptic sequences by exploring alternative recurrence relations which an arbitrary elliptic sequence satisfies. We also determine the minimal number of initial terms needed to uniquely define an elliptic sequence.

Proposition 2.1.3. Let (W_n) be an elliptic sequence over K with $W_1 W_2 \neq 0$. Then W_n satisfies the two equations

$$W_{2n+1} W_1^3 = W_{n+2} W_n^3 - W_{n-1} W_{n+1}^3 \ \forall n \geq 2, \tag{2.3}$$

$$W_{2n} W_2 W_1^2 = W_n W_{n+2} W_{n-1}^2 - W_n W_{n-2} W_{n+1}^2 \ \forall n \geq 3. \tag{2.4}$$

Moreover the sequence (W_n) is uniquely determined by W_1, W_2, W_3, and W_4.

Proof. Let (W_n) be an elliptic sequence. Thus W_n satisfies equation (2.1). Setting $m = n + 1$ yields equation (2.3), while setting $m = n' + 1$ and $n = n' - 1$ yields equation (2.4). The fact that W_n is uniquely determined by W_1, W_2, W_3, and W_4 follows by an induction using (2.3) and (2.4), and the assumption $W_1 W_2 \neq 0$. □

Proposition 2.1.4. Let (W_n) be an elliptic sequence with $W_1 \neq 0$. Then W_n satisfies the more general recurrence relation

$$W_{m+n} W_{m-n} W_r^2 = W_{m+r} W_{m-r} W_n^2 - W_{n+r} W_{n-r} W_m^2 \text{ for all } m > n > r > 0. \tag{2.5}$$

Proof. Let (W_n) be an elliptic sequence with $W_1 \neq 0$, and let $m > n > r > 0$. Then by equation (2.1) we have

$$W_{m+r} W_{m-r} = (W_{m+1} W_{m-1} W_r^2 - W_{r+1} W_{r-1} W_m^2)/W_1^2, \tag{2.6}$$

and

$$W_{n+r} W_{n-r} = (W_{n+1} W_{n-1} W_r^2 - W_{r+1} W_{r-1} W_n^2)/W_1^2. \tag{2.7}$$

Substituting (2.6) and (2.7) into the right hand side of (2.5) gives the result. □

Throughout this chapter we will make use of (2.1), (2.3), (2.4), and (2.5) to explore deeper relations between the terms of an elliptic sequence. However, using equations

(2.1), (2.3), (2.4), and (2.5) in practice, relies on computing terms of an elliptic sequence recursively. We give an explicit means of calculating arbitrary terms of an elliptic sequence, modulo a prime p, from a finite set of initial terms.

Before continuing down this path, we first digress to study which operations can be applied to an elliptic sequence, which result in another elliptic sequence. We use these operations to define a notion of equivalence of elliptic sequences. We then explore certain divisibility properties which will be needed to give an effective means of calculating terms in an elliptic sequence modulo a prime p.

2.1.2 Scale equivalence and normalization

In this section we are interested in defining an equivalence relation on elliptic sequences.

Proposition 2.1.5. Let (W_n) be an elliptic sequence over K and let $c \in K$, then the following hold:

i) The sequence (cW_n) is an elliptic sequence.

ii) The sequence $(c^{n^2}W_n)$ is an elliptic sequence.

Proof. Let (W_n) be an elliptic sequence, so W_n satisfies equation (2.1). Hence for all $m > n > 0$, we have

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2.$$

Multiplying both sides by c^4, where $c \in K$, gives

$$(cW_{m+n})(cW_{m-n})(cW_1)^2 = (cW_{m+1})(cW_{m-1})(cW_n)^2 - (cW_{n+1})(cW_{n-1})(cW_m)^2,$$

which proves the first statement.

For the second statement, define

$$W_n' = c^{n^2}W_n.$$

Then, we have:

$$\begin{aligned} W'_{m+1}W'_{m-1}W'^2_n - W'_{n+1}W'_{n-1}W'^2_m &= c^{(m+1)^2}W_{m+1}c^{(m-1)^2}W_{m-1}(c^{n^2}W_n)^2 \\ &\quad -c^{(n+1)^2}W_{n+1}c^{(n-1)^2}W_{n-1}(c^{m^2}W_m)^2 \\ &= c^{2m^2+2n^2+2}(W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2) \\ &= c^{(m+n)^2}c^{(m-n)^2}c^2W_{m+n}W_{m-n}W_1^2 \\ &= W'_{m+n}W'_{m-n}W'^2_1. \end{aligned}$$

Thus, (W'_n) is an elliptic sequence. □

Definition 2.1.6. Let (W_n) and (W'_n) be elliptic sequences over K. We say that (W_n) and (W'_n) are *scale equivalent* if there exist non-zero constants $c_1, c_2 \in K^*$ such that $(W'_n) = (c_1 c_2^{n^2} W_n)$.

Definition 2.1.7. Let (W_n) be an elliptic sequence. We say that (W_n) is *normalized* provided that $W_1 = 1$.

We remark that if (W_n) is an elliptic sequence with $W_1 \neq 0$ then we can normalize (W_n) by setting $c = W_1^{-1}$ and considering the elliptic sequence defined by $W'_n := c^{n^2}W_n$. As such, we may assume for simplicity that an elliptic sequence (W_n) is normalized.

2.1.3 Elliptic divisibility sequences over integral domains

Throughout this section we let R denote an arbitrary integral domain.

Definition 2.1.8. Let (a_n) be any sequence over an integral domain R. We call (a_n) a *divisibility sequence* provided that $a_n \mid a_m$ whenever $n \mid m$.

Definition 2.1.9. Let (W_n) be an elliptic sequence over R. If (W_n) is also a divisibility sequence, then we refer to (W_n) as an *elliptic divisibility sequence* (EDS) over R.

Lemma 2.1.10. Let (W_n) be an elliptic sequence over K, with not both $W_2 = 0$ and $W_3 = 0$. If there exists $n \in \mathbb{N}$ such that $W_n = W_{n+1} = 0$, then $W_n = 0$ for all $n \geq 4$.

Proof. [10, Lemma 4.1] □

Proposition 2.1.11. Let (W_n) be a non-degenerate elliptic sequence over R, with the additional condition that $W_1 = 1$. If $W_2 \mid W_4$ then (W_n) is an elliptic divisibility sequence.

Proof. [10, Theorem 4.1] □

We remark that all the sequences given in example 2.1.2 are in fact elliptic divisibility sequences. Note that the sequence (0) is clearly a divisibility sequence, while the rest of the examples satisfy the assumptions of Proposition 2.1.11.

Next, we show that if (W_n) is an elliptic divisibility sequence, then for every prime $p \in R$ there exists n such that $p \mid W_n$. We then discuss the structure of the terms of an elliptic divisibility sequence divisible by p.

Definition 2.1.12. Let (W_n) be an elliptic divisibility sequence over an integral domain R. An element $m \in R$ is said to be a *divisor* of (W_n) if $m \mid W_n$ for some $n > 1$. If $m \mid W_\rho$, and $m \nmid W_r$ for some $r \mid \rho$, then we call ρ a *rank of apparition of* m.

For the elliptic sequence (W_n) given in (2.2) we note that the rank of apparition of 5 is 6. To see this, note that reducing (W_n) mod 5 gives the sequence

$$1, 3, 2, 1, 4, 0, 4, \ldots$$

Proposition 2.1.13. Let (W_n) be an elliptic divisibility sequence over an integral domain R. For every prime $p \in R$, there exists $n \in \mathbb{N}$ such that $p \mid W_n$.

Proof. [10, Theorem 5.1] □

Lemma 2.1.14. Let p be a prime divisor of an elliptic sequence (W_n), and let ρ be the smallest rank of apparition of p. If $p \mid W_{\rho+1}$, then $\rho \leq 3$, and $p \mid W_n$ for all $n \geq \rho$.

Proof. [10, Theorem 6.1] □

Finally, we give necessary and sufficient conditions that a prime has a unique rank of apparition in an elliptic sequence (W_n).

Lemma 2.1.15. Let W_n be an elliptic sequence over an integral domain R. A necessary and sufficient condition that a prime $p \in R$ has a unique rank of apparition is that $p \nmid \gcd(W_3, W_4)$.

Proof. [10, Theorem 6.2] □

Theorem 2.1.16. Let W_n be an elliptic sequence over an integral domain R. A necessary and sufficient condition that every prime $p \in R$ has a unique rank of apparition is that $\gcd(W_3, W_4) = 1$.

Proof. [10, Theorem 6.3] □

2.1.4 Symmetries of an EDS

Throughout this section we assume that (W_n) is a normalized elliptic divisibility sequence over integral domain R.

Theorem 2.1.17. Let p be any prime, with rank of apparition $\rho > 3$. Then there exist integers a and b such that

$$W_{\rho-i} \equiv -ab^{-i}W_i \pmod{p} \text{ for } 0 \leq i \leq \rho. \tag{2.8}$$

For a proof of Theorem 2.1.17 which relies heavily on the theory of elliptic functions see [10, Chapter V].

Throughout this section, we will first show how the terms a and b, from Theorem 2.1.17, can be calculated, as well as exploring the relations between a and b. We also give a version of Theorem 2.1.17, which can be used to calculate arbitrary terms of an elliptic divisibility sequence modulo a prime p.

Lemma 2.1.18. For a, b, and ρ, as in Theorem 2.1.17, we have the following congruences modulo p.

(i) $b \equiv W_2W_{\rho-1}/W_{\rho-2},\ a \equiv -W_2W_{\rho-1}^2/W_{\rho-2},\ a \equiv -bW_{\rho-1}$.

(ii) $a^2 \equiv b^\rho$.

(iii) $b^2 \equiv -W_{\rho+1}/W_{\rho-1},\ a^2 \equiv -W_{\rho+1}W_{\rho-1}$.

Proof. Setting $i = 1$ in (2.8) yields

$$W_{\rho-1} \equiv -ab^{-1}W_1 \pmod{p}.$$

Under the assumption that $W_1 = 1$, we see $a \equiv -bW_{\rho-1} \pmod{p}$. Then, setting $i = \rho - 1$ in (2.8) gives

$$1 = W_1 \equiv -ab^{-\rho+1}W_{\rho-1} \pmod{p}.$$

From the preceding identity and the fact that $a \equiv -bW_{\rho-1} \pmod{p}$, it follows that

$$a^2 \equiv b^{\rho} \pmod{p}.$$

This proves that the congruence in (ii) holds.

Setting $i = 2$ in (2.8) yields

$$W_{\rho-2} \equiv -ab^{-2}W_2 \equiv b^{-1}W_{\rho-1}W_2 \pmod{p},$$

since $a \equiv -bW_{\rho-1} \pmod{p}$. It now follows that

$$b \equiv W_{\rho-1}W_2/W_{\rho-2} \pmod{p} \text{ and } a \equiv -W_2W_{\rho-1}^2/W_{\rho-2} \pmod{p}.$$

Hence, the identities in (i) hold.

To establish the congruences in (iii) we set $m = \rho - 1$ and $n = 2$ in (2.1) to get

$$W_{\rho+1}W_{\rho-3} = W_{\rho}W_{\rho-2}W_2^2 - W_3W_1W_{\rho-1}^2.$$

From which it follows that

$$-W_{\rho+1}ab^{-3}W_3 \equiv -W_3W_{\rho-1}^2 \pmod{p}.$$

Hence,

$$W_{\rho+1} \equiv a^{-1}b^3W_{\rho-1}^2 \pmod{p}.$$

Using the identity $a^{-1}b \equiv -W_{\rho-1}^{-1} \pmod{p}$, from (i), in the preceding equation yields

$$b^2 \equiv -W_{\rho+1}/W_{\rho-1} \pmod{p}.$$

It then follows that

$$a^2 \equiv b^2W_{\rho-1}^2 \equiv -W_{\rho+1}W_{\rho-1} \pmod{p},$$

which completes the proof of (iii). □

Note that Theorem 2.1.17 shows how the terms W_i and $W_{\rho-i}$, for $0 \leq i \leq \rho$, are related. We use this relation along with the congruences from Lemma 2.1.18, in order to establish a relation between the terms W_i and $W_{\rho+i}$ for all $i \geq 0$.

Theorem 2.1.19. With the notation of Theorem 2.1.17 and Lemma 2.1.18, we have

$$W_{\rho+i} \equiv ab^i W_i \pmod{p} \tag{2.9}$$

for all positive integers i.

We remark that the main objective for this chapter is to introduce a higher dimensional generalization of elliptic sequences, called elliptic nets, and to provide an analogue of Theorem 2.1.19, applicable for elliptic nets. We first give a proof of Theorem 2.1.19 and present alternative versions of the theorem, which are useful in determining the periodicity of an elliptic sequence.

Proof of Theorem 2.1.19. First note that if $i = 0$ or ρ, then $W_{\rho+i} \equiv W_i \equiv 0$ modulo p, so (2.9) clearly holds. Next assume that $0 < i < \rho$. Since

$$W_{\rho+i}W_{\rho-i} = W_{\rho+1}W_{\rho+1}W_i^2 - W_{i+1}W_{i-1}W_\rho^2,$$

and $W_\rho \equiv 0 \pmod{p}$, we have

$$W_{\rho+i}W_{\rho-1} \equiv W_{\rho+1}W_{\rho-1}W_i^2 \pmod{p}.$$

It then follows from Theorem 2.1.17 and Lemma 2.1.18 that

$$-W_{\rho+i}ab^{-i}W_i \equiv -a^2W_i^2 \pmod{p}.$$

Hence,

$$W_{\rho+i} \equiv ab^i W_i \pmod{p}.$$

Thus (2.9) holds for $0 \leq i \leq \rho$.

Next assume that (2.9) holds for $0 \leq i \leq n\rho$, and let $n\rho < i < (n+1)\rho$. Note that (2.9) clearly holds when i is any multiple of ρ. Then, as before, we have

$$W_{i+\rho}W_{i-\rho} = W_{i+1}W_{i-1}W_\rho^2 - W_{\rho+1}W_{\rho-1}W_i^2,$$

from which we get

$$W_{i+\rho}W_{i-\rho} \equiv -W_{\rho+1}W_{\rho-1}W_i^2 \pmod{p}. \tag{2.10}$$

Note that Lemma 2.1.18 yields

$$-W_{i+\rho}W_{i-\rho} \equiv a^2 \pmod{p}. \tag{2.11}$$

We also have

$$W_{i-\rho} \equiv a^{-1}b^{\rho-i}W_i \pmod{p}, \tag{2.12}$$

from the induction hypothesis.

Substituting (2.11) and (2.12) into (2.10) we see that

$$W_{i+\rho}a^{-1}b^{\rho-i}W_i \equiv a^2W_i^2 \pmod{p}.$$

It now follows that

$$W_{i+\rho} \equiv a^3b^{i-\rho}W_i \pmod{p}.$$

Finally, since $a^2b^{-\rho} \equiv 1$ modulo p by Lemma 2.1.18 (ii), we have

$$W_{\rho+i} \equiv ab^iW_i \pmod{p}.$$

□

Corollary 2.1.20. With the notation of Theorem 2.1.17, we have

$$W_{n\rho+i} \equiv a^nb^{ni+\rho\frac{n(n-1)}{2}}W_i \pmod{p} \tag{2.13}$$

for all positive integers n and i.

Proof. The case $n = 1$ holds as a direct result of Theorem 2.1.19. Assume (2.13) holds

for all $n \leq k$, and consider the case $n = k + 1$. From Theorem 2.1.19 it follows that

$$W_{(k+1)\rho+i} \equiv ab^{k\rho+i} W_{k\rho+i} \pmod{p}.$$

By employing the induction hypothesis, we have that

$$\begin{aligned} W_{(k+1)\rho+i} &\equiv ab^{k\rho+i} a^k b^{ki+\rho\frac{k(k-1)}{2}} W_i \pmod{p} \\ &\equiv a^{k+1} b^{(k+1)i+\rho\frac{(k+1)k}{2}} W_i \pmod{p}. \end{aligned}$$

□

Corollary 2.1.21. With the notation of Theorem 2.1.17, we have

$$W_{n\rho+i} \equiv a^{n^2} b^{ni} W_i \pmod{p}.$$

Proof. This follows immediately from Corollary 2.1.20 and identity (ii) of Lemma 2.1.18 . □

We remark that Corollary 2.1.21 gives a more effective means of calculating terms of an elliptic sequence modulo p, since we need only know the first $\rho + 1$ terms of the sequence. Furthermore, the preceding discussion shows that an elliptic sequence becomes periodic when reduced modulo p, where the length of the period is a multiple of the rank of apparition of p. For example the elliptic sequence considered in (2.2), reduced mod 5 is

$$1, 3, 2, 1, 4, 0, 4, 4, 2, 2, 1, 0, 4, 3, 3, 1, 1, 0, 1, 4, 3, 2, 4, 0, 1, 3, 2, 1, 4, 0, \ldots$$

which can be seen to have period 24.

2.2 Elliptic Nets

We are now in a position to give a generalization of elliptic sequences. Our treatment of elliptic nets will closely follow the structure of our discussion of elliptic sequences. We note that many of the results included in this section are due to Stange [9], and are included here, with proofs, for completeness.

2.2.1 Elliptic nets over integral domains

Definition 2.2.1. Let A be a finite rank free Abelian group, and R be an integral domain. An *elliptic net* is any map $W : A \to R$ with $W(0) = 0$ satisfying the homogeneous equation

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\quad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\quad + W(r+p+s)W(r-p)W(q+s)W(q) = 0, \end{aligned} \tag{2.14}$$

for all $p, q, r, s \in A$.

Throughout, we will let K denote an arbitrary field, R a principal ideal domain with $\mathrm{frac}(R) = K$, $\mathfrak{p}$ a prime ideal in R, and k the residue field $R/\mathfrak{p}$. In this thesis, we are primarly concerned with elliptic nets mapping into a residue field k.

Example 2.2.2. We give an example of an elliptic net $W : \mathbb{Z}^2 \to \mathbb{Z}$ as the following array, where $W(\mathbf{v})$ is given by the term in the array indexed by $\mathbf{v}$. For example we have $W(0,0) = 0$ is the term in the lower left corner, and $W(2,1) = 51$.

$$\begin{array}{ccccccc} & & \vdots & & & & \\ & -9886 & -15775 & -30396 & -397241 & 547912280 & \\ & -153 & -134 & -1099 & -112698 & -144855449 & \\ \cdots & 8 & 3 & -20 & -17083 & -93695568 & \cdots \\ & 1 & 2 & 51 & 14446 & -1106143 & \\ & 0 & 1 & 116 & 149895 & 2470140424 & \\ & & & \vdots & & & \end{array}$$

This is the elliptic net associated to the elliptic curve $y^2 = x^3 - 11$ and the points $(3, 4)$, and $(15, 58)$. The manner in which an elliptic curve, together with a set of points is associated to an elliptic net will be described in Chapter 3. We also note that the elliptic sequence given in (2.2), associated to the elliptic curve $y^2 = x^3 - 11$ and point $(3, 4)$, is given by $W(0, n)$ for $n \geq 1$.

Definition 2.2.3. Let $W : A \to k$ be an elliptic net, and let B be a subgroup of A. We define the *restriction* of W to B, denoted $W|_B$, by

$$\begin{array}{rccc} W|_B: & B & \longrightarrow & k \\ & v & \longmapsto & W(v). \end{array}$$

Definition 2.2.4. For an elliptic net $W : A \to k$, we define the *rank* of W to be the rank of A.

Definition 2.2.5. Let $W : A \to k$ be a elliptic net, and let $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$ be a basis for A. We say that $\mathcal{B}$ is *appropriate* provided that $W(b_i), W(2b_i) \neq 0$, and $W(b_i \pm b_j) \neq 0$ for $i \neq j$. If $r = 1$, we also require that $W(3b_1) \neq 0$.

Definition 2.2.6. Let $W : A \to k$ be an elliptic net. We say W is *non-degenerate* if there exists an appropriate basis $\mathcal{B}$, for A.

Lemma 2.2.7. If $W : A \to k$ is an elliptic net, then we have

$$W(-v) = -W(v) \ \forall \ v \in A.$$

Proof. If $W(v) = W(-v) = 0$, then we are done. Otherwise we may assume, without loss of generality, that $W(v) \neq 0$. Then, setting $q = p = v$ and $r = s = 0$ in (2.14) yields

$$W(v)^4 + W(v)^3 W(-v) = 0.$$

Since $W(v) \neq 0$, we have $W(-v) = -W(v)$. □

Proposition 2.2.8. Rank 1 elliptic nets are elliptic sequences.

Proof. Let $W : \mathbb{Z} \to R$ be an elliptic net. Taking $p = m, q = n, r = 1, s = 0$ in (2.14) gives the relation

$$W(m+n)W(m-n)W(1)^2 = W(m+1)W(m-1)W(n)^2 - W(n+1)W(n-1)W(m)^2.$$

If $m > n > 0$, this is exactly the relation (2.1) given in the definition of an elliptic sequence. □

2.2.2 Scale equivalence and normalization

For two Abelian groups A and B, a quadratic form is any function $f : A \to B$ that satisfies

$$f(x+y+z) - f(x+y) - f(x+z) - f(y+z) + f(x) + f(y) + f(z) = 0,$$

for all $x, y, z \in A$. For our purposes, A is taken to be a group under addition, while B will be taken to be a group under multiplication, so a quadratic form $f : A \to B$ satisfies

$$f(x+y+z)f(x)f(y)f(z)f(x+y)^{-1}f(x+z)^{-1}f(y+z)^{-1} = 1,$$

for all $x, y, z \in A$. For example, letting $c \in \mathbb{Q}^*$, the map

$$\begin{array}{rccc} f: & \mathbb{Z}^2 & \longrightarrow & \mathbb{Q}^* \\ & (x_1, x_2) & \longmapsto & c^{x_1^2+x_1x_2+x_2^2} \end{array}$$

is a quadratic form.

Proposition 2.2.9. Let $W : A \to K$ be an elliptic net and let $f : A \to K^*$ be a quadratic form. The map $W^f : A \to K$ defined by

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

is an elliptic net.

Proof. See [9, Proposition 8.1.1] □

Definition 2.2.10. Let $W : A \to K$ and $W' : A \to K$ be elliptic nets. If there exists a quadratic form $f : A \to K^*$ and non-zero constant $c \in K^*$ such that

$$W'(v) = cf(v)W(v),$$

then W and W' are said to be *scale equivalent*.

The concept of equivalent elliptic nets is analogous to the concept of equivalent elliptic sequences. Next, we generalize the notion of normalized elliptic sequences to normalized elliptic nets and show that every non-degenerate elliptic net is equivalent to a normalized elliptic net.

Definition 2.2.11. Let $W : A \to R$ be a non-degenerate elliptic net with an appropriate basis $\mathcal{B} = \{b_1, \ldots, b_r\}$ for A. We say W is *normalized* with respect to $\mathcal{B}$, provided that $W(b_i) = 1$ and $W(b_i + b_j) = 1$.

Proposition 2.2.12. Let $W : A \to K$ be a non-degenerate elliptic net with an appropriate basis $\mathcal{B} = \{b_1, \ldots, b_r\}$ for A. Then there exists a quadratic form $f : A \to K^*$ such that W^f is normalized with respect to $\mathcal{B}$.

Proof. Since W is assumed to be non-degenerate and $\mathcal{B} = \{b_1, \ldots, b_r\}$ is an appropriate basis for A, we have that $W(b_i), W(b_i + b_j) \in K^*$ for $i \neq j$. We define

$$A_{ij} := \frac{W(b_i)W(b_j)}{W(b_i + b_j)},$$

for $1 \leq i < j \leq r$, and $A_{ii} := W(b_i)^{-1}$. Then, by letting $v = \sum_{i=1}^{r} n_i b_i \in A$ and defining the quadratic form

$$f(v) := \prod_{1 \leq i \leq j \leq r} A_{ij}^{n_i n_j},$$

we have that W^f is normalized. □

We remark that if $W : A \to K$ is a non-degenerate elliptic net of rank 1, with an appropriate basis $\{b_1\}$ for A, then the normalization process described in the proof of Proposition 2.2.12 gives

$$W^f(nb_1) = c^{n^2} W(nb_1),$$

where $c = W(b_1)^{-1}$. Note that this is exactly the normalization process for elliptic sequences described in §2.1.2.

2.2.3 Zeros of an elliptic net

We remind the reader that the ultimate goal for this chapter is to provide a generalization of Theorem 2.1.19 for elliptic nets. Recall that Theorem 2.1.19 provides a relation between the terms $W_{\rho+i}$ and W_i, modulo p, of an elliptic sequence, where $W_\rho \equiv 0 \pmod{p}$. This suggests studying the set

$$\{v \in A : W(v) = 0\}$$

for an elliptic net $W : A \to k$. We first introduce the necessary terminology, then state our main theorem regarding the structure of the set $\{v \in A : W(v) = 0\}$.

Definition 2.2.13. Let $W : A \to k$ be an elliptic net with an appropriate basis $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$ for A. We say that W has a unique *zero-rank of apparition* (with respect to $\mathcal{B}$) if there exists an r-tuple $(\rho_1, \rho_2, \ldots, \rho_r)$ of positive integers, with $\rho_i > 1$ for $1 \leq i \leq r$, such that the following holds:

$$W(nb_i) = 0 \iff \rho_i \mid n$$

for all $1 \leq i \leq r$.

Theorem 2.2.14. Let $W : A \to k$ be an elliptic net with $\mathcal{B} = \{b_1, \ldots, b_r\}$ a basis for A. Assume that $W(b_i) \neq 0$ for $1 \leq i \leq r$ and moreover that W has a unique zero-rank of apparition. Let

$$\Lambda := \{v \in A : \ W(v) = 0\}$$

be the zero set of W. Then Λ is a lattice.

In order to prove Theorem 2.2.14 we assume throughout that $W : A \to k$ is an elliptic net with $\mathcal{B} = \{b_1, \ldots, b_r\}$ a basis for A. We also suppose that $W(b_i) \neq 0$ for $1 \leq i \leq r$ and moreover that W has a unique zero-rank of apparition. It is also assumed that, unless otherwise stated, $p,\ q,\ r,$ and s are arbitrary elements of A.

We also consider the following two sets:

$$A_i := \langle b_1, b_2, \cdots, b_i \rangle \text{ and } \Lambda_i := \{v \in A_i : \ W(v) = 0\}.$$

We prove three lemmas regarding the structure of the zero set Λ.

Lemma 2.2.15. Suppose that $\rho_i \mid n$. Then we have

$$W(p + nb_i) = 0 \Longleftrightarrow p \in \Lambda.$$

Proof. First let $p \in \Lambda$. Taking $q = -nb_i,\ r = b_i,$ and $s = 2nb_i$ in (2.14) yields

$$W(p + nb_i)^2 W((2n+1)b_i) W(b_i) = 0.$$

Note that since $\rho_i \mid n$ and $\rho_i \neq 1$, we have $\rho_i \nmid 2n+1$ and so $W((2n+1)b_i) \neq 0$. Thus $W(p + nb_i) = 0$ for all $p \in \Lambda$.

Conversely, assume that $p \notin \Lambda$. Taking $q = nb_i,\ r = b_i,$ and $s = 0$ in (2.14) yields

$$W(p+nb_i)W(p-nb_i)W(b_i)^2 + W((n+1)b_i)W(n-1)b_i)W(p)^2 = 0.$$

Since $p \notin \Lambda$ and $\rho_i \mid n$, we have $W((n+1)b_i)W(n-1)b_i)W(p)^2 \neq 0$. Hence, we have that $W(p+nb_i) \neq 0$ for all $p \notin \Lambda$. □

The following is a straightforward consequence of Lemma 2.2.15.

Corollary 2.2.16. We have

$$\{n_1b_1 + n_2b_2 + \cdots + n_rb_r :\ \rho_i \mid n_i \ for\ 1 \leq i \leq r\} \subseteq \Lambda.$$

Lemma 2.2.17. Suppose that Λ_{i-1} is a lattice in A_{i-1} for a fixed $i > 1$. Then for all $p \in \Lambda_{i-1}$, we have

$$W(p+nb_i) = 0 \iff \rho_i \mid n.$$

Proof. First, if $p \in \Lambda_{i-1}$ then $p \in \Lambda$, and so it follows from Lemma 2.2.15 that if $\rho_i \mid n$ then $W(p+nb_i) = 0$.

Conversely, assume that $\rho_i \nmid n$. Taking $q = nb_i,\ r \in A_{i-1} \setminus \Lambda_{i-1}$, and $s = 0$ in (2.14) yields

$$W(p+nb_i)W(p-nb_i)W(r)^2 + W(r+p)W(r-p)W(nb_i)^2 = 0. \tag{2.15}$$

Since $p \in \Lambda_{i-1},\ r \in A_{i-1} \setminus \Lambda_{i-1}$, and Λ_{i-1} is a lattice in A_{i-1}, it follows that $p \pm r \in A_{i-1} \setminus \Lambda_{i-1}$, hence $W(p \pm r) \neq 0$. It therefore follows from (2.15) that $W(p+nb_i) \neq 0$. □

Lemma 2.2.18. Suppose that Λ_{i-1} is a lattice in A_{i-1} for a fixed $i > 1$ with $\rho_i > 2$. If $p, q \in \Lambda_i$ with $p = p_0 + nb_i$, and $q = q_0 + nb_i$ for $p_0, q_0 \in A_{i-1}$, then $p - q = p_0 - q_0 \in \Lambda_{i-1}$.

Proof. Setting $p = p_0 + nb_i,\ q = q_0 + nb_i,\ r = mb_i$, and $s = -2nb_i$ in (2.14) gives

$$W(p_0+q_0)W(p_0-q_0)W((2n-m)b_i)W(mb_i) = 0. \tag{2.16}$$

Since $\rho_i > 2$, we have $W(b_i),\ W(2b_i) \neq 0$. So we can choose $m \in \{1, 2\}$ such that

$$W((2n-m)b_i)W(mb_i) \neq 0.$$

Thus from (2.16) we conclude that $W(p_0+q_0)W(p_0-q_0)=0$. Now if $W(p_0-q_0)=0$ we are done. Otherwise we assume that $W(p_0-q_0)\neq 0$, hence $W(p_0+q_0)=0$. We show that this gives a contradiction.

Setting $p=p_0+nb_i,\ q=q_0+nb_i,\ r=b_i$, and $s=0$ in (2.14) gives

$$W(p_0+q_0+2nb_i)W(p_0-q_0)W(b_i)^2=0,$$

hence $W(p_0+q_0+2nb_i)=0$ (recall that $W(p_0-q_0)\neq 0$). Since $p_0+q_0\in\Lambda_{i-1}$, it follows from Lemma 2.2.17 that $\rho_i \mid 2n$. Now we consider two cases.

Case 1: If $\rho_i \mid n$, then from Lemma 2.2.15 it follows that $p_0, q_0 \in \Lambda_{i-1}$, hence $p_0-q_0\in\Lambda_{i-1}$, contradicting our assumption that $W(p_0-q_0)\neq 0$.

Case 2: If $\rho_i \nmid n$, then $W(p_0+q_0+nb_i)\neq 0$ by Lemma 2.2.17. Setting $p=p_0+nb_i,\ q=q_0+nb_i,\ r=b_i$, and $s=-nb_i$ in (2.14) gives

$$W(p_0+q_0+nb_i)W(p_0-q_0)W((n-1)b_i)W(b_i)=0,$$

hence $W((n-1)b_i)=0$ and so $\rho_i \mid n-1$. Similarly by setting $p=p_0+nb_i,\ q=q_0+nb_i,\ r=-b_i$, and $s=-nb_i$ in (2.14) we find that $W((n+1)b_i)=0$ and so $\rho_i \mid n+1$. Since $\rho_i \mid n-1$ and $\rho_i \mid n+1$, we have $\rho_i=2$. This is a contradiction, as we assumed that $\rho_i>2$. □

We are ready to prove our main result on zeros of an elliptic net.

Proof. (*of Theorem 2.2.14*) We proceed by induction on Λ_i. Note that Λ_1 is a lattice in A_1, since $W(nb_1)=0$ if and only if $\rho_1|n$.

Assume that Λ_{i-1} is a lattice in A_{i-1} and consider $p=p_0+nb_i,\ q=q_0+mb_i\in\Lambda_i$, where $p_0, q_o\in A_{i-1}$ such that $p-q\notin\Lambda_i$.

It follows from (2.14), for p, q, $r=p+r_1$, and $s=-2p$, that

$$W(p-q)W(p-r_1)W(p+r_1)=0.$$

Since $W(p-q)\neq 0$ and $p=p_0+nb_i$, we conclude that

$$W(p_0+nb_i+r_1)W(p_0+nb_i-r_1)=0. \tag{2.17}$$

We claim that (2.17) implies that $\rho_i \mid n$. To show this assume otherwise that $\rho_i \nmid n$, hence by Lemma 2.2.17 we have $p_0 \notin \Lambda_{i-1}$. We consider two cases.

Case 1: If $\rho_i > 2$, then setting $r_1 = p_0$ in (2.17) yields

$$W(2p_0 + nb_i)W(nb_i) = 0.$$

Thus, we have that $W(2p_0 + nb_i) = 0$ and $W(p_0 + nb_i) = 0$. Then it follows from Lemma 2.2.18 that $p_0 \in \Lambda_{i-1}$, a contradiction.

Case 2: If $\rho_i = 2$, then setting $r_1 = b_i$ in (2.17) yields

$$W(p_0 + (n+1)b_i)W(p_0 + (n-1)b_i) = 0,$$

from which it follows that $p_0 \in \Lambda_{i-1}$ (since both $n-1$ and $n+1$ are even). This is a contradiction.

In either case, the assumption $\rho_i \nmid n$ leads to a contradiction. Thus, we have $p = p_0 + nb_i$, with $p_0 \in \Lambda_{i-1}$ and $\rho_i \mid n$. Similarly we have $q = q_0 + mb_i$, with $q_0 \in \Lambda_{i-1}$ and $\rho_i | m$. Hence, $p - q = p_0 - q_0 + (n-m)b_i$, with $p_0 - q_0 \in \Lambda_i$ and $\rho_i \mid (n-m)$. Thus it follows from Lemma 2.2.17 that $W(p-q) = 0$. This is a contradiction as we assumed that $W(p-q) \neq 0$.

Since the assumption $p - q \notin \Lambda_i$ leads to a contradiction, we conclude that both $p - q,\ p + q \in \Lambda_i$, thus Λ_i is a lattice in A_i. □

2.2.4 Symmetries of an elliptic net

Throughout this section we assume $W : A \to k$ is an elliptic net with a unique zero-rank of apparition $(\rho_1, \rho_2, \ldots, \rho_r)$ with respect to the basis $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$ for A. We also assume that there exists i such that $\rho_i \geq 3$. In the case that W has rank 1, we will assume that $\rho_1 \geq 4$. We also let Λ denote the zero-set for W.

Our aim for this section is to give generalizations of Theorem 2.1.17 and Theorem 2.1.19 for elliptic nets. In order to do so, we first define the auxiliary function

$$\begin{array}{rccc} \phi: & \Lambda \times A \setminus \Lambda & \longrightarrow & k \\ & (\lambda, v) & \longmapsto & \frac{W(\lambda+v)}{W(v)}, \end{array}$$

and explore the properties of ϕ.

Lemma 2.2.19. For all $\lambda \in \Lambda$, and $a, b, c, d \in A \backslash \Lambda$ such that $a + b = c + d$, we have

$$\phi(\lambda, a)\phi(\lambda, b) = \phi(\lambda, c)\phi(\lambda, d).$$

Proof. Assume that $p + s, p, q + s, q \notin \Lambda$. Then, setting $r = \lambda$ in (2.14) gives

$$W(\lambda + q + s)W(\lambda - q)W(p + s)W(-p) \\ = W(\lambda + p + s)W(\lambda - p)W(q + s)W(-q).$$

Since $p + s, p, q + s, q \notin \Lambda$ we have $W(p + s)W(p)W(q + s)W(q) \neq 0$, hence

$$\frac{W(\lambda + q + s)W(\lambda - q)}{W(q + s)W(-q)} = \frac{W(\lambda + p + s)W(\lambda - p)}{W(p + s)W(-p)}.$$

Thus

$$\phi(\lambda, q + s)\phi(\lambda, -q) = \phi(\lambda, p + s)\phi(\lambda, -p).$$

Taking

$$q + s = a, \ -q = b, \ p + s = c, \text{ and } -p = d,$$

gives the result. □

The next two propositions show that

$$\frac{\phi(\lambda, v + p)}{\phi(\lambda, p)}$$

is well defined for all $\lambda \in \Lambda$, $v \in A$, and $p \in A \setminus \Lambda$, and moreover it is independent of p.

Proposition 2.2.20. For all $v, p_1, p_2 \in A$, with $p_1, v + p_1, p_2, v + p_2 \notin \Lambda$ we have

$$\frac{\phi(\lambda, v + p_1)}{\phi(\lambda, p_1)} = \frac{\phi(\lambda, v + p_2)}{\phi(\lambda, p_2)}.$$

Proof. From Lemma 2.2.19 we have

$$\phi(\lambda, v + p_1)\phi(\lambda, p_2) = \phi(\lambda, v + p_2)\phi(\lambda, p_1).$$

Since $\phi(\lambda, p_1) \neq 0$ and $\phi(\lambda, p_2) \neq 0$, the result follows.

□

Proposition 2.2.21. For all $v \in A$, there exists $p \in A \backslash \Lambda$ such that $v + p \notin \Lambda$.

Proof. First, we note that since $(\rho_1, \rho_2, \ldots, \rho_r)$ is assumed to be the zero-rank of apparition for W for which there exists i such that $\rho_i \geq 3$, we have $b_i, 2b_i \notin \Lambda$. We claim that not both $v + b_i, v + 2b_i \in \Lambda$.

If $v + b_i \in \Lambda$ and $v + 2b_i \in \Lambda$, then from Theorem 2.2.14 we have

$$b_i = (v + 2b_i) - (v + b_i) \in \Lambda,$$

a contradiction. □

In light of propositions 2.2.20 and 2.2.21 we may define

$$\begin{array}{rccc} \chi: & \Lambda \times A & \longrightarrow & k \\ & (\lambda, v) & \longmapsto & \frac{\phi(\lambda, v+p)}{\phi(\lambda, p)}, \end{array}$$

for any $p \in A \backslash \Lambda$ with $v + p \notin \Lambda$. The following Lemma summarizes some of the useful properties of χ.

Lemma 2.2.22. For all $\lambda, \lambda_1, \lambda_2 \in \Lambda$, and $v, v_1, v_2 \in A$, we have the following:

i) $\chi(\lambda, v_1 + v_2) = \chi(\lambda, v_1)\chi(\lambda, v_2)$.

ii) $\chi(\lambda_1 + \lambda_2, v) = \chi(\lambda_1, v)\chi(\lambda_2, v)$.

iii) $\chi(\lambda_1, \lambda_2) = \chi(\lambda_2, \lambda_1)$.

iv) $\chi(\lambda, -v) = \chi^{-1}(\lambda, v)$.

Proof. First, we let $p \in A \backslash \Lambda$ be such that $v_1 + v_2 + p, v_2 + p \notin \Lambda$. Then we have

$$\begin{aligned} \chi(\lambda, v_1)\chi(\lambda, v_2) &= \frac{\phi(\lambda, v_1 + v_2 + p)}{\phi(\lambda, v_2 + p)} \frac{\phi(\lambda, v_2 + p)}{\phi(\lambda, p)} \\ &= \frac{\phi(\lambda, v_1 + v_2 + p)}{\phi(\lambda, p)} \\ &= \chi(\lambda, v_1 + v_2). \end{aligned}$$

For the second statement, we let $p \in A\backslash\Lambda$ be such that $v + p \notin \Lambda$. Then we have

$$\begin{aligned}
\chi(\lambda_1, v)\chi(\lambda_2, v) &= \frac{\phi(\lambda_1, v + p + \lambda_2)\phi(\lambda_2, v + p)}{\phi(\lambda_1, p + \lambda_2)\phi(\lambda_2, p)} \\
&= \frac{W(v + p + \lambda_1 + \lambda_2)W(p + \lambda_2)W(v + p + \lambda_2)W(p)}{W(v + p + \lambda_2)W(p + \lambda_1 + \lambda_2)W(v + p)W(p + \lambda_2)} \\
&= \frac{W(v + p + \lambda_1 + \lambda_2)W(p)}{W(v + p)W(p + \lambda_1 + \lambda_2)} \\
&= \frac{\phi(\lambda_1 + \lambda_2, v + p)}{\phi(\lambda_1 + \lambda_2, p)} \\
&= \chi(\lambda_1 + \lambda_2, v).
\end{aligned}$$

Next, we have

$$\chi(\lambda_1, \lambda_2) = \frac{\phi(\lambda_1, \lambda_2 + p)}{\phi(\lambda_1, p)} = \frac{W(\lambda_1 + \lambda_2 + p)W(p)}{W(\lambda_2 + p)W(\lambda_1 + p)} = \frac{\phi(\lambda_2, \lambda_1 + p)}{\phi(\lambda_2, p)} = \chi(\lambda_2, \lambda_1).$$

The last statement follows from (i) and the fact that $\chi(\lambda, 0) = 1$. □

For each $\lambda \in \Lambda$ and $v \in A\backslash\Lambda$, we define the function

$$a(\lambda, v) := \frac{\phi(\lambda, v)}{\chi(\lambda, v)}.$$

The next Lemma shows that $a(\lambda, v)$ is independent of v.

Lemma 2.2.23. For all $v_1, v_2 \in A\backslash\Lambda$ we have

$$a(\lambda, v_1) = a(\lambda, v_2).$$

Proof. First, if $v_1 + v_2 \notin \Lambda$ we have

$$a(\lambda, v_1) = \frac{\phi(\lambda, v_1)}{\chi(\lambda, v_1)} = \frac{\phi(\lambda, v_1)\phi(\lambda, v_2)}{\phi(\lambda, v_1 + v_2)} = \frac{\phi(\lambda, v_2)}{\chi(\lambda, v_2)} = a(\lambda, v_2). \tag{2.18}$$

Next, we suppose that $v_1 + v_2 \in \Lambda$. We also assume that $2v_1 \in \Lambda$. Then, since

$v_1 + v_2 \in \Lambda$, it follows that $2v_1 + 2v_2 \in \Lambda$, so we also have $2v_2 \in \Lambda$. Taking i such that $\rho_i \geq 3$, we have

$$v_1 + v_2 + b_i, 2v_1 + v_2 + b_i, v_1 + 2v_2 + b_i \notin \Lambda.$$

To see this, note that if $v_1 + v_2 + b_i \in \Lambda$ we would have

$$(v_1 + v_2 + b_i) - (v_1 + v_2) = b_i \in \Lambda.$$

If $2v_1 + v_2 + b_i \in \Lambda$, then it follows that

$$(2v_1 + v_2 + b_i) - (v_1 + v_2) = v_1 + b_i \in \Lambda.$$

Then, since $2v_1 \in \Lambda$, we have

$$(2v_1) - (v_1 + b_i) = v_1 - b_i \in \Lambda.$$

Hence

$$(v_1 + b_i) - (v_1 - b_i) = 2b_i \in \Lambda.$$

Similarly, in the case that $v_1 + 2v_2 + b_i \in \Lambda$, we conclude that $2b_i \in \Lambda$. Thus, in each case we get a contradiction with our assumption that $\rho_i \geq 3$. It therefore follows from (2.18) that we have

$$a(\lambda, v_1) = a(\lambda, v_1 + v_2 + b_1) = a(\lambda, v_2).$$

Next we assume that $v_1 + v_2 \in \Lambda$ and $2v_1, 2v_2 \notin \Lambda$. Then, we have that $v_1 - v_2 \notin \Lambda$, since if $v_1 - v_2 \in \Lambda$, we would have

$$(v_1 + v_2) \pm (v_1 - v_2) \in \Lambda.$$

It then follows that

$$2v_1, 2v_2 \in \Lambda,$$

contradicting our assumptions on v_1 and v_2.

Since $v_1, -v_2, v_1 - v_2 \notin \Lambda$ we can conclude, from (2.18) that

$$a(\lambda, v_1) = a(\lambda, -v_2).$$

Then since $-v_2, v_2, 2v_2 \notin \Lambda$ we can conclude from (2.18) that

$$a(\lambda, -v_2) = a(\lambda, v_2).$$

From which it follows that

$$a(\lambda, v_1) = a(\lambda, v_2),$$

which completes the proof. □

In light of Lemma 2.2.23, we have that

$$a : \Lambda \times A \setminus \Lambda \to k$$

is well defined and independent of v. Since $a(\lambda, v)$ does not depend on v, we use the notation $a(\lambda) := a(\lambda, v)$ for any $v \in A \setminus \Lambda$.

We are now in a position to give a generalization of Theorem 2.1.19.

Theorem 2.2.24. Let $W : A \to k$ be an elliptic net with a unique zero-rank of apparition $(\rho_1, \ldots, \rho_r)$ for which there exists i such that $\rho_i \geq 3$, if $r = 1$ we assume that $\rho_1 \geq 4$. Then, for all $\lambda \in \Lambda$ and $p \in A$, we have

$$W(\lambda + p) = a(\lambda)\chi(\lambda, p)W(p).$$

Proof. If $p \notin \Lambda$, then the statement follows immediately from the definitions of a, χ, and ϕ.

If on the other hand $p \in \Lambda$, then $p + \lambda \in \Lambda$. Thus, $W(p) = 0 = W(\lambda + p)$ and so the statement holds. □

Corollary 2.2.25. With the notation of Theorem 2.2.24 we have

$$W(\lambda - p) = -a(\lambda)\chi(\lambda, p)^{-1}W(p).$$

Proof. This follows immediately from Theorem 2.2.24, using property (iv) of Lemma 2.2.22 and Lemma 2.2.7. □

We remark that if $\text{rank}(W) = 1$, then letting $\{b_1\}$ be a basis for A, and writing $p = nb_1$, Corollary 2.2.25 gives

$$W(\lambda - nb_1) = -a(\lambda)\chi(\lambda, nb_1)^{-1}W(nb_1) = -a(\lambda)\chi(\lambda, b_1)^{-n}W(nb_1).$$

If $\lambda = \rho_1 b_1$, this gives the identity in Theorem 2.1.17.

Next, we explore the relations between the functions $a(\lambda)$ and $\chi(\lambda, v)$, before giving a generalization of Corollary 2.1.21.

Lemma 2.2.26. Under the assumptions of Theorem 2.2.24, we have for all $\lambda_1, \lambda_2 \in \Lambda$

$$a(\lambda_1 + \lambda_2) = a(\lambda_1)a(\lambda_2)\chi(\lambda_1, \lambda_2).$$

Proof. Taking $p \in A\backslash\Lambda$, it follows from Theorem 2.2.24 and Lemma 2.2.22 that we have

$$\begin{aligned} W((\lambda_1 + \lambda_2) + p) &= a(\lambda_1 + \lambda_2)\chi(\lambda_1 + \lambda_2, p)W(p) \\ &= a(\lambda_1 + \lambda_2)\chi(\lambda_1, p)\chi(\lambda_2, p)W(p). \quad (2.19) \end{aligned}$$

We also have,

$$\begin{aligned} W(\lambda_1 + (\lambda_2 + p)) &= a(\lambda_1)\chi(\lambda_1, \lambda_2 + p)W(\lambda_2 + p) \\ &= a(\lambda_1)a(\lambda_2)\chi(\lambda_1, \lambda_2)\chi(\lambda_1, p)\chi(\lambda_2, p)W(p). \quad (2.20) \end{aligned}$$

Then since $p \notin \Lambda$, it follows that $W(p) \neq 0$. Comparing (2.19) and (2.20) gives

$$a(\lambda_1 + \lambda_2) = a(\lambda_1)a(\lambda_2)\chi(\lambda_1, \lambda_2).$$

□

Lemma 2.2.27. Under the assumptions of Theorem 2.2.24, for all $\lambda \in \Lambda$, we have

$$a(\lambda)^2 = \chi(\lambda, \lambda).$$

Proof. Let $p \in A \backslash \Lambda$. From Corollary 2.2.25 we have

$$W(\lambda - p) = -a(\lambda)\chi(\lambda, p)^{-1}W(p). \tag{2.21}$$

Also, from Theorem 2.2.24 we have

$$W(\lambda + (p - \lambda)) = -a(\lambda)\chi(\lambda, \lambda)^{-1}\chi(\lambda, p)W(\lambda - p). \tag{2.22}$$

Combining (2.21) and (2.22) yields

$$W(p) = a(\lambda)^2\chi(\lambda, \lambda)^{-1}W(p).$$

Since $p \notin \Lambda$ we have $W(p) \neq 0$. Thus, the result follows. □

Lemma 2.2.28. Under the assumptions of Theorem 2.2.24, for all $\lambda \in \Lambda$ and $n \in \mathbb{Z}$, we have

$$a(n\lambda) = a(\lambda)^{n^2}.$$

Proof. The statement trivially holds for $n = 1$. We proceed by induction. Assume the statement is true for some $k \geq 1$. From Lemma 2.2.26 and Lemma 2.2.22, we have

$$a((k+1)\lambda) = a(\lambda)a(k\lambda)\chi(\lambda, k\lambda) = a(\lambda)a(k\lambda)\chi(\lambda, \lambda)^k.$$

From the induction hypothesis and Lemma 2.2.27, it follows that

$$a((k+1)\lambda) = a(\lambda)^{k^2+1}a(\lambda)^{2k} = a(\lambda)^{(k+1)^2}.$$

Next we note that if $n = -1$, then since $a_\lambda(v)$ is independent of v, we have

$$\begin{aligned} a(\lambda) = a(\lambda, -v) = \frac{\phi(\lambda, -v)}{\chi(\lambda, -v)} &= \frac{W(\lambda - v)}{W(-v)\chi(-\lambda, v)} \\ &= \frac{W(-\lambda + v)}{W(v)\chi(-\lambda, v)} = \frac{\phi(-\lambda, v)}{\chi(-\lambda, v)} = a(-\lambda, v) = a(-\lambda). \end{aligned} \tag{2.23}$$

Hence, for any $n < 0$, we have

$$a(n\lambda) = a((-n)(-\lambda)) = a(-\lambda)^{(-n)^2} = a(\lambda)^{n^2}.$$

Finally if $n = 0$ we have $a(0) = 1$, since $\chi(0, v) = 1 = \phi(0, v)$. Thus the statement holds. □

Lemma 2.2.29. Under the assumptions of Theorem 2.2.24, for any $r \geq 1$, and $\lambda_1, \lambda_2, \ldots, \lambda_r \in \Lambda,\ n_1, n_2, \ldots, n_r \in \mathbb{Z}$, we have

$$a\left(\sum_{i=1}^{r} n_i\lambda_i\right) = \left(\prod_{i=1}^{r} a(\lambda_i)^{n_i^2}\right) \prod_{1\leq i<j\leq r} \chi(\lambda_i, \lambda_j)^{n_i n_j}. \tag{2.24}$$

Proof. We note that the case $r = 1$ is given by Lemma 2.2.28. For the case $r = 2$, from Lemma 2.2.26 we have

$$a(n_1\lambda_1 + n_2\lambda_2) = a(n_1\lambda_1)a(n_2\lambda_2)\chi(n_1\lambda_1, n_2\lambda_2).$$

It then follows from Lemma 2.2.28 and Lemma 2.2.22, that

$$a(n_1\lambda_1 + n_2\lambda_2) = a(\lambda_1)^{n_1^2}a(\lambda_2)^{n_2^2}\chi(\lambda_1, \lambda_2)^{n_1 n_2}.$$

Next assume (2.24) holds for some $k \geq 2$ and consider $r = k + 1$. From Lemma 2.2.26 and Lemma 2.2.28, we have that

$$\begin{aligned} a\left(\sum_{i=1}^{k+1} n_i\lambda_i\right) &= a\left(\sum_{i=1}^{k} n_i\lambda_i\right) a(n_{k+1}\lambda_{k+1})\chi\left(\sum_{i=1}^{k} n_i\lambda_i, n_{k+1}\lambda_{k+1}\right) \\ &= a\left(\sum_{i=1}^{k} n_i\lambda_i\right) a\left(\lambda_{k+1}\right)^{n_{k+1}^2} \prod_{i=1}^{k} \chi(\lambda_i, \lambda_{k+1})^{n_i n_{k+1}}. \end{aligned}$$

Then from the induction hypothesis we get

$$\begin{aligned} a\left(\sum_{i=1}^{k+1} n_i\lambda_i\right) &= \left(\prod_{i=1}^{k} a(\lambda_i)^{n_i^2}\right) \prod_{1\leq i<j\leq k} \chi(\lambda_i, \lambda_j)^{n_i n_j} \\ &\quad \times a(\lambda_{k+1})^{n_{k+1}^2} \prod_{i=1}^{k} \chi(\lambda_i, \lambda_{k+1})^{n_i n_{k+1}} \\ &= \left(\prod_{i=1}^{k+1} a(\lambda_i)^{n_i^2}\right) \prod_{1\leq i<j\leq k+1} \chi(\lambda_i, \lambda_j)^{n_i n_j}. \end{aligned}$$

□

Theorem 2.2.30. Under the assumptions of Theorem 2.2.24, for any $r \in \mathbb{N}$, and $\lambda_1, \lambda_2, \ldots, \lambda_r \in \Lambda,\ n_1, n_2, \ldots, n_r \in \mathbb{Z},$ and $p \in A$ we have

$$W\left(\left(\sum_{i=1}^{r} n_i\lambda_i\right) + p\right) = \left(\prod_{0\le i<j\le r} a(\lambda_j)^{n_j^2}\chi(\lambda_j, p)^{n_j}\chi(\lambda_i, \lambda_j)^{n_i n_j}\right) W(p). \tag{2.25}$$

In the above product we take $\lambda_0 = 0$.

Proof. From Theorem 2.2.24 and Lemma 2.2.22 we have

$$\begin{aligned} W\left(\sum_{i=1}^{r}(n_i\lambda_i) + p\right) &= a\left(\sum_{i=1}^{r} n_i\lambda_i\right)\chi\left(\sum_{i=1}^{r} n_i\lambda_i, p\right) W(p) \\ &= a\left(\sum_{i=1}^{r} n_i\lambda_i\right)\left(\prod_{i=1}^{r}\chi(\lambda_i, p)^{n_i}\right) W(p). \end{aligned}$$

It follows from Lemma 2.2.29 that

$$\begin{aligned} W\left(\sum_{i=1}^{r}(n_i\lambda_i) + p\right) &= \left(\prod_{i=1}^{r} a(\lambda_i)^{n_i^2}\right)\left(\prod_{1\le i<j\le r}\chi(\lambda_i, \lambda_j)^{n_i n_j}\right) \\ &\quad \times \left(\prod_{i=1}^{r}\chi(\lambda_i, p)^{n_i}\right) W(p) \\ &= \left(\prod_{i=1}^{r} a(\lambda_i)^{n_i^2}\chi(\lambda_i, p)^{n_i}\right)\left(\prod_{1\le i<j\le r}\chi(\lambda_i, \lambda_j)^{n_i n_j}\right) W(p). \end{aligned}$$

Then, since $\lambda_0 = 0$ and $\chi(0, v) = 1$, we have

$$W\left(\left(\sum_{i=1}^{r} n_i\lambda_i\right) + p\right) = \left(\prod_{0\le i<j\le r} a(\lambda_j)^{n_j^2}\chi(\lambda_j, p)^{n_j}\chi(\lambda_i, \lambda_j)^{n_i n_j}\right) W(p). \tag{2.26}$$

□

We remark that if $r = 1$, Theorem 2.2.30 gives

$$W(n\lambda + p) = a(\lambda)^{n^2}\chi(\lambda, p)^n W(p).$$

Letting $\{b_1\}$ be a basis for A, writing $p = mb_1$, and employing Lemma 2.2.22 on the preceding identity yields

$$W(n\lambda + mb_1) = a(\lambda)^{n^2}\chi(\lambda, b_1)^{nm} W(mb_1).$$

For $\lambda = \rho_1 b_1$ this is exactly the identity given in Corollary 2.1.21.

Chapter 3

Connection With Elliptic Curves

3.1 Elliptic functions

We remark that many of the results of this section are classical, and are included here with proofs for completeness, for more details see [8], and [5].

Throughout this chapter, we let $\Lambda \subset \mathbb{C}$ denote a lattice. That is,

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

for some $\mathbb{R}$-linearly independent $\omega_1, \omega_2 \in \mathbb{C}$. We denote by Λ^* the set of non-zero elements in Λ. Thus,

$$\Lambda^* := \{\omega \in \Lambda : \ \omega \neq 0\}.$$

Definition 3.1.1. Let $\Lambda \subset \mathbb{C}$ be a lattice. An *elliptic function* (relative to Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ that satisfies

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

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

We begin this section by introducing some of the fundamental functions in the theory of elliptic functions (namely the Weierstrass $\wp$, σ, and ζ functions) and discussing some of their elementary relations.

Definition 3.1.2. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass $\wp$-function* (relative to Λ) is defined by

$$\wp(z) = \wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\omega\in\Lambda^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2)} \right). \tag{3.1}$$

Lemma 3.1.3. For any lattice $\Lambda \subset \mathbb{C}$, the series defining $\wp(z;\Lambda)$ converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$ and defines a meromorphic function on $\mathbb{C}$ which has a double pole with residue 0 at each lattice point and no other poles. Moreover, $\wp(z;\Lambda)$ is an even elliptic function.

Proof. See [8, Theorem VI.3.1]. □

Definition 3.1.4. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass σ-function* (relative to Λ) is defined by

$$\sigma(z) = \sigma(z;\Lambda) := z \prod_{\omega \in \Lambda^*} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}(\frac{z}{\omega})^2}. \tag{3.2}$$

Lemma 3.1.5. For any lattice $\Lambda \subset \mathbb{C}$, we have the following:

i) The infinite product defining $\sigma(z;\Lambda)$ defines a holomorphic function on all of $\mathbb{C}$, with simple zeros at each $z \in \Lambda$ and no other zeros.

ii) $\frac{d^2}{dz^2}\log\sigma(z;\Lambda) = -\wp(z;\Lambda)$ for all $z \in \mathbb{C}$.

iii) For every $\omega \in \Lambda$ there exists constants $a = a_\omega, b = b_\omega \in \mathbb{C}$, such that

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

iv) $\sigma(z;\Lambda)$ is an odd function.

Proof. See [8, Lemma VI.3.3]. □

Definition 3.1.6. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass ζ-function* (relative to Λ) is defined by

$$\zeta(z) = \zeta(z;\Lambda) := \frac{1}{z} + \sum_{\omega \in \Lambda^*} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right). \tag{3.3}$$

Lemma 3.1.7. For any lattice $\Lambda \subset \mathbb{C}$, the Weierstrass ζ-function satisfies the following:

i) $\frac{d}{dz}\log\sigma(z;\Lambda) = \zeta(z;\Lambda)$.

ii) $\frac{d}{dz}\zeta(z;\Lambda) = -\wp(z;\Lambda)$.

iii) $\zeta(z;\Lambda)$ is an odd function.

Proof. See [8, Chapter VI] □

We also need to introduce the Weierstrass η-function, defined on a lattice, and explore the properties of η.

Definition 3.1.8. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass η-function* (relative to Λ) is defined by

$$\eta(\omega) = \eta(\omega; \Lambda) := \zeta(z + \omega; \Lambda) - \zeta(z; \Lambda), \tag{3.4}$$

for any $z \in \mathbb{C} \setminus \Lambda$.

Proposition 3.1.9. For any lattice $\Lambda \subset \mathbb{C}$, the function $\eta(\omega; \Lambda)$ is well defined and it is independent of z. Moreover $\eta(\omega)$ is precisely the term a_ω introduced in part (iii) of Lemma 3.1.5.

Proof. We have,

$$\begin{aligned}
\eta(\omega) &= \zeta(z+\omega) - \zeta(z) \\
&= \frac{\sigma'(z+\omega)}{\sigma(z+\omega)} - \frac{\sigma'(z)}{\sigma(z)} \\
&= \frac{a_\omega e^{a_\omega z + b_\omega}\sigma(z) + e^{a_\omega z + b_\omega}\sigma'(z)}{e^{a_\omega z + b_\omega}\sigma(z)} - \frac{\sigma'(z)}{\sigma(z)} = a_\omega.
\end{aligned}$$

□

Proposition 3.1.10. For all $\omega_1, \omega_2 \in \Lambda$, we have

$$\eta(\omega_1 + \omega_2) = \eta(\omega_1) + \eta(\omega_2)$$

Proof. Let $\omega_1, \omega_2 \in \Lambda$. We have

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

□

Next, we give an alternative version of the transformation property of σ given in part (iii) of Lemma 3.1.5.

Lemma 3.1.11. For all $z \in \mathbb{C}$ and $\omega \in \Lambda$, we have

$$\sigma(z+\omega) = \delta(\omega) e^{\eta(\omega)(z+\omega/2)} \sigma(z), \tag{3.5}$$

where

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

Proof. We start by defining the function $\delta : \Lambda \to \mathbb{C}$ by

$$\delta(\omega) := \frac{\sigma(z+\omega)}{e^{\eta(\omega)(z+\omega/2)}\sigma(z)}, \tag{3.6}$$

for any $z \notin \Lambda$. If $\omega \notin 2\Lambda$, then $\pm\omega/2 \notin \Lambda$. Taking $z = -\omega/2$ in (3.6) gives

$$\delta(\omega) = \frac{\sigma(\omega/2)}{\sigma(-\omega/2)} = -1.$$

On the other hand, for any $\omega \in \Lambda$ we have

$$\frac{\sigma(z+2\omega)}{\sigma(z)} = \frac{\sigma(z+2\omega)\sigma(z+\omega)}{\sigma(z+\omega)\sigma(z)}.$$

Hence, from (3.6), we have

$$\delta(2\omega) e^{\eta(2\omega)(z+\omega)} = \delta(\omega)^2 e^{2\eta(\omega)(z+\omega)}.$$

It then follows, since $\eta(2\omega) = 2\eta(\omega)$ from Proposition 3.1.10, that

$$\delta(2\omega) = \delta(\omega)^2. \tag{3.7}$$

Now, if $\omega \in 2\Lambda$, then $\omega = 2^n\omega_0$ for some $\omega_0 \in \Lambda$, with $\omega_0 \notin 2\Lambda$. Hence, by employing (3.7), we have

$$\delta(\omega) = \delta(\omega_0)^{2^n} = (-1)^{2^n} = 1.$$

□

Before exploring deeper connections between the functions introduced in the preced-

ing discussion, we first provide a means of determining whether two elliptic functions are equal.

Proposition 3.1.12. Let f be an elliptic function. If f has no zeros (respectively poles) then f is constant.

Proof. See [8, Proposition VI.2.1]. □

Lemma 3.1.13. Let $f, g : \mathbb{C} \to K$ be elliptic functions such that f and g have the same zeros (respectively poles). Then there exists a constant $c \in K^*$ such that

$$f = cg.$$

Proof. Let $f, g : \mathbb{C} \to K$ be elliptic functions, such that f and g have the same zeros (respectively poles). Then the function f/g is elliptic, and does not have any zeros (respectively poles). Hence, it follows from Proposition 3.1.12 that f/g is constant. □

We remark that Lemma 3.1.13 suggests that we will frequently need to find all the zeros (respectively poles) of an elliptic function. However, if f is an elliptic function with $f(z) = 0$, then we have $f(z + \omega) = 0$ for all $\omega \in \Lambda$. As such we can limit our search to any set

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

where $a \in \mathbb{C}$, and $\{\omega_1, \omega_2\}$ is a basis for Λ.

Definition 3.1.14. The fundamental parallelogram for a lattice $\Lambda \subset \mathbb{C}$ is any set of the form

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

where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a basis for Λ.

The next lemma is useful in determining the number of zeros (respectively poles) of an elliptic function in the fundamental parallelogram.

Lemma 3.1.15. Let f be an elliptic functions relative to a lattice $\Lambda \subset \mathbb{C}$, with D the fundamental parallelogram for Λ. Then f has the same number of zeros and poles in D, counted with multiplicity.

Proof. See [8, §VI.3] □

The following lemma gives a means of constructing elliptic functions by using the Weierstrass σ-function, and moreover relates the Weierstrass σ-function with the Weierstrass $\wp$-function.

Lemma 3.1.16. Fix a lattice $\Lambda \subset \mathbb{C}$. For every $u, v \in \mathbb{C}$, we have

$$\wp(u) - \wp(v) = -\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}. \tag{3.8}$$

Proof. We note that the left hand side of (3.8) is elliptic (doubly periodic) in both variables. We show that the right hand side is also elliptic in both variables.

We define the function

$$f(u,v) := -\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}.$$

Then for any $\omega \in \Lambda$, we have

$$\begin{aligned} f(u+\omega, v) &= -\frac{\sigma(u+v+\omega)\sigma(u-v+\omega)}{\sigma(u+\omega)^2\sigma(v)^2} \\ &= -\frac{\psi(\omega)e^{\eta(\omega)(u+v+\omega/2)}\sigma(u+v)\psi(\omega)e^{\eta(\omega)(u-v+\omega/2)}\sigma(u-v)}{\psi(\omega)^2 e^{2\eta(\omega)(u+\omega/2)}\sigma(u)^2\sigma(v)^2} \\ &= -\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = f(u,v). \end{aligned}$$

Similarly, we have $f(u, v+\omega) = f(u,v)$. Thus, f is elliptic in both variables.

Now, fix $a \in \mathbb{C}$ and define $g(z) : \mathbb{C}/\Lambda \to \mathbb{C}$ by

$$g(z) = \wp(z) - \wp(a).$$

It follows from Lemma 3.1.3 that the only zeros of g occur at $\pm a$, and g has a double pole at 0. Thus, it follows from Lemma 3.1.13 that for some constant $c \in \mathbb{C}$, we have

$$g(z) = c\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2}, \tag{3.9}$$

since the right hand side of (3.9) has the same zeroes and poles as g. Hence

$$\lim_{z\to 0} z^2\wp(z) - z^2\wp(a) = \lim_{z\to 0} z^2 g(z) = \lim_{z\to 0} cz^2 \frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2}.$$

Now, we have

$$\lim_{z\to 0} z^2\wp(z) = 1 \text{ and } \lim_{z\to 0} z^2/\sigma(z)^2 = 1.$$

Hence,

$$1 = c\lim_{z\to 0} z^2 \frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2} = -c\sigma(a)^2.$$

Thus, $c = -1/\sigma(a)^2$, which gives

$$\wp(z) - \wp(a) = -\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2\sigma(a)^2}.$$

□

Next, we explore further connections between the Weierstrass σ and ζ functions. The following result is due to Stange [9].

Lemma 3.1.17. Fix a lattice $\Lambda \subset \mathbb{C}$ and let $x, y, z \in \mathbb{C}$. Then we have

$$\zeta(x+y) - \zeta(y) - \zeta(x+z) + \zeta(z) = \frac{\sigma(x+y+z)\sigma(x)\sigma(y-z)}{\sigma(x+y)\sigma(x+z)\sigma(y)\sigma(z)}. \tag{3.10}$$

Proof. We consider the function

$$f(x,y,z) := \zeta(x+y) - \zeta(y) - \zeta(x+z) + \zeta(z).$$

For any $\omega \in \Lambda$, we have

$$\begin{aligned} f(x+\omega, y, z) &= \zeta(x+y+\omega) - \zeta(y) - \zeta(x+z+\omega) + \zeta(z) \\ &= \eta(\omega) + \zeta(x+y) - \zeta(y) - \eta(\omega) - \zeta(x+z) + \zeta(z) \\ &= \zeta(x+y) - \zeta(y) - \zeta(x+z) + \zeta(z) = f(x,y,z). \end{aligned}$$

Similarly, we have

$$f(x, y+\omega, z) = f(x, y, z) \text{ and } f(x, y, z+\omega) = f(x, y, z).$$

Hence, f is elliptic in each variable.

We also define

$$g(x, y, z) := \frac{\sigma(x+y+z)\sigma(x)\sigma(y-z)}{\sigma(x+y)\sigma(x+z)\sigma(y)\sigma(z)}.$$

Then by Lemma 3.1.5 we have, for any $\omega \in \Lambda$,

$$\begin{aligned} g(x+\omega, y, z) &= \frac{\sigma(x+y+z+\omega)\sigma(x+\omega)\sigma(y-z)}{\sigma(x+y+\omega)\sigma(x+z+\omega)\sigma(y)\sigma(z)} \\ &= \frac{e^{a_\omega(x+y+z)+b_\omega} e^{a_\omega x+b_\omega}\sigma(x+y+z)\sigma(x)\sigma(y-z)}{e^{a_\omega(x+y)+b_\omega} e^{a_\omega(x+z)+b_\omega}\sigma(x+y)\sigma(x+z)\sigma(y)\sigma(z)} \\ &= g(x, y, z). \end{aligned}$$

Similarly, we have

$$g(z, y+\omega, z) = g(x, y, z) \text{ and } g(z, y, z+\omega) = g(x, y, z).$$

Thus, g is also elliptic in each variable.

Now, fix $y, z \in \mathbb{C} \setminus \Lambda$ and consider

$$f_{y,z}(x) := f(x, y, z),$$

and

$$g_{y,z}(x) := g(x, y, z)$$

as functions on $\mathbb{C}/\Lambda$. Then, $f_{y,z}$ has poles at $-y, -z$, and zeros at $0, -y-z$. These are exactly the poles and zeros of $g_{y,z}$. It then follows from Lemma 3.1.13 that there exists $c_1 \in \mathbb{C} \setminus \{0\}$ such that

$$f_{y,z}(x) = c_1 g_{y,z}(x).$$

Let

$$\begin{aligned} F(x) &= (\zeta(x+y)-\zeta(y)-\zeta(x+z)+\zeta(z))\sigma(x+y)\sigma(x+z), \\ G(x) &= \sigma(x+y+z)\sigma(x). \end{aligned}$$

The preceding discussion shows that

$$F(x) = c_2 G(x),$$

where

$$c_2 = \frac{c_1\sigma(y-z)}{\sigma(y)\sigma(z)} \tag{3.11}$$

is a constant. Hence, taking derivatives yields

$$F'(x) = c_2 G'(x),$$

where

$$\begin{aligned} F'(x) &= (\zeta'(x+y)-\zeta'(x+z))\sigma(z+y)\sigma(x+z) \\ &\quad +(\zeta(x+y)-\zeta(y)-\zeta(x+z)+\zeta(z))\sigma'(x+y)\sigma(x+z) \\ &\quad +\zeta(x+y)-\zeta(y)-\zeta(x+z)+\zeta(z))\sigma(x+y)\sigma'(x+z), \\ G'(x) &= \sigma'(x+y+z)\sigma(x)+\sigma(x+y+z)\sigma'(x). \end{aligned}$$

By evaluating F' and G' at 0, then applying Lemma 3.1.7, and noting that $\sigma(0)=0$ and $\sigma'(0)=1$, we have

$$c_2 = -\frac{\sigma(z-y)}{\sigma(y)\sigma(z)} = \frac{\sigma(y-z)}{\sigma(y)\sigma(z)}.$$

Putting the latter value for c_2 into (3.11), we find that $c_1 = 1$. Thus (3.10) holds. □

3.2 Division Polynomials

Before introducing division polynomials, we first describe the Uniformization Theorem for elliptic curves

Theorem 3.2.1 (Uniformization Theorem)**.** Let $E/\mathbb{C}$ be an elliptic curve. There exists

a lattice $\Lambda \subset \mathbb{C}$ such that

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda.$$

Proof. See [8, VI.5.1]. □

Throughout this section we let K be a field with a fixed embedding $K \hookrightarrow \mathbb{C}$, and E/K be an elliptic curve given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.12}$$

and let $\Lambda \subset \mathbb{C}$ be the lattice associated to E. We also define the sets

$$(\mathbb{C}/\Lambda)_n := \{u \in \mathbb{C}/\Lambda : \ nu \in \Lambda\},$$

and

$$(\mathbb{C}/\Lambda)_n^* := (\mathbb{C}/\Lambda)_n \backslash \{0\}.$$

We set

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, \\ b_4 &:= 2a_4 + a_1a_3, \\ b_6 &:= a_3^2 + 4a_6, \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Definition 3.2.2. Let E/K be an elliptic curve defined by equation (3.12). We define the n^{th} *division polynomial* ψ_n, associated to E, using the initial values

$$\begin{aligned} \psi_1 &= 1, \\ \psi_2 &= 2y + a_1x + a_3, \\ \psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6 + b_8, \\ \psi_4 &= \psi_2\big(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\big), \end{aligned}$$

then inductively using the formulas

$$\begin{aligned} \psi_{2k+1} &= \quad \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3 \qquad \text{for } k \geq 2, \\ \psi_2\psi_{2k} &= \psi_{k-1}^2\psi_k\psi_{k+2} - \psi_{k-2}\psi_k\psi_{k+1}^2 \quad \text{for } k \geq 3. \end{aligned}$$

Proposition 3.2.3. For an elliptic curve E/K defined by (3.12), let ψ_n denote the n^{th} division polynomial associated to E. Then $\psi_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]$, for all $n \in \mathbb{N}$.

Proof. See [8, Chapter 3]. □

This section is devoted to showing that the sequence (ψ_n) of n^{th} division polynomials, associated to an elliptic curve E and a rational point P, is an elliptic sequence.

Theorem 3.2.4. For an elliptic curve E/K, the division polynomials ψ_n associated to E satisfy the relation

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

for all $m, n, r \in \mathbb{Z}$, with $m > n > r \geq 1$.

In order to prove Theorem 3.2.4 we first define functions $\tilde{\psi}_n$ and show that the sequence $(\tilde{\psi}_n)$ is an elliptic sequence. Finally, we show that the sequences $(\tilde{\psi}_n)$ and (ψ_n) agree on the first four terms, hence by Proposition 2.1.3 agree everywhere.

Let E/K be an elliptic curve with $E(\mathbb{C})$ isomorphic to $\mathbb{C}/\Lambda$ and let $z \in \mathbb{C}/\Lambda$. For each $n \in \mathbb{N}$, we let $\tilde{\psi}_n : \mathbb{C} \to \mathbb{C}$ be such that

$$\tilde{\psi}_n(z)^2 = n^2 \prod_{u \in (\mathbb{C}/\Lambda)_n^*} \big(\wp(z) - \wp(u)\big) \tag{3.13}$$

Remark 3.2.5. Since $\wp$ is an even function, all of the terms in the product defining $\tilde{\psi}_n^2$, except those with $u \in (\mathbb{C}/\Lambda)_2$, occur with multiplicity 2. Hence, if n is odd, $\tilde{\psi}_n^2$ is a perfect square. If n is even, then we have

$$\tilde{\psi}_n(z)^2 = g_n(z) \prod_{u \in (\mathbb{C}/\Lambda)_2^*} (\wp(z) - \wp(u)),$$

where $g_n(z)$ is a perfect square, and

$$\prod_{u \in (\mathbb{C}/\Lambda)_2^*} (\wp(z) - \wp(u)) = 4\wp'(z)^2,$$

see [8, VI.3.6]. Hence, $\tilde{\psi}_n$ is a perfect square for all n, and we may define

$$\tilde{\psi}_n(z) = \begin{cases} n\wp(z)^{(n^2-1)/2} + \dots & \text{if } n \text{ is odd} \\ \frac{n}{2}\wp'(z)\wp(z)^{(n^2-4)/2} + \dots & \text{if } n \text{ is even.} \end{cases}$$

Theorem 3.2.6. For all $n\mathbb{Z}$ with $n \geq 1$ and $z \in \mathbb{C}$, we have

$$\wp(nz) - \wp(z) = -\frac{\tilde{\psi}_{n+1}(z)\tilde{\psi}_{n-1}(z)}{\tilde{\psi}_n(z)^2}.$$

Proof. [5, Page 34] □

Theorem 3.2.7. For all $m, n, r \in \mathbb{Z}$ with $m > n > r \geq 1$, the functions $\tilde{\psi}_n$ satisfy

$$\tilde{\psi}_{m+n}(z)\tilde{\psi}_{m-n}(z)\tilde{\psi}_r(z)^2 = \tilde{\psi}_{m+r}(z)\tilde{\psi}_{m-r}(z)\tilde{\psi}_n(z)^2 - \tilde{\psi}_{n+r}(z)\tilde{\psi}_{n-r}(z)\tilde{\psi}_m(z)^2.$$

Proof. For the case $r = 1$, see [5, Page 36]. The result then follows from Proposition 2.1.4. □

We are now ready to prove Theorem 3.2.4.

Proof of Theorem 3.2.4. By direct calculation, we have

$$\begin{aligned} \tilde{\psi}_1(z) &= 1, \\ \tilde{\psi}_2(z) &= 2y + a_1x + a_3, \\ \tilde{\psi}_3(z) &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6 + b_8 \\ \tilde{\psi}_4(z) &= \tilde{\psi}_2(z)\big(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\big) \end{aligned}$$

Since $\tilde{\psi}_n(z)$ and $\psi_n(P)$ are both uniquely determined by their first four terms, and they agree on their first four terms, it follows that $\psi_n = \tilde{\psi}_n$ for all n. Hence, we have

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

which completes the proof of Theorem 3.2.4. □

Proposition 3.2.8. Let E/K be an elliptic curve defined by (3.12), $P \in E(K)$, and ψ_n be the n^{th} division polynomial associated to E and P. Then, taking Λ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, there exists $u \in \mathbb{C}/\Lambda$ such that

$$\psi_n(P) = (-1)^{n^2-1} \frac{\sigma(nu;\Lambda)}{\sigma(u;\Lambda)^{n^2}}.$$

Proof. [10, Pg. 183, exercise 6.15] □

3.3 Valuations of division polynomials

Let E/K be an elliptic curve defined by (3.12). For a rational point $P = (x, y) \in E(K)$ there exists polynomials ψ_n, ϕ_n and $\omega_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]$ such that

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

We note the ψ_n is the n^{th} *division polynomial* associated to E, described in section 3.2. See [8, Chapter 3] for a description of $\phi_n(P)$ and $\omega_n(P)$.

From now on we assume that K is a number field with the ring of integers $\mathcal{O}_K$. We denote by $\nu_{\mathfrak{p}}$ the valuation associated to the prime ideal ideal $\mathfrak{p}$. We also denote the reduction modulo $\mathfrak{p}$ of a point P by $P \pmod{\mathfrak{p}}$. See [8, Chapter 7] for more on the reduction of an elliptic curve.

In [1, Theorem A], Ayad proved the following theorem on the $\mathfrak{p}$-adic valuation of $\psi_n(P)$.

Theorem 3.3.1 (Ayad). Let E be an elliptic curve defined by (3.12) with $a_i \in \mathcal{O}_K$ for $i = 1, 2, 3, 4, 6$. Let $P \in E(K)$ be a point other than the point at infinity $\mathcal{O}$. Suppose that the reduction modulo $\mathfrak{p}$ of P is not the point at infinity. Then the following assertions are equivalent:

(a) $\nu_{\mathfrak{p}}(\psi_2(P))$ and $\nu_{\mathfrak{p}}(\psi_3(P)) > 0$.

(b) For all integers $n \geq 2$, we have $\nu_{\mathfrak{p}}(\psi_n(P)) > 0$.

(c) There exists an integer $n \geq 2$ such that $\nu_{\mathfrak{p}}(\psi_n(P)) > 0$ and $\nu_{\mathfrak{p}}(\psi_{n+1}(P)) > 0$.

(d) There exists an integer $m \geq 2$ such that $\nu_{\mathfrak{p}}(\psi_m(P)) > 0$ and $\nu_{\mathfrak{p}}(\phi_m(P)) > 0$.

(e) $P \pmod{\mathfrak{p}}$ is singular.

In the next section, we provide a generalization of Theorem 3.3.1. However, we first describe an application of Theorem 3.3.1.

Let K be a number field for which the ring of integers $\mathcal{O}_K$ is a principal ideal domain, and let E/K be an elliptic curve. From Proposition 1.1.4, we have that any point $P \in E(K)$ can be represented uniquely (up to units) by

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

with $\gcd(A_P, D_P) = \gcd(B_P, D_P) = 1$. Let (D_{nP}) be the sequence of denominators of the multiples of P. More precisely D_{nP} is given by the identity

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

with $\gcd(A_{nP}, D_{nP}) = \gcd(B_{nP}, D_{nP}) = 1$. One can show that (D_{nP}) is a divisibility sequence. Some authors call this sequence an elliptic divisibility sequence. In this thesis, in order to distinguish this sequence from the classical elliptic divisibility sequences studied by Ward, we call the sequence (D_{nP}) the *elliptic denominator sequence* associated to the elliptic curve E and the point P.

We are interested in relation between $\psi_n(P)$ and D_{nP}. In order to describe this we note that

$$nP = \left(\frac{\phi_n(P)}{\psi_n^2(P)}, \frac{\omega_n(P)}{\psi_n^3(P)}\right) = \left(\frac{\hat{\phi}_n(P)}{D_P^2\hat{\psi}_n^2(P)}, \frac{\hat{\omega}_n(P)}{D_P^3\hat{\psi}_n^3(P)}\right),$$

where $\hat{\phi}_n(P) := D_P^{2n^2}\phi_n(P)$, $\hat{\omega}_n(P) := D_P^{3n^2}\omega_n(P)$, and $\hat{\psi}_n(P) := D_P^{n^2-1}\psi_n(P)$. Note that $\hat{\phi}_n(P), \hat{\omega}_n(P)$, and $\hat{\psi}_n(P)$ are the results of clearing the denominators in $\phi_n(P), \omega_n(P)$, and $\psi_n(P)$ and so they are integral in K. Hence, $\hat{\phi}_n(P), \hat{\omega}_n(P), \hat{\psi}_n(P) \in \mathcal{O}_K$. Now let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ and denote the valuation attached to $\mathfrak{p}$ by $\nu_{\mathfrak{p}}$. We note that if the reduction mod $\mathfrak{p}$ of P is not the point at infinity then $\nu_{\mathfrak{p}}(D_P) = 0$ and so in this

case

$$\nu_{\mathfrak{p}}(\phi_n(P)) = \nu_{\mathfrak{p}}(\hat{\phi}_n(P)),$$

$$\nu_{\mathfrak{p}}(\omega_n(P)) = \nu_{\mathfrak{p}}(\hat{\omega}_n(P)),$$

and

$$\nu_{\mathfrak{p}}(\psi_n(P)) = \nu_{\mathfrak{p}}(\hat{\psi}_n(P)).$$

From here, under conditions of Theorem 3.3.1 for E, P, and all primes of bad reduction $\mathfrak{p}$, we can conclude that if $P \pmod{\mathfrak{p}}$ is non-singular for all primes of bad reduction $\mathfrak{p}$ then $\gcd(\hat{\phi}_n(P), D_P^2\hat{\psi}_n^2(P)) = 1$. So we have the following result.

Proposition 3.3.2. Suppose the assumptions of Theorem 3.3.1 hold for E, P, and all primes of bad reduction $\mathfrak{p}$. Moreover suppose that $P \pmod{\mathfrak{p}}$ is non-singular for all primes of bad reduction $\mathfrak{p}$. Let (D_{nP}) be the elliptic denominator sequence associated to E and P. Then we have

$$D_{nP} = uD_P\hat{\psi}_n(P) = uD_P^{n^2}\psi_n(P).$$

More generally if the assumptions of Theorem 3.3.1 hold for E, P, and a prime $\mathfrak{p}$, and if $P \pmod{\mathfrak{p}}$ is non-singular, then

$$\nu_{\mathfrak{p}}(D_{nP}) = n^2\nu_{\mathfrak{p}}(D_P) + \nu_{\mathfrak{p}}(\psi_n(P)) = \nu_{\mathfrak{p}}(\psi_n(P)).$$

In the next two sections we give a generalization of Ayads theorem for higher rank elliptic nets. These generalizations will play a fundamental role in the applications described in Chapter 4.

3.4 Net polynomials

Definition 3.4.1. Let $\Lambda \subset \mathbb{C}$ be a lattice and fix $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$. We define the function $\tilde{\Psi}_{\mathbf{v}}$ on $\mathbb{C}^n$ in variable $\mathbf{z} = (z_1, z_2, \ldots, z_n)$ as

$$\tilde{\Psi}_{\mathbf{v}}(\mathbf{z}) = \tilde{\Psi}_{\mathbf{v}}(\mathbf{z}; \Lambda) := -(-1)^{\sum_{1\le i\le j\le r} v_iv_j} \frac{\sigma(v_1z_1 + v_2z_2 + \cdots + v_nz_n)}{\left(\prod_{i=1}^{n}\sigma(z_i)^{2v_i^2 - \sum_{j=1}^{n} v_iv_j}\right)\left(\prod_{1\le i<j\le n}\sigma(z_i + z_j)^{v_iv_j}\right)} \tag{3.14}$$

Remark 3.4.2. For each $n \in \mathbb{Z}$ and $z \in \mathbb{C}$, we have

$$\tilde{\Psi}_n(z) = -(-1)^{n^2} \frac{\sigma(nz)}{\sigma(z)^{n^2}}.$$

Proposition 3.4.3. Let $\Lambda \subset \mathbb{C}$ be a lattice. The functions $\tilde{\Psi}_{\mathbf{v}}$ are elliptic (doubly periodic) in each variable.

Proof. Let $\omega \in \Lambda$, $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$, and $\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n$, and let $w_i = \omega e_i$, where $\{e_1, e_2, \ldots, e_n\}$ is the standard basis for $\mathbb{Z}^n$. Then from Lemma 3.1.11, and equation (3.14), we have

$$\tilde{\Psi}_{\mathbf{v}}(\mathbf{z} + w_i) = \frac{\delta(v_i\omega)}{\delta(\omega)^{v_i^2}} \tilde{\Psi}_{\mathbf{v}}(\mathbf{z}).$$

Hence,

$$\frac{\tilde{\Psi}_{\mathbf{v}}(\mathbf{z} + w_i)}{\tilde{\Psi}_{\mathbf{v}}(\mathbf{z})} = \frac{\delta(v_i\omega)}{\delta(\omega)^{v_i^2}} = 1.$$

□

Next, we use Lemma 3.1.16 to relate the functions $\tilde{\Psi}_v$ to the Weierstrass $\wp$-function.

Lemma 3.4.4. Fix a lattice $\Lambda \subset \mathbb{C}$, and let $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^n$ and $\mathbf{z} \in \mathbb{C}^n$. Then, we have

$$\wp(\mathbf{v} \cdot \mathbf{z}) - \wp(\mathbf{w} \cdot \mathbf{z}) = -\frac{\tilde{\Psi}_{\mathbf{v}+\mathbf{w}}(\mathbf{z})\tilde{\Psi}_{\mathbf{v}-\mathbf{w}}(\mathbf{z})}{\tilde{\Psi}_{\mathbf{v}}(\mathbf{z})^2\tilde{\Psi}_{\mathbf{w}}(\mathbf{z})^2}.$$

Proof. From (3.14) and Lemma 3.1.16, we have

$$\begin{aligned} -\frac{\tilde{\Psi}_{\mathbf{v}+\mathbf{w}}(\mathbf{z})\tilde{\Psi}_{\mathbf{v}-\mathbf{w}}(\mathbf{z})}{\tilde{\Psi}_{\mathbf{v}}(\mathbf{z})^2\tilde{\Psi}_{\mathbf{w}}(\mathbf{z})^2} &= -\frac{\sigma(\mathbf{v} \cdot \mathbf{z} + \mathbf{w} \cdot \mathbf{z})\sigma(\mathbf{v} \cdot \mathbf{z} - \mathbf{w} \cdot \mathbf{z})}{\sigma(\mathbf{v} \cdot \mathbf{z})^2\sigma(\mathbf{w} \cdot \mathbf{z})^2} \\ &= \wp(\mathbf{v} \cdot \mathbf{z}) - \wp(\mathbf{w} \cdot \mathbf{z}). \end{aligned}$$

□

The following Theorem shows that $\tilde{\Psi}_{\mathbf{v}}$ satisfies the elliptic net recurrence (2.14).

Theorem 3.4.5 (Stange). Fix a lattice $\Lambda \subset \mathbb{C}$ and fix $\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n$. The function

$$\begin{aligned} W : \mathbb{Z}^n &\to \mathbb{C} \\ \mathbf{v} &\mapsto \tilde{\Psi}_{\mathbf{v}}(\mathbf{z}) \end{aligned}$$

is an elliptic net.

Proof. We need to show that W satisfies

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

for all $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s} \in \mathbb{Z}^n$.

First, if $\mathbf{r} = \mathbf{0}$, then we have

$$\begin{aligned} &W(\mathbf{q}+\mathbf{s})W(\mathbf{q})W(\mathbf{p}+\mathbf{s})W(\mathbf{p}) + W(\mathbf{p}+\mathbf{s})W(-\mathbf{p})W(\mathbf{q}+\mathbf{s})W(\mathbf{q}) \\ &\qquad = \tilde{\Psi}_{\mathbf{q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q}+\mathbf{s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p}+\mathbf{s}}(\mathbf{z})\Big(\tilde{\Psi}_{\mathbf{p}}(\mathbf{z}) + \tilde{\Psi}_{-\mathbf{p}}(\mathbf{z})\Big) = 0. \end{aligned}$$

The latter equality can be seen to hold from the definition of $\tilde{\Psi}_{\mathbf{v}}$ and the fact that σ is an odd function. Similarly, (3.15) can be seen to hold if either $\mathbf{p} = \mathbf{0}$ or $\mathbf{q} = \mathbf{0}$.

If $\mathbf{s} = \mathbf{0}$, then we have

$$\begin{aligned} &W(\mathbf{p}+\mathbf{q})W(\mathbf{p}-\mathbf{q})W(\mathbf{r})^2 + W(\mathbf{q}+\mathbf{r})W(\mathbf{q}-\mathbf{r})W(\mathbf{p})^2 + W(\mathbf{r}+\mathbf{p})W(\mathbf{r}-\mathbf{p})W(\mathbf{q})^2 \\ &\quad = \tilde{\Psi}_{\mathbf{p}+\mathbf{q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p}-\mathbf{q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r}}(\mathbf{z})^2 + \tilde{\Psi}_{\mathbf{q}+\mathbf{r}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q}-\mathbf{r}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p}}(\mathbf{z})^2 + \tilde{\Psi}_{\mathbf{r}+\mathbf{p}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r}-\mathbf{p}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q}}(\mathbf{z})^2. \end{aligned}$$

From Lemma 3.4.4, we have

$$\begin{aligned} &\frac{\tilde{\Psi}_{\mathbf{p}+\mathbf{q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p}-\mathbf{q}}(\mathbf{z})}{\tilde{\Psi}_{\mathbf{p}}(\mathbf{z})^2\tilde{\Psi}_{\mathbf{q}}(\mathbf{z})^2} + \frac{\tilde{\Psi}_{\mathbf{q}+\mathbf{r}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q}-\mathbf{r}}(\mathbf{z})}{\tilde{\Psi}_{\mathbf{q}}(\mathbf{z})^2\tilde{\Psi}_{\mathbf{r}}(\mathbf{z})^2} + \frac{\tilde{\Psi}_{\mathbf{r}+\mathbf{p}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r}-\mathbf{p}}(\mathbf{z})}{\tilde{\Psi}_{\mathbf{r}}(\mathbf{z})^2\tilde{\Psi}_{\mathbf{p}}(\mathbf{z})^2} \\ &\qquad = \wp(\mathbf{q}\cdot\mathbf{z}) - \wp(\mathbf{p}\cdot\mathbf{z}) + \wp(\mathbf{r}\cdot\mathbf{z}) - \wp(\mathbf{q}\cdot\mathbf{z}) + \wp(\mathbf{p}\cdot\mathbf{z}) - \wp(\mathbf{r}\cdot\mathbf{z}) = 0. \end{aligned}$$

Hence

$$\tilde{\Psi}_{\mathbf{p+q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p-q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r}}(\mathbf{z})^2 + \tilde{\Psi}_{\mathbf{q+r}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q-r}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p}}(\mathbf{z})^2 + \tilde{\Psi}_{\mathbf{r+p}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r-p}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q}}(\mathbf{z})^2 = 0.$$

If none of $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s} = \mathbf{0}$, we have

$$\begin{aligned}\frac{\tilde{\Psi}_{\mathbf{p+q+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p-q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{s}}(\mathbf{z})}{\tilde{\Psi}_{\mathbf{p+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q}}(\mathbf{z})} &= \frac{\sigma(\mathbf{p}\cdot\mathbf{z}+\mathbf{q}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z})\sigma(\mathbf{p}\cdot\mathbf{z}-\mathbf{q}\cdot\mathbf{z})\sigma(\mathbf{s}\cdot\mathbf{z})}{\sigma(\mathbf{p}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z})\sigma(\mathbf{p}\cdot\mathbf{z})\sigma(\mathbf{q}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z})\sigma(\mathbf{q}\cdot\mathbf{z})} \\ &= \zeta(\mathbf{p}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z}) - \zeta(\mathbf{p}\cdot\mathbf{z}) - \zeta(\mathbf{q}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z}) + \zeta(\mathbf{q}\cdot\mathbf{z}).\end{aligned}$$

Hence

$$\frac{\tilde{\Psi}_{\mathbf{p+q+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p-q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{s}}(\mathbf{z})}{\tilde{\Psi}_{\mathbf{p+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q}}(\mathbf{z})} + \frac{\tilde{\Psi}_{\mathbf{q+r+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q-r}}(\mathbf{z})\tilde{\Psi}_{\mathbf{s}}(\mathbf{z})}{\tilde{\Psi}_{\mathbf{q+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r}}(\mathbf{z})} + \frac{\tilde{\Psi}_{\mathbf{r+p+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r-p}}(\mathbf{z})\tilde{\Psi}_{\mathbf{s}}(\mathbf{z})}{\tilde{\Psi}_{\mathbf{r+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p}}(\mathbf{z})}$$

$$\begin{aligned}&= \zeta(\mathbf{p}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z}) - \zeta(\mathbf{p}\cdot\mathbf{z}) - \zeta(\mathbf{q}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z}) + \zeta(\mathbf{q}\cdot\mathbf{z}) \\ &+ \zeta(\mathbf{q}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z}) - \zeta(\mathbf{q}\cdot\mathbf{z}) - \zeta(\mathbf{r}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z}) + \zeta(\mathbf{r}\cdot\mathbf{z}) \\ &+ \zeta(\mathbf{r}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z}) - \zeta(\mathbf{r}\cdot\mathbf{z}) - \zeta(\mathbf{p}\cdot\mathbf{z}+\mathbf{s}\cdot\mathbf{z}) + \zeta(\mathbf{p}\cdot\mathbf{z}) = 0.\end{aligned}$$

Since $\tilde{\Psi}_{\mathbf{s}}(\mathbf{z}) \neq 0$, we have

$$\begin{aligned}&\tilde{\Psi}_{\mathbf{p+q+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p-q}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r}}(\mathbf{z}) \\ &\qquad + \tilde{\Psi}_{\mathbf{q+r+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q-r}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{p}}(\mathbf{z}) \\ &\qquad\qquad + \tilde{\Psi}_{\mathbf{r+p+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{r-p}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q+s}}(\mathbf{z})\tilde{\Psi}_{\mathbf{q}}(\mathbf{z}) = 0.\end{aligned}$$

□

3.5 Valuations of net polynomials

For the elliptic curve E/K defined by (3.12), let $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$, where $P_i = (x_i, y_i)$. Let

$$S = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x_1, y_1, \cdots, x_r, y_r],$$

and consider the polynomial ring

$$\mathcal{R}_r = S[(x_i - x_j)^{-1}]_{1\leq i<j\leq r}/\langle f(x_i, y_i)\rangle_{1\leq i\leq r},$$

where f is the function defined by

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

Let $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$, then Stange [9, Section 4] has shown the existence of $\Psi_{\mathbf{v}}, \Phi_{\mathbf{v}}, \Omega_{\mathbf{v}} \in \mathcal{R}_r$ such that

$$\mathbf{v}\cdot\mathbf{P} = v_1P_1 + v_2P_2 + \cdots + v_rP_r = \Big(\frac{\Phi_{\mathbf{v}}(\mathbf{P})}{\Psi^2_{\mathbf{v}}(\mathbf{P})}, \frac{\Omega_{\mathbf{v}}(\mathbf{P})}{\Psi^3_{\mathbf{v}}(\mathbf{P})}\Big). \tag{3.16}$$

We refer to $\Psi_{\mathbf{v}}$ as the $\mathbf{v}^{th}$ *net polynomial* associated to E. Note that $\Psi_{n\mathbf{e_i}}(\mathbf{P}) = \psi_n(P_i)$, the n^{th} division polynomial associated to E evaluated at P_i.

For $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$ let $\mathbf{z} = (z_1, z_2, \ldots, z_r) \in \mathbb{C}^r$ be such that for each $1 \leq i \leq r$ we have $P_i = (\wp(z_i), \wp'(z_i)/2)$, from [8, VI.3.6]. Thus for $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$ we may consider $\tilde{\Psi}_{\mathbf{v}} : \mathbb{C}^r \to K$, by setting $\tilde{\Psi}_{\mathbf{v}}(\mathbf{z}) := \Psi_{\mathbf{v}}((\wp(z_1), \wp'(z_1)/2), \ldots, (\wp(z_r), \wp'(z_r)/2)) = \Psi_{\mathbf{v}}(\mathbf{P})$.

Throughout, we let K be a number field with ring of integers $\mathcal{O}_K$, and R a principal ideal domain with $\mathrm{frac}(R) = K$. For a prime ideal $\mathfrak{p}$, we let $\nu_{\mathfrak{p}}$ denote the valuation associated to $\mathfrak{p}$. We give the following theorem on the $\mathfrak{p}$-adic valuation of $\Psi_{\mathbf{v}}(\mathbf{P})$.

Theorem 3.5.1. Let E/K be an elliptic curve given by the Weierstrass equation (3.12) with $a_i \in \mathcal{O}_K$ for $i = 1, 2, 3, 4, 6$. Let $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$ be such that P_i, for $1 \leq i \leq r$, and $P_i \pm P_j$, for $1 \leq i < j \leq r$, are not the point at infinity. Moreover assume that $P_i \pmod{\mathfrak{p}} \neq \mathcal{O}$, for $1 \leq i \leq r$, and $P_i \pm P_j \pmod{\mathfrak{p}} \neq \mathcal{O}$, for $1 \leq i < j \leq r$. We also assume that $\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) \geq 0$ for all $\mathbf{v}$.

Then the following are equivalent:

(a) There exists $1 \leq i \leq r$ such that

$$\nu_{\mathfrak{p}}(\Psi_{2\mathbf{e_i}}(\mathbf{P})) > 0 \text{ and } \nu_{\mathfrak{p}}(\Psi_{3\mathbf{e_i}}(\mathbf{P})) > 0.$$

(b) There exists $1 \leq i \leq r$ such that for all $n \geq 2$ we have $\nu_{\mathfrak{p}}(\Psi_{n\mathbf{e_i}}(\mathbf{P})) > 0$.

(c) There exists $\mathbf{v} \in \mathbb{Z}^r$ and $1 \leq i \leq r$ such that

$$\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) > 0 \text{ and } \nu_{\mathfrak{p}}(\Psi_{\mathbf{v}+\mathbf{e_i}}(\mathbf{P})) > 0.$$

(d) There exists $\mathbf{v} \in \mathbb{Z}^r$ such that

$$\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) > 0 \text{ and } \nu_{\mathfrak{p}}(\Phi_{\mathbf{v}}(\mathbf{P})) > 0.$$

(e) There exists $1 \leq i \leq r$ such that $P_i \pmod{\mathfrak{p}}$ is singular.

Proof. $(a) \Longrightarrow (b)$. Observe that $\Psi_{ne_i}(\mathbf{P}) = \psi_n(P_i)$. So the result follows from Theorem 3.3.1.

$(b) \Longrightarrow (c)$ is clear.

$(c) \Longleftrightarrow (d)$. From Lemma 3.4.4 we know that for all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^r$ we have

$$\wp(\mathbf{v} \cdot \mathbf{z}) - \wp(\mathbf{u} \cdot \mathbf{z}) = -\frac{\tilde{\Psi}_{\mathbf{v}+\mathbf{u}}(\mathbf{z})\tilde{\Psi}_{\mathbf{v}-\mathbf{u}}(\mathbf{z})}{\tilde{\Psi}^2_{\mathbf{v}}(\mathbf{z})\tilde{\Psi}^2_{\mathbf{u}}(\mathbf{z})}. \tag{3.17}$$

Setting $\mathbf{u} = \mathbf{e_i}$ in equation (3.17) we have

$$\tilde{\Psi}^2_{\mathbf{v}}(\mathbf{z})\wp(\mathbf{v} \cdot \mathbf{z}) = \tilde{\Psi}^2_{\mathbf{v}}(\mathbf{z})x_i - \tilde{\Psi}_{\mathbf{v}+\mathbf{e_i}}(\mathbf{z})\tilde{\Psi}_{\mathbf{v}-\mathbf{e_i}}(\mathbf{z}), \tag{3.18}$$

where x_i is the x-coordinate of P_i. Now we observe that

$$\tilde{\Psi}^2_{\mathbf{v}}(\mathbf{z})\wp(\mathbf{v} \cdot \mathbf{z}) = \Phi_{\mathbf{v}}(\mathbf{P}),$$

where $\Phi_{\mathbf{v}}(\mathbf{P})$ is defined in (3.16). Thus from (3.18) we have

$$\Phi_{\mathbf{v}}(\mathbf{P}) = \Psi^2_{\mathbf{v}}(\mathbf{P})x_i - \Psi_{\mathbf{v}+\mathbf{e_i}}(\mathbf{P})\Psi_{\mathbf{v}-\mathbf{e_i}}(\mathbf{P}). \tag{3.19}$$

Now it is straightforward to conclude from (3.19) that (c) and (d) are equivalent.

$(c) \Longrightarrow (e)$. For a prime ideal $\mathfrak{p}$ of R, we assume that $k_{\mathfrak{p}}$ is the residue field associated to $\mathfrak{p}$. We observe that $\Psi_{\mathbf{v}}(\mathbf{P}) \pmod{\mathfrak{p}}$ is an elliptic net with values in $k_{\mathfrak{p}}$. (Note that under the conditions of the theorem $\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) \geq 0$ and therefore the reduction mod $\mathfrak{p}$ is well defined.) Under the assumptions of (c) we have $\Psi_{\mathbf{v}}(\mathbf{P}) \pmod{\mathfrak{p}} = 0$ and

$\Psi_{\mathbf{v}+\mathbf{e_i}}(\mathbf{P}) \pmod{\mathfrak{p}} = 0$ in $k_\mathfrak{p}$. Now if the zero set of $\Psi_\mathbf{v}(\mathbf{P}) \pmod{\mathfrak{p}}$ forms a lattice then we have $\Psi_{\mathbf{e_i}}(\mathbf{P}) \pmod{\mathfrak{p}} = \psi_1(P_i) \pmod{\mathfrak{p}} = 0$ which is a contradiction, since $\psi_1 = 1$. So the zero set of $\Psi_\mathbf{v}(\mathbf{P}) \pmod{\mathfrak{p}}$ does not form a lattice and thus by Theorem 2.2.14 we conclude that $\Psi_\mathbf{v}(\mathbf{P}) \pmod{\mathfrak{p}}$ does not have a unique zero-rank of apparition (with respect to $\{(P_1, \mathcal{O}, \ldots, \mathcal{O}), \ldots, (\mathcal{O}, \mathcal{O} \ldots, P_r)\}$). So there exists $1 \leq i \leq r$ such that $\Psi_{n\mathbf{e_i}}(\mathbf{P}) \pmod{\mathfrak{p}}$ does not have a unique zero-rank of apparition. Since $\Psi_{n\mathbf{e_i}}(\mathbf{P})$ is an elliptic sequence with values in $k_\mathfrak{p}$ which does not have a unique $\mathfrak{p}$-rank of apparition, thus from Lemma 2.1.15 we conclude that $\nu_\mathfrak{p}(\Psi_{3\mathbf{e_i}}(\mathbf{P})) = \nu_\mathfrak{p}(\psi_3(P_i)) > 0$ and $\nu_\mathfrak{p}(\Psi_{4\mathbf{e_i}}(\mathbf{P})) = \nu_\mathfrak{p}(\psi_4(P_i)) > 0$. Now since condition (c) in Theorem 3.3.1 is satisfied, we conclude from Theorem 3.3.1 that $P_i \pmod{\mathfrak{p}}$ is singular.

$(e) \implies (a)$ Since $P_i \pmod{\mathfrak{p}}$ is singular, then from Theorem 3.3.1 we know that $\nu_\mathfrak{p}(\psi_2(P_i)) > 0$ and $\nu_\mathfrak{p}(\psi_3(P_i)) > 0$. Now the result follows since $\psi_n(P_i) = \Psi_{ne_i}(\mathbf{P})$ for $n \in \mathbb{N}$. □

We note that if R is a principal ideal domain with $\mathrm{frac}(R) = K$ and E/K is an elliptic curve defined by (3.12) with $a_i \in R$ for $i = 1, 2, 3, 4, 6$, then by Proposition 1.1.4, any point $P \in E(K)$ has a unique representation (up to units) of the form

$$P = \left(\frac{A_P}{D_P^2}, \frac{B_P}{D_P^3}\right).$$

For $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$, and $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$, we define the *elliptic denominator net* $(D_{\mathbf{v}\cdot\mathbf{P}})$ by

$$\mathbf{v} \cdot \mathbf{P} = v_1P_1 + v_2P_2 + \cdots + v_rP_r = \left(\frac{A_{\mathbf{v}\cdot\mathbf{P}}}{D_{\mathbf{v}\cdot\mathbf{P}}^2}, \frac{B_{\mathbf{v}\cdot\mathbf{P}}}{D_{\mathbf{v}\cdot\mathbf{P}}^3}\right).$$

We are interested in the relation between the elliptic denominator net element $D_{\mathbf{v}\cdot\mathbf{P}}$ and the value of the $\mathbf{v}^{th}$ net polynomial $\Psi_\mathbf{v}$ at $\mathbf{P}$. Note that if $\mathbf{v} \cdot \mathbf{P} \neq \mathcal{O}$ then $D_{\mathbf{v}\cdot\mathbf{P}} \in R$, however $\Psi_\mathbf{v}(\mathbf{P}) \in K$, similar to the case of the division polynomials. Under the assumptions that $P_i \neq \mathcal{O}$ for $1 \leq i \leq r$ and $P_i + P_j \neq \mathcal{O}$ for $1 \leq i < j \leq r$, it follows that $D_{P_i} \neq 0$ for $1 \leq i \leq r$ and $D_{P_i+P_j} \neq 0$ for $1 \leq i < j \leq r$. Letting $A_{ii} = D_{P_i}$ for

$1 \leq i \leq r$ and $A_{ij} = D_{P_i+P_j}/D_{P_i}D_{P_j}$ for $1 \leq i < j \leq r$, we define the quadratic form

$$f_{\mathbf{v}}(\mathbf{P}) = \prod_{1\leq i\leq j\leq r} A_{ij}^{v_i v_j}. \tag{3.20}$$

In [9] it is shown that $f_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P})$, $\hat{\Phi}_{\mathbf{v}}(\mathbf{P}) := f_{\mathbf{v}}^2(\mathbf{P})\Phi_{\mathbf{v}}(\mathbf{P})$, and $\hat{\Omega}_{\mathbf{v}}(\mathbf{P}) := f_{\mathbf{v}}^3(\mathbf{P})\Omega_{\mathbf{v}}(\mathbf{P})$ are integral and moreover

$$\mathbf{v}\cdot\mathbf{P} = v_1P_1 + v_2P_2 + \cdots + v_rP_r = \Big(\frac{\hat{\Phi}_{\mathbf{v}}(\mathbf{P})}{f_{\mathbf{v}}^2(\mathbf{P})\Psi_{\mathbf{v}}^2(\mathbf{P})}, \frac{\hat{\Omega}_{\mathbf{v}}(\mathbf{P})}{f_{\mathbf{v}}^3(\mathbf{P})\Psi_{\mathbf{v}}^3(\mathbf{P})}\Big).$$

The following proposition, analogous to Proposition 3.3.2, relates the $\mathfrak{p}$-adic valuations of $\Psi_{\mathbf{v}}(\mathbf{P})$ and $D_{\mathbf{v}\cdot\mathbf{P}}$

Proposition 3.5.2. Suppose that E, $\mathbf{P} = (P_1, P_2, \ldots, P_r)$, and $\mathfrak{p}$ satisfy the assumptions of Theorem 3.5.1. Moreover, assume that R is a principal ideal domain with $\mathrm{frac}(R) = K$, and $P_i \pmod{\mathfrak{p}}$ is non-singular for all i. Then,

$$\nu_{\mathfrak{p}}(D_{\mathbf{v}\cdot\mathbf{P}}) = \nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})).$$

Proof. From the preceding discussion, we have

$$\frac{f_{\mathbf{v}}^2(\mathbf{P})\Phi_{\mathbf{v}}(\mathbf{P})}{f_{\mathbf{v}}^2(\mathbf{P})\Psi_{\mathbf{v}}^2(\mathbf{P})} = \frac{A_{\mathbf{v}\cdot\mathbf{P}}}{D_{\mathbf{v}\cdot\mathbf{P}}^2},$$

with $f_{\mathbf{v}}^2(\mathbf{P})\Phi_{\mathbf{v}}(\mathbf{P}), f_{\mathbf{v}}^2(\mathbf{P})\Psi_{\mathbf{v}}^2(\mathbf{P}), A_{\mathbf{v}\cdot\mathbf{P}}, D_{\mathbf{v}\cdot\mathbf{P}}^2 \in R$. Hence

$$\nu_{\mathfrak{p}}(f_{\mathbf{v}}^2(\mathbf{P})\Phi_{\mathbf{v}}(\mathbf{P})) = \nu_{\mathfrak{p}}(f_{\mathbf{v}}^2(\mathbf{P})) + \nu_{\mathfrak{p}}(\Phi_{\mathbf{v}}(\mathbf{P})) \geq 0,$$

and

$$\nu_{\mathfrak{p}}(f_{\mathbf{v}}^2(\mathbf{P})\Psi_{\mathbf{v}}^2(\mathbf{P})) = \nu_{\mathfrak{p}}(f_{\mathbf{v}}^2(\mathbf{P})) + \nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}^2(\mathbf{P})) \geq 0.$$

Then, since $P_i \not\equiv \mathcal{O} \pmod{\mathfrak{p}}$, and $P_i + P_j \not\equiv \mathcal{O} \pmod{\mathfrak{p}}$, it follows from (3.20) that

$$\nu_{\mathfrak{p}}(f_{\mathbf{v}}(\mathbf{P})) = 0.$$

Thus

$$\nu_{\mathfrak{p}}(\Phi_{\mathbf{v}}(\mathbf{P})) \geq 0 \text{ and } \nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}^2(\mathbf{P})) \geq 0.$$

Since $P_i \pmod{\mathfrak{p}}$ is assumed to be non-singular for all i, it follows from Theorem 3.5.1 that not both $\nu_{\mathfrak{p}}(\Phi_{\mathbf{v}}(\mathbf{P})) > 0$ and $\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}^2(\mathbf{P})) > 0$.

Finally, since $(A_{\mathbf{v}\cdot\mathbf{P}}, D_{\mathbf{v}\cdot\mathbf{P}}) = 1$ and

$$\nu_{\mathfrak{p}}(\Phi_{\mathbf{v}}(\mathbf{P})) - \nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}^2(\mathbf{P})) = \nu_{\mathfrak{p}}(A_{\mathbf{v}\cdot\mathbf{P}}) - \nu_{\mathfrak{p}}(D_{\mathbf{v}\cdot\mathbf{P}}^2),$$

we have

$$\nu_{\mathfrak{p}}(D_{\mathbf{v}\cdot\mathbf{P}}) = \nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})).$$

□

We remark that if K is a number field, R a principal ideal domain with $\mathrm{frac}(R) = K$, and E/K is an elliptic curve given by (3.12) with $a_i \in R$ for $i = 1, 2, 3, 4, 6$, and $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$ is a tuple of points satisfying $P_i \neq \mathcal{O}$, and $P_i \pm P_j \neq \mathcal{O}$, then the preceding proposition shows that

$$\nu_{\mathfrak{p}}(D_{\mathbf{v}\cdot\mathbf{P}}) = \nu_{\mathfrak{p}}(f_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P})) \tag{3.21}$$

for all but finitely many primes. We believe that (3.21) holds for all primes $\mathfrak{p} \subset R$, provided that the points $P_i \pmod{\mathfrak{p}}$ are non-singular.

Conjecture 3.5.3. Let K be a number field, and R a principal ideal domain with $\mathrm{frac}(R) = K$. Let E/K be an elliptic curve defined by (3.12) with $a_i \in R$ for $i = 1, 2, 3, 4, 6$, and $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$. We also define the set

$$S := \{\mathfrak{p} \subset R : P_i \equiv \mathcal{O} \pmod{\mathfrak{p}}, \text{ or } P_i \pm P_j \equiv \mathcal{O} \pmod{\mathfrak{p}}\}.$$

Under the assumptions that the net polynomials $\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) \geq 0$ for all $\mathfrak{p} \notin S$ and all $\mathbf{v} \in \mathbb{Z}^r$, and that the points P_i are non-singular $\pmod{\mathfrak{p}}$ for all primes of bad reduction $\mathfrak{p}$, we have

$$D_{\mathbf{v}\cdot\mathbf{P}} = u f_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P}),$$

where u is a unit in R.

We remark that under the assumptions of Conjecture 3.5.3, it follows from Proposition 3.5.2 that

$$\nu_{\mathfrak{p}}(D_{\mathbf{v}\cdot\mathbf{P}}) = \nu_{\mathfrak{p}}(f_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P})),$$

for all $\mathfrak{p} \notin S$. It therefore remains to be shown that the same is true for the finitely many primes $\mathfrak{p} \in S$. Ayad [1] has proved this result for the rank 1 case, where $\mathbf{v} = n \in \mathbb{Z}$, and $\mathbf{P} = P \in E(K)$.

Chapter 4

Applications to Diophantine Equations

4.1 From Diophantine equations to elliptic nets

In this chapter, we discuss how our results on elliptic nets can be applied in solving certain Diophantine equations.

A *Diophantine equation* is a polynomial equation in several variables, to which we restrict the solutions to integers. For example, the equation

$$X^n + Y^n = Z^n \tag{4.1}$$

is known to have infinitely many solutions $(X, Y, Z) \in \mathbb{Z}^3$ provided that $n = 1$ or 2. For $n > 2$ it was famously conjectured by Fermat in 1637, and proved by Wiles in 1995, that (4.1) has no non-trivial integer solutions.

Here we are interested in finding solutions $(X, Y, Z) \in \mathbb{Z}^3$ to the Diophantine equation

$$Y^2 = X^3 + dZ^{12}, \tag{4.2}$$

under the conditions that $d \mid Z$ and $\gcd(X, Y, Z) = 1$. By dividing through by Z^{12} and making the substitutions

$$y = Y/Z^6 \text{ and } x = X/Z^4,$$

we observe that any integer solution (X, Y, Z) of (4.2) corresponds to a rational point $P = (\frac{A}{D^2}, \frac{B}{D^3}) \in E_d(\mathbb{Q})$, where D is a perfect square and E_d is given by

$$E_d : y^2 = x^3 + d. \tag{4.3}$$

In order to make the above correspondence explicit, we first define the sets

$$C_d := \{(X, Y, Z) \in \mathbb{Z}^3 : Y^2 = X^3 + dZ^{12},\ \gcd(X, Y, Z) = 1,\ \text{and } d \mid Z\}$$

and

$$E_d^s(\mathbb{Q}) := \left\{ \left(\frac{A}{D^2}, \frac{B}{D^3} \right) \in E_d(\mathbb{Q}) : d \mid D,\ \text{and } D \text{ is a perfect square} \right\}.$$

It is clear from the preceding discussion that the following proposition holds.

Proposition 4.1.1. The map

$$\begin{array}{rccc} \varphi_d : & C_d & \longrightarrow & E_d^s(\mathbb{Q}) \\ & (X, Y, Z) & \longmapsto & (X/Z^4, Y/Z^6). \end{array}$$

is well defined.

Next we explain how we can use elliptic nets to study the set $E_d^s(\mathbb{Q})$.

Proposition 4.1.2. For E_d given by (4.3), let $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E_d(\mathbb{Q})^r$ and $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$. We also let $\Psi_{\mathbf{v}}(\mathbf{P})$ denote the $\mathbf{v}^{th}$ net polynomial associated to E_d and $\mathbf{P}$, and $f(\mathbf{v})$ be the quadratic form defined by (3.20). We also define the set

$$S := \{p \text{ prime} : P_i \equiv \mathcal{O} \pmod p),\ P_i \pm P_j \equiv \mathcal{O} (\text{mod } p),\ \text{or } P_i (\text{mod } p) \text{ is singular}\}.$$

Then, if $\mathbf{v} \cdot \mathbf{P} \in E_d^s$, there exists an S-unit c,with p-adic valuation $\nu_p(c) = 0$ or 1 for all $p \in S$, such that $cf(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P})$ is a perfect square.

Proof. We let $(D_{\mathbf{v}\cdot\mathbf{P}})$ be the elliptic denominator net (described in §3.6) associated to E_d and $\mathbf{P}$. We recall that by taking

$$f(\mathbf{v}) = \prod_{1 \le i \le j \le r} A_{ij}^{v_i v_j},$$

where $A_{ii} = D_{P_i}$ for $1 \le i \le r$ and $A_{ij} = D_{P_i+P_j}/D_{P_i}D_{P_j}$ for $1 \le i < j \le r$, we have $f_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P}) \in \mathbb{Z}$.

For a prime $p \notin S$, it follows from Proposition 3.5.2 that

$$\nu_p(D_{\mathbf{v}\cdot\mathbf{P}}) = \nu_p(f_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P})),$$

since $\nu_p(f_{\mathbf{v}}(\mathbf{P})) = 0$ for all $p \notin S$.

Under the assumption that $\mathbf{v} \cdot \mathbf{P} \in E_d^s(\mathbb{Q})$, we have $D_{\mathbf{v}\cdot\mathbf{P}}$ is a perfect square. Thus for all but finitely many primes p, we have that $\nu_p(f_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P}))$ is even. Furthermore, the primes for which $\nu_p(f_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P}))$ is not necessarily even are precisely the primes such that one of the following hold:

(i) $P_i \equiv \mathcal{O} \pmod{p}$ for some $1 \leq i \leq r$,

(ii) $P_i \pm P_j \equiv \mathcal{O} \pmod{p}$ for some $1 \leq i < j \leq r$,

(iii) $P_i \pmod{p}$ is singular for some $1 \leq i \leq r$.

These are precisely the primes in S. Thus, we can choose c to be an S-unit satisfying $\nu_p(c) = 0$ or 1 for all $p \in S$ such that $\nu_p(cf_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P}))$ is even for all p. Replacing c with $-c$ if necessary, it follows that $cf_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P})$ is a perfect square. □

Letting $\mathbf{P} = (P_1, \ldots, P_r) \in E(\mathbb{Q})^r$ and taking $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$, we recall that $\mathbf{v} \cdot \mathbf{P} \in E_d^s(\mathbb{Q})$ provided that $D_{\mathbf{v}\cdot\mathbf{P}}$ is a perfect square and $d \mid D_{\mathbf{v}\cdot\mathbf{P}}$. We note that Proposition 4.1.2 gives a means of testing whether $D_{\mathbf{v}\cdot\mathbf{P}}$ is a perfect square. We also need to be able to check the condition that $d \mid D_{\mathbf{v}\cdot\mathbf{P}}$.

Letting p be a prime dividing d, we note that if p satisfies the conditions of Proposition 3.5.2 then we have

$$\nu_p(D_{\mathbf{v}\cdot\mathbf{P}}) = \nu_p(f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P})),$$

hence $\nu_p(f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P})) > 0$. We define

$$\Lambda_p := \{\mathbf{v} \in \mathbb{Z}^r : \nu_p(f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P})) > 0\},$$

and

$$\Lambda_d := \bigcap_{p \mid d} \Lambda_p.$$

Thus, if every prime p dividing d satisfies the assumptions of Proposition 3.5.2, then

$$\mathbf{v} \cdot \mathbf{P} \in E_d^s(\mathbb{Q}) \Longrightarrow \mathbf{v} \in \Lambda_d.$$

Letting $W(\mathbf{v}) = f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P})$, we see that that the set $E_d^s(\mathbb{Q})$ is empty, provided that none of the 2^{k+1} elliptic nets

$$\pm \prod_k (p_k^{\alpha_k}) W|_{\Lambda_d},$$

contain perfect squares, where $\alpha_k \in \{0, 1\}$, and p_k are primes in S as defined in Proposition 4.1.2.

4.2 Squares in elliptic nets

In this section we give a method for finding terms in a non-degenerate elliptic net $W : A \to \mathbb{Z}$ with an appropriate basis $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$, which are potentially perfect squares. Rather than searching for squares directly, our approach is to show that if v lies in certain equivalence classes in A, then $W(v)$ is not a perfect square.

We note that $W(v)$ is a perfect square if and only if the Legendre symbol

$$\left(\frac{W(v)}{p}\right) \neq -1$$

for every prime p. This motivates looking at the sets

$$S_p := \{v \in A : \left(\frac{W(v)}{p}\right) \neq -1\}.$$

Letting $\mathcal{PR}$ denote the set of all primes, we see that there exists $z \in \mathbb{Z}$ such that

$$W(v) = z^2 \iff v \in \bigcap_{p \in \mathcal{PR}} S_p.$$

The next lemma provides an explicit description of the set S_p.

Lemma 4.2.1. For a non-degenerate elliptic net $W : A \to \mathbb{Z}$, there exists $a_1, a_2, \ldots, a_k \in A$ such that

$$S_p = \bigcup_{i=1}^{k} (a_i + L_p),$$

where L_p is a subgroup of A depending on p.

Proof. Let $W : A \to \mathbb{Z}$ be a non-degenerate elliptic net and let p be a prime such that

the elliptic net

$$\begin{array}{rccc} W_p: & A & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ & v & \longmapsto & W(v) \bmod p, \end{array}$$

has a unique zero-rank of apparition $(\rho_1, \rho_2, \ldots, \rho_r)$. It then follows from Theorem 2.2.14 that the zero set Λ of W_p is a lattice. Hence Theorem 2.2.30 holds and we have

$$W_p\left((\sum_{i=1}^{r} n_i\lambda_i) + v\right) = \prod_{0\le i<j\le r} \left(a(\lambda_j)^{n_j^2}\chi(\lambda_j, v)^{n_j}\chi(\lambda_i, \lambda_j)^{n_i n_j}\right) W_p(v),$$

for all $v \in A$, $\lambda_1, \lambda_2, \ldots, \lambda_r \in \Lambda$ and integers n_i. In particular, we see that

$$W_p\left((\sum_{i=1}^{r} 2n_i\lambda_i) + v\right) = \prod_{0\le i<j\le r} \left(a(\lambda_j)^{2n_j^2}\chi(\lambda_j, v)^{n_j}\chi(\lambda_i, \lambda_j)^{2n_i n_j}\right)^2 W_p(v).$$

Thus, if we let

$$L'_p = \langle \rho_1 b_1, \rho_2 b_2, \ldots, \rho_r b_r \rangle,$$

then we see that the map

$$\begin{array}{rccc} \tilde{W}_p: & A & \longrightarrow & \{0, \pm 1\} \\ & v & \longmapsto & \left(\frac{W(v)}{p}\right), \end{array}$$

is invariant under addition with elements of $L_p := 2L'_p$. Setting

$$M_p := \{v \in A/L_p : \left(\frac{W(v)}{p}\right) \neq -1\}, \tag{4.4}$$

it follows that

$$S_p = \pi_p^{-1}(M_p) = \bigcup_{i=1}^{k} (a_i + L_p),$$

where π_p is the natural projection

$$\pi_p : A \to A/L_p.$$

This completes the proof since $|M_p|$ is finite. □

Next we give an example to illustrate the periodicity of the Legendre symbol in an elliptic net.

Example 4.2.2. We consider the rank 2 elliptic net

$$\begin{array}{rccc} W: & \mathbb{Z}^2 & \longrightarrow & \mathbb{Z} \\ & \mathbf{v} & \longmapsto & f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P}), \end{array}$$

where $\Psi_{\mathbf{v}}(\mathbf{P})$ is the $\mathbf{v}^{th}$ net polynomial associated to the elliptic curve

$$E_{-11} : y^2 = x^3 - 11$$

and points $\mathbf{P} = (P, Q) = \big((3, 4), (15, 58)\big)$. Here $f(\mathbf{v}) = 2^{v_1 v_2}$ is as in Theorem 3.5.1.

We write the elliptic net W as the following array, where $W(\mathbf{v})$ is given by the term in the array indexed by $\mathbf{v}$. For example we have $W(0, 0) = 0$ is the term in the lower left corner, and $W(2, 1) = 51$.

$$\begin{array}{ccccccccc} & & & & \vdots & & & & \\ & & -9886 & -15775 & -30396 & -397241 & 547912280 & & \\ & & -153 & -134 & -1099 & -112698 & -144855449 & & \\ \cdots & & 8 & 3 & -20 & -17083 & -93695568 & & \cdots \\ & & 1 & 2 & 51 & 14446 & -1106143 & & \\ & & 0 & 1 & 116 & 149895 & 2470140424 & & \\ & & & & \vdots & & & & \end{array}$$

Then, W_5 is given by

$$
\begin{array}{ccccccccccccc}
 & & & & & & \vdots & & & & & & \\
 & & 3 & 3 & 0 & 2 & 2 & 0 & 3 & 3 & 0 & 2 & 0 & \\
 & & 4 & 3 & 4 & 4 & 3 & 4 & 4 & 3 & 4 & 4 & 4 & \\
 & & 0 & 1 & 1 & 0 & 4 & 4 & 0 & 1 & 1 & 0 & 4 & \\
 & & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 2 & \\
 & & 2 & 0 & 3 & 3 & 0 & 2 & 2 & 0 & 3 & 3 & 2 & \\
 & & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & \\
 & & 4 & 4 & 0 & 1 & 1 & 0 & 4 & 4 & 0 & 1 & 1 & \\
\cdots & & 4 & 3 & 4 & 4 & 3 & 4 & 4 & 3 & 4 & 4 & 3 & \cdots \\
 & & 0 & 2 & 2 & 0 & 3 & 3 & 0 & 2 & 2 & 0 & 3 & \\
 & & 4 & 4 & 3 & 4 & 4 & 3 & 4 & 4 & 3 & 4 & 4 & \\
 & & 1 & 0 & 4 & 4 & 0 & 1 & 1 & 0 & 4 & 4 & 0 & \\
 & & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & \\
 & & 3 & 3 & 0 & 2 & 2 & 0 & 3 & 3 & 0 & 2 & 2 & \\
 & & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & \\
 & & 0 & 1 & 1 & 0 & 4 & 4 & 0 & 1 & 1 & 0 & 4 & \\
 & & & & & & \vdots & & & & & &
\end{array}
$$

Note that the zero-rank of apparition of W_5 can be seen to be $(3, 6)$.

Then $\tilde{W}_5$ is given by

$$
\begin{array}{cccccccccccc}
 & & & & & \vdots & & & & & & \\
 & - & - & 0 & - & - & 0 & - & - & 0 & - & - & \\
 & + & - & + & + & - & + & + & - & + & + & - & \\
 & \heartsuit & + & + & 0 & + & + & \heartsuit & + & + & 0 & + & \\
 & + & + & - & + & + & - & + & + & - & + & + & \\
 & - & 0 & - & - & 0 & - & - & 0 & - & - & 0 & \\
 & - & + & + & - & + & + & - & + & + & - & + & \\
 & + & + & 0 & + & + & 0 & + & + & 0 & + & + & \\
\cdots & + & - & + & + & - & + & + & - & + & + & - & \cdots \\
 & 0 & - & - & 0 & - & - & 0 & - & - & 0 & - & \\
 & + & + & - & + & + & - & + & + & - & + & + & \\
 & + & 0 & + & + & 0 & + & + & 0 & + & + & 0 & \\
 & - & + & + & - & + & + & - & + & + & - & + & \\
 & - & - & 0 & - & - & 0 & - & - & 0 & - & - & \\
 & + & - & + & + & - & + & + & - & + & + & - & \\
 & \bigstar & + & + & 0 & + & + & \heartsuit & + & + & 0 & + & \\
 & & & & & \vdots & & & & & &
\end{array}
$$

where the $+$ denotes a term with $\left(\frac{W(\mathbf{v})}{5}\right) = 1$, and $-$ denotes a term with $\left(\frac{W(\mathbf{v})}{5}\right) = -1$. We also note that $L_5 = \langle (6,0), (0,12) \rangle$ and for $\mathbf{v} \in L_5$ we indicate $\tilde{W}_5(\mathbf{v})$ by $\heartsuit$, with the exception of $\tilde{W}_5(0,0)$ which is denoted by $\bigstar$.

We remark that $|\{x \in \mathbb{Z}/p\mathbb{Z} : (\frac{x}{p}) \neq -1\}| = (p+1)/2 \approx p/2$, and $|\mathbb{Z}/p\mathbb{Z}| = p$. Hence the probability that a randomly chosen element of $\mathbb{Z}/p\mathbb{Z}$ satisfies $(\frac{x}{p}) \neq -1$ is given by

$$P(x) = \frac{|\{x \in \mathbb{Z}/p\mathbb{Z} : (\frac{x}{p}) \neq -1\}|}{|\mathbb{Z}/p\mathbb{Z}|} \approx \frac{1}{2}.$$

In light of this, we note that the expected size of M_p, as defined in (4.4), can be given by

$$P(x)|A/L_p| \approx \frac{1}{2} \prod_{i=1}^{r} 2\rho_i.$$

Definition 4.2.3. Let $W : A \to \mathbb{Z}$ be a non-degenerate elliptic net with an appropriate basis $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$. Let $\mathcal{P} = \{p_1, p_2, \ldots p_n\}$ be a set of primes such that for each p_i, W_{p_i} has a unique zero-rank of apparition $(\rho_{i1}, \rho_{i2}, \ldots, \rho_{ir})$. We say that $\mathcal{P}$ is *admissible* provided that

$$2^{-n}|A/L_{\mathcal{P}}| < 1,$$

where

$$L_{\mathcal{P}} := \bigcap_{p \in \mathcal{P}} L_p,$$

and the sets L_p are as defined in Proposition 4.1.2.

One may ask the following question.

Question 4.2.4. For any elliptic net W, is it possible to find an admissible set of primes $\mathcal{P}$.

We remark that in practice, for the elliptic nets we are interested in, we had no problem finding admissible sets of primes.

We note that with the notation of the preceding definition, we have

$$|A/L_{\mathcal{P}}| = 2^r \prod_{i=1}^{r} lcm(\rho_{1i}, \rho_{2i}, \ldots, \rho_{ni}).$$

In order to find an admissible set of primes, we precompute the zero-rank of apparitions $(\rho_1, \rho_2, \ldots, \rho_r)$ of W_p, for primes $p < N$, for some large $N \in \mathbb{N}$. We then choose $(n_1, n_2, \ldots, n_r) \in \mathbb{N}^r$, and set

$$\mathcal{P} = \{p \in \mathcal{PR} : \rho_i \mid n_i \text{ for } 1 \leq i \leq r\},$$

and check if the condition

$$2^{r-|\mathcal{P}|} \prod_{i=1}^{r} n_i < 1 \tag{4.5}$$

holds. If (4.5) is satisfied, we conclude that $\mathcal{P}$ is admissible, otherwise we choose a different tuple $(n_1, n_2, \ldots, n_r) \in \mathbb{N}^r$ and repeat the process until we find a set $\mathcal{P}$ which satisfies (4.5).

We remark that for a set of primes $\mathcal{P}$, if we let

$$S'_p := \pi_{\mathcal{P}}(S_p),$$

for the natural projection

$$\pi_{\mathcal{P}} : A \to A/L_{\mathcal{P}},$$

then heuristically, we expect that

$$|\bigcap_{p\in\mathcal{P}} S'_p| = 2^{-n}|A/L_{\mathcal{P}}|.$$

Hence, if $\mathcal{P}$ is an admissible set of primes, we expect

$$\bigcap_{p\in\mathcal{P}} S'_p = \emptyset,$$

since $2^{-n}|A/L_{\mathcal{P}}| < 1$.

Unfortunately this is a stronger result than we can obtain since for each $n_i \in \{0, lcm(\rho_{1i}, \rho_{2i}, \ldots, \rho_{ni})\}$, we have

$$\sum_{i=1}^{r} n_i b_i \in A/L_{\mathcal{P}}$$

and for each $p \in \mathcal{P}$, we necessarily have

$$\sum_{i=1}^{r} n_i b_i \in S'_p,$$

since $p \mid W(\sum_{i=1}^{r} n_i b_i)$. Hence, the best result we can obtain is

$$|\bigcap_{p\in\mathcal{P}} S'_p| = 2^r.$$

Example 4.2.5. Continuing from example 4.2.2, we remark that the points P and Q are integral and non-singular modulo p for every prime p, however $P + Q \equiv \mathcal{O} \bmod 2$ and $P - Q \equiv \mathcal{O} \bmod 2$ and 3. It therefore follows from Proposition 4.1.2 that if

$\mathbf{v} \cdot \mathbf{P} \in E^s_{-11}(\mathbb{Q})$ then one of

$$\pm f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P}),\ \pm 2f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P}),\ \pm 3f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P}),\ \text{or}\ \pm 6f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P})$$

is a perfect square. Since $\left(\frac{-1}{p}\right) = 1$ for all primes $p \equiv 1 \pmod 4$, we note that by only considering primes $p \equiv 1 \pmod 4$ we can ignore the sign of the net. Hence we can study the set $E^s_{-11}(\mathbb{Q})$ by looking for perfect squares in the four nets

$$W(\mathbf{v}),\ 2W(\mathbf{v}),\ 3W(\mathbf{v}),\ \text{and}\ 6W(\mathbf{v}).$$

We first need to find an admissible set of primes $\mathcal{P}$. Letting $(n_1, n_2) = (60060, 60060)$ we find

$$\begin{aligned}\mathcal{P} \ = \ & \{5, 17, 29, 37, 41, 73, 197, 229, 233, 349, 389, 421, 461, 577, 857, 1021, 1249,\\ & 1889, 2029, 2309, 2521, 2729, 4289, 4357, 4621, 8221, 8581, 9241, 13093,\\ & 15361, 15541, 17293, 20641, 24181, 25117, 30757, 36241, 36781, 46381,\\ & 63361, 63841, 82141, 91081, 91309, 91873, 121309, 121441, 122497, 169093,\\ & 170197, 190261, 226777, 326701, 364717, 365509, 366697, 397489, 429661\}.\end{aligned}$$

Then,

$$|\mathcal{P}| = 58$$

and

$$2^{r-|\mathcal{P}|}\prod_{i=1}^{r} n_i = 2^{-56} \cdot 60060^2 \approx 5.006 \cdot 10^{-8}.$$

Hence, $\mathcal{P}$ is an admissible set of primes.

By computer calculation we find

$$\bigcap_{p \in \mathcal{P}} S'_p = \{(0,0), (60060, 0), (0, 60060), (60060, 60060)\},$$

for each of the elliptic nets W, $2W$, $3W$, and $6W$. We therefore conclude that

$$E^s_{-11}(\mathbb{Q}) \subset \{nP + mQ \in E_{-11}(\mathbb{Q}); (n, m) \equiv (0, 0) \bmod (60060, 60060)\}.$$

Proposition 4.2.6. Let $E_{\pm p} : y^2 = x^3 \pm p$ be a rank two elliptic curve, where $p \in \{11, 1737, 43, 67, 73, 83\}$ is prime. Let $P, Q \in E(\mathbb{Q})$ be such that $\langle P, Q\rangle = E(\mathbb{Q})$. Then there exists $n_{\pm p} \in \mathbb{N}$ such that

$$E^s_{\pm p}(\mathbb{Q}) \subset \{nP + mQ : n, m \equiv 0 \bmod n_{\pm p}\}.$$

Proof. The proof is computational.

For each prime $p \in \{11, 17, 37, 43, 67, 73, 83\}$ such that $E_{\pm p}$ is a rank two elliptic curve, In the following table we give a natural number $n_{\pm p}$, the size of the admissible set $\mathcal{P}$, and the S-units c, used to show

$$E^s_{\pm p}(\mathbb{Q}) \subset \{nP + mQ : n, m \equiv 0 \bmod n_{\pm p}\}.$$

$E_{\pm p}$	$n_{\pm p}$	$\lvert\mathcal{P}\rvert$	c
E_{-11}	60060	58	1,2,3,6
E_{17}	8568	42	1
E_{37}	18648	48	1,2
E_{43}	93912	55	1,2,3,6,7,14,21,42
E_{-67}	438984	48	1,2,3,5,6,10,15,30
E_{73}	220752	45	1
E_{-83}	271908	52	1,2,3,5,6,10,15,30

□

List of notation

A	Finite rank free Abelian group
$\mathcal{B}$	Basis for A
$\langle b_1, b_2, \ldots, b_r \rangle$	Group generated by $\{b_1, b_2, \ldots, b_r\}$
R	Ring
R^*	Group of units in R
K	Field
K^*	$K \setminus \{0\}$
$\mathcal{O}_K$	Ring of integers of K
$\mathfrak{p}$	Prime ideal
$\nu_{\mathfrak{p}}(x)$	$\mathfrak{p}$-adic valuation of x
I	Fractional ideal
k	Residue field $R/\mathfrak{p}$
E/K	Elliptic curve defined over K
$E(K)$	Set of K-rational points on E/K
$E_{ns}(k)$	Set of nonsingular points in $E(k)$
$\mathcal{O}$	Point at infinity on E/K
$\bar{E}$	Reduction of elliptic curve mod $\mathfrak{p}$
$\bar{P}$	Reduction of a point mod $\mathfrak{p}$
Λ	Lattice
Λ^*	$\Lambda \setminus \{0\}$
D	Fundamental parallelogram for Λ
W	Elliptic net
$(\rho_1, \rho_2, \ldots, \rho_r)$	Zero-rank of apparition for an elliptic net

Bibliography

[1] M. Ayad. Points S-entiers des courbes elliptiques. *Manuscripta mathematica*, 76:305–324, 1992.

[2] H. Cohen. *Number Theory Volume 1: Tools and Diophantine Equations*. Springer, 2007.

[3] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence Sequences*. AMS, 2003.

[4] L. K. Hua. *Introduction to Number Theory*. Springer, 1982.

[5] S. Lang. *Elliptic Curves Diophantine Analysis*. Springer-Verlag, 1978.

[6] J. Reynolds. Perfect powers in elliptic divisibility sequences. *Journal of Number Theory*, 132:998–1015, 2012.

[7] R. Shipsey. *Elliptic divisibility sequences*. Ph.D. Thesis, Goldsmith's college (University of London), 2000.

[8] J. Silverman. *The Arithematic of Elliptic Curves*. Springer, 1986.

[9] K. Stange. *Elliptic Nets*. Ph.D. Thesis, Brown University, 2008.

[10] M. Ward. Memoir on elliptic divisibility sequences. *American Journal of Mathematics*, 70:31–74, 1948.