KATHOLIEKE UNIVERSITEIT
LEUVEN

FACULTY OF SCIENCE
Department Mathematics
Section Algebra

Elliptic nets and their use in Cryptography

by

Mohamed AHKIM

Supervisor: dr. A. Perucca

Dissertation presented in fulfillment of the requirements for the degree of Master in Mathematics

Academic year 2011-2012

Dankwoord

Mijn oprechte dank gaat uit naar mijn promotor dr. Antonella Perucca voor haar advies en hulp waardoor deze masterproef tot zijn geheel is kunnen komen. Vervolgens wil ik mijn ouders en mijn naaste omgeving bedanken voor de onvoorwaardelijke steun die ik heb gekregen tijdens het schrijven van deze masterproef. Dankzij deze steun heb ik steeds weer met interesse en plezier aan deze masterproef gewerkt.

Eveneens veel dank aan mijn lezers dr. Wouter Castryck en dr. Joeri Van der Veken.

Samenvatting

Elliptic divisibility sequences (EDS) vormen een speciale klasse van *recurrente rijen*. Recurrente rijen zijn rijen die gedefinieerd zijn eenmaal enkele begintermen gegeven zijn: elke volgende term is bepaald door de voorgaande termen. Deze objecten komen voor in allerlei domeinen binnen de wiskunde.

Een eenvoudige maar reeds interessante type van een recurrente rij is de *Lucas rij*. Dit zijn rijen van gehele getallen die voldoen aan de betrekking

$$x_n = Px_{n-1} - Qx_{n-2},$$

waarbij P en Q vaste gehele getallen zijn. Nemen we $P = 1$ en $Q = -1$ in de Lucas rij, dan vinden we de bekende *Fibonacci rij*. Vele andere bekende bekende rijen zijn Lucas rijen.

In deze masterproef zijn we geïnteresseerd in elliptic divisibility sequences. Deze rijen zijn verbonden met *elliptische krommen*. Een elliptische kromme E gedefinieerd over een veld K is een kromme in het projectieve vlak gegeven door de vergelijking

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

met coefficiënten $a_i \in K$. De punten op de kromme E hebben een interessante groepsbewerking. Elliptische krommen zijn belangrijke objecten binnen de wiskunde. Zij spelen bijvoorbeeld een sleutelrol in het bewijs van *de laatste stelling van Fermat*. In de jaren 1980 begon men elliptische krommen te gebruiken in de cryptografie. Dit resulteerde in baanbrekende technieken voor het factoriseren van gehele getallen en priemtesten. Sindsdien werden elliptische krommen intensief bestudeerd en vormen ze nog steeds een belangrijke onderzoekstopic.

Een elliptic divisibility sequence $W : \mathbb{Z} \to R$ is een rij van elementen in een integriteitsdomein R dat voldoet aan het eigenschap

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

Deze rijen zijn nauw verbonden met de veelvouden van een punt $P = [x, y, 1]$ op een elliptische kromme E. Aan de kromme E kunnen we een rij van polynomen $\psi_n(x, y)$ associëren, *division polynomials* genoemd. Er zijn formules die de cordinaten van een veelvoud van het punt P uitdrukken in termen van deze division polynomials. Het is een feit dat alle *niet-ontaarde* EDS over een veld K kunnen bekomen worden door het evalueren van de division polynomials in een punt $P = (x_P, y_P)$ op een elliptische kromme

E. Deze rijen werden eerst bestudeerd door Morgan Ward [41] in de jaren veertig van de vorige eeuw. Sinsdien werd er niet veel aandacht besteed aan deze rijen tot ongeveer het jaar 2000. De rijke structuur in deze rijen heeft geleid tot een aantal heuristieken en resultaten wat betreft de getaltheorie. De meest bestudeerde problemen in deze context zijn priemgetalverschijningen, termen met een primitieve deler (een priemgetal welke geen deler is van de voorgaande termen) en de groei. Er is de conjectuur dat zegt dat alle *niet singuliere* EDS over de gehele getallen alleen maar eindig veel priemgetallen bevatten [11]. Joseph Silverman toonde in [34] dat alle termen, op een eindig aantal na, van een niet periodische niet singuliere EDS over $\mathbb{Z}$ primitieve delers hebben. Het is ook bekend dat zulke EDS W enorm snel groeien: er is een positieve getal h zodat

$$\lim_{n\to\infty} \frac{\log |W(n)|}{n^2} = h > 0.$$

Een overzicht van deze resultaten en meer vind men in [14]. EDS hebben ook toepassingen in de logica [29] en cryptografie.

Katherine Stange (2008) introduceerde *elliptic nets* om elliptic divisibility sequences te veralgemenen naar hoger dimensionale netten. Een elliptic net is een functie $W : \mathbb{Z}^n \to R$ van een eindig voortgebrachte vrije commutatieve groep naar een integriteitsdomein R dat voldoet aan de *recurrentierelatie*

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

voor alle $p, q, r, s \in \mathbb{Z}^n$. Het geval $n = 1$ komt overeen met een EDS. Met de rang van een elliptisch net W bedoelen we het getal n. In de meeste gevallen komt een elliptisch net van rang n overeen met een elliptische kromme E en een n tal punten $(P_1, \cdots, P_n) \in E^n$. Deze correspondentie is gebaseerd op de constructie van *net polynomials* $\Psi_{\mathbf{v}} : E^n \to K$ die afhangen van $\mathbf{v} \in \mathbb{Z}^n$. In het geval $n = 1$ komen ze overeen met de division polynomials. Deze uitbreiding laat toe om verschillende uitspraken te doen over een n-tal punten $(P_1, \cdots, P_n) \in E^n$ door alleen maar te werken met de geassocieerde elliptic net.

Rachel Shipsey (2001) toonde in haar doctoraatsthesis [30] hoe *EDS* kunnen gebruikt worden om het elliptische kromme discreet logaritme probleem (ECDLP) op te lossen in enkele gevallen. De *moeilijkheid* van het ECDLP is de hoofdreden voor het gebruiken van elliptische krommen (over eindige velden) in de cryptografie. Shipsey's toepassingen in de cryptografie zijn gebaseerd op een elegante (lineaire) algoritme dat de termen van een EDS berekent. De veralgemening uitgevoerd door Stange gaat verder en ze toont aan dat de *paringen* gebruikt in de cryptografie kunnen berekend worden met behulp van rang twee elliptische netten [36]. Dit vormde de eerste alternatief voor Miller's algoritme [26]. Kristien Lauter en Katherine Stange bewezen enkele interessante equivalenties tussen het ECDLP en *moeilijke problemen* voor elliptische netten [21].

Het doel van deze thesis was het bestuderen van elliptic nets en haar toepassingen in de cryptografie. Daarom zijn we begonnen met het bestuderen van Stange's constructie en haar artikels die elliptische netten toepassen in de cryptografie. Daarna bestudeerden

we twee topics omtrent elliptische krommen in de cryptografie waar elliptic nets kunnen toegepast worden. Tot dusver zijn alle toepassingen van elliptic nets in de cryptografie *essentieel* gebaseerd op rang 1 elliptic nets. Een reden hiervoor is dat er nog geen efficiënte algoritme was die de termen berekent van een rang twee (of hoger) elliptic net. We hebben een efficiënte algoritme gevonden dat de termen van bijna alle rang 2 elliptic nets berekent. Het algoritme is gebaseerd op Shipsey's algoritme voor rang 1 veralgemeend tot rang 2 door Stange. Dit algoritme leidt bijvoorbeeld tot een efficiente methode om te bepalen of een lineaire combinatie $nP + mQ$ van punten op een elliptische kromme nul is of niet. Verder onderzoek zou kunnen leiden tot andere toepassingen in de cryptografie.

Contents

Introduction

Elliptic divisibility sequences (EDS) are some particular kind of *recurrence sequences*. Recurrence sequences are sequences that are defined once some initial terms are given: each further term of the sequence is then defined as a function of the preceding terms. These objects occur in many areas of mathematics.

A particularly simple but already interesting type of recurrence sequence is the Lucas sequence. They are integer sequences that satisfy the recurrence relation

$$x_n = Px_{n-1} - Qx_{n-2},$$

where P and Q are fixed integers. By taking $P = 1$ and $Q = -1$ in the Lucas sequence we get the famous Fibonacci sequence. Many other famous sequences are Lucas sequences.

In this thesis, we are concerned with elliptic divisibility sequences (EDS), which are related to *elliptic curves*. An elliptic curve E defined over a field K is a curve in the projective plane given by the equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

with coefficients $a_i \in K$. The set of points on the curve E has an interesting group structure. Elliptic curves are important objects in mathematics. For example, they play a key role in the proof of Fermat's Last Theorem. In the 1980s elliptic curves started being used in cryptography and elliptic curve techniques were developed for factorization of integers and primality testing. In the last three decades elliptic curves were intensively studied and they still are.

An elliptic divisibility sequence $W : \mathbb{Z} \to R$ is a sequence with values in an integral domain R satisfying the property

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

Elliptic divisibility sequences are closely related to multiples of a point P on the elliptic curve E. To the curve E we can associate a sequence of polynomials $\psi_n(x, y)$, called *division polynomials*. It is a fact that all *non-degenerate* EDS can be obtained by evaluating the division polynomials in a point $P = (x_P, y_P)$ on E, i.e. $W(n) = \psi_n(x_P, y_P)$ for all $n \in \mathbb{Z}$. These sequences were first studied by Morgan Ward [41] in the 1940s. They attracted only sporadic attention until around 2000, when EDS were taken up as a class of nonlinear recurrences that are more amenable to analysis than most such sequences. The rich structure in EDS resulted in many heuristics and results in number theory.

The most common problems in this setting are prime appearences, terms having a primitive divisor (having a prime divisor which does not divide the preceding terms) and growth. It is conjectured that a *nonsingular* integer EDS contains only finitely many primes [11]. Joseph Silverman showed in [34] that all but finitely many terms in a nonsingular integer EDS admit a primitive divisor. It is also known that a not periodic nonsingular integer EDS W grows quadratic exponentially in the sense that there is a positive number h such that

$$\lim_{n\to\infty} \frac{\log |W(n)|}{n^2} = h > 0.$$

An overview of these number theorical results and more can be found in [14]. EDS have also applications in logic [29] and cryptography.

Katherine Stange (2008) introduced in [37] *elliptic nets* to generalize elliptic divisibility sequences to higher dimension nets. An *elliptic net* is a function $W : \mathbb{Z}^n \to R$ from a finitely generated free abelian group to an integral domain R satisfying the *recurrence relation*

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

for all $p, q, r, s \in \mathbb{Z}^n$. The case $n = 1$ corresponds to the definition of an EDS. By the rank of the elliptic net W we mean the integer n. In most cases an elliptic net W of rank n corresponds to an elliptic curve E and a tuple of points $(P_1, \cdots, P_n) \in E^n$. This correspondence is based on the construction of *net polynomials* $\Psi_{\mathbf{v}} : E^n \to K$ depending on $\mathbf{v} \in \mathbb{Z}^n$. These are for rank 1 the usual division polynomials.

Rachel Shipsey (2001) showed in her PhD thesis [30] how EDS may be used to solve the elliptic curve discrete logarithm problem (ECDLP) in certain weak cases. Her applications in Cryptography are based on an elegant (linear time) algorithm which computes terms of an EDS. Stange's generalisation goes further and shows that the pairings used in Elliptic Curve Cryptography can be computed using rank two elliptic nets [36], being the first alternative for Miller's Algorithm [26]. Kristin Lauter and Katherine Stange proved some interesting equivalences between the ECDLP and certain *hard problems* for elliptic nets [21].

The aim of this thesis was to study elliptic nets and their use in Cryptography. Therefore we started this thesis with the study of Stange's generalization of elliptic divisibility sequences to elliptic nets including all her papers concerning this subject. Then we studied two topics in Elliptic Curve Cryptography (ECC) where elliptic nets apply. So far, all the applications of elliptic nets in Cryptography concern rank one elliptic nets. One reason is that there is no efficient algorithm yet for computing terms of rank two (or higher) elliptic nets. We have found an efficient algorithm which computes terms of almost all rank two elliptic nets. The algorithm is based on Shipsey's algorithm, as generalized to rank two elliptic nets by Stange.

The thesis is structured as follows:

- In Chapter 1 we start with results about elliptic curves over $\mathbb{C}$ which form the heart of constructing net polynomials. We introduce division polynomials and show that they form an EDS. We end with a brief description of the results of Ward.

- In Chapter 2 we explain Stange's theory about elliptic nets and the construction of net polynomials in detail. Many results in the following chapters are based on this construction. In section 3 of chapter 2 we prove that the net polynomials of rank 2 and 3 over the field of complex numbers are *more or less* just polynomials. This completes the proof in [35].

- Chapter 3 concerns Stange's bijection between non-degenerate elliptic nets and elliptic curves with specified points on them. This generalizes the rank one case proven by Ward.

- *Pairings* play an important role in ECC and form the core of chapter 4. We define the frequently used *Weil* and *Tate pairings*. Then we explain Stange's paper on how to compute these pairings via elliptic nets. Her algorithm is based on Shipsey's algorithm for computing terms of a rank one elliptic net. Notice, even more *advanced* pairings can be calculated via elliptic nets.

- Elliptic curve cryptography is based on the *assumption* that the ECDLP is hard. In chapter 5 we show the relevance of elliptic nets for the ECDLP. In particular, we describe the work of Lauter and Stange.

- The algorithm for computing rank two elliptic nets is presented in chapter 6. Rachel Shipseys thesis [30] provides a double-and-add method of calculating the n-th term of an elliptic divisibility sequence in $\log n$ time. The first step is to slightly generalize the algorithm that Stange used to compute the pairings. Then we construct *square blocks* which will allow us to compute a term $W(n, m)$ in quadratic time via a *double and add* algorithm in $O(\log(n)^2)$ steps. Another feature of this chapter is the fact that using only elliptic nets one can determine efficiently whether a linear combination $nP + mQ$ of points on an elliptic curve E is the zero point. The proof of the previous includes that in most cases we can compute the ratio $W(n, m)/W(n, m + 1)$ in linear time. In the final section we formulate possible applications of the algorithm.

- In an appendix, we write the Sage code for the algorithm that computes whether a linear combination $nP + mQ$ of two points on an elliptic curve is the zero point.

Chapter 1

Division Polynomials and EDS

Our main references for elliptic curves are [33],[12] and [40]. We begin this chapter with an overview of the properties of an elliptic curve over $\mathbb{C}$. We will need this because Stanges construction of the generalization starts with elliptic curves over $\mathbb{C}$, which we will explain in chapter 2. Then we define the division polynomials associated to an elliptic curve and see that they form an elliptic divisibility sequence. We end this chapter with a brief discussion of Morgan Ward's results [41] concerning EDS and a simplified version of Shipsey's algorithm.

1 Elliptic curves over $\mathbb{C}$

A lattice in $\mathbb{C}$ is a subgroup Λ of the additive group $\mathbb{C}$ which is generated by two elements $w_1, w_2 \in \mathbb{C}$ that are linearly independent over $\mathbb{R}$. Elliptic curves over the field of complex numbers carry a lot of structure because they are the quotient of $\mathbb{C}$ modulo a lattice.

Definition 1.1. *Let Λ be a lattice. An elliptic function is a meromorphic function on $\mathbb{C}$ that satisfies*

$$f(z+w) = f(z) \quad \textit{for all } z \in \mathbb{C} \textit{ and all } w \in \Lambda.$$

Any lattice Λ gives rise to an elliptic function. Denote by $\mathbb{C}(\Lambda)$ the set of all such functions. It is clear that $\mathbb{C}(\Lambda)$ is a field. Set $\Lambda_0 := \Lambda \setminus \{0\}$.

Definition 1.2. *The Weierstrass $\wp$-function is defined by the series*

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda_0} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

The Weierstrass $\wp$-function is an even elliptic function having a double pole at each lattice point and no other poles [33, Theorem VI.3.1b]. To a lattice Λ we can also associate the series

$$G_{2k} = \sum_{w \in \Lambda_0} \frac{1}{w^2} \quad \text{for all } k \geq 2.$$

We call $G_{2k}(\Lambda)$ an *Eisenstein serie of weight* $2k$. These series are absolutely convergent [33, Theorem VI.3.1a].

Theorem 1.3 ([33, Theorem VI.3.5]). *The Laurent series for $\wp(z)$ around $z = 0$ is given by*

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

Set $g_2 = 60G_4(\Lambda)$ and $g_3 = 140G_6(\Lambda)$. Then the polynomial

$$f(x) = 4x^3 - g_2x - g_3$$

has distinct zeros, hence its discriminant is nonzero: $\Delta = g_2^3 - 27g_3^3 \neq 0$.

Theorem 1.4. *Let Λ be a lattice and $E/\mathbb{C}$ an elliptic curve given by $y^2 = 4x^3 - g_2x - g_3$. The map*

$$\begin{array}{rcl} \Phi : \mathbb{C}/\Lambda & \to & E(\mathbb{C}) \\ z & \mapsto & [\wp(z), \wp'(z), 1] \end{array}$$

is an isomorphism of groups.

Any elliptic curve over $\mathbb{C}$ can be transformed by an affine transformation to an elliptic curve with Weierstrass equation

$$E: \ y^2 = 4x^2 - Ax - B.$$

There exists a unique lattice $\Lambda \subset \mathbb{C}$ satisfying $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$, see [33, Theorem VI.5.1].

Theorem 1.5. *Let $E/\mathbb{C}$ be an elliptic curve. There exists a lattice Λ, unique up to homethety, such that the following is a group isomorphism*

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

where Φ is as in theorem 1.4.

Proof. See [33, Corollary VI.5.5.1]. □

Definition 1.6. *Define the Weierstrass ζ-function as*

$$\zeta(z) = \frac{1}{z} + \sum_{w \in \Lambda_0}\Big(\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2}\Big).$$

By [8, Chapter IV, section 1], the function $\zeta(z)$ is a holomorphic function on $\mathbb{C} \setminus \Lambda$. The following proposition entails important properties for the Weierstrass ζ-function.

Proposition 1.7. *Denote by $\zeta(z)$ the Weierstrass ζ-function relative to the lattice Λ. Then one gets the following properties:*

1. *there exists a constant $\eta(w) \in \mathbb{C}$ such that for all z*

$$\zeta(z+w) = \zeta(z) + \eta(w)$$

2. $\frac{d}{dz}\zeta(z) = -\zeta(z)$ *on* $\mathbb{C} \setminus \Lambda$.

3. $\zeta(-z) = -\zeta(z)$ *on* $\mathbb{C} \setminus \Lambda$.

Proof. For the first item, see the remark just above [8, Theorem 2, page 50]. Differentiating $\zeta(z)$ gives the series for $-\wp(z)$, which is known to be convergent. This proves the second statement. For the last statement, notice that we can replace w by $-w$ in the summation without changing $\zeta(z)$. Clearly, evaluating at $-z$ gives $-\zeta(z)$. □

Definition 1.8. *Let Λ be a lattice. The Weierstrass σ-function relative to Λ is defined by the product*

$$\sigma(z) = \sigma(z;\Lambda) = z \prod_{w \in \Lambda_0} \Big(1 - \frac{z}{w}\Big) e^{(z/w)+\frac{1}{2}(z/w)^2}.$$

This function is holomorphic on $\mathbb{C}$. It has simple zeros at each $z \in \Lambda$ and no other zeros [33, Theorem VI.3.3a]. The Weierstrass σ-function is *almost* periodic with respect to Λ: for all $z \in \mathbb{C}$ we have the property ([8, Theorem 3, page 53])

$$\sigma(z + w) = \lambda(w) e^{\eta(w)(z+\frac{w}{2})} \sigma(z),$$

where η is defined as in proposition 1.7 and

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

The following proposition is immediate by definition 1.8.

Proposition 1.9.

$$\sigma(\lambda z; \lambda\Lambda) = \lambda\sigma(z;\Lambda).$$

Theorem 1.10 (The addition theorem)**.** *If $z_1 \not\equiv z_2 \bmod \Lambda$, then we have that*

$$\wp(z_1 + z_2) = \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2).$$

Proof. See [8, Theorem 6, page 34]. □

2 Division polynomials

This section is based on [12, Chapter 3]. Let E be an elliptic curve over a field K. Suppose that $char(K) = 0$. A way to characterise the group of m-torsion points $E[m]$, for a nonzero integer m, is by introducing a *function* $f(X, Y)$ satisfying

$$div(f) = \sum_{P \in E[m]} (P) - m^2(\mathcal{O}).$$

This function has zeros exactly at the points in $E[m] - \{\mathcal{O}\}$ and only one pole at $\mathcal{O}$. Notice that the m-torsion points sum up to zero. By proposition [12, 2.34], if such a function exists it must be a polynomial and by corollary [12, 2.47] such a polynomial exists if the m-torsion points sum up to zero. So we know such a polynomial exists and

by corollary [12, 2.35] it is unique up to a constant in $\bar{K}$. Therefore we will first specify what the *leading coefficient* is for an element in $K[E]$ in reduced form, i.e. polynomials of the form $v(X)+Yw(X)$ where the polynomials v and w have degree smaller than 2. It is the coefficient of the highest degree term if we assign degree 2 to X and degree 3 to Y. For a rational function $r \in K(E)$ we use the following definition which is the extension of the case that r is a polynomial.

Definition 2.1 ([12, Definition 3.40])**.** *The leading coefficient of a rational function $r \in K(E)$ is*

$$l(r) := \left(\left(\frac{X}{Y}\right)^{-ord_{\mathcal{O}} r} r\right)(\mathcal{O})$$

One of the interesting results about these polynomials is that they satisfy the recurrence relation of an elliptic divisibility sequence. We will also define *such* polynomials for $char(K) = p > 0$ by reducing modulo p.

2.1 In zero characteristic

Definition 2.2. *For every nonzero integer m, denote by ψ_m the unique rational function with divisor*

$$div(f) = \sum_{P \in E[m]} (P) - m^2(\mathcal{O}),$$

and leading coefficient m. Set $\psi_0 = 0$ by definition. We call ψ_m the m^{th} division polynomial of the elliptic curve E.

We can already prove some identies.

Proposition 2.3. *For positive integers m and n, the following properties hold:*

i. $\psi_{-m} = -\psi_m$,

ii. Denote by $x(P)$ de x-coordinate of a point $P = (x_P, y_P)$ on E. Then

$$\psi_m^2 = m^2 \prod_{P \in E[m] \setminus \{\mathcal{O}\}} (X - x(P)),$$

iii. $\psi_m \in K[X]$ *whenever m is odd, while* $\psi_m \in (2Y + a_1X + a_3)K[X]$ *is m even,*

iv. $\psi_m\psi_n \in K[X]$ *if m and n have the same parity*

Proof.

i. This follows directly from the definition of the division polynomial and the fact that $E[m] = E[-m]$.

ii. We have that $div(X - x(P)) = (P) + (-P) - 2(\mathcal{O})$ since the only zeros of $X - x(P)$ are P and $-P$. We find by definition 2.2 that

$$div(\psi_m^2) = \sum_{P \in E[m]} 2(P) - 2m^2(\mathcal{O}),$$

while

$$\begin{aligned} div(m^2 \prod_{P\in E[m]-\{\mathcal{O}\}} (X - x(P))) &= \sum_{P\in E[m]-\{\mathcal{O}\}} div((X - x(P)) \\ &= \sum_{P\in E[m]-\{\mathcal{O}\}} (P) + (-P) - 2(\mathcal{O}) \\ &= \big(\sum_{P\in E[m]} 2(P)\big) - 2m^2(\mathcal{O}), \end{aligned}$$

the last equation holds because $E[m] = -E[m]$. Moreover, the leading coefficients of both rational functions are m^2, hence they must be equal.

iii. If m is odd, then $E[m]$ contains no point of order 2. We can write $E[m]$ as $S \cup -S \cup \{\mathcal{O}\}$ for some set S where $-S = \{-P \mid P \in S\}$. By comparing divisors and leading coefficients we find

$$\psi_m = m \sum_{P\in S} \big(X - X(P)\big) \in K[X] \subset K[E].$$

In the other case, it follows that $E[2] \subset E[m]$, so we can decompose

$$E[m] = S \cup -S \cup E[2].$$

By the same argument as in the previous case we have $\psi_m = \dfrac{m}{2}\psi_2 \sum_{P\in S} \big(X - X(P)\big)$. Since $|E[2]| = 4$ there are three non-zero points of order 2. A point (x, y) is a 2-torsion point if and only if $2y + a_1x + a_3 = 0$. Therefore $\psi_2 = 2Y + a_1X + a_3$ and the proof of the assertion is complete.

iv. If m and n are odd, then the assertion is trivial by iii. Thus it is sufficient to remark the following

$$\begin{aligned} (2Y + a_1X + a_3)^2 &= 4Y^2 + 4Y(a_1X + a_3) + (a_1X + a_3)^2 \\ &= 4(X^3 + a_2X^2 + a_4X + a_6) + (a_1X + a_3)^2 \\ &\in K[X]. \end{aligned}$$

□

Consider the multiplication by m map

$$[m] : E \to E : P \mapsto mP,$$

by theorem [12, 3.9] this is a rational map. Hence we can write $[m] = (g_m, h_m)$ for some rational functions $g_m, h_m \in \bar{K}(E)$.

Lemma 2.4. *For nonzero integers m, n we have the equation*

$$g_m - g_n = -\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}. \tag{1.1}$$

Proof. We prove the lemma by comparing the divisors on both sides. For the left-hand side we find that

$$div(g_m - g_n) = \langle E[m+n]\rangle + \langle E[m-n]\rangle - 2\langle E[m]\rangle - 2\langle E[n]\rangle$$

by proposition [12, 3.45]. By definition 2.2, the right-hand side of (1.1) has the same divisor. Now we only need to verify the leading coefficients. Proposition [12, 3.43] says that

$$l(g_m - g_n) = \frac{1}{m^2} - \frac{1}{n^2} = -\frac{(m+n)(m-n)}{m^2n^2},$$

where $l(r)$ denotes the leading coefficient of the rational function r. By definition 2.2, the last equation is also the leading coefficient of

$$-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2},$$

which completes the proof of the lemma. □

Suppose that $P \notin E[m]$ and $[2]P \neq \mathcal{O}$. The previous lemma says that we can compute $x([m]P)$ by knowledge of the terms $\psi_{m-1}(P), \psi_m(P)$ and $\psi_{m+1}(P)$:

$$x([m]P) - x = -\frac{\psi_{m-1}(P)\psi_{m+1}(P)}{\psi_m(P)^2}.$$

For the y-coordinate we have by [12, Proposition 3.55]

$$y([m]P) - y(P) = \frac{\psi_{m-1}^2(P)\psi_{m+2}(P)}{\psi_2(P)\psi_m(P)} + (3x^2 + 2a_2x + a_4 - a_1y)\frac{\psi_{m-1}(P)\psi_{m+1}(P)}{\psi_2(P)\psi_m^2(P)}.$$

Therefore, division polynomials provide a way to calculate multiples of points on elliptic curves. The following proposition shows that the division polynomials satisfy a recurrence relation.

Proposition 2.5. *The division polynomials $\{\psi_m\}_{m\in\mathbb{Z}}$ satisfy*

$$\begin{aligned}
&\psi_0 = 0,\\
&\psi_1 = 1,\\
&\psi_2 = 2Y + a_1X + a_3,\\
&\psi_3 = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8\\
&\psi_4 = \psi_2 \cdot (2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)),
\end{aligned}$$

where the b_i quantities are as usual. Moreover, the recursion

$$\psi_{m+n}\psi_{m-n} = \psi_n^2\psi_{m+1}\psi_{m-1} - \psi_m^2\psi_{n+1}\psi_{n-1} \tag{1.2}$$

holds for all integers m, n.

Proof. By definition $\psi_0 = 0$ and $div(\psi_1) = (\mathcal{O}) - (\mathcal{O}) = 0$, which means that ψ_1 is a constant. This constant is the leading coefficient which is 1 by definition. For the

expression of ψ_2 see the proof of 2.3.iii. For ψ_3, we use proposition [12, 3.52] with $m = 2$ and $n = 1$, which gives

$$\psi_3 = -(g_2 - X)\psi_2^2.$$

Let $\lambda = \dfrac{X^2 + 2a_2X + a_4 - a_1Y}{2Y + a_1X + a_3}$, then by the duplication formula $g_2 = -2X+\lambda^2+a_1\lambda-a_2$ and the former equation becomes

$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8.$$

In the same way we find

$$\psi_4 = \psi_2 \cdot \big(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\big).$$

It remains to prove (1.2), which is trivial for $m = 0$ or $n = 0$. Suppose that $n \neq 0$ and $m \neq 0$. Proposition [12, 3.52] gives the following relation

$$g_m - g_n = (g_m - g_1) - (g_n - g_1),$$

or equivalently by lemma 2.4:

$$\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2} = \frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2} - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2},$$

which gives the recurrence (1.2) after multiplying the equation by $\psi_m^2\psi_n^2$.

□

Now it is clear that the division polynomials are determined by $\psi_1, \psi_2, \psi_3, \psi_4$.

Corollary 2.6.

$$\begin{aligned}\psi_2\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m+1}^3\psi_{m-1}\ .\end{aligned}$$

Proof. The first equation follows from (1.2) by substituting $m+1$ into m and $m-1$ into n. The second equation can be obtained by replacing n by m and m by $m+1$. □

Corollary 2.7. *The division polynomials ψ_m satisfy*

$$\psi_m \in \begin{cases}\mathbb{Z}[X, a_1, a_2, a_3, a_4, a_6]/(E) & \text{if } m \text{ is odd,}\\ \psi_2\mathbb{Z}[X, a_1, a_2, a_3, a_4, a_6]/(E) & \text{if } m \text{ is even.}\end{cases}$$

Proof. The proof is by induction on m. Because of proposition 2.3 we only need to consider $m \geq 0$. The cases $m = 0, 1, \ldots, 4$ are trivial. Suppose the lemma holds for $m - 1 \geq 4$, we prove it also holds for m. We need to consider two cases:
Suppose m is odd, i.e. $m = 2k + 1$ and $k \geq 2$. Note that $2k + 1 > k + 2$. By corollary 2.6, we have

$$\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k+1}^3\psi_{k-1},$$

If k is even, by induction the first term of the right-hand side is a product of

$$\psi_2^4 = 16(X^3 + a_2X^2 + a_4X + a_6) + (a_1X + a_3)^4$$

and a polynomial in $\mathbb{Z}[X, a_1, a_2, a_3, a_4, a_6]$, the second term of the right-hand side is also contained in $\mathbb{Z}[X, a_1, a_2, a_3, a_4, a_6]$, therefore $\psi_m \in \mathbb{Z}[X, a_1, a_2, a_3, a_4, a_6]$. The same reasoning proves the case $k \equiv 1 \bmod 2$.
For $m = 2k$ such that $k \geq 3$ and hence $2k > k + 2$, we use again corollary 2.6:

$$\psi_{2k} = \frac{\psi_k}{\psi_2}(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2).$$

Consider the polynomial $\psi_k(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2)$, by induction it is equal to ψ_2^2 times a polynomial in $\mathbb{Z}[X, a_1, a_2, a_3, a_4, a_6]$. The latter statement is obvious by considering the cases $k \equiv 0 \bmod 2$ and $k \equiv 1 \bmod 2$. This proves the induction step in the other case. □

Lemma 2.8 ([40, Lemma 3.5])**.**

$$\psi_n(X, Y) = \begin{cases} (2Y + a_1X + a_3)\left(\frac{n}{2}X^{(n^2-4)/2} + f(X)\right) & \text{if } n \text{ is even} \\ nX^{(n^2-1)/2} + g(X) & \text{if } n \text{ is odd} \end{cases},$$

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

Proof. The proof is by induction. We are allowed to restrict ourselves to division polynomials ψ_m for positive m. By corollary 2.7, we only need to prove that the two expressions have the same leading coefficient. The statements trivially hold for $\psi_1, \ldots, \psi_4$. Suppose that the statment holds for a positive integers m such that

$$0 \leq m \leq n - 1$$

and $n-1 \geq 4$, we prove it also holds for $0 \leq m \leq n$. We consider only the case $n = 2k+1$ and $k \geq 2$ even, the other cases can be treated similarly. Because $2k + 1 > k + 2$, the induction hypothesis yields that the leading term of $\psi_{k+2}\psi_k^3$ is

$$(k + 2)k^3x^{\frac{(2k+1)^2-1}{2}}, \tag{1.3}$$

since the leading term of $(2y + ax + a_3)^4$ is $16x^6$, by the proof of proposition 2.3.iv. By the induction hypothesis, the leading term of $\psi_{k+1}^3\psi_{k-1}$ is

$$(k + 1)^3(k - 1)x^{\frac{(2k+1)^2-1}{2}}. \tag{1.4}$$

By the formula

$$\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k+1}^3\psi_{k-1},$$

subtracting (1.3) by (1.4) yields

$$\begin{aligned} \psi_n &= \psi_{2k+1} \\ &= (2k + 1)x^{((2k+1)^2-1)/2} + \ldots \\ &= nx^{(n^2-1)/2} + \ldots \quad . \end{aligned}$$

□

2.2 In positive characteristic

From now on let $char(K) = p > 0$ and let E be an elliptic curve defined over K. The definition of *the division polynomial* ψ_m is inspired by corollaries 2.5 and 2.6. We obtain the division polynomials by reducing modulo p.

Definition 2.9. *The division polynomials $\psi_m \in \bar{K}[X,Y]/(E)$ are defined by the polynomials*

$$\begin{aligned}
&\psi_0 = 0,\\
&\psi_1 = 1,\\
&\psi_2 = 2Y + a_1X + a_3,\\
&\psi_3 = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8\\
&\psi_4 = \psi_2 \cdot (2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)),
\end{aligned}$$

where the b_i are the usual quantities, and for $m \geq 2$ by the recursion

$$\psi_2\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \tag{1.5}$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m+1}^3\psi_{m-1}\ . \tag{1.6}$$

We also set $\psi_{-m} = -\psi_m$ for all positive integers m. By corollary 2.6, we have that for all integers m

$$\psi_m \in \mathbb{F}_p[X, Y, a_1, a_2, a_3, a_4, a_6]/(E).$$

We have the important lemma [12, 3.56], which says that for $m \neq 0$ the corresponding division polynomial is also non-zero. By induction the above definition shows that the division polynomials are *determined* by $\psi_1, \psi_2, \psi_3, \psi_4$. By construction, the main results still hold in positive characteristic.

Theorem 2.10 ([4, Lemma III.5, Theorem III.6])**.** *Let E be an elliptic curve defined over a field K and m an integer. There exist polynomials θ_m and $\omega_m \in K[x,y]$ such that for all points $P = (x,y)$ in $E(\bar{K})$ with $[m]P \neq \mathcal{O}$ we have*

$$[m]P = \left(\frac{\theta_m(x,y)}{\psi_m(x,y)^3}, \frac{\omega_m(x,y)}{\psi_m(x,y)^3}\right).$$

For all points $P \in E \setminus \{\mathcal{O}\}$ and integers n

$$[n]P = \mathcal{O} \iff \psi_n(x,y) = 0.$$

Let E be an elliptic curve defined over K given by Weierstrass equation

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

The only change over variables fixing the point at infinity $\mathcal{O} = [0,1,0]$ and preserving the Weiestrass equation is

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + u^2sx' + t,$$

where $u, r, s, t \in \bar{K}$ and $u \neq 0$. We call such a transformation an *admissible change of variables*. An admissible change of variables is called *unihomothetic* if $u = 1$.

Theorem 2.11 ([32, Theorem 3.10.7]). *Let E be an elliptic curve defined over a field K. Let E' be the elliptic curve obtained from E by an admissible change of variables*

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + u^2sx' + t.$$

Then

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

3 Elliptic divisibility sequences

We start this section with the definition of an elliptic divisibility sequence which was introduced by Morgan Ward [41].

Definition 3.1. *Let R be an integral domain. An elliptic divisibility sequence is a sequence $W : \mathbb{Z} \to R$ satisfying*

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

Ward worked with the ring $R = \mathbb{Z}$ and required *the divisibility property*: $n|m \implies W_n|W_m$. We now know a wealth of examples of elliptic divisibility sequences. Namely the sequence $W_n = \psi_n(P)$ for some elliptic curve E and a point P on it. The following theorem due to Ward shows the strong relation between integer elliptic divisibility sequences and elliptic curves over $\mathbb{C}$.

Theorem 3.2 ([41, Theorem 12.1]). *If W is an integer elliptic divisibility sequence with the properties*

1. *$W(1) = 1$,*
2. *$W(2)W(3) \neq 0$,*
3. *and $W(2)|W(4)$,*

then there exists an elliptic curve over $\mathbb{C}$ given by a lattice Λ and a complex number z such that

$$W(n) = \frac{\sigma(nz)}{\sigma(z)^{n^2}} \quad \text{for all } n \in \mathbb{Z}.$$

In particular, the sequence $\left(\dfrac{\sigma(nz)}{\sigma(z)^{n^2}}\right)_n$ is an EDS. We know that an elliptic curve over the complex numbers can be viewed as the quotient group $\mathbb{C}/\Lambda$ for some complex lattice Λ. The claim is that the associated function $\dfrac{\sigma(nz)}{\sigma(z)^{n^2}}$ corresponds to the division polynomial $\psi_n(x, y)$ of the elliptic curve. We will give the isomorphism explicitely. Therefore, suppose that E is an elliptic curve over $\mathbb{C}$ given by the equation

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

Then, we can define the division polynomials $\psi_n(x, y)$ as usual. We start with a change of variables so that $E(\mathbb{C})$ is isomorphic to an elliptic curve $\bar{E}(\mathbb{C})$ given by

$$y^2 = 4x^3 - g_2x - g_3.$$

Let Λ be the lattice corresponding to the above elliptic curve. Then $\mathbb{C}/\Lambda$ is isomorphic to $\bar{E}(\mathbb{C})$ and hence $\mathbb{C}/\Lambda$ is isomorphic to $E(\mathbb{C})$. We can summarize with the following group isomorphisms

$$\mathbb{C}/\Lambda \xrightarrow{z \mapsto [\wp(z), \wp'(z), 1]} \bar{E}(\mathbb{C}) \xrightarrow{(x,y)\mapsto \left(x-\frac{b_2}{12}, \frac{y}{2}-\frac{a_1}{2}(x-\frac{b_2}{12})-\frac{a_3}{2}\right)} E(\mathbb{C}),$$

Then define

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

We *expect* Ψ_n and $\Omega_n(z) = \dfrac{\sigma(nz)}{\sigma(z)^{n^2}}$ to be equal. Well, they are equal up to a sign. The following theorem is inspired by [33, Exercise 6.15]

Theorem 3.3.

$$\Psi_n(z) = (-1)^{n+1}\Omega_n(z)$$

Proof. The field of elliptic functions $\mathbb{C}(\Lambda)$ is generated by the set $\{\wp(z)\wp'(z)\}$ and $\Psi_n(z)$ is a rational function on those functions. Hence $\Psi_n(z)$ is an elliptic function. It is known that $\Omega_n(z)$ is also elliptic. So we can use elliptic function theory. The first step is to show that $\Psi_n(z)$ and $\Omega_n(z)$ are proportional. From the diagram it is clear that $\mathbb{C}/\Lambda[n]$ corresponds to $E[n]$. The division polynomial $\psi_n(x, y)$ vanishes exactly at the non-zero n-torsion points of E. So we deduce that Ψ_n vanishes at the same points as Ω_n. From the definition of $\wp(z;\Lambda)$ and the division polynomial ψ_m both complex functions have exactly one pole (with order $n^2 - 1$), namely $z \in \Lambda$. The number of non-zero n-torsion points is $n^2 - 1$, therefore the order of vanishing at each point is one. This shows that both elliptic functions have the same divisor, hence they are proportional. It remains to find the constant ratio. We know that Ψ_n and Ω_n have a pole of order $n^2 - 1$ at 0, then it is a good idea to consider

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

Both functions are analytic at 0, so we are allowed to take the limit for $z \to 0$. For the right-hand side, we simplify

$$z^{n^2-1}\frac{\sigma(nz)}{\sigma(z)^{n^2}} = n\prod_{w\in\Lambda_0}\left(e^{\frac{nz}{w}(1-n)}\right)\frac{1-\frac{nz}{w}}{(1-\frac{z}{w})^{n^2}},$$

if $z \to 0$, the right-hand side tends to n. For the left-hand side we use lemma 2.8

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

This means that

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

We know that $\wp$ hase a pole of order two at 0, hence $\wp'$ has a pole of order three at 0. Recall the corresponding Laurent series around zero:

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

We arrive at

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

from which we find the desired result

$$\Psi_n(z) = (-1)^{n+1}\Omega_n(z).$$

□

Remark 3.4. *By the previous theorem both complex functions are equal up to a sign. But we can resolve that problem by using the fact $\sigma(-z) = -\sigma(z)$: replace $\Omega_n(z)$ by*

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

to get the same function.

We list some of Wards results.

Theorem 3.5 ([41, Theorem 5.1])**.** *Let W be an elliptic divisibility sequence satisfying $W(1) = 1$, $W(2)W(3) \neq 0$ and $W(2)|W(4)$. Assume that $W(i) \in \mathbb{Z}$ for $1 \leq i \leq 4$. Then W is an integer elliptic divisibility sequence satisfying the divisibility property.*

Proof. See [41, Thm 4.1] for the proof. It is a long induction proof and is based on the previous proposition. □

Proposition 3.6. *Let W be an elliptic divisibility sequence, such that $W(1) = 1$ and $W(2)W(3) \neq 0$. If two consecutive terms of W vanish then*

$$W(n) = 0, \quad \text{for } n \geq 4$$

.

Proof. See [41, lemma 4.1]. The proof remains valid if $\mathbb{Z}$ is replaced by R. □

Suppose that W is an integer elliptic divisibility sequence. One can wonder how the sequence $W(n)$ behaves modulo a prime $p \in \mathbb{Z}$.

Definition 3.7. *For any integer elliptic divisibility sequence W, let r denote the smallest positive integer such that $W(r) \equiv 0 \bmod p$. We call r the rank of apparition of W with respect to p.*

The following result due to Ward shows that the definition makes sense.

Theorem 3.8 ([41, Thm. 5.1])**.** *Let W be any integer elliptic divisibility sequence. For any prime p the rank of apparition r exists. A fortiore, we have*

$$1 \leq r \leq 2p + 1.$$

Proof. Without loss of generality, we may assume that none of $W(1), \cdots, W(p+2)$ is divisible by p. Hence we can consider

$$\frac{W(r-1)W(r+1)}{W(r)^2} \quad \text{for } r = 2, \ldots, p+1$$

as non zero elements of the field $\mathbb{F}_p$. By the pigeon hole principle there exist integers $2 \leq n < m \leq p+1$ and an integer c such that

$$\frac{W(n-1)W(n+1)}{W(n)^2} \equiv \frac{W(m-1)W(m+1)}{W(m)^2} \equiv c \bmod p.$$

The recurrence relation of an elliptic divisibility sequence gives the congruence

$$W(m+n)W(m-n) \equiv 0 \bmod p.$$

Since $m - n < p + 2$, we have that $W(m-n) \not\equiv 0 \bmod p$, hence $p|W(m+n)$. Clearly $m+n \leq 2p+1$, from which we conclude that the rank of apparition r exists and is smaller or equal to $2p+1$. Note that this bound is sharp in general. □

In particular we have:

Remark 3.9. *Let p be a prime number. For any integer elliptic divisibility sequence W there exists a positive integer m such that $p|W(m)$.*

Theorem 3.10 ([41, Theorem 5.2])**.** *Let W be an integer elliptic divisibility sequence and p a prime, denote by r the corresponding rank of apparition. If $W(r+1) \not\equiv 0 \bmod p$, then $W(n) \equiv 0 \bmod p$ if and only if $n \equiv 0 \bmod r$.*

For more periodicity properties of elliptic divisibility sequences modulo primes and powers of primes, see Swart's PhD thesis [32]. For an overview of current research and results on EDS, see [14].

4 Shipsey's Algorithm

Rachel Shipsey provided in her thesis [30, Theorem 3.1.1] a double and add algorithm to compute the terms of a *non-degenerate* elliptic divisibility sequence $W(n) = \psi_n(P)$, where P is a point on the elliptic curve E defined over a field K having order at least four. Here, non-degenerate means that $W(1)W(2)W(3) \neq 0$. We give a simplified version of the algorithm due to Stange. Denote by $\langle W(k) \rangle$ the *block centred at* k of 8 terms $W(k-3)$, $W(k-2)$, …, $W(k+3)$, $W(k+4)$. The recurrence relation of an EDS enables us to find the terms of the block centred on $2k$ or $2k+1$ from the block centred on k. The transition is based on the following instances of definition 3.1

$$\begin{aligned} W(2i-1) &= W(i+1)W(i-1)^3 - W(i-2)W(i)^3 \ , \\ W(2i) &= \big(W(i)W(i+2)W(i-1)^2 \\ &\qquad - W(i)W(i-2)W(i+1)^2\big)\, /W(2) \ . \end{aligned}$$

To begin we must calculate the block centred at 1. That is not a problem since $\psi_{-n}(P) = -\psi_n(P)$ and we have explicit formulas for $\psi_1, \ldots, \psi_4$.

Chapter 2

Elliptic Nets and Net Polynomials

In the previous chapter we have seen that an elliptic divisibility sequence arises from an elliptic curve and a point on it. Stange presented a higher dimensional-analogue over arbitrary base fields [35]. This chapter describes her generalization. She first finds the *correct* recurrence relation for arrays $\mathbb{Z}^n \to K$, called *elliptic nets*. Then she constructs *net polynomials*, which satisfy the recurrence relation of an elliptic net. In section 3 we prove that net polynomials of rank smaller than three are more or less polynomials.

1 Elliptic Nets

1.1 What is an elliptic net?

Definition 1.1. *Let A be a finitely generated free abelian group, i.e. $A \cong \mathbb{Z}^n$ for some $n > 0$, and let R be an integral domain. An elliptic net is any map $W : A \to R$ where*

$$W(0) = 0 \tag{2.1}$$

and such that for all $p, q, r, s \in A$, we have

$$\begin{aligned} W(p+q+s)W(p-q)W(r+s)W(r) \\ + W(q+r+s)W(q-r)W(p+s)W(p) \\ + W(r+p+s)W(r-p)W(q+s)W(q) = 0 \end{aligned} \tag{2.2}$$

If R is a domain with $char(R) \neq 3$ then we could omit condition (2.1): take $p = q = r = s = 0$ in (2.2), then we find $3W(0) = 0$. Since R is domain with $3 \neq 0$ we find $W(0) = 0$.

The best way to get a feeling about how elliptic nets 'work' is by looking at some examples.

Example 1.2.

1. *The trivial elliptic net $W : \mathbb{Z}^n \to R$ is the zero net, which is defined by*

$$W(\mathbf{v}) = 0, \quad \text{for all } \mathbf{v} \in \mathbb{Z}^n.$$

2. *For the rank one case we can define the identity map*

$$W_{id} : \mathbb{Z} \to R : n \mapsto n \cdot 1_R.$$

The equation below shows that W_{id} is indeed an elliptic net.

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

3. *The Legendre symbol $\left(\frac{n}{3}\right)$ forms an elliptic net. Observe that for at least one of $p, q, r, p-q, q-r$ and $r-p$ is divisible by 3. We consider only the cases $p \equiv 0 \bmod 3$ and $p - q \equiv 0 \bmod 3$ since (2.2) is symmetric in p, q and r. For the former case, this means that*

$$\left(\frac{q+s}{3}\right)\left(\frac{-q}{3}\right)\left(\frac{r+s}{3}\right)\left(\frac{r}{3}\right) + \left(\frac{r+s}{3}\right)\left(\frac{r}{3}\right)\left(\frac{q+s}{3}\right)\left(\frac{q}{3}\right)$$

should be zero. This is indeed true since

$$\left(\frac{-q}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{q}{3}\right) = -\left(\frac{q}{3}\right).$$

Now suppose that $p - q \equiv 0 \bmod 3$, in order to satisfy (2.2), we should have

$$\left(\frac{q+r+s}{3}\right)\left(\frac{q-r}{3}\right)\left(\frac{p+s}{3}\right)\left(\frac{p}{3}\right) + \left(\frac{r+p+s}{3}\right)\left(\frac{r-p}{3}\right)\left(\frac{q+s}{3}\right)\left(\frac{q}{3}\right) = 0.$$

Since $p \equiv q \bmod 3$, we can replace every q by p. This shows that p, q, r and s also satisfy the elliptic net relation.

4. *A more interesting example is given by the elliptic net $W : \mathbb{Z} \to \mathbb{Z}$ such that*

$$W(v) = \begin{cases} F_{2v} & v > 0 \\ -F_{2v} & v < 0 \\ 0 & v = 0 \end{cases}$$

where F_{2v} is the $2v$-th Fibonacci number. One can verify the claim by using the closed form of the Fibonacci sequence:

$$F_v = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^v - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^v$$

We deduce some elementary properties of elliptic nets.

Proposition 1.3. *Let $W : A \to R$ be an elliptic net. Suppose that $f : B \to A$ is a homomorphism of finitely generated free abelian groups, and $g : R \to S$ is a homomorphism of integral domains. Then*

1. *$W \circ f : B \to R$ is an elliptic net, and*
2. *$g \circ W : A \to S$ is an elliptic net.*

Proof. For the first claim, we clearly have $W(f(0)) = 0$. It remains to consider

$$\begin{aligned} (2.3)\quad & W(f(p+q+s))W(f(p-q))W(f(r+s))W(f(r)) \\ & + W(f(q+r+s))W(f(q-r))W(f(p+s))W(f(p)) \\ & + W(f(r+p+s))W(f(r-p))W(f(q+s))W(f(q)) = 0 \end{aligned}$$

Since f is a group homomorphism, (2.3) is actually the elliptic net recurrence for W evaluated in $f(p), f(q), f(r), f(s)$.
The proof for the second claim follows directly from the fact that g is a ring morphism. □

1.2 More about elliptic nets

The following definition will give a manner to *rescale* a given elliptic net, see proposition 1.7.

Definition 1.4. *Let B and C be abelian groups (in additive notation). We call a function $f : B \to C$ a* quadratic function *if for all $x, y, z \in B$, the function f satisfies the relation*

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

A quadratic form $f : B \to C$ is an even quadratic function, i.e. $f(x) = f(-x)$ for all $x \in B$.

Lemma 1.5. *A quadratic form $f : B \to C$ satisfies the parallelogram law:*

$$f(x+y) + f(x-y) = 2f(x) + 2f(y).$$

Proof. Set $x = y = z = 0$ in definition 1.4 to find $f(0) = 0$. Substitute $z = -x$ to obtain

$$f(x+y) + f(x-y) = 2f(x) + 2f(y).$$

□

By the previous it is easy to show that a quadratic form f is homogenuous of degree 2 with respect to the integers, i.e.

$$f(nx) = n^2 f(x) \qquad \text{for all } n \in \mathbb{Z}.$$

Lemma 1.6. *Let $f : \mathbb{Z}^n \to C$ is a quadratic form, suppose that $f(\mathbf{e}_i) = 0$ and $f(\mathbf{e_i} + \mathbf{e_j}) = 0$ for $i \neq j$. Then f is the zero function.*

Proof. The parallelogram law for the function f implies the existence of the inner product

$$\langle x, y \rangle = \frac{f(x+y) - f(x-y)}{4} \quad \text{such that } \langle x, x \rangle = f(x).$$

Let $x \in \mathbb{Z}^n$ and write $x = \sum_{i=1}^{n} a_i \mathbf{e_i}$. Then we obtain by linearity and symmetry of the inner product the formula

$$f\big(\sum_{i=1}^{n} a_i \mathbf{e_i}\big) = \sum_{i=1}^{n} \big(2a_i^2 + \sum_{j=1}^{n} a_i a_j\big) f(\mathbf{e_i}) + \sum_{1 \leq i < j \leq n} a_i a_j f(\mathbf{e_i} + \mathbf{e_j}).$$

□

Proposition 1.7. *Let K be a field and $W : A \to K$ an elliptic net. Let $f : A \to K^*$ be a quadratic form. Define $W^f : A \to K$ by*

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

Then W^f is also an elliptic net.

Proof. As usual, we use multiplicative notation for the group K^*. The parallelogram law for f says that

$$f(p-q)f(p+q) = f(p)^2 f(q)^2, \tag{2.4}$$

for all $p, q \in A$. Let $p, q, r, s \in A$. From definition 1.4 we get the following equation

$$f(p+q+s)f(p)f(q)f(s)f(p+q)^{-1} = f(q+s)f(p+s). \tag{2.5}$$

By multiplying equations (2.4) and (2.5) one finds

$$f(p+q+s)f(p-q) = f(p)f(q)f(p+s)f(q+s)f(s)^{-1}.$$

We multiply the above equation by $f(r)f(r+s)$ to find

$$f(p+q+s)f(p-q)f(r+s)f(r) = f(p)f(q)f(r)f(p+s)f(q+s)f(r+s)f(s)^{-1}.$$

Notice that the right-hand side is symmetric in p, q and r, hence

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

Replacing W by W^f in the recurrence (2.2) and using the distributive law in K one immediately sees that the recurrence also holds for W^f.

□

We call W and W^f *scale equivalent*. In general, if V and W are elliptic nets with the property that there exists a quadratic function f and a constant $k \in K^*$ such that $W = kV^f$, then we call them scale equivalent and write $W \sim V$.

Lemma 1.8. *The relation $\sim$ on the set of elliptic nets is an equivalence relation.*

Proof. The relation is reflexive: take for f the quadratic function which maps everything to 1. Suppose that $W \sim V$, hence there exists a constant $c \in K^*$ and a quadratic form f as in proposition 1.7 such that $W(x) = cf(x)V(x)$. Clearly $V(x) = \dfrac{W(x)}{cf(x)}$ and $1/(cf)$ is also a quadratic form, which means that $V \sim W$, i.e. $\sim$ is symmetric. Let U,V and W be elliptic nets such that $U \sim V$ and $V \sim W$. We have constants $c, d \in K^*$ and quadratic forms f and g such that

$$U(x) = cf(x)V(x), \quad V(x) = dg(x)W(x).$$

We obtain $U(x) = cdf(x)g(x)W(x)$, define the quadratic form $h = cdfg$ so that $U = W^h$, hence $U \sim W$. This proves the transitivity. □

Let W be an elliptic net, we say that W is *normalised* if $W(\mathbf{e_i}) = 1$ for all i and $W(\mathbf{e_i} + \mathbf{e_j}) = 1$ for all $1 \leq i < j \leq n$. This property of an elliptic net clearly depends on the choice of a basis for $\mathbb{Z}^n$.

We will only be concerned with *non-degenerate* elliptic nets.

Definition 1.9. *Let W be an elliptic net of rank n.*

- *for $n = 1$: we say that W is degenerate if one of the terms $W(1), W(2)$ or $W(3)$is zero.*
- *for $n \geq 2$: we say that W is degenerate if any term of the form $W(\mathbf{e_i})$, $W(2\mathbf{e_i})$, $W(\mathbf{e_i}+\mathbf{e_j})$ or $W(\mathbf{e_i}-\mathbf{e_j})$ is zero, where $i \neq j$.*

We call W non-degenerate when W does not meet one of these two conditions.

Proposition 1.10. *Let W be a non-degenerate elliptic net. There is exactly one scaling W^f which is normalised.*

Proof. We first prove the existence, since W is non-degenerate we define

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

Claiming that f is a quadratic form is equivalent with the claim that

(2.6)
$$(p_i+q_i+s_i)(p_j+q_j+s_j)+p_ip_j+q_iq_j+s_is_j = (p_i+q_i)(p_j+q_j)+(q_i+s_i)(q_j+s_j)+(p_i+s_i)(p_j+s_j),$$

for $1 \leq i \leq j \leq n$. It is not difficult to verify equation (2.6), so f is a quadratic form. We also have

$$W^f(\mathbf{e_i}) = A_{ii}W(\mathbf{e_i}) = 1, \quad \text{for all } 1 \leq i \leq n,$$

and

$$W^f(\mathbf{e_i}+\mathbf{e_j}) = A_{ij}A_{ii}A_{jj}W(\mathbf{e_i}+\mathbf{e_j}) = 1, \quad \text{for all } 1 \leq i < j \leq n,$$

hence W^f is a normalised scaling of W. It remains to prove the uniqueness. Therefore suppose that W^g is also a normalised elliptic net. Then

$$\big(f(\mathbf{v}) - g(\mathbf{v})\big)W(\mathbf{v}) = 0, \quad \text{for all } \mathbf{v} \in \big\{\mathbf{e_i}\big\} \cup \big\{\mathbf{e_i}+\mathbf{e_j} |\ i \neq j\big\}.$$

Since W is non degenerate, the image of $f - g$ (which is also a quadratic form) restricted to those values of $\mathbf{v}$ is zero. Therefore, by lemma 1.6 we have proved that $f = g$. □

We can speak about *the normalisation* $\widetilde{W}$ of a non-degenerate elliptic net.

In the following subsection we will create an *universal* ring from which we can prove general results about elliptic nets.

1.3 Universal ring $\mathcal{W}$

Let $I \cong \mathbb{Z}^n$ be an abelian group. To each $i \in I$ we associate a symbol T_i. We let $\mathcal{M} \lhd \mathbb{Z}[T_i]_{i\in I}$ be the ideal generated by T_0 and the polynomials of the form

(2.7) $$T_{p+q+s}T_{p-q}T_{r+s}T_r + T_{q+r+s}T_{q-r}T_{p+s}T_p + T_{r+p+s}T_{r-p}T_{q+s}T_q, \quad \text{for all } p,q,r,s \in I.$$

We call these polynomials *recurrence relations*. Denote by Z the ring $\mathbb{Z}[T_i]_{i\in I}/\mathcal{M}$ and write $\mathcal{N}(A)$ for the nilradical of a ring A. Then we define *the universal ring associated to* I

$$\mathcal{W}_I = \frac{Z}{\mathcal{N}(Z)}.$$

Remark 1.11. *The ring $\mathcal{W}_I$ is not trivial.*

Proof. We first need to show that Z is not the trivial ring. Suppose that this does not hold, i.e. $\mathbb{Z}[T_i]_{i\in I} = \mathcal{M}$, then there exists a relation (in $\mathbb{Z}[T_i]_{i\in I}$

$$1 = a_0 T_0 + \sum_{j\in J} b_j r_j,$$

where J is a finite subset of I, r_j are recurrence relations and both a_0 and b_j are contained in $\mathbb{Z}[T_i]_{i\in I}$. It is clear that if we would simplify the right- hand side by writing it as a sum of different monomials, we either get the zero polynomial or a polynomial without a constant term. Since we work in the ring $\mathbb{Z}[T_i]_{i\in I}$ both cases are not possible, this is a contradiction. It remains to show that $Z \neq \mathcal{N}(Z)$. Note that $\mathcal{N}(Z)$ equals the intersection of all prime ideals in Z. By the bijection between prime ideals

(2.8)
$$\pi : \big\{I|\ I \lhd \mathbb{Z}[T_i]_{i\in I} \text{ is a prime ideal containing } \mathcal{M}\big\} \to \big\{J|\ J \lhd Z \text{ is a prime ideal}\big\}$$
$$i \mapsto i + \mathcal{M},$$

this corresponds to the intersection of prime ideals in $\mathbb{Z}[T_i]_{i\in I}$ containing $\mathcal{M}$. Since $\mathcal{M}$ is contained in some maximal ideal $\mathcal{M} \subset J \lhd \mathbb{Z}[T_i]_{i\in I}$, this intersection is also contained in $J + \mathcal{M} \subsetneq Z$. □

The following proposition states exactly how elliptic nets are related to the universal ring $\mathcal{W}_I$.

Proposition 1.12. *There is a bijection between elliptic nets $W : I \to R$ and homomorphisms $\mathcal{W}_I \to R$.*

Proof. Suppose that we have been given an elliptic net $W : I \to R$. Consider the map

$$\psi : \mathbb{Z}[T_i] \to R \qquad T_i \mapsto W(i).$$

Then ψ is a well-defined ring homomorphism. Observe that ψ induces a ring homomorphism

$$\bar{\psi} : \mathcal{W}_I \to R \qquad \bar{T}_i \mapsto W(i).$$

To prove that $\bar{\psi}$ is well-defined it suffices, by the definition of $\mathcal{W}_I$, to show that the kernel of ψ contains all the elements that have some power in $\mathcal{M}$. Because R is an integral domain, this property follows once we have proven that $\mathcal{M}$ is contained in the kernel of ψ. By the definition of $\mathcal{M}$, the properties (2.1) and (2.2) satisfied by the elliptic net W imply that $\mathcal{M} \subset \ker \psi$.
We now prove that the correspondence that we have just defined is a bijection. By construction, the image of $\bar{T}_i$ is $W(i)$ thus different elliptic nets give rise to different ring homomorphisms $\bar{\psi} : \mathcal{W}_I \to R$, this proves the injectivity. To prove the surjectivity, suppose that we have been given a ring homomorphism

$$\phi : \mathcal{W}_I \to R.$$

Then consider the following function:

$$W : I \to R \quad W(i) = \phi(\bar{T}_i)\,.$$

Since ϕ is a ring homomorphism and $T_0 \in \mathcal{M}$, we have $W(0) = \phi(\bar{T}_0) = \phi(0) = 0$. Moreover, relations (2.2) are satisfied because the corresponding combinations of the T_i's belong to $\mathcal{M}$ by definition. This proves that W is an elliptic net, and we conclude by remarking that ϕ is the image of W via the correspondence defined above. □

One application is the following

Proposition 1.13. *Let $W : I \to R$ be an elliptic net. Then $W(-i) = -W(i)$ for all $i \in I$*

Proof. By proposition 1.12, we only need to demonstrate that $T_{-i} = -T_i$ in $\mathcal{W}_I$. Take $p = q = i, r = s = 0$ in the recurrence relation to show that $T_i^3(T_i + T_{-i}) \in \mathcal{M}$. Similarly $T_{-i}^3(T_i + T_{-i}) \in \mathcal{M}$. Take a prime ideal $\mathcal{P} \supset \mathcal{M}$, then it contains $T_i + T_{-i}$; for if it did not then surely it contains T_i and T_{-i}, a contradiction. We know that

$$\mathcal{N}(Z) = \pi\left(\bigcap_{\mathcal{P}\supset\mathcal{M}} \mathcal{P}\right),$$

where π is defined by (2.8). Hence $T_i + T_{-i} \in \mathcal{N}(Z)$, which shows that $W(-i) = -W(i)$ for all $i \in I$. □

1.4 Base sets

Our goal is to show that elliptic nets are determined by some *initial values*. Therefore, we introduce some terminology/ techniques that will be used in the induction proofs below. Take $i \in I$ and consider finite sets $S, J \subset I$ where $0, i \notin S \cup J$.

Definition 1.14. *The index i is S-integrally implied by J if there exists a polynomial $P_S \in \mathbb{Z}[T_s]_{s\in S}$ and a polynomial $Q_J \in \mathbb{Z}[T_j]_{j\in J}$ such that*

$$T_i P_S = Q_J \tag{2.9}$$

in $\mathcal{W}_I$. A set $K \subset I$ is S-integrally implied by J if the previous holds for any index $k \in K$.

In light of proposition 1.12, definition 1.14 is very useful to study elliptic nets. Suppose that $W(s) \neq 0$ for all $s \in S$. If i is S-integrally implied by J, then it follows by proposition 1.12 (if we impose some extra conditions on W) that $W(i)$ can be written as the quotient of integer polynomials f_J/f_s such that $f_j \in \mathbb{Z}[T_j]_{j\in J}$ and $f_S \in \mathbb{Z}[T_s]_{s\in S}$. Therefore the following definition is well motivated.

Definition 1.15. *A set $B \subset I$ is an S-integral baseset for $\mathcal{W}_I$ if all of I is S-integrally implied by B.*

Note that if i is S-integrally implied by J and every $j \in J$ is S-integrally implied by J', then i is S-integrally implied by J'.
The higher the rank the more cumbersome it gets to write an element of $\mathcal{W}_I$. For instance, take $n = 3$ and the recurrence relation (which is zero in $\mathcal{W}_I$)

$$\begin{aligned} &T_{(1,1,0)}T_{(1,-1,0)}T_{(0,0,1)}T_{(0,0,1)} + \\ &\qquad T_{(0,1,1)}T_{(0,1,-1)}T_{(1,0,0)}T_{(1,0,0)} + \\ &\qquad\qquad T_{(1,0,1)}T_{(-1,0,1)}T_{(0,1,0)}T_{(0,1,0)}. \end{aligned}$$

The indices come from (2.7) with

$$\mathbf{p} = (1,0,0), \quad \mathbf{q} = (0,1,0), \quad \mathbf{r} = (0,0,1), \quad \mathbf{s} = (0,0,0).$$

Let us introduce a handy notation for the information explained above:

$$\begin{array}{ccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array} \left[\begin{array}{cccc|cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right]. \tag{2.10}$$

The first four columns denote the vectors $\mathbf{p}, \mathbf{q}, \mathbf{r}$,$\mathbf{s}$, while everything between the square brackets denotes the recurrence relation corresponding to these four vectors. The square brackets contain three sub arrays seperated by a vertical line. It is convenient to call them the *terms of the square bracket*. We call an expression like (2.10) *an extended bracket*. Hence, one can show that $i \in I$ is S-integrally implied by J, by finding an extended bracket such that one term contains one index i and three indices from S while the other two terms contain only indices from J. Observe that an extended bracket of n rows can be obtained by writing down n extended brackets with one row and put them on top of each other.

Definition 1.16. *The sup-norm of a vector* $\mathbf{v} = (v_1, \cdots, v_n) \in \mathbb{Z}^n$ *is defined by*

$$N(\mathbf{v}) = \max_{i=1,\cdots,n} |v_i|.$$

1.5 Generate terms of an elliptic net

Our goal is to show that an *extension* of the universal ring $\mathcal{W}_I$ is finitely generated as a $\mathbb{Z}$-algebra. We search a finite subset $0 \notin J \subset I$ such that the localization $\mathcal{W}_I[T_j^{-1}]_{j\in J}$ is finitely generated as a $\mathbb{Z}$-algebra and to give generators. In order for the localization $\mathcal{W}_I[T_j^{-1}]_{j\in J}$ to be a non-trivial ring we must have that $T_i \neq 0$ in $\mathcal{W}_I$ for $i \in I \setminus \{0\}$.

Lemma 1.17. *If* $i \in I \setminus \{0\}$*, then* $T_i \neq 0$ *in* $\mathcal{W}_I$*.*

Proof. By proposition 1.12, the consequence of $T_i = 0$ is that for every elliptic net $W : \mathbb{Z}^n \to \mathbb{R}$ we have $W(i) = 0$. Suppose that $i \neq 0$ and $T_i = 0$, then i has a non-zero component i_k. We have a group homomorphism $p_k : \mathbb{Z}^n \to \mathbb{Z} : p_k(\mathbf{v}) = v_k$ and a map on $\mathbb{Z}^n$ defined by

$$W = W_{id} \circ p_k : \mathbb{Z}^n \to \mathbb{Z} : \mathbf{v} \mapsto W(\mathbf{v}) = v_k,$$

which is also an elliptic net by proposition (3.3). We have $W(i) = W_{id}(i_k) = i_k \neq 0$: a contradiction. □

Theorem 1.18. *The ring* $\mathcal{W}_{\mathbb{Z}}[T_1^{-1}, T_2^{-1}]$ *is generated as a* $\mathbb{Z}$*-algebra by the set*

$$\left\{T_1, T_1^{-1}, T_2, T_2^{-1}, T_3, T_4\right\}.$$

Each T_i *can be written as an integer polynomial in*

$$T_1, T_1^{-1}, T_2, T_3, T_4T_2^{-1}.$$

Proof. It was shown that $T_{-n} = -T_n$ in $\mathcal{W}_{\mathbb{Z}}$, hence it suffices to prove the statements for positive n. Replace (p, q, r, s) in equation (2.7) by $(n+1, n, 1, 0)$ and $(n+1, n-1, 1, 0)$ respectively, to get the following equations in $\mathcal{W}_{\mathbb{Z}}$

$$T_{2n+1}T_1^3 + T_{n-1}T_{n+1}^3 + T_{n+2}T_{-n}T_n^2 = 0, \tag{2.11}$$

$$T_{2n}T_2T_1^2 + T_nT_{n-2}T_{n+1}^2 + T_{n+2}T_{-n}T_{n-1}^2 = 0. \tag{2.12}$$

The proof of both statements is by induction. The first statement is obviously true for T_n such that $0 \leq n \leq 4$. Take $k \geq 4$ and suppose that T_i $(0 \leq i \leq k)$ is generated as a $\mathbb{Z}$-algebra by the set given in the first statement. We prove that T_{k+1} is also generated by the same set. Suppose that $k+1 \geq 5$ is odd, say $2m+1$ (hence $m \geq 2$), then using (2.11) and the fact that $2m+1 > m+2$, the statement is obviously true for T_{k+1}. In the other case we can write $k+1 = 2m$ with $m \geq 3$. Now we use (2.12) and the given $2m > m+2$ to finish this case. The proof of the first statement is complete. The proof by induction of the second statement is analogous. □

Corollary 1.19. *Let $W : \mathbb{Z} \to \mathbb{Q}$ be an elliptic net satisfying*

$$W(1) = 1, \quad W(2) \neq 0, \quad \textit{for } 2 \leq i \leq 4 : \ W(i) \in \mathbb{Z} \quad \textit{and } W(2)|W(4).$$

Then $W(\mathbb{Z}) \subset \mathbb{Z}$.

Proof. By the previous theorem and proposition 1.12, $W(i)$ can be expressed as a $\mathbb{Z}$-coefficient polynomial expression in $W(2), W(3), W(4)/W(2) \in \mathbb{Z}$ □

We can find similar results for the rank two case, but we first need a lemma.

Lemma 1.20. *The ring $\mathcal{W}_{\mathbb{Z}^2}[T_{(1,-1)}^{-1}, T_{(1,0)}^{-1}, T_{(0,1)}^{-1}]$ is generated as a $\mathbb{Z}$-algebra by the set*

$$\left\{T_{\mathbf{v}} \mid N(\mathbf{v}) \leq 4\right\} \cup \left\{T_{(1,1)}^{-1}, T_{(1,0)}^{-1}, T_{(0,1)}^{-1}\right\}.$$

Proof. Set $S = \{(1,0), (0,1), (1,1)\}$ and $B = \{\mathbf{v} \in \mathbb{Z}^2 \mid N(\mathbf{v}) \leq 4\}$. We need to prove that $\mathbb{Z}^2$ is S-integrally implied by B. This proof proceeds by induction on the sup-norm. The base case $N(\mathbf{v}) \leq 4$ is trivial. Let $c > 4$, suppose that all terms with indices with sup-norm less than c, denote it by K_c, are S-integrally implied by B. Suppose that $N(\mathbf{v}) = c$. We will show that $\mathbf{v}$ is S-integrally implied by K_c, then it follows immediately that $\mathbf{v}$ is S-integrally implied by B. For $i = 1, 2$, let $w_i = \lceil v_i \rceil$. We consider three cases.

- Case 1: $\mathbf{v}$ has one odd entry and one even entry. For the odd entry, we use the extended bracket

$$\begin{matrix} w_i & w_i{-}1 & 0 & 0 \end{matrix} \left[\begin{matrix} v_i & 1 & 0 & 0 \end{matrix} \middle| \begin{matrix} w_i{-}1 & w_i{-}1 & w_i & w_i \end{matrix} \middle| \begin{matrix} w_i & -w_i & w_i{-}1 & w_i{-}1 \end{matrix} \right].$$

  For the even entry, we use the extended bracket

$$\begin{matrix} w_i & w_i & 1 & 0 \end{matrix} \left[\begin{matrix} v_i & 0 & 1 & 1 \end{matrix} \middle| \begin{matrix} w_i{+}1 & w_i{-}1 & w_i & w_i \end{matrix} \middle| \begin{matrix} w_i{+}1 & -w_i{+}1 & w_i & w_i \end{matrix} \right].$$

- Case 2: $\mathbf{v}$ has two odd entries. Use the extended bracket

$$\begin{matrix} w_1 & w_1{-}1 & 0 & 0 \\ w_2 & w_2{-}1 & 1 & 0 \end{matrix} \left[\begin{matrix} v_1 & 1 & 0 & 0 \\ v_2 & 1 & 1 & 1 \end{matrix} \middle| \begin{matrix} w_1{-}1 & w_1{-}1 & w_1 & w_1 \\ w_2 & w_2{-}2 & w_2 & w_2 \end{matrix} \middle| \begin{matrix} w_1 & -w_1 & w_1{-}1 & w_1{-}1 \\ w_2{+}1 & -w_2{+}1 & w_2{-}1 & w_2{-}1 \end{matrix} \right]$$

- Case 3: $\mathbf{v}$ has two even entries. Use the extended bracket

$$\begin{matrix} w_1 & w_1{-}1 & 0 & 1 \\ w_2 & w_2 & 1 & 0 \end{matrix}\left[\begin{matrix} v_1 & 1 & 1 & 0 \\ v_2 & 0 & 1 & 1 \end{matrix}\middle|\begin{matrix} w_1 & w_1{-}1 & w_1{+}1 & w_1 \\ w_2{+}1 & w_2{-}1 & w_2 & w_2 \end{matrix}\middle|\begin{matrix} w_1{+}1 & -w_1 & w_1 & w_1{-}1 \\ w_2{+}1 & -w_2{+}1 & w_2 & w_2 \end{matrix}\right]$$

For even v_i, either $|v_i| \leq 2$ or $|v_i| > 3$. In the former case, $|w_i| + 1 \leq 2 < c$. In the latter case, we have $|w_i|+1 \leq (|v_i|+2)/2 < |v_i| \leq c$. For odd v_i, either $|v_i| \leq 3$ or $|v_i| > 4$. In the former case $|w_i| + 2 \leq 4 < c$. In the latter case, we have $|w_i| + 2 \leq (|v_i| + 5)/2 < |v_i| \leq c$. Therefore all indices occurring in the second and third term of the extended brackets are contained in K_c. The index $\mathbf{v}$ occurs in the first term of each extended bracket, each time the remaining three indices are contained in S. We demonstrated that $\mathbf{v}$ is S-integrally implied by K_c and hence by B, which completes the proof of the induction step. □

Theorem 1.21. *The ring $\mathcal{W}_{\mathbb{Z}^2}[T_{(1,-1)}^{-1}, T_{(1,0)}^{-1}, T_{(0,1)}^{-1}]$ is generated as a $\mathbb{Z}$-algebra by the elements*

$$\left\{T_{\mathbf{v}} \mid N(\mathbf{v}) \leq 2,\ \mathbf{v} \neq (0,0)\right\} \cup \left\{T_{(1,1)}^{-1}, T_{(1,0)}^{-1}, T_{(0,1)}^{-1}\right\}$$

Proof. By the previous lemma it suffices to show B is S-integrally implied by the set

$$\big\{(1,0),(0,1),(1,1),(2,0),(0,2),(2,1),(1,2),(2,2)\big\}.$$

This can be done in a similar way as in the proof of the previous lemma. See [35, Theorem 2.5]. □

Corollary 1.22. *Let $W : \mathbb{Z}^2 \to \mathbb{Q}$ be an elliptic net for which*

1. $W(1,0) = W(0,1) = W(1,1) = 1$,
2. $W(2,0)$, $W(0,2)$, $W(1,2) \neq W(2,1)$ *are integers, and*
3. $W(1,2) - W(2,1)$ *divides* $W(0,2)W(2,1) - W(2,0)W(1,2)$,

then all terms of the elliptic net are determined by these seven values and are integers.

Proof. Consider the extended brackets

$$\begin{matrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{matrix}\left[\begin{matrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{matrix}\middle|\begin{matrix} 1 & -1 & 1 & 1 \\ 2 & 0 & 0 & 0 \end{matrix}\middle|\begin{matrix} 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{matrix}\right], \tag{2.13}$$

$$\begin{matrix} 1 & 1 & -1 & 0 \\ 1 & 2 & 1 & -1 \end{matrix}\left[\begin{matrix} 2 & 0 & -1 & -1 \\ 2 & -1 & 0 & 1 \end{matrix}\middle|\begin{matrix} 0 & 2 & 1 & 1 \\ 2 & 1 & 0 & 1 \end{matrix}\middle|\begin{matrix} 0 & -2 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{matrix}\right],$$

from which we obtain the identities

$$\begin{aligned} T_{(1,-1)}T_{(1,1)}^3 &= T_{(1,0)}^3 T_{(1,2)} - T_{(0,1)}^3 T_{(2,1)}, \\ T_{(2,2)}T_{(1,-1)}T_{(1,0)}T_{(0,1)} &= T_{(1,1)}\left(T_{(0,2)}T_{(2,1)}T_{(1,0)} - T_{(0,1)}T_{(2,0)}T_{(1,2)}\right). \end{aligned}$$

Again, the given elliptic net provides a ring morphism $\mathcal{W}_{\mathbb{Z}^2} \to \mathbb{Q}$ as was demonstrated in proposition 1.12. We then find the relations

$$\begin{aligned} W(1,-1) &= W(1,2) - W(2,1), \\ W(2,2) &= \frac{W(0,2)W(2,1) - W(2,0)W(1,2)}{W(1,-1)} \in \mathbb{Z}. \end{aligned}$$

By the previous theorem we conclude that the elliptic net is determined by the seven values and that all terms of the net are integers. □

Theorem 1.23 ([35, Theorem 2.8])**.** *Let $n \geq 2$. For each ℓ in the set*

$$L = \{0,1\}^n \setminus \{(0,0,\ldots,0),(1,1,\ldots,1)\},$$

choose a vector $\mathbf{x}_\ell$ having $N(\mathbf{x}_\ell) = 1$ and having non-zero entries exactly where ℓ does. Let $G_n = \{\mathbf{x}_\ell\}_{\ell \in L}$. Let

$$H_n = G_n \cup \{\mathbf{e}_i\} \cup \{\mathbf{e}_i \pm \mathbf{e}_j, i \neq j\} \cup \{2\mathbf{e}_i\},$$
$$H'_n = H_n \cup \{2\mathbf{e}_i + \mathbf{e}_j, i \neq j\}.$$

Then $\mathbb{Z}^n$ is H_n-integrally implied by H'_n.

Proof. The proof is by induction on the rank n. Theorem 1.21 delivers the base case $n = 2$. If $\mathbf{v}$ contains a zero, we can reduce the problem to a lower rank. Therefore one can assume that $\mathbf{v}$ contains no zeroes. The proof proceeds by looking at the number of odd and even components of $\mathbf{v}$. □

2 Elliptic nets over $\mathbb{C}$.

In this section we explain Stanges construction of an elliptic net of any rank from an elliptic curve $E/\mathbb{C}$ over the field of complex numbers. This will constitute a generalisation of the rank one case studied by M. Ward, see theorem 3.2, chapter 1.

2.1 The functions $\Omega_{\mathbf{v}}$

Definition 2.1. *Fix a lattice Λ corresponding to an elliptic curve $E/\mathbb{C}$. Fix $\mathbf{v} \in \mathbb{Z}^n$. Define a meromorphic function $\Omega_{\mathbf{v}}$ on $\mathbb{C}^n$ as follows*

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

If $\mathbf{v} = \mathbf{0}$ we set $\Omega_{\mathbf{v}} \equiv 0$.

In the rank one case we obtain the function

$$\Omega_{\mathbf{v}}(z) = \frac{\sigma(vz)}{\sigma(z)^{2v^2 - v^2}} = \frac{\sigma(vz)}{\sigma(z)^{v^2}}.$$

For $n = 2$ we have for each pair $(v_1, v_2) \in \mathbb{Z}^2$ the function

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

Proposition 2.2. *Let E be an elliptic curve over $\mathbb{C}$. Denote by Λ the lattice which corresponds to the elliptic curve E. For every $\mathbf{v} \in \mathbb{Z}^n$, the function $\Omega_{\mathbf{v}}$ has the following property*

$$\Omega_{\mathbf{v}}(\mathbf{z} + w\mathbf{e_i}) = \Omega_{\mathbf{v}}(\mathbf{z}) \quad \textit{for all } w \in \Lambda \textit{ and for } 1 \leq i \leq n,$$

where $\mathbf{e_i}$ denotes the standard basis.

Proof. It suffices to show that the $\Omega_{\mathbf{v}}$ are elliptic in the first variable. To see this, take $\mathbf{v} \in \mathbb{Z}^n, \mathbf{z} \in \mathbb{C}^n$, and define

$$\mathbf{v}' = (v_k, \ldots, v_1, \ldots, v_n), \quad \mathbf{z}' = (z_k, \ldots, z_1, \ldots, z_n),$$

i.e the first and k^{th} component are interchanged. Clearly

$$\Omega_{\mathbf{v}'}(\mathbf{z}') = \Omega_{\mathbf{v}}(\mathbf{z}),$$

hence if we prove the ellipticness in the first variable, then the ellipticness in the k^{th} variable follows immediately. We calculate

$$\frac{\Omega_{\mathbf{v}}(\mathbf{z} + w\mathbf{e}_1)}{\Omega_{\mathbf{v}}(\mathbf{z})} = \frac{\lambda(v_1 w)}{\lambda(w)^{v_1^2}} = 1, \tag{2.14}$$

the last equation follows from the definition of λ. This shows the ellipticness in the first variable. The proof is complete. □

Proposition 2.3. *Fix a lattice Λ, let $\mathbf{z} \in \mathbb{C}^n$ and $v \in \mathbb{Z}^m$. Let T be a matrix in $\mathbb{Z}^{n\times m}$ and denote the transpose by T^{tr}. Then*

$$\Omega_{\mathbf{v}}(T^{tr}(\mathbf{z})) = \frac{\Omega_{T(\mathbf{v})}(\mathbf{z})}{\prod_{i=1}^{m} \Omega_{T(\mathbf{e_i})}(\mathbf{z})^{2v_i^2 - \sum_j v_i v_j} \prod_{1\le i<j\le m} \Omega_{T(\mathbf{e_i}+\mathbf{e_j})}(\mathbf{z})^{v_i v_j}}. \tag{2.15}$$

Proof. We first set some notations to make the calculations more transparent. Let $T \in \mathbb{Z}^{n\times m}, \mathbf{v} \in \mathbb{Z}^m$ and $\mathbf{z} \in \mathbb{C}^n$. Denote by k_i the i^{th} column of the matrix T and k_{ij} the j^{th} term of the vector k_i, for all $1 \le i \le m$ and $1 \le j \le n$. Similarly, for the rows of T we have the row vector r_i and denote by r_{ij} the j^{th} component of r_i. By definition 2.1, the left hand side of (2.15) is

$$\Omega_{\mathbf{v}}(T^{tr}(\mathbf{z})) = \frac{\sigma(v_1 k_1 \cdot \mathbf{z} + \cdots + v_m k_m \cdot \mathbf{z})}{\prod_{i=1}^{n} \sigma(k_i \cdot \mathbf{z})^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1\le i<j\le n} \sigma(k_i \cdot \mathbf{z} + k_j \cdot \mathbf{z})^{v_i v_j}}. \tag{2.16}$$

To make the calculations clearer, we split the right hand side of (2.15). The numerator is

$$\Omega_{T\mathbf{v}}(z) = \frac{\sigma(r_1 \cdot \mathbf{v} z_1 + \cdots + r_n \cdot \mathbf{v} z_n)}{\prod_{i=1}^{n} \sigma(z_i)^{2(r_i\cdot\mathbf{v})^2 - r_i\cdot\mathbf{v}\sum_{j=1}^{n} r_j\cdot\mathbf{v}} \prod_{1\le l<s\le n} \sigma(z_l + z_s)^{r_l\cdot\mathbf{v}\ r_s\cdot\mathbf{v}}}, \tag{2.17}$$

the denumerator can be written as

$$\prod_{i=1}^{m} \left\{ \frac{\sigma(k_i \cdot \mathbf{z})}{\prod_{l=1}^{m} \sigma(z_l)^{2k_{il}^2 - k_{il}\sum_j k_{ij}} \prod_{l<s} \sigma(z_l + z_s)^{k_{il}k_{is}}} \right\}^{2v_i^2 - v_i \sum_j v_j} \cdot \tag{2.18}$$

$$\prod_{1\le i<j\le m} \left\{ \frac{\sigma((k_{i1}+k_{j1})z_1 + \cdots + (k_{in}+k_{jn})z_n)}{\prod_l \sigma(z_l)^{(k_{il}+k_{jl})(2(k_{il}+k_{jl}) - \sum_p k_{ip}+k_{jp})} \prod_{l<s} \sigma(z_l + z_s)^{(k_{il}+k_{jl})(k_{is}+k_{js})}} \right\}^{v_i v_j}$$

After cancellation of some terms, we see that (2.15) holds if and only if

$$\begin{aligned}(2.19)\quad \prod_{i=1}^{n}\sigma(z_i)^{2(r_i\cdot\mathbf{v})^2-r_i\cdot\mathbf{v}\sum_{j=1}^{n}r_j\cdot\mathbf{v}}\prod_{1\le l<s\le n}\sigma(z_l+z_s)^{r_l\cdot\mathbf{v}\ r_s\cdot\mathbf{v}} = \\ \prod_{i=1}^{m}\Big\{\prod_{l=1}^{m}\sigma(z_l)^{2k_{il}^2-k_{il}\sum_j k_{ij}}\prod_{l<s}\sigma(z_l+z_s)^{k_{il}k_{is}}\Big\}^{2v_i^2-v_i\sum_j v_j}\cdot \\ \prod_{1\le i<j\le m}\Big\{\prod_{l}\sigma(z_l)^{(k_{il}+k_{jl})(2(k_{il}+k_{jl})-\sum_p k_{ip}+k_{jp})}\prod_{l<s}\sigma(z_l+z_s)^{(k_{il}+k_{jl})(k_{is}+k_{js})}\Big\}^{v_iv_j}.\end{aligned}$$

Compare the powers of $\sigma(z_l+z_s)$ and $\sigma(z_i)$ on both sides to complete the proof. □

2.2 From elliptic curves over $\mathbb{C}$ to elliptic nets.

Fix a lattice Λ corresponding to an elliptic curve $E/\mathbb{C}$. The main result is the following theorem

Theorem. *Fix $\mathbf{z}\in\mathbb{C}^n$. The function $W:\mathbb{Z}^n\to\mathbb{C}$ defined by*

$$W(\mathbf{v})=\Omega_{\mathbf{v}}(z_1,\cdots,z_n;\Lambda)$$

is an elliptic net.

We first start with two lemmas.

Lemma 2.4. *Suppose that $\wp$ is the Weierstrass $\wp$-function corresponding to the lattice Λ. We have the following properties*

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

Proof. A proof for the first equation can be found in [7]. The first statement implies the second one: by definition 2.1 we get

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

□

Recall the definitions of the functions $\wp,\zeta,\sigma$. Recall that $\mathbb{C}(\Lambda)$ denotes the field of elliptic functions with respect to the lattice Λ. We will need next lemma, which gives a relation between these Weierstrass functions.

Lemma 2.5. *Let ζ denote the Weierstrass ζ-function.*

$$\begin{aligned}\zeta(x+a)-\zeta(a)-\zeta(x+b)+\zeta(b) &= \frac{\sigma(x+a+b)\sigma(x)\sigma(a-b)}{\sigma(x+a)\sigma(x+b)\sigma(a)\sigma(b)},\\ \zeta(x+a+b)-\zeta(x+a)-\zeta(x+b)+\zeta(x) &= \frac{\sigma(2x+a+b)\sigma(a)\sigma(b)}{\sigma(x+a+b)\sigma(x+a)\sigma(x+b)\sigma(x)}.\end{aligned}$$

Proof. The second equation follows from the first one after a change of variables

$$x \leftarrow a,\ a \leftarrow x+b,\ b \leftarrow x.$$

Now we prove the first equation:
Define the functions

$$f(\xi) = \zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b) \quad \text{and} \quad g(\xi) = \frac{\sigma(x+a+b)\sigma(x)\sigma(a-b)}{\sigma(x+a)\sigma(x+b)\sigma(a)\sigma(b)},$$

where ξ denotes one of the variables x, a or b. These functions are elliptic considered as a function in one variable, i.e. these are elements of $\mathbb{C}(\Lambda)$. We can prove the latter by recalling the properties

$$\zeta(z+w) = \zeta(z) + \eta(w) \quad \text{and } \sigma(z+w) = \lambda(w)e^{\eta(w)(z+\frac{w}{2})}\sigma(z) \quad \text{for all } w \in \Lambda.$$

Suppose that $a, b \notin \Lambda$ and consider $f(x)$ and $g(x)$ as meromorphic functions in x. If $a \equiv b \pmod{\Lambda}$ then $f = g = 0$ in $\mathbb{C}(\Lambda)$. So we can take $a \not\equiv b$, then $f(x)$ and $g(x)$ have the same simple poles, namely $\{-a, -b\}$, and no other poles. The meromorphic function $g(x)$ vanishes exactly at $x = -a-b$ and $x = 0$, both with order one. We have seen that ζ is an odd function, hence

$$f(-a-b) = \zeta(-b) - \zeta(a) - \zeta(-a) + \zeta(b) = 0 \quad \text{and } f(0) = \zeta(a) - \zeta(a) - \zeta(b) + \zeta(b) = 0.$$

These are the only vanishing points of $f(x)$, and are both of order 1. The last two statements can easily be proven by using the fact $deg(div(f(x))) = 0$. So there is a constant c (depending on a and b) such that $f(x)/g(x) = c$. Define

$$\begin{aligned} F &= (\zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b))\sigma(x+a)\sigma(x+b), \\ G &= \sigma(x+a+b)\sigma(x), \end{aligned}$$

which implies that

$$F(x) = \frac{c}{\sigma(a)\sigma(b)}G(x).$$

Then, $F(x)$ is holomorphic on $\mathbb{C}$ because $G(x)$ is holomorphic on $\mathbb{C}$. Take the derivative of both sides at $x = 0$ to find

$$\begin{aligned} (\wp(b) - \wp(a))\sigma(a)\sigma(b) &= \frac{c}{\sigma(a)\sigma(b)}(\sigma'(a+b)\sigma(0) + \sigma(a+b)\sigma'(0)) \\ &= \frac{c}{\sigma(a)\sigma(b)}(\sigma(a+b)\sigma'(0)). \end{aligned}$$

For the left-hand side we have used property $\dfrac{d}{dz}\zeta(z) = -\wp(z)$, see proposition 1.7 in chapter 1. By the previous lemma we then have

$$\frac{c}{\sigma(a)\sigma(b)} = -\frac{\sigma(a-b)}{\sigma(a)\sigma(b)}.$$

This proves both statements of the lemma. □

Theorem 2.6. *Fix $\boldsymbol{z} \in \mathbb{C}^n$. The function $W : \mathbb{Z}^n \to \mathbb{C}$ defined by*

$$W(\mathbf{v}) = \Omega_{\mathbf{v}}(z_1, \cdots, z_n; \Lambda)$$

is an elliptic net.

Proof. In definition 2.1 we have set $\Omega_v \equiv 0$ if $\mathbf{v} = 0$. Conversely, suppose that $\Omega_{\mathbf{v}} \equiv 0$, which means that $\sigma(\mathbf{v} \cdot \mathbf{z}) = 0$ for all $\mathbf{z}$ in the domain of Ω_v, hence $\mathbf{v} = \mathbf{0}$. We want to prove that (2.2) holds for all $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s} \in \mathbb{Z}^n$. Suppose that $\mathbf{p} = \mathbf{0}$, so $W(\mathbf{p}) = 0$. The Weierstrass σ-function is odd, from which it follows that $W(-\mathbf{v}) = -W(\mathbf{v})$ for all $\mathbf{v} \in \mathbb{Z}^n$. Now it is a simple check that the recurrence (2.2) is satisfied. The recurrence is symmetric in $\mathbf{p}, \mathbf{q}, \mathbf{r}$, hence we can assume without loss of generality that none of them is $\mathbf{0}$. This is equivalent with the assumption that none of the functions $\Omega_{\mathbf{p}}(\mathbf{z}), \Omega_{\mathbf{q}}(\mathbf{z})$ or $\Omega_{\mathbf{r}}(\mathbf{z})$ is zero. It follows directly by lemma 2.4 that

$$\frac{\Omega_{\mathbf{p+q}}(\mathbf{z})\Omega_{\mathbf{p-q}}(\mathbf{z})}{\Omega_{\mathbf{p}}(\mathbf{z})^2\Omega_{\mathbf{q}}(\mathbf{z})^2} = \wp(\mathbf{q} \cdot \mathbf{z}) - \wp(\mathbf{p} \cdot \mathbf{z}). \tag{2.20}$$

We can do the same for the couples $(\mathbf{q}, \mathbf{r})$ and $(\mathbf{r}, \mathbf{p})$. The sum of these differences is zero:

$$\frac{\Omega_{\mathbf{p+q}}(\mathbf{z})\Omega_{\mathbf{p-q}}(\mathbf{z})}{\Omega_{\mathbf{p}}(\mathbf{z})^2\Omega_{\mathbf{q}}(\mathbf{z})^2} + \frac{\Omega_{\mathbf{q+r}}(\mathbf{z})\Omega_{\mathbf{q-r}}(\mathbf{z})}{\Omega_{\mathbf{q}}(\mathbf{z})^2\Omega_{\mathbf{r}}(\mathbf{z})^2} + \frac{\Omega_{\mathbf{r+p}}(\mathbf{z})\Omega_{\mathbf{r-p}}(\mathbf{z})}{\Omega_{\mathbf{r}}(\mathbf{z})^2\Omega_{\mathbf{p}}(\mathbf{z})^2} = 0,$$

hence

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

This gives exactly the recurrence relation of an elliptic net for $\mathbf{s} = \mathbf{0}$:

$$W(\mathbf{p}+\mathbf{q})W(\mathbf{p}-\mathbf{q})W(\mathbf{r})^2 + W(\mathbf{q}+\mathbf{r})W(\mathbf{q}-\mathbf{r})W(\mathbf{p})^2 + W(\mathbf{r}+\mathbf{p})W(\mathbf{r}-\mathbf{p})W(\mathbf{q})^2 = 0.$$

We prove the case $\mathbf{s} \neq \mathbf{0}$ by noticing that the exponents of the terms in de denumator of $\Omega_{\mathbf{v}}(\mathbf{z})$ are quadratic forms f for which the following holds (by definition)

$$f(\mathbf{p}+\mathbf{q}+\mathbf{s}) + f(\mathbf{p}-\mathbf{q}) + f(\mathbf{s}) - f(\mathbf{p}+\mathbf{s}) - f(\mathbf{q}+\mathbf{s}) - f(\mathbf{p}) - f(\mathbf{q}) = 0, \quad \text{for all } \mathbf{p}, \mathbf{q}, \mathbf{s} \in \mathbb{Z}^n.$$

Hence, by the last remark and lemma 2.5

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

Therefore

$$\frac{\Omega_{\mathbf{p+q+s}}\Omega_{\mathbf{p-q}}\Omega_{\mathbf{s}}}{\Omega_{\mathbf{p+s}}\Omega_{\mathbf{p}}\Omega_{\mathbf{q+s}}\Omega_{\mathbf{q}}} + \frac{\Omega_{\mathbf{q+r+s}}\Omega_{\mathbf{q-r}}\Omega_{\mathbf{s}}}{\Omega_{\mathbf{q+s}}\Omega_{\mathbf{q}}\Omega_{\mathbf{r+s}}\Omega_{\mathbf{r}}} + \frac{\Omega_{\mathbf{r+p+s}}\Omega_{\mathbf{r-p}}\Omega_{\mathbf{s}}}{\Omega_{\mathbf{r+s}}\Omega_{\mathbf{r}}\Omega_{\mathbf{p+s}}\Omega_{\mathbf{p}}} = 0,$$

or, more simply,

$$\Omega_{\mathbf{p+q+s}}\Omega_{\mathbf{p-q}}\Omega_{\mathbf{r+s}}\Omega_{\mathbf{r}} + \Omega_{\mathbf{q+r+s}}\Omega_{\mathbf{q-r}}\Omega_{\mathbf{p+s}}\Omega_{\mathbf{p}} + \Omega_{\mathbf{r+p+s}}\Omega_{\mathbf{r-p}}\Omega_{\mathbf{q+s}}\Omega_{\mathbf{q}} = 0,$$

□

2.3 Net Polynomials over $\mathbb{C}$

Let $\mathbf{z} \in \mathbb{C}^n$, this vector corresponds (see the comment before theorem 3.3) to an n-tuple $\{P_1, \ldots, P_n\}$ on the elliptic curve. We consider the functions $\Omega_{\mathbf{v}}(\mathbf{z})$ as rational functions in $(x_1, y_1, \ldots, x_n, y_n)$ and write $\Omega_{\mathbf{v}}(x_1, y_1, \ldots, x_n, y_n)$ or $\Psi_{\mathbf{v}}(x_1, y_1, \ldots, x_n, y_n)$. We call these rational functions *the net polynomials corresponding to the functions* Ω_v.
We wonder how they look like. For the rank one case, see theorem 3.3 and the definition of the division polynomials in chapter 1. In view of theorem 1.21 the important rank two net polynomials are

Proposition 2.7.

$$\Omega_{(1,0)} = \Omega_{(0,1)} = \Omega_{(1,1)} = 1,$$
$$\Omega_{(1,-1)} = x_2 - x_1, \qquad \Omega_{(-1,1)} = x_1 - x_2,$$
$$\Omega_{(2,1)} = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2,$$
$$\Omega_{(1,2)} = x_1 + 2x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2;$$

Proof. The first three statements follow immediately from definition 2.1 and the rank one results. For the other statements, we use lemma 2.4 and find

$$\Omega_{(1,-1)}(z,w) = \wp(w) - \wp(z), \qquad \Omega_{(-1,1)}(z,w) = \wp(z) - \wp(w),$$
$$\Omega_{(2,1)}(z,w) = \wp(z) - \wp(z+w), \qquad \Omega_{(1,2)}(z,w) = \wp(w) - \wp(z+w).$$

For the last two equations we need the addition theorem 1.10:

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4}\Big(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\Big)^2,$$

hence

$$\Omega_{(2,1)}(z,w) = 2\wp(z) + \wp(w) - \frac{1}{4}\Big(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\Big)^2 \tag{2.21}$$

Using the following substitutions in equation (2.21) (obtained from the group morhpisms described above theorem 3.3, chapter 1)

$$\wp(z) = x_1 + \frac{b_1}{12}, \quad \wp(w) = x_2 + \frac{b_1}{12}, \quad \wp'(z) = 2y_1 + a_1x_1 + a_3, \quad \wp'(w) = 2y_2 + a_1x_2 + a_3,$$

one obtains

$$\begin{aligned}
\Omega_{(2,1)}(x_1, y_1, x_2, y_2) &= 2x_1 + \frac{b_2}{6} + x_2 + \frac{b_2}{12} - \frac{1}{4}\left(\frac{2(y_2 - y_1) + a_1(x_2 - x_1)}{x_2 - x_1}\right)^2 \\
&= 2x_1 + \frac{3b_2}{12} + x_2 - \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\frac{y_2 - y_1}{x_2 - x_1} + \frac{a_1^2}{4}\right) \\
&= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\frac{y_2 - y_1}{x_2 - x_1} + \frac{b_2 - a_1^2}{4} \\
&= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2 \ ,
\end{aligned}$$

because $\dfrac{b_2 - a_1^2}{4} = a_2$. One can prove the last statement in the same way. □

Some rank three net polynomials are:

Proposition 2.8.

$$\Omega_{(1,0,0)} = \Omega_{(0,1,0)} = \Omega_{(0,0,1)} = \Omega_{(1,1,0)} = \Omega_{(0,1,1)} = \Omega_{(1,0,1)} = 1,$$

$$\begin{aligned} \Omega_{(1,-1,0)} &= x_2 - x_1, \quad & \Omega_{(0,1,-1)} &= x_3 - x_2, \quad & \Omega_{(-1,0,1)} &= x_1 - x_3, \\ \Omega_{(-1,1,0)} &= x_1 - x_2, \quad & \Omega_{(0,-1,1)} &= x_2 - x_3, \quad & \Omega_{(1,0,-1)} &= x_3 - x_1, \end{aligned}$$

$$\begin{aligned} \Omega_{(1,1,1)} &= \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)}, \\ \Omega_{(-1,1,1)} &= \frac{y_1(x_2 - x_3) - y_2(x_3 - x_1) - y_3(x_1 - x_2)}{(x_2 - x_3)} + a_1 x_1 + a_3, \\ \Omega_{(1,-1,1)} &= \frac{-y_1(x_2 - x_3) + y_2(x_3 - x_1) - y_3(x_1 - x_2)}{(x_3 - x_1)} + a_1 x_2 + a_3, \\ \Omega_{(1,1,-1)} &= \frac{-y_1(x_2 - x_3) - y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)} + a_1 x_3 + a_3. \end{aligned}$$

Proof. The statements having at least one zero index follow from the previous proposition. There remains to prove the last four equations. It seems difficult to apply lemma 2.4 to

$$\Omega_{(1,1,1)} = \frac{\sigma(z_1 + z_2 + z_3)\sigma(z_1)\sigma(z_2)\sigma(z_3)}{\sigma(z_1 + z_2)\sigma(z_2 + z_3)\sigma(z_3 + z_1)}.$$

We proceed in another fashion (as it is done in [37, Proposition 6.1.3]). We use theorem 2.6 which says that the map $\mathbf{v} \mapsto \Omega_{\mathbf{v}}(\mathbf{z})$ forms an elliptic net, hence the corresponding net polynomials also forms an elliptic net. Write down the extended bracket

$$\begin{array}{cccc|cccc|cccc} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & -1 & 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & 1 \end{array} \tag{2.22}$$

We extract

$$\Omega_{(1,1,1)}\Omega_{(1,1,-1)} + \Omega_{(-1,0,1)} - \Omega_{(2,1,0)} = 0.$$

By the previous proposition we have

$$\Omega_{(1,1,1)}\Omega_{(1,1,-1)} = x_1 + x_2 + x_3 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2. \tag{2.23}$$

The extended bracket

$$\begin{array}{cccc|cccc|cccc} 1 & 1 & 0 & -1 & 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 & 1 & 0 & 1 & -1 & 0 & 1 & 1 & 0 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 \end{array} \tag{2.24}$$

gives

$$\Omega_{(1,1,1)}\Omega_{(-1,0,1)} + \Omega_{(1,1,-1)} - \Omega_{(0,0,2)} = 0.$$

By the previous proposition we find

$$\Omega_{(1,1,1)}(x_1 - x_3)(x_2 - x_3) + \Omega_{(1,1,-1)} = 2y_3 + a_1 x_3 + a_3. \tag{2.25}$$

Multiplying (2.25) by $\Omega_{(1,1,1)}$ and using relation (2.23), we obtain

$$(2.26)\quad (2y_3 + a_1x_3 + a_3)\Omega_{(1,1,1)} - (x_1 - x_3)(x_2 - x_3)\Omega_{(1,1,1)}^2 = x_1 + x_2 + x_3 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2.$$

And similarly

$$(2.27)\quad (2y_2 + a_1x_2 + a_3)\Omega_{(1,1,1)} - (x_1 - x_2)(x_3 - x_2)\Omega_{(1,1,1)}^2 = x_1 + x_2 + x_3 - \left(\frac{y_3 - y_1}{x_3 - x_1}\right)^2 - a_1\left(\frac{y_3 - y_1}{x_3 - x_1}\right) + a_2.$$

$$(2.28)\quad (2y_1 + a_1x_1 + a_3)\Omega_{(1,1,1)} - (x_2 - x_1)(x_3 - x_1)\Omega_{(1,1,1)}^2 = x_1 + x_2 + x_3 - \left(\frac{y_3 - y_2}{x_3 - x_2}\right)^2 - a_1\left(\frac{y_3 - y_2}{x_3 - x_2}\right) + a_2.$$

Now add $(x_3 - x_1)$ times (2.27) and $(x_3 - x_2)$ times (2.28) to obtain

$$(2.29)\quad \Omega_{(1,1,1)} = \frac{(2x_3 - x_1 - x_2)(x_1 + x_2 + x_3 + a_2) + \frac{(y_1-y_3)^2}{x_1-x_3} + \frac{(y_2-y_3)^2}{x_2-x_3} - a_1(2y_3 - y_1 - y_2)}{(x_3 - x_1)(2y_2 + a_1x_2 + a_3) + (x_3 - x_2)(2y_1 + a_1x + a_3)}.$$

Multiplying top and bottom by $(x_3 - x_1)(2y_2 + a_1x_2 + a_3) - (x_3 - x_2)(2y_1 + a_1x_1 + a_3)$ gives the desired expression. From this and (2.23) we also obtain the desired expression for $\Omega_{(1,1,-1)}$ and similarly for the expressions of $\Omega_{(1,-1,1)}$ and $\Omega_{(-1,1,1)}$. □

3 Qualitative remarks on net polynomials

We claim that the denominators of all net polynomials over $\mathbb{C}$ with rank $n \leq 3$ do only *depend* on the $(x_i - x_j)$ for $i \neq j$. More precisely we have

Proposition 3.1. *For all $\mathbf{v} \in \mathbb{Z}^n$ with $n \leq 3$, the functions $\Psi_{\mathbf{v}}$ are elements of the ring*

$$\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x_i, y_i]_{i=1}^n \left[(x_i - x_j)^{-1}\right]_{1\leq i<j\leq n} / \langle f(x_i, y_i)\rangle_{i=1}^n$$

Proof. For $n = 1$, we have seen that that each term of the elliptic net $W(n) = \Omega_n$ (the division polynomials) derived from an elliptic curve E can be written as a $\mathbb{Z}$-polynomial expression in

$$W(1) = 1, W(1)^{-1} = 1, W(2), W(3), W(4)W(2)^{-1}.$$

Since $W(2) \mid W(4)$ one sees immediately that each denumerator is 1.

For $n = 2$, by proposition 2.7 and theorem 1.21, every net polynomial can be written as a $\mathbb{Z}$-polynomial in

$$\Omega_{(2,1)}, \quad \Omega_{(1,2)}, \quad \Omega_{(2,0)}, \quad \Omega_{(0,2)}, \quad \Omega_{(2,2)}.$$

Only $\Omega_{(2,2)}$ may cause a problem, fortunately we have the extended bracket

$$\begin{matrix} 1 & 1 & -1 & 0 \\ 1 & 2 & 1 & -1 \end{matrix} \left[\begin{array}{cccc|cccc|cccc} 2 & 0 & -1 & -1 & 0 & 2 & 1 & 1 & 0 & -2 & 1 & 1 \\ 2 & -1 & 0 & 1 & 2 & 1 & 0 & 1 & 1 & 0 & 1 & 2 \end{array}\right],$$

which means that

$$\Omega_{(2,2)} = \frac{\Omega_{(1,2)}(2y_1 + a_1x_1 + a_3) - \Omega_{(2,1)}(2y_2 + a_1x_2 + a_3)}{x_1 - x_2}.$$

By proposition 2.7 we deduce that $\Omega_{(2,2)}$ can be written as a rational function having $(x_1 - x_2)$ as denumerator.

For $n = 3$ we prove it by induction on the sup-norm of $\mathbf{v} \in \mathbb{Z}^3$. By propositions 2.8 and 1.13, all net polynomials $\Omega_{\mathbf{v}}$ with $N(\mathbf{v}) \leq 1$ satisfy the statement. Now suppose that $N(\mathbf{v}) = 2$, if $\mathbf{v}$ contains a zero component then we fall back on the case $n = 2$. Hence we can assume that all components are non-zero.

- Case 1: one component has absolute value 2.

$$\begin{matrix} \pm 2 & \pm 1 & \pm 1 & \mp 1 \\ 0 & 0 & 0 & \pm 1 \\ 0 & 0 & \mp 1 & \pm 1 \end{matrix} \left[\begin{array}{cccc|cccc|cccc} \pm 2 & \pm 1 & 0 & \pm 1 & \pm 1 & 0 & \pm 1 & \pm 2 & \pm 2 & \mp 1 & 0 & \pm 1 \\ \pm 1 & 0 & \pm 1 & 0 & \pm 1 & 0 & \pm 1 & 0 & \pm 1 & 0 & \pm 1 & 0 \\ \pm 1 & 0 & 0 & \mp 1 & 0 & \pm 1 & \pm 1 & 0 & 0 & \mp 1 & \pm 1 & 0 \end{array}\right].$$

- Case 2: two components have absolute value 2

$$\begin{matrix} 0 & 0 & \mp 1 & \pm 1 \\ \pm 2 & \pm 1 & \pm 1 & \mp 1 \\ 0 & \pm 1 & 0 & \pm 1 \end{matrix} \left[\begin{array}{cccc|cccc|cccc} \pm 1 & 0 & 0 & \mp 1 & 0 & \pm 1 & \pm 1 & 0 & 0 & \mp 1 & \pm 1 & 0 \\ \pm 2 & \pm 1 & 0 & \pm 1 & \pm 1 & 0 & \pm 1 & \pm 2 & \pm 2 & \mp 1 & 0 & \pm 1 \\ \pm 2 & \mp 1 & \pm 1 & 0 & \pm 2 & \pm 1 & \pm 1 & 0 & \pm 1 & 0 & \pm 2 & \pm 1 \end{array}\right].$$

- Case 3: three components have absolute value 2

$$\begin{matrix} \pm 2 & \pm 1 & \pm 1 & \mp 1 \\ 0 & \pm 1 & 0 & \pm 1 \\ \pm 1 & \pm 1 & 0 & 0 \end{matrix} \left[\begin{array}{cccc|cccc|cccc} \pm 2 & \pm 1 & 0 & \pm 1 & \pm 1 & 0 & \pm 1 & \mp 2 & \pm 2 & \mp 1 & 0 & \pm 1 \\ \pm 2 & \mp 1 & \pm 1 & 0 & \pm 2 & \pm 1 & \pm 1 & 0 & \pm 1 & 0 & \pm 2 & \pm 1 \\ \pm 2 & 0 & 0 & 0 & \pm 1 & \pm 1 & \pm 1 & \pm 1 & \pm 1 & \mp 1 & \pm 1 & \pm 1 \end{array}\right].$$

It is clear that the above extended brackets treat all cases $\mathbf{v} \in \mathbb{Z}^3$ with norm $N(\mathbf{v}) = 2$ (permute the rows if necessary). Now we prove the induction step. Suppose that the statement holds for all vectors $\mathbf{v} \in \mathbb{Z}^3$ with $N(\mathbf{v}) \leq N$ and $N \geq 2$. We need the prove that the statement holds for all $\mathbf{v}$ with norm $N(\mathbf{v}) = N + 1$. For every component v_i of $\mathbf{v}$ write $w_i = \left\lceil \frac{v_i}{2} \right\rceil$.

- Case 1: all components are even. Consider the extended bracket

$$\begin{matrix} w_i{-}1 & w_i & 0 & 1 \\ w_i & w_i{-}1 & 0 & 1 \\ w_i & w_i & 0 & 0 \end{matrix} \left[\begin{array}{cccc|cccc|cccc} v_i & -1 & 1 & 0 & w_i{+}1 & w_i & w_i & w_i{-}1 & w_i & -w_i{+}1 & w_i{+}1 & w_i \\ v_i & 1 & 1 & 0 & w_i & w_i{-}1 & w_i{+}1 & w_i & w_i{+}1 & -w_i & w_i & w_i{-}1 \\ v_i & 0 & 0 & 0 & w_i & w_i & w_i & w_i & w_i & -w_i & w_i & w_i \end{array}\right]$$

- Case 2: two components are even. For the odd component take the extended bracket

$$\begin{matrix} w_i & w_i{-}1 & 0 & 0 \end{matrix} \left[\begin{array}{cccc|cccc|cccc} v_i & 1 & 0 & 0 & w_i{-}1 & w_i{-}1 & w_i & w_i & w_i & -w_i & w_i{-}1 & w_i{-}1 \end{array}\right],$$

  and add to it the extended bracket

$$\begin{matrix} w_i{-}1 & w_i & 0 & 1 \\ w_i & w_i & 0 & 0 \end{matrix} \left[\begin{array}{cccc|cccc|cccc} v_i & -1 & 1 & 0 & w_i{+}1 & w_i & w_i & w_i{-}1 & w_i & -w_i{+}1 & w_i{+}1 & w_i \\ v_i & 0 & 0 & 0 & w_i & w_i & w_i & w_i & w_i & -w_i & w_i & w_i \end{array}\right]$$

- Case 3: one component is even. For the even component use

$$\begin{matrix} w_i & w_i & 0 & 0 \end{matrix} \left[\begin{matrix} v_i & 0 & 0 & 0 \end{matrix} \middle| \begin{matrix} w_i & w_i & w_i & w_i \end{matrix} \middle| \begin{matrix} w_i & -w_i & w_i & w_i \end{matrix} \right],$$

  and add to it

$$\begin{matrix} w_i & w_i{-}1 & 0 & 0 \\ w_i{-}1 & w_i & 0 & 0 \end{matrix} \left[\begin{matrix} v_i & 1 & 0 & 0 \\ v_i & -1 & 0 & 0 \end{matrix} \middle| \begin{matrix} w_i{-}1 & w_i{-}1 & w_i & w_i \\ w_i & w_i & w_i{-}1 & w_i{-}1 \end{matrix} \middle| \begin{matrix} w_i & -w_i & w_i{-}1 & w_i{-}1 \\ w_i{-}1 & 1{-}w_i & w_i & w_i \end{matrix} \right]$$

- Case 4: all components are odd. Now use

$$\begin{matrix} w_i & w_i{-}1 & 0 & 0 \\ w_i{-}1 & w_i & 0 & 0 \\ w_i & w_i & 1 & -1 \end{matrix} \left[\begin{matrix} v_i & 1 & 0 & 0 \\ v_i & -1 & 0 & 0 \\ v_i & 0 & 0 & 1 \end{matrix} \middle| \begin{matrix} w_i{-}1 & w_i{-}1 & w_i & w_i \\ w_i & w_i & w_i{-}1 & w_i{-}1 \\ w_i & w_i{-}1 & w_i{-}1 & w_i \end{matrix} \middle| \begin{matrix} w_i & -w_i & w_i{-}1 & w_i{-}1 \\ w_i{-}1 & 1{-}w_i & w_i & w_i \\ w_i & 1{-}w_i & w_i{-}1 & w_i \end{matrix} \right]$$

It is easy to check that for all the four cases the absolute value of each entry of the second and third term is smaller than $N+1$. We see that for each first term it is 'allowed' to invert by the corresponding net polynomial. This finishes the induction step. □

4 Net polynomials over arbitrary fields: a sketch

Let $R = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6]$ be a polynomial ring over $\mathbb{Q}$ in the variables α_i. Define an irreducible polynomial $f(x, y) \in R[x, y]$ by

$$f(x, y) = y^2 + \alpha_1 xy + \alpha_3 y - x^3 - \alpha_2 x^2 - \alpha_4 x - \alpha_6$$

Denote by i the natural injection $R \hookrightarrow R[x, y]/(f(x, y))$. This ring morphism induces by [13, Theorem I-40] a morphism of affine schemes from $\mathcal{E} = Spec(R[x, y]/(f(x, y)))$ to $Spec(R)$ by the map

$$i^* : \mathcal{E} \to Spec(R) : \quad \mathfrak{p} \longmapsto i^{-1}(\mathfrak{p}).$$

To connect the ring R with the field of complex numbers, we define the ring morphism

$$s_a : R \to \mathbb{C} : \alpha_i \mapsto a_i,$$

for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{C}$, and a polynomial

$$f_s(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6.$$

Note that f_s is irreducible. If A is a ring containing R, we denote by $\otimes_R^n A$ the n-fold tensor product of A over R. We similarly define $\otimes_{\mathbb{C}}^n A$ if A contains $\mathbb{C}$. The ring morphism s_a induces a ring morphism

$$\begin{aligned} R[x,y]/\big(f(x,y)\big) \otimes_R \cdots \otimes_R R[x,y]/\big(f(x,y)\big) &\to \mathbb{C}[x,y]/\big(f_s(x,y)\big) \otimes_{\mathbb{C}} \cdots \otimes_{\mathbb{C}} \mathbb{C}[x,y]/\big(f_s(x,y)\big) \\ (r_1 \otimes_R \cdots \otimes_R r_n) &\mapsto (s_a(r_1) \otimes_{\mathbb{C}} \cdots \otimes_{\mathbb{C}} s_a(r_n)). \end{aligned}$$

To make the notations more transparent, this ring morphism is also denoted by s_a. We also denote by i the injection $\mathbb{C} \hookrightarrow \mathbb{C}[x, y]/\big(f_s(x, y)\big)$.
Let

$$\mathcal{E}^n = Spec\ \left(R[x,y]/\big(f(x,y)\big) \otimes_R \cdots \otimes_R R[x,y]/\big(f(x,y)\big)\right),$$

and

$$C_a^n = Spec\ \left(\mathbb{C}[x,y]/\big(f_s(x,y)\big) \otimes_{\mathbb{C}} \cdots \otimes_{\mathbb{C}} \mathbb{C}[x,y]/\big(f_s(x,y)\big)\right).$$

These ring morphisms give rise to a commutative diagram

$$\begin{array}{ccc} \otimes_R^n R[x,y]/(f(x,y)) & \xrightarrow{s_a} & \otimes_{\mathbb{C}}^n \mathbb{C}[x,y]/(f_s(x,y)) \\ \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle i} \\ R & \xrightarrow[s_a]{} & \mathbb{C} \end{array}$$

By [13, Theorem I-40], the above diagram leads to a commutative diagram of affine schemes

$$\begin{array}{ccc} \mathcal{E}^n & \xleftarrow[s_a^*]{} & C_a^n \\ \downarrow & & \downarrow \\ Spec\ R & \xleftarrow{s_a^*} & Spec\ \mathbb{C} \end{array}$$

The ring of regular functions on $\mathcal{E}^n$ is

$$R[x,y]/(f) \otimes_R \cdots \otimes_R R[x,y]/(f) \cong \frac{R[x_1,y_1,\ldots,x_n,y_n]}{\big(f(x_1,y_1),\cdots,f(x_n,y_n)\big)}$$

Since the latter is an integral domain we find that the field of rational functions on $\mathcal{E}^n$ is

$$\mathcal{K}(\mathcal{E}^n) = Frac\big(R[x,y]/(f) \otimes_R \cdots \otimes_R R[x,y]/(f)\big) = \mathcal{K}(\mathcal{E}) \otimes_R \cdots \otimes_R \mathcal{K}(\mathcal{E}),$$

where $\mathcal{K}(\mathcal{E}) = Frac\big(R[x,y]/(f)\big)$. Suppose that C_a is an elliptic curve, then by definition each term of the elliptic net $\Omega_{\mathbf{v}}(x_1,y_1,\ldots,x_n,y_n)$ is contained in the field of fractions of

$$\frac{\mathbb{C}[a_1,a_2,a_3,a_4,a_6][x_1,y_1,\cdots,x_n,y_n]}{\big(f_s(x_1,y_1),\cdots,f_s(x_n,y_n)\big)}.$$

The net polynomials corresponding to $\Omega_{\mathbf{v}}$ are given by rational expressions in the variables (x_i,y_i) and a_i. Replacing the a_i by α_i in the expression of $\Omega_{\mathbf{v}}$ we get an element $\Psi_{\mathbf{v}} \in \mathcal{K}(\mathcal{E}^n)$.

Theorem 4.1 ([35, Theorem 4.1])**.** *Let $n \geq 1$ and $\boldsymbol{a} = (a_1,a_2,a_3,a_4,a_6) \in \mathbb{C}^5$. The functions $\Psi_v \in \mathcal{K}(\mathcal{E}^n)$ are an unique system of functions in $\mathcal{K}(\mathcal{E}^n)$ such that*

1. *the map*
$$\mathbb{Z}^n \to \mathcal{K}(\mathcal{E}^n) : \mathbf{v} \mapsto \Psi_{\mathbf{v}}$$
is an elliptic net, and

2. *whenever $\Delta(a_1,a_2,a_3,a_4,a_6) \neq 0$ the restriction of $\Psi_{\mathbf{v}}$ to a fibre $C_{\boldsymbol{a}}^n$ is the rational function $\Omega_{\mathbf{v}}$.*

3. *$\Psi_{\mathbf{v}} = 1$ whenever $\mathbf{v} = \mathbf{e_i}$ for $1 \leq i \leq n$ or $\mathbf{v} = \mathbf{e_i} + \mathbf{e_j}$ for $1 \leq i < j \leq n$*

Definition 4.2. *We call the unique system of functions $\Psi_{\mathbf{v}} \in \mathcal{K}(\mathcal{E}^n)$ satisfying theorem 4.1 net polynomials.*

We can say more about these net polynomials. By [35, Theorem 4.4] they are contained in the ring

$$S[x_i, y_i]_{1\leq i\leq n}\left[(x_i - x_j)^{-1}\right]_{1\leq i<j\leq n} \Big/ \langle f(x_i, y_i)\rangle_{1\leq i\leq n},$$

where $S = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6]$.

Now there is a natural way to define a net polynomial associated to any cubic Weierstrass curve over any field K. Let

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

be defined over K and denote by C the curve defined by $f(x, y) = 0$. To this we can associate a ring morphism

$$R = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6] \to K, \quad \alpha_i \mapsto a_i.$$

A similar argumentation yields a cartesian diagram

$$\begin{array}{ccc} \mathcal{E}^n & \longleftarrow & C^n \\ \downarrow & & \downarrow \\ Spec\ R & \longleftarrow & Spec\ K \end{array}$$

and denote by $\phi_{\mathbf{v}} \in \mathcal{K}(C^n)$ the pullback of $\Psi_{\mathbf{v}}$. We will often write $\Psi_{\mathbf{v}}$ to denote $\phi_{\mathbf{v}}$. We have the following *transformation formula.*

Proposition 4.3 ([35, Proposition 4.3])**.** *Let* $\mathbf{v} \in \mathbb{Z}^n$*. Let* T *be any matrix contained in* $\mathbb{Z}^{n\times m}$ *and transpose* T^{tr}*. Then*

$$(\Psi_{\mathbf{v}} \circ T)\prod_{i=1}^{n} \Psi_{T^{tr}(\mathbf{e_i})}^{2v_i^2 - \sum_{j=1}^{n} v_iv_j} \prod_{1\leq i<j\leq n} \Psi_{T^{tr}(\mathbf{e_i}+\mathbf{e_j})}^{v_iv_j} = \Psi_{T^{tr}(\mathbf{v})}.$$

Chapter 3

The Curve-Net Theorem

The previous two chapters provide the material necessary to state and proof Stanges *Curve-Net theorem*: there is a bijection between the sets of non-degenerate elliptic nets and the set of elliptic curves with specified points on it. In this chapter, by *a curve* we mean an elliptic curve with possible singular points (the discriminant Δ can be zero).

1 Elliptic nets from elliptic curves

We start with a definition.

Definition 1.1. *We call a set of non-singular points* $\{P_1, \ldots, P_n\}$ *of a cubic curve* C *appropriate if the following hold:*

1. $P_i \neq \mathcal{O} \neq 2P_i$ *for all* i*;*
2. $P_i \neq \pm P_j$ *for any* $i \neq j$*; and*
3. $3P_i \neq \mathcal{O}$ *whenever* $n = 1$*.*

We have seen that the net polynomials associated to any cubic Weierstrass C over a field K forms an elliptic net in the appropriate field of rational functions. These net polynomials have a special form: they can be written as a polynomial divided by some polynomial expression in $(x_i - x_j)$ for $i \neq j$. Hence, it is possible to evaluate these net polynomials at *appropriate* points. Then we get a normalised non-degenerate elliptic net $\mathbb{Z}^n \to K$. We know that the non-singular points of C, denoted $C_{ns}(K)$ form a group.

Definition 1.2. *Let* $\boldsymbol{P} \in C_{ns}(K)^n$ *be an appropriate* n*-tuple of points, then we may define an elliptic net*

$$W_{C,\boldsymbol{P}} : \mathbb{Z}^n \to K : \mathbf{v} \mapsto \Psi_{\mathbf{v}}(\boldsymbol{P}).$$

We also have a generalization of theorem 2.10 in chapter 1:

Proposition 1.3 ([35, Corollary 5.2])**.** *Let* $W_{C,\boldsymbol{P}}$ *be an elliptic net associated to a curve* C *and appropriate points* $\boldsymbol{P}$*. Then* $W_{C,\boldsymbol{P}}$ *vanishes at* $\mathbf{v} = (v_1, \ldots, v_n)$ *if and only if*

$$v_1 P_1 + \ldots + v_n P_n = \mathcal{O}.$$

2 Elliptic Curves From Elliptic Nets.

It is time to go the other way around: construct elliptic curves and points from normalised non-degenerate elliptic nets over any field K. Suppose that a cubic curve over K in Weierstrass form. In the following propositions we will require that the non-degenerate elliptic nets are normalised. This is a necessity condition because elliptic nets arising from elliptic curves are normalised, see proposition 2.8 in chapter 2. But this is not a problem since W has a unique normalisation by proposition 1.10 in the same chapter. The case of rank one is as follows

Proposition 2.1. *Let $W : \mathbb{Z} \to K$ be a normalised non-degenerate elliptic net. Then the family of curve-point pairs (C, P) such that $W = W_{C,P}$ is three dimensional. These are the curve and non-singular point*

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad P = (0, 0),$$

where

$$a_1 = \frac{W(4) + W(2)^5 - 2W(2)W(3)}{W(2)^2W(3)}, \tag{3.1}$$

$$a_2 = \frac{W(2)W(3)^2 + (W(4) + W(2)^5) - W(2)W(3)}{W(2)^3W(3)},$$

$$a_3 = W(2), \qquad a_4 = 1, \qquad a_6 = 0,$$

or any image of these under a unihomothetic change of coordinates.

Proof. It is given that W is non degenerate, i.e. $W(2) \neq 0 \neq W(3)$, therefore the curve C in the statement is defined. By proposition 2.5 in chapter 1

$$W_{C,P}(1) = 1, \quad W_{C,P}(2) = a_3 = W(2),$$

and,

$$\begin{aligned} W_{C,P}(3) &= b_8 = -a_1a_3 + a_2a_3^2 - 1 = \frac{W(2)^2W(3)(W(3)+1)}{W(2)^2W(3)} - 1 = W(3), \\ W_{C,P}(4) &= W_{C,P}(2)(b_4b_8 - b_6^2) = W(2)(2W(3) + a_1W(2)W(3) - W(2)^4) \\ &= 2W(2)W(3) + W(4) + W(2)^5 - 2W(2)W(3) - W(2)^5 \\ &= W(4). \end{aligned}$$

Any non-degenerate elliptic net V of rank one is determined by the four values $V(1)$, $V(2)$, $V(3)$ and $V(4)$ by proposition 1.18 chapter 2, hence $W = W_{C,P}$. The division polynomials are invariant under an unihomothetic change of coordinates (theorem 2.11, chapter 1), hence $W_{C,P} = W_{C',P'}$ where C' is the curve corresponding to an unihomothetic coordinate change of C. The non-singularity of the point P follows from the fact that the nonzero term $W_{C,P}(2)$ is also a partial derivative of the Weierstrass equation with respect to Y and evaluated at P.

Now suppose that $W = W_{C',P'}$. We need to prove that we can obtain C' by a unihomothetic change of C. In other words, our objective is to find a unihomothetic transformation

such that P' maps to $(0,0)$ and the coefficients a'_i are transformed to coefficients a_i of the curve C. This will be achieved by mapping P to $(0,0)$ and a'_4 to 1, hence we search a transformation of the form

$$(X,Y) \longmapsto (X + x', Y + sX + y'), \tag{3.2}$$

such that $a'_4 \mapsto 1$, where s depends on P' and the coefficients of C' . Transformation (3.2) take a point (x,y) on C' to $(x - x', y - sx - y' + x's)$ on the curve defined by (3.3), see below. Transformation (3.2) yields the Weierstrass equation

$$\begin{aligned} &Y^2 + XY(2s + a'_1) + Y(2y' + a'_1x' + a'_3) = \\ &X^3 + X^2(3x' + a'_2 - s^2 - a'_1s) + X(3x'^2 + a'_4 + 2a'_2x' - a'_1y' + s(-a'_3 - a'_1x' + 2y')). \end{aligned} \tag{3.3}$$

We have $W(2) = W_{C',P'}(2) \neq 0$, this means that P' is non-singular. Therefore we can set

$$s = \frac{1 + a'_1y' - (3x'^2 + a'_4 + 2a'_2x')}{-(2y' + a'_1x' + a'_3)}.$$

One can easily verify that the coeffients of the image of C' under the given transformation satisfy (3.1). The proof is complete. □

Proposition 2.2. *Let $W : \mathbb{Z}^2 \to K$ be a normalised non-degenerate elliptic net. The family of 3-tuples (C, P_1, P_2) such that $W = W_{C,P_1,P_2}$ is three dimensional. These are the curve and non-singular points*

$$\begin{aligned} C &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \\ P_1 &= (0,0), \quad P_2 = (W(1,2) - W(2,1), 0), \end{aligned}$$

with

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

or any change of these under a unihomothetic change of coordinates.

Proof. The proof of corollay 1.22 gives the following identity in the ring $\mathcal{W}_{\mathbb{Z}^2}$

$$T_{(1,-1)}T_{(1,1)} = T_{(1,0)}T_{(1,2)} - T_{(0,1)}T_{(2,1)},$$

which translates to a relation for the normalised non degenerate elliptic net W

$$0 \neq W(1,-1) = W(1,2) - W(2,1). \tag{3.3}$$

We claim that $W = W_{C,P_1,P_2}$. By proposition 2.5 (chapter 1) we have

$$\begin{aligned} W_{C,P_1,P_2}(2,0) &= a_3 = W(2,0) \\ W_{C,P_1,P_2}(0,2) &= a_1\big(W(1,2) - W(2,1)\big) + W(2,0) = W(0,2) - W(2,0) + W(2,0), \end{aligned}$$

and by proposition 2.7 (chapter 2)we have

$$\begin{aligned} W_{C,P_1,P_2}(2,1) &= W(1,2) - W(2,1) + a_2 \\ &= W(2,1), \end{aligned}$$

and similarly

$$W_{C,P_1,P_2}(1,2) = W(2,1).$$

In $\mathcal{W}_{\mathbb{Z}^2}$ we have the identity

$$T_{(2,2)}T_{(1,-1)}T_{(1,0)}T_{(0,1)} = T_{(1,1)}\left(T_{(0,2)}T_{(2,1)}T_{(1,0)} - T_{(0,1)}T_{(2,0)}T_{(1,2)}\right),$$

which means that $W(2,2) = W_{C,P_1,P_2}(2,2)$ by the information obtained above. The elliptic nets agree on a base set by the proof of theorem 1.21 (chapter 2) , hence we get $W = W_{C,P_1,P_2}$. One applies the same argument as in the previous proposition to demonstrate the non-singularity of the points P_1, P_2.

Conversely, suppose that

$$W = W_{C',P_1',P_2'}, \quad P_1 = (x_1', y_1'),\ P_2 = (x_2', y_2').$$

Note that $x_1' \neq x_2'$, because by equation (3.3) and proposition 2.7 (chapter 2) we have

$$W(1,-1) = x_2' - x_1' = W(1,2) - W(2,1) = W(1,1) \neq 0.$$

Clearly, P_1' and P_2' are non singular. Define $s = \dfrac{y_1' - y_2'}{x_1' - x_2'}$ and the unihomothetic transformation

$$(X, Y) \mapsto (X + x_1', Y + sX + y_1').$$

The last transformation yields a curve C with coefficients a_i. The transformation takes the point P_1 to $(0,0)$ and P_2 to $\big(W(1,2) - W(2,1), 0\big)$, while the coefficients a_i' (of the curve C') are mapped to a_i for all i. We will show that the curve C is exactly the curve in the statement. Take $i = 1$ for example, then $a_1 = a_1' + 2s$. We can use the expressions of the division polynomials to obtain

$$W(2,0) - W(0,2) = 2y_1' - 2y_2' + a_1'(x_1' - x_2'),$$

so

$$\begin{aligned} a_1 &= \frac{-W(2,0) + W(0,2) - 2(y_2' - y_1') + 2(y_2' - y_1')}{W(1,2) - W(2,1)} \\ &= \frac{W(2,0) - W(0,2)}{W(2,1) - W(1,2)}. \end{aligned}$$

The same is true for the other coefficients. □

Theorem 2.3. *Let $n \geq 1$. Let $W : \mathbb{Z}^n \to K$ be a normalised non-degenerate EN. Then the set of curves C and $\boldsymbol{P} \in C^n$ such that $W = W_{C,\boldsymbol{P}}$ forms a three-dimensional family of tuples $(C, \boldsymbol{P})$. Furthermore, none of the points $P \in \boldsymbol{P}$ are singular. In particular, the family consists of one such tuple and all its images under unihomothetic changes of coordinates.*

Sketch of proof. The proof is by strong induction on n. The inductive statement has two parts: (I) that the theorem holds for n; and (II) that $W(\mathbf{v}) \neq 0$ for some $\mathbf{v} \in \{\pm 1\}^n$. The base case consists of ranks $n = 1, 2$: part (I) is established by propositions 2.1 and 2.2; part (II) is by non-degeneracy (definition 1.9, chapter 2), which implies $W(\boldsymbol{e}_1) \neq 0$ and $W(\boldsymbol{e}_1 + \boldsymbol{e}_2) \neq 0$.

Inductive step: suppose that $n \geq 3$ and the statement of the theorem holds for all $k < n$, we will prove that both statements hold for $k = n$. Let $W : \mathbb{Z}^n \to K$ be a non-degenerate elliptic net. Set $L_i = \{\mathbf{v} = (v_1, \cdots, v_n) \in \mathbb{Z}^n \mid v_i = 0\}$. We can identify each L_i with $\mathbb{Z}^{n-1}$. Define elliptic nets W_i on $\mathbb{Z}^{n-1}$ by $W_i \coloneqq W|_{L_i}$. These rank $n-1$ elliptic nets are also normalised and non-degenerate (by definition, non-degeneracy at rank n implies non-degeneracy on rank $n-1$ sublattices for $n > 2$). By the inductive hypothesis part (I), we have $W_i = W_{C_i, \boldsymbol{P}_i}$ for curves C_i and non-singular points $\boldsymbol{P}_i \in C_i^{n-1}$.

Suppose that $V_1 : \mathbb{Z}^n \to K$ is an elliptic net of rank m associated to C and $\boldsymbol{P} = (P_1, \cdots, P_m)$. Then we have the rank $m-1$ elliptic net

$$V_2 : \mathbb{Z}^{m-1} \to K : v \mapsto V_1(v, 0),$$

which is associated to the same curve C and points $(P_1, \cdots, P_{m-1})$ (the first $m-1$ points of $\boldsymbol{P}$) by proposition 4.3 of the previous chapter. This fact also holds for the other coordinate hyperplanes (the hyperplances obtained by letting the i-th coordinate to be zero).

Consider now two of the rank $n-1$ subnets of W construced above, say W_i and W_j $(i < j)$. Define the rank $n-2$ elliptic net

$$W_{ij} : \mathbb{Z}^{n-2} \to K : v = (v_1, \cdots, v_{n-2}) \mapsto W(v_1, \cdots, v_{i-1}, 0, v_i, \cdots, v_{j-1}, 0, v_j, \cdots, v_{n-2}).$$

Then, $W_{ij} = W_{C_{ij}, \boldsymbol{P}_{ij}}$ for some curve $\boldsymbol{P}_{ij} \in C_{ij}^{n-2}$. By the foregoing, $C_i = C_j = C_{ij}$, $\boldsymbol{P}_{ij}$ is just $\boldsymbol{P}_j$ with the i-th coordinate deleted, and $\boldsymbol{P}_{ij}$ is just $\boldsymbol{P}_i$ with the $(j-1)$-th coordinate deleted.

We can do this for every such a pair (i, j). Therefore define the candidate curve $C = C_i$ for all i and $\boldsymbol{P} \in C^n$ as the unique tuple which results in $\boldsymbol{P}_i$ upon deleting the i-th coordinate of $\boldsymbol{P}$. Note that W agrees with $W_{C,\boldsymbol{P}}$ on all coordinate sublattices of rank $n-1$. By the inductive statement part (II) and theorem 1.23 of the previous chapter, the net W is determined by its sublattices of rank $n-1$. Therefore $W = W_{C,\boldsymbol{P}}$.

Now we show part (II) of the inductive statement. Observe that if $W(\mathbf{v}) = 0$ for all $\mathbf{v} \in \{\pm 1\}^n$, then $\sum_i v_i P_i = \mathcal{O}$ by proposition 1.3. This would imply $[2]P_i = \mathcal{O}$ for $1 \leq i \leq n$, and by proposition 1.3 this contradicts the non-degeneracy of the net W.

Now we finish the proof of the inductive step of part (I). Suppose we apply a unihomothetic change of variables on the curve C and tuple $\boldsymbol{P}$ associated to W. By the induction hypothesis, the rank $n-1$ subnets W_i obtained from W do not change. By theorem 1.23 (chapter 2) the net W is completely determined by the values on the coordinate hyperplanes. So, the net associated to the transformation is just W. Further, if the

tuples $(C, \boldsymbol{P})$ and $(C', \boldsymbol{P}')$ generate the same normalised non-degenerate rank n elliptic net, and are not unihomothetic with respect to each other, then the same holds for one of the rank $n-1$ subnets (obtained by considering a coordinate hyperplane). This contradicts the induction hypothesis of part (I). □

3 The Curve-Net theorem

The previous propositions tell us that the elliptic net associated to a curve E and points on it is invariant under an unihomothetic change of variables.

Theorem 3.1. *Take a field K, there exists a bijection of sets*

$$\mathcal{A} \coloneqq \left\{ \begin{array}{l} \textit{scale equivalence classes of} \\ \textit{non-degenerate elliptic nets} \\ W : \mathbb{Z}^n \to K \textit{ for some } n \end{array} \right\}$$

$$\updownarrow$$

$$\mathcal{B} \coloneqq \left\{ \begin{array}{l} \textit{tuples } (C, P_1, \ldots, P_m) \textit{ for some } m, \textit{ where } C \\ \textit{is a cubic curve in Weierstrass form over } K, \\ \textit{considered modulo unihomothetic changes} \\ \textit{of variables, and such that } \{P_i\} \in C_{ns}(K)^m \\ \textit{is appropriate} \end{array} \right\}$$

Proof. We first show that there is an injective map $\mathcal{A} \to \mathcal{B}$. Take an equivalence class from $\mathcal{A}$. By proposition 1.10 (chapter 2), that equivalence class corresponds to a unique normalised non-degenerate elliptic net. Theorem 2.3 shows that this elliptic net maps to $\mathcal{B}$, and that this map gives an injection $\mathcal{A} \to \mathcal{B}$.
Now we show the existence of the inverse map. Let $C, \boldsymbol{P}$ be an element of an equivalence class contained in $\mathcal{B}$. Definition 1.2 together with proposition 1.3 assures us that $W_{C,\boldsymbol{P}}$ is a non-degenerate elliptic net. It is also normalised by theorem 4.1 (chapter 2). Theorem 2.3 shows that this map is well defined and that is the inverse of the map $\mathcal{A} \to \mathcal{B}$ construced above. □

Chapter 4

Pairings

Let G_1, G_2 and G_3 be abelian groups. A *pairing* is a bilinear function

$$e : G_1 \times G_2 \to G_3.$$

Often, the groups G_1 and G_2 are equal while G_3 is cyclic. Pairings are important tools in cryptography. Pairings have been used to design ingenious protocols for such tasks as one-round three-party key agreement, identity-based encryption and signatures [23]. In this chapter we explain the Weil and Tate pairing, both are frequently used in Cryptography. We will also see how elliptic nets provide an alternative and yet efficient way to compute these pairings.

1 The Weil Pairing

The Weil pairing on the n-torsion on an elliptic curve is a major tool in the study of elliptic curves. The Weil pairing can be used to prove Hasse's theorem on the number of points on the elliptic curve. More important for us is the fact that it can be used to attack the elliptic curve DLP in certain cases. It can also be used cryptographic settings.

1.1 Definition

Let E/K be an elliptic curve defined over a field K. Fix an integer $m \geq 2$ which we assume to be prime to $p = char(K)$ if $char(K) > 0$. By [33, 3.3.5] we know that a divisor

$$D = \sum n_i(P_i)$$

is a principal divisor if and only if $deg(D) = 0$ and $\sum n_i P_i = \mathcal{O}$. Let $T \in E[m]$ and take a point $T' \in E$ with $[m]T' = T$. This is possible since the map $[m]$ is non-constant by [33, Proposition 3.4.2(a)] and surjective on $E(\bar{K})$ by [33, Theorem 4.10]. Note that $\#E[m] = m^2$. By [33, Corollary III.3.5] there is a function $g_T \in \bar{K}(E)$

$$div(g_T) = \sum_{R \in E[m]} (T' + R) - (R). \tag{4.1}$$

If $T = \mathcal{O}$ we let g_T be any constant in K^*. Note that $g_T \neq 0$ is determined up to a constant multiple in $\bar{K}^*$ [33, Proposition II.3.1]. For any $P \in E$, let $\mathcal{T}_P : E \to E$ be the translation by P map , i.e.

$$\mathcal{T}_P(Q) = Q + P \text{ for } Q \in E. \tag{4.2}$$

Lemma 1.1. *Suppose that $S, T \in E[m]$. Then*

$$div(g_T \circ \mathcal{T}_S) = div(g_T).$$

Proof. By definition of g_T (equation (4.1))

$$div(g_T) = \sum_{R \in E[m]} (T' + R) - (R).$$

Therefore

$$\begin{aligned} div(g_T \circ \mathcal{T}_S) &= \sum_{R \in E[m]} (T' + R - S) - (R - S) \qquad \text{(by [12, Proposition 3.13])} \\ &= \sum_{R' \in E[m]} (T' + R') - (R'). \end{aligned}$$

□

So, as elements of $\bar{K}(E)$, $g_T(X)$ and $g_T(X+S)$ have the same divisor. By [33, Proposition II.3.1] the ratio (in $\bar{K}(E)$) of these functions is a constant:

$$g_T(X + S)/g_T(X) = c_{S,T}.$$

Observe that

$$c_{S,T} = \frac{g_T(X + S)}{g_T(X)} = \frac{g_T(X + 2S)}{g_T(X + S)} = \cdots = \frac{g_T(X + mS)}{g_T(X + (m - 1)S)},$$

which leads to

$$c_{S,T}^m = \prod_{i=0}^{m-1} \frac{g_T(X + [i + 1]S)}{g_T(X + [i]S)} = g_T(X + mS)/g_T(X) = 1,$$

since $S \in E[m]$. So $c_{S,T} \in \bar{K}^*$ is an m-th root of unity. Note that on arriving at the constant $c_{S,T}$ we only made one choice, namely that g_T is determined up to a constant $c \in \bar{K}^*$. This choise does not affect $c_{S,T}$, since

$$\frac{c \cdot g_T(P + S)}{c \cdot g_T(X)} = \frac{g_T(P + S)}{g_T(X)}.$$

The value $c_{S,T}$ does not depend on the choices of T and S. As usual, $\boldsymbol{\mu}_m$ denotes the group of m^{th}-roots of unity in $\bar{K}$. We are now in a position to define the *Weil pairing*.

Definition 1.2. *Let S, T be points $\in E[m]$. The Weil pairing e_m is defined by the map*

$$e_m : E[m] \times E[m] \longrightarrow \boldsymbol{\mu}_m : \ e_m(S, T) = \frac{g_T \circ \mathcal{T}_S}{g_T},$$

where g_T and $\mathcal{T}_S$ are as in (4.1) and (4.2).

Proposition 1.3. *The Weil e_m-pairing has the following properties:*

1. *It is bilinear:*

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T), \tag{4.3}$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2). \tag{4.4}$$

2. *It is alternating:*

$$e_m(T, T) = 1. \tag{4.5}$$

   So $e_m(S, T) = e_m(T, S)^{-1}$.

3. *It is nondegenerate: If* $e_m(S, T) = 1$ *for all* $S \in E[m]$, *then* $T = \mathcal{O}$.

4. *It is Galois invariant:*

$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma) \quad \text{for all } \sigma \in G_{\bar{K}/K}. \tag{4.6}$$

5. *It is compatible:*

$$e_{mm'}(S, T) = e_m([m']S, T) \quad \text{for all } S \in E[mm'] \text{ and } T \in E[m]. \tag{4.7}$$

Proof. See [33, 3.8.1]. □

1.2 Computing the Weil Pairing

There exists a double-and-add algorithm due to Victor Miller [26] that computes the Weil pairing in linear time. We can restrict ourselves to pairs $(P, Q) \in E \setminus \{\mathcal{O}\} \times E \setminus \{\mathcal{O}\}$, else the Weil pairing would be just 1. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be nonzero points on an elliptic curve E defined over a field K given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.8}$$

Let λ be the slope of the line connecting P and Q (if $P = Q$ we take the slope of the tangent line at E and if the line is vertical set $\lambda = \infty$). Next we define a function $h_{P,Q} \in \bar{K}(E)$ as follows

$$h_{P,Q} = \begin{cases} \dfrac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2 - a_1\lambda + a_2} & \text{if } \lambda \neq \infty, \\ x - x_P & \text{if } \lambda = \infty. \end{cases}$$

Lemma 1.4. *We have that*

$$div(h_{P,Q}) = (P) + (Q) - (P + Q) - (\mathcal{O}).$$

Proof. First consider the case $\lambda \neq \infty$. Let $y = \lambda x + \nu$ be the line through the points P, Q. By Bezout's theorem this line intersects the curve at a third point S. So $S = -P - Q$ by the definition of the group law on E. Therefore

$$div(y - \lambda x - \nu) = (P) + (Q) + (-P - Q) - 3(\mathcal{O}).$$

The denumerator of $h_{P,Q}$ is equal to $x - x_{P+Q}$ and vanishes exactly at two points on E. The second point must be $-P-Q$, since for a point S we know that $x_S = x_{-S}$. Therefore

$$div(x - x_{P+Q}) = (P + Q) + (-P - Q) - 2(\mathcal{O}).$$

It follows that

$$div(h_{P,Q}) = (P) + (Q) - (P + Q) - (\mathcal{O}).$$

Suppose now that $\lambda = \infty$, hence $P + Q = \mathcal{O}$. The function $x - x_P$ has only zeros in P, Q, therefore

$$div(x - x_P) = (P) + (Q) - 2(\mathcal{O}) = (P) + (Q) - (P + Q) - (\mathcal{O}).$$

We conclude that $h_{P,Q}$ has the desired divisor in both cases. □

Let $m \geq 1$ and write m as

$$m = b_0 + b_1 \cdot 2 + \cdots + b_t \cdot 2^t \quad \text{with } b_i \in \{0, 1\} \text{ and } b_t \neq 0.$$

The pseudo-code of Miller's Algorithm is the following

Input: $m = \sum_{i=0}^{t} b_i 2^i$ with $b_i \in \{0, 1\}$, $P \in E$;
Output: f_P such that $div(f_P) = m(P) - ([m]P) - (m - 1)(\mathcal{O})$;
$T \leftarrow P$, $f \leftarrow 1$;
for $i = t - 1$ **to** 0 **do**
1 $\quad f \leftarrow f^2 h_{T,T}$, $T \leftarrow 2T$;
$\quad$ **if** $b_i = 1$ **then**
2 $\quad\quad f \leftarrow f h_{T,P}$, $T \leftarrow T + P$;
$\quad$ **end**
end
return f

Algorithm 1: Miller's Algorithm

Theorem 1.5. *Algorithm 1 returns a function f_P whose divisor satisfies*

$$div(f_P) = m(P) - ([m]P) - (m - 1)(\mathcal{O}),$$

in $\log_2(m)$ steps. In particular, if $P \in E[m]$, then $div(f_P) = m(P) - m(\mathcal{O})$.

Proof. The proof is based on the previous lemma. We refer to [33, Chapter XI, theorem 8.1.b]. □

Let $P \in E[m]$. Miller's Algorithm returns a function f_P whose divisor is $m(P) - m(\mathcal{O})$. An adjustment of algorithm 1 allows us to evaluate $f_P(Q)$ for $Q \neq \mathcal{O}$. This can be achieved by evaluating $h_{T,T}(Q)$ in 1 and $h_{T,P}(Q)$ in 2.

There is an alternative definition of the Weil pairing for which we can apply Miller's algorithm:
Let E be an elliptic curve. We want to define a pairing

$$\tilde{e}_m : E[m] \times E[m] \longrightarrow \boldsymbol{\mu}_m.$$

Let σ denote the surjective group homomorphism from the group of degree-0 divisors to the elliptic curve

$$\sigma : Div^0(E) \xrightarrow{D \sim (P)-(\mathcal{O}) \ \mapsto P} E. \tag{4.9}$$

Let $P, Q \in E[m]$ and choose degree zero divisors D_P and D_Q such that $\sigma(D_P) = P$ and $\sigma(D_Q) = Q$. We can choose these divisors in such way that they have disjoint support. For example, we can take $D_P = (P) - (\mathcal{O})$ and $D_Q = (Q + R) - (R)$ where $R \notin \{\mathcal{O}, P, -Q, P - Q\}$.
Since P and Q are in $E[m]$ there exist functions $f_P, f_Q \in \bar{K}(E)$ satisfying

$$div(f_P) = mD_P \quad \text{and} \quad div(f_Q) = mD_Q.$$

For a function $f \in \bar{K}(E)$ and a divisor $D = \sum_i n_i(P_i)$ such that $div(f)$ and D have disjoint support, we can evaluate f in D as follows

$$f(D) = \prod_i f(P_i)^{n_i}.$$

Now let

$$\tilde{e}_m(P, Q) := \frac{f_P(D_Q)}{f_Q(D_P)}.$$

We will need the Weak Weil Reciprocity.

Theorem 1.6 (Weak Weil reciprocity)**.** *Let E be an elliptic curve defined over K. Suppose that f and g are non-zero functions on the curve E. If $div(f)$ and $div(g)$ have disjoint support, then*

$$f(div(g)) = g(div(f)).$$

Proof. We refer to [3, Pages 212-213]. □

Lemma 1.7. *The pairing $\tilde{e}_m$ is well defined.*

Proof. We need to prove that

1. $\tilde{e}_m(P, Q)$ does not depend on the choises D_P and D_Q
2. $\tilde{e}_m(P, Q)^m = 1$

Let $D'_P \sim D_P$ and $D'_Q \sim D_Q$ such that D'_P and D'_Q have disjoint support. Hence there exists rational functions $r, s \in \bar{K}(E)$ such that

$$D'_P = D_P + div(r) \tag{4.10}$$
$$D'_Q = D_Q + div(s). \tag{4.11}$$

Recall that D_P and D_Q have disjoint support, therefore $div(r)$ and $div(s)$ also have disjoint support. It follows that D'_P and D_Q have disjoint support, similarly D_P and D'_Q have disjoint support. Let $f'_P, f'_Q \in \bar{K}(E)$ such that

$$div(f'_P) = mD'_P \qquad div(f'_Q) = mD'_Q.$$

From (4.10), we find that (up to a constant) $f'_P = f_P r^m$ and $f'_Q = f_Q s^m$. Then

$$\begin{aligned}
\frac{f'_P(D'_Q)}{f'_Q(D'_P)} &= \frac{f_P r^m(D'_Q)}{f_Q s^m(D'_P)} \\
&= \frac{f_P(D'_Q) r(D'_Q)^m}{f_Q(D'_P) s^(D'_P)^m} \\
&= \frac{f_P(D'_Q) r(mD'_Q)}{f_Q(D'_P) s(mD'_P)} \\
&= \frac{f_P(D_Q + div(s)) r(mD'_Q)}{f_Q(D_P + div(r)) s(mD'_P)} \\
&= \frac{f_P(D_Q + div(s)) r(mD'_Q)}{f_Q(D_P + div(r)) s(mD'_P)} \\
&= \frac{f_P(D_Q) f_P(div(s)) r(mD'_Q)}{f_Q(D_P) f_Q(div(r)) s(mD'_P)}
\end{aligned}$$

Now we use the Weak Weil Reciprocity. The last term becomes

$$\begin{aligned}
\frac{f_P(D_Q) s(div(f_P)) r(mD'_Q)}{f_Q(D_P) r(div(f_Q)) s(mD'_P)} &= \frac{f_P(D_Q) s(mD_P) r(mD'_Q)}{f_Q(D_P) r(mD_Q) s(mD'_P)} \\
&= \frac{f_P(D_Q) s(mD_P - mD'_P) r(mD'_Q - mD_Q)}{f_Q(D_P)} \\
&= \frac{f_P(D_Q) s(-div(r)) r(div(s))}{f_Q(D_P)} \\
&= \frac{f_P(D_Q)}{f_Q(D_P)} \qquad \text{(Weak Weil Reciprocity).}
\end{aligned}$$

Note that many functions were defined up to a constant multiple, but these constants vanish either by taking the quotient or by evaluating in degree zero divisors. By the latter we mean that for rational functions f, g such that $f = c \cdot g$ for some constant $c \in K^*$, we can evaluate f in a degree divisor $D = \sum_i a_i(P_i)$ having disjoint support with $div(f)$. Then

$$f(D) = \prod_i f(P_i)_i^a = \prod_i c^{a_i} g(P_i) = g(D)$$

since $\sum_i a_i = 0$. Now it remains to be shown that $\tilde{e}(P,Q)^m = 1$, which is nothing but an application of the Weak Weil Reciprocity. □

Proposition 1.8. *If we denote by e_m the Weil pairing, then $\tilde{e}_m = e_m$.*

Proof. A proof sketch is provided in [33, Page 462]. □

We now take

$$D_Q = (Q+S) - (S) \sim (Q) - (\mathcal{O}) \quad \text{and} \quad D_P = (P-S) - (-S) \sim (P) - (\mathcal{O}).$$

Here we assume that $S \in E$ such that D_P and D_Q have disjoint support. By proposition 1.8

$$e_m(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{f_Q(P-S)}{f_Q(-S)}$$

hence we can use Miller's algorithm and evaluate the function at four points.
In elliptic curve cryptography we work with finite fields $\mathbb{F}_q$. Therefore, for practical applications of the Weil pairing it is sufficient to work over the smallest extension field $\mathbb{F}_{q^k}$ such that $E[n] \subset E(\mathbb{F}_{q^k})$. We denote by k the *(Weil-) embedding degree of the curve with respect to n*. The pairing defined in the next section gives a faster computable pairing.

2 The Tate-Lichtenbaum Pairing

Frey and Ruck introduced the Tate pairing to cryptography as a mean to translate (in certain cases) a discrete logarithm problem on an abelian curve over a finite field to a discrete logarithm problem in finite extension [16]. We will define the Tate-Lichtenbaum pairing for elliptic curves over a finite field $K = \mathbb{F}_q$, which is always the case in cryptography. For a general treatment see [33, section XI.9].

Let E be an elliptic curve defined over $\mathbb{F}_q$. Let n be a positive integer coprime to q such that $n|\#E(\mathbb{F}_q)$. Suppose that k is the least positive integer such that $n|q^k - 1$. This value is called the *(Tate-) embedding degree of the curve with respect to n*. The field $\mathbb{F}_{q^k}$ is the smallest field containing both $\mathbb{F}_q$ and $\boldsymbol{\mu}_n$. In cases most relevant to cryptography, the Tate-embedding degree is equal to the Weil-embedding degree.

Theorem 2.1 (Balasubramanian and Koblitz [5])**.** *Let E be an elliptic curve over $\mathbb{F}_q$ and let r be a prime dividing $\#E(\mathbb{F}_q)$. Suppose that r does not divide $(q-1)$ and that* $\gcd(r,q) = 1$. *Then $E[r] \subset E(\mathbb{F}_q)$ if and only if r divides $(q^k - 1)$.*

Assume $E(\mathbb{F}_{q^k})$ contains an element of order n.

Theorem 2.2. *We have a non-degenerate bilineair pairing*

$$\langle \cdot, \cdot \rangle_n : E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$$

which is called the Tate-Lichtenbaum (or Tate) pairing.

Proof.

- The definition of the Tate pairing is as follows. Let $P \in E(\mathbb{F}_{q^k})[n]$. We let D_P be a divisor defined over $\mathbb{F}_{q^k}$ of degree 0 with sum P. Then $D_P - (P) + (\mathcal{O})$ is a divisor of a function $h \in \overline{\mathbb{F}}_{q^k}(E)$. This is the same as requiring D_P to be linearly equivalent to $(P) - (\mathcal{O})$, then $nD_P \sim n(P) - n(\mathcal{O})$. Hence, there exists a function $f \in \overline{\mathbb{F}}_{q^k}(E)$ with divisor nD_P:

$$div(f) = nD_P. \tag{4.12}$$

Now let $D_Q = \sum_i a_i(Q_i)$ be a degree zero divisor with sum Q and defined over $\mathbb{F}_{q^k}$ such that D_P and D_Q have disjoint support. Define

$$\langle P, Q \rangle_n = f(D_Q) \left(\mathrm{mod} (\mathbb{F}_{q^k}^*)^n \right), \tag{4.13}$$

where the definition of $f(D_Q)$ is as described above lemma 1.7.

- Well defined: Note that the function f is determined up to a constant multiple. The constant factor cancels out in (4.13) since D_Q is a degree zero divisor. We have showed that the definition (4.13) is independent of the choice of the function f.
We claim that $f(D_Q) \in \mathbb{F}_{q^k}$. We can prove it using Galois theory, therefore set $G := Gal(\overline{\mathbb{F}}_{q^k}/\mathbb{F}_{q^k})$ and take $D_P = (P) - (\mathcal{O})$. Let $\sigma \in G$, then $\sigma(D_P) = D_P$ since D_P is defined over $\mathbb{F}_{q^k}$. Therefore f^σ has the same divisor as f, so f^σ/f is a constant $c_\sigma \in \mathbb{F}_{q^k}^*$. The map $\alpha : G \to \overline{\mathbb{F}}_{q^k} : \sigma \mapsto c_\sigma$ represents a cocycle in the Galois cohomology group $H_1(G, \overline{\mathbb{F}}_{q^k}^*) = Z(G, \overline{\mathbb{F}}_{q^k}^*)/B(G, \overline{\mathbb{F}}_{q^k}^*)$. This is true because $\sigma_1\sigma_2$ gets mapped to
$$f^{\sigma_2\sigma_1}/f = f^{\sigma_1}/f \cdot f^{\sigma_2\sigma_1}/f^{\sigma_1}.$$
For an introduction about Galois cohomology see [40, Section 8.9]. Hilbert's theorem 90 says that $H_1(G, \overline{\mathbb{F}}_{q^k}^*)$ is trivial. Therefore α is contained in $B(G, \overline{\mathbb{F}}_{q^k}^*)$, which means that there exists a constant $c_1 \in \overline{\mathbb{F}}_{q^k}^*$ such that

$$c_\sigma = c_1^\sigma / c_1 \quad \text{for all} \quad \sigma \in G.$$

This eventually means that f/c_1 is defined over $\mathbb{F}_{q^k}$ and we can use this function in (4.13).
Now let $R \in E(\mathbb{F}_{q^k}) \setminus \{\mathcal{O}, P, -Q, Q - P\}$, so

$$f(D_Q) = \frac{f(Q+R)}{f(R)} \in \mathbb{F}_{q^k}^*. \tag{4.14}$$

In cryptographical applications it is always possible to choose such an R (the group $E(\mathbb{F}_{q^k})$ is large). Anyhow, using Galois theory, one can show that the condition in (4.14) holds even if we choose such a point R defined over an extension field of $\mathbb{F}_{q^k}$.

In the definition of the Tate pairing we factor out by the subgroup $(\mathbb{F}_{q^k}^*)^n$ to make (4.14) independent of the choices of D_P and D_Q. The previous statement can be proven using the Weil reciprocity, similar as in the proof of lemma 1.7.

- Linearity. Now we show linearity in the second variable. If Q_1 and Q_2 are points in $E(\mathbb{F}_{q^k})$, and D_{Q_1} and D_{Q_2} are corresponding divisors, then

$$D_{Q_1} + D_{Q_2} \sim (Q_1) - (\mathcal{O}) + (Q_2) - (\mathcal{O}).$$

The latter is linearly equivalent to $(Q_1 + Q_2) - (\mathcal{O})$ by the group morphism σ (4.9) , so $D_{Q_1+Q_2} \sim D_{Q_1} + D_{Q_2}$. Consequently

$$\langle P, Q_1 + Q_2\rangle_n = f(D_{Q_1})f(D_{Q_2}) = \langle P, Q_1\rangle_n\langle P, Q_2\rangle_n$$

Take $P_1, P_2 \in E(\mathbb{F}_{q^k})[n]$ and let D_{P_1} and D_{P_2} denote corresponding divisors. Let f_1, f_2 be functions corresponding to P_1, P_2. Similarly, we have that $D_{P_1+P_2} \sim D_{P_1} + D_{P_2}$, therefore we can let $D_{P_1+P_2} = D_{P_1} + D_{P_2}$. We also have that

$$div(f_1 f_2) = nD_{P_1} + nD_{P_2} = nD_{P_1+P_2},$$

so we can use the function $f_1 f_2$ to compute

$$\langle P_1 + P_2, Q\rangle_n = f_1(D_Q)f_2(D_Q) = \langle P_1, Q\rangle_n\langle P_2, Q\rangle_n.$$

This proves the bilinearity in the first variable.

- The non-degeneracy of the Tate pairing is much more difficult to prove. For a proof see [18, theorem 4].

□

It is often the case in cryptographic applications that one wants a *unique* outcome. This is why we consider the *modified* Tate pairing

$$\tau_n(P, Q) = \langle P, Q\rangle_n^{\frac{q^k-1}{n}} \tag{4.15}$$

which takes values in $\boldsymbol{\mu}_n$, the group of n-th roots of unity. The lemma below shows that we essentially obtain the same non-degenerate bilinear pairing.

Lemma 2.3. *Suppose that n divides $q-1$. We have the group isomorphism*

$$\zeta : \mathbb{F}_q^*/(\mathbb{F}_q^*)^n \to \boldsymbol{\mu}_n : \overline{x} \mapsto x^{(q-1)/n}$$

Proof. We can write $\mathbb{F}_q^* = \{1, a, \cdots, a^{q-2}\}$, since $\mathbb{F}_q^*$ is cyclic with order $q-1$. Consider the group morphism $\zeta' : \mathbb{F}_q^* \to \boldsymbol{\mu}_n : x \mapsto x^{(q-1)/n}$. Suppose that $x = a^b$ gets mapped to 1, i.e. $x^{(q-1)/n} = a^{b(q-1)/n} = 1$. We claim that n divides b. If not, then we can find integers k, r such that $b = kn+r$ and $0 < r < n$. We obtain $a^{r(q-1)/n} = 1$. But $r(q-1)/n < (q-1)$, this is a contradiction since a has exact order $q-1$. Therefore the kernel is exactly the group $(\mathbb{F}_q^*)^n$. Write $q - 1 = nd$, then we see that $\zeta'(a) = a^d$ has order n and hence generates the group $\boldsymbol{\mu}_n$. We have proved the injectivity and surjectivity of ζ. □

3 The Tate-Lichtenbaum Pairing via Elliptic Nets

A standard algorithm for computing pairings is Miller's algorithm. In this section we discuss Stanges new method of computing the Tate pairing, arising from the theory of elliptic nets [36]. In section 3.3 we will see that this new method has the same complexity as Miller's algorithm.

3.1 Preliminaries.

Fix an elliptic curve E defined over $\mathbb{C}$. Let $\mathbf{P} = (P_1, \ldots, P_n) \in E^n$ denote an appropriate (definition 1.1, chapter 3) n-tuple of points. Then $W(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \cdots, P_n)$ is an elliptic net $\mathbb{Z}^n \to \mathbb{C}$. This choice of an n-tuple induces a group homomorphism

$$\phi : \mathbb{Z}^n \to E,$$

defined by $\phi(\mathbf{e_i}) = P_i$. This prompts the following definition.

Definition 3.1. *Let E be an elliptic curve defined over a field K. Let $\phi : \mathbb{Z}^n \to E(K)$ be a homomorphism such that the points $\phi(\mathbf{e_i})$, for $i = 1, \cdots, n$ form an appropriate n-tuple on $E(K)$. Define the elliptic net $W_\phi : \mathbb{Z}^n \to K$ by*

$$W_\phi(\mathbf{v}) = \Psi_{\mathbf{v}}(\phi(\mathbf{e}_1), \ldots, \phi(\mathbf{e}_n)).$$

It can happen that $W_{\mathbf{v}}(\phi(\mathbf{e}_1), \ldots, \phi(\mathbf{e}_n)) \neq W_{\mathbf{v}'}(\phi'(\mathbf{e}_1), \ldots, \phi'(\mathbf{e}_n))$ even when

$$\sum_i v_i \phi(\mathbf{e}_i) = \sum_i v_i' \phi'(\mathbf{e}_i),$$

i.e. we cannot consider a net W as a map on $E(K)$. For example, take the elliptic curve $E : y^2 + y = x^3 + x^2 - 2x$ which contains $P = (0, 0)$ and $Q = (1, 0)$. By proposition 2.7 (chapter 2) we find

$$\Psi_{(1,-1)}(2P, Q) = 2 \qquad \Psi_{(2,1)}(P, -Q) = -1.$$

Let $K = \mathbb{F}_q$ be a finite field and E_K an elliptic curce defined over K. Stange obtains a free abelian group of finite rank $\hat{E}_K \cong \mathbb{Z}^r$ with a surjective homomorphism

$$\pi : \hat{E}_K \to E_K(K),$$

to exploit the freedom of choosing points on the elliptic curve $E(K)$ by means of a homomorphism. Then she considers $\hat{\Gamma} \cong \mathbb{Z}^n$ a subgroup of $\hat{E}_K$. Let $\Gamma = \pi(\hat{\Gamma})$. The claim is that for any surjective morphism $\phi : \mathbb{Z}^n \to \Gamma$ there exists a lift $\hat{\phi} : \mathbb{Z}^n \to \hat{\Gamma}$ which is an isomorphism. Define $V_\phi = W_\phi \circ \hat{\phi}^{-1}$. We note that some conditions have to be ensured for the lift to exist. For suppose that $n = 1$ and consider the surjective morphisms

$$f : \mathbb{Z} \to \mathbb{Z}/8\mathbb{Z} \qquad \text{and} \qquad \phi : \mathbb{Z} \to \mathbb{Z}/8\mathbb{Z},$$

where $f(x) = 3x \bmod 8$ and $\phi(x) = x \bmod 8$. Clearly, no isomorphism $\hat{\phi} : \mathbb{Z} \to \mathbb{Z}$ exists such that $f \circ \hat{\phi} = \phi$.

Lemma 3.2. *Given the elliptic net W_ϕ and a homomorphism $T : \mathbb{Z}^n \to \mathbb{Z}^n$, then*

$$W_{\phi \circ T} \sim W_\phi \circ T.$$

Proof. By definition we have that

$$W_\phi \circ T(\mathbf{v}) = \Psi_{T\mathbf{v}}(\phi(\mathbf{e}_1), \ldots, \phi(\mathbf{e}_n))$$

and

$$\begin{aligned} W_{\phi\circ T}(\mathbf{v}) &= \Psi_{\mathbf{v}}(\phi(T\mathbf{e}_1),\ldots,\phi(T\mathbf{e}_n)) \\ &= \Psi_{\mathbf{v}}(T^t(\phi(\mathbf{e}_1),\ldots,\phi(\mathbf{e}_n))^t). \end{aligned}$$

For the latter, the transformation formula (proposition 4.3, chapter 2) yields

$$\frac{\Psi_{T(\mathbf{v})}(\phi(\mathbf{e}_1),\ldots,\phi(\mathbf{e}_n))}{\prod_{i=1}^{n}\Psi_{T(\mathbf{e_i})}(\phi(\mathbf{e}_1),\ldots,\phi(\mathbf{e}_n))^{2v_i^2-\sum_j v_iv_j}\prod_{1\le i<j\le n}\Psi_{T(\mathbf{e_i}+\mathbf{e_j})}(\phi(\mathbf{e}_1),\ldots,\phi(\mathbf{e}_n))^{v_iv_j}}.$$

The above denumerator is a product of quadratic forms $\mathbb{Z}^n \to K^*$ which is also a quadratic form. Therefore, both nets are equivalent. □

The elliptic net V_ϕ is unique up to a rescaling.

Theorem 3.3. *We have that $V_\phi : \hat{\Gamma} \to K$ is an elliptic net and the equivalence class of V_ϕ is independent of the choice of the surjective homomorphism ϕ.*

Proof. We first verify that V_ϕ is an elliptic net. Note that for $p, q \in \hat{\Gamma}$, we find by definition

$$\begin{aligned} V_\phi(p+q) &= W_\phi(\hat{\phi}^{-1}(p+q)) = W_{\hat{\phi}^{-1}(p+q)}(\phi(\mathbf{e}_1),\ldots,\phi(\mathbf{e}_n)) \\ &= W_{\hat{\phi}^{-1}(p)+\hat{\phi}^{-1}(q)}(\phi(\mathbf{e}_1),\ldots,\phi(\mathbf{e}_n)). \end{aligned}$$

So for $p, q, r, s \in \hat{\Gamma}$ the map V_ϕ satisfies the elliptic net relation (equation (2.2), chapter 2) since this is equivalent with the elliptic net relation for W_ϕ with p, q, r, s equal to $\hat{\phi}^{-1}(p), \hat{\phi}^{-1}(q), \hat{\phi}^{-1}(r), \hat{\phi}^{-1}(s) \in \mathbb{Z}^n$. It remains to show that $[V_\phi]$ is independent of the choice ϕ. Choose another surjective morphism $\phi' : \mathbb{Z}^n \to \Gamma$. Then there exists an isomorphism $T : \mathbb{Z}^n \to \mathbb{Z}^n$ such that $\hat{\phi} \circ T = \hat{\phi}'$ and $\phi \circ T = \phi'$. By definition

$$V_{\phi'} = W_{\phi'} \circ \hat{\phi}'^{-1} = W_{\phi\circ T} \circ T^{-1} \circ \hat{\phi}^{-1}.$$

By the previous lemma, the latter is equivalent to $V_\phi = W_\phi \circ \hat{\phi}^{-1}$. □

We have defined a unique class $[V_\phi]$ of elliptic nets from $\hat{\Gamma} \cong \mathbb{Z}^n$ to K. We can do this for every subgroup $\mathbb{Z}^m \cong \hat{\Gamma} \subset \hat{E}_K$.

Definition 3.4. *Let $\mathcal{W}_{\hat{E}_K}$ denote the set*

$\{W : \hat{E}_K \to K \mid W'(\mathbf{v}) \sim V_\phi(\mathbf{v})$, *where ϕ is defined as above and W' is the restriction of W*$\}$.

Note that since K is a finite field, the condition $V \sim W$ for elliptic nets over K exactly means that there exist $\alpha, \beta \in K^*$ and a quadratic form $g : \mathbb{Z}^n \to \mathbb{Z}$ such that

$$V(\mathbf{v}) = \alpha\beta^{g(\mathbf{v})}.$$

3.2 Tate Pairing using elliptic nets

Recall the properties of the Weierstrass σ-function. The divisor of the function $\Omega_{1,v_2,\ldots,v_n}(z_1,\ldots,z_n)$ considered as a function in z_1 (hence an elliptic function) is

$$\{1\}(\sum_{j=2}^{n} -v_j z_j) - \{1 - \sum_{j=2}^{n} v_j\}(0) - \sum_{j=2}^{n}\{v_j\}(-z_j) \tag{4.16}$$

We know that the field of elliptic functions on $\mathbb{C}/\Lambda$ is isomorphic to the field of rational functions on E. The associated rational function (considered as a function in P_1) has divisor

$$div(\Psi_{1,v_2,\ldots,v_n}(P_1,\ldots,P_n)) = \{1\}(\sum_{j=2}^{n} -v_j P_j) - \{1 - \sum_{j=2}^{n} v_j\}(\mathcal{O}) - \sum_{j=2}^{n}\{v_j\}(-P_j).$$

We then find

$$div(\Psi_{(1,0,0)}) = 0, \quad div(\Psi_{(1,m,0)}) = (-mP_2) + (m-1)(\mathcal{O}) - m(-P_2)$$
$$div(\Psi_{(1,0,1)}) = 0, \quad div(\Psi_{(1,m,1)}) = (-mP_2 - P_3) + m(\mathcal{O}) - m(-P_2) - (-P_3)$$

By [36, Theorem 3], the same holds for appropriate points $P_1,\ldots,P_n \in E_K(K)$ and net polynomials over $K = \mathbb{F}_q$. So for net polynomials $\Psi_{\mathbf{v}}$ over K, we obtain

$$div(\Psi_{1,v_2,\ldots,v_n}(P_1,\ldots,P_n)) = \{1\}(\sum_{j=2}^{n} -v_j P_j) - \{1 - \sum_{j=2}^{n} v_j\}(\mathcal{O}) - \sum_{j=2}^{n}\{v_j\}(-P_j).$$

Theorem 3.5. *Fix a positive integer $m \in \mathbb{Z}$. Let E be an elliptic curve defined over a finite field K such that $\boldsymbol{\mu}_m \subset K$. Let $P, Q \in E(K)$ with $mP = \mathcal{O}$. Choose $S \in E(K) \setminus \{\mathcal{O}, -Q\}$. Since π is a surjective group morphism we can find $p, q, s \in \hat{E}_K$ such that $\pi(p) = P, \pi(q) = Q$ and $\pi(s) = S$. Let $W \in \mathcal{W}_{\hat{E}_K}$. Then the quantity*

$$T_m(P,Q) = \frac{W(s+mp+q)W(s)}{W(s+mp)W(s+q)} \tag{4.17}$$

is the Tate pairing.

Proof. By proposition 1.3 (chapter 3) and the assumption on the choice of S, any W in the equivalence class is not vanishing at those four arguments. We first prove that T_m is independent of the choice of an element in in $\mathcal{W}_{\hat{E}_K}$. Let W_1 and W_2 be elliptic nets contained in $\mathcal{W}_{\hat{E}_K}$, then by definition $W_2(\mathbf{v}) = \alpha\beta^{f(\mathbf{v})}W_1(\mathbf{v})$ for some $\alpha, \beta \in K^*$. Denote by T_m and T'_m the maps (4.17) corresponding to the nets W_1 and W_2, respectively. Then

$$\frac{T_m(P,Q)}{T'_m(P,Q)} = \frac{W_1(s+mp+q)W_1(s)W_2(s+mp)W_2(s+q)}{W_1(s+mp)W_1(s+q)W_2(s+mp+q)W_2(s)} \tag{4.18}$$

$$= \frac{\beta^{f(s+mp)+f(s+q)}}{\beta^{f(s+mp+q)+f(s)}} \tag{4.19}$$

$$= \beta^{f(s+mp)+f(s+q)-f(s+mp+q)-f(s)} \tag{4.20}$$

By the definition of a quadratic form we have that

$$-f(s+mp+q) = -f(s+mp) - f(mp+q) - f(q+s) + f(s) + f(mp) + f(q),$$

Using lemma 1.6 (chapter 2) and the parallelogram law, the exponent in equation (4.20) becomes

$$f(mp) + f(q) - f(mp+q) = m(f(p) + f(q) - f(p+q)).$$

Therefore $T_m(P,Q) = T'_m(P,Q) \bmod (K^*)^m$. Let $\Gamma \subset E_K(K)$ denote the subgroup generated by S, P and Q. Let

$$f_P = \frac{\Psi_{1,0,0}(-S,P,Q)}{\Psi_{1,m,0}(-S,P,Q)}.$$

By our previous remarks, the divisor of f_P as a function of S is

$$div(f_P) = m(P) - ([m]P) + (1-m)(\mathcal{O}) = m(P) - m(\mathcal{O}).$$

Let D_Q be the divisor $(-S) - (-S-Q)$, then we obtain in $K^*/(K^*)^m$

$$\begin{aligned} f_P(D_Q) &= \frac{f_P(-S)}{f_P(-S-Q)} \\ &= \frac{\Psi_{1,0,0}(S,P,Q)\Psi_{1,m,0}(S+Q,P,Q)}{\Psi_{1,m,0}(S,P,Q)\Psi_{1,0,0}(S+Q,P,Q)} \\ &= \frac{\Psi_{1,0,0}(S,P,Q)\Psi_{1,m,1}(S,P,Q)}{\Psi_{1,m,0}(S,P,Q)\Psi_{1,0,1}(S,P,Q)}. \end{aligned}$$

The last equation follows from the transformation formula for net polynomials. We now choose a homomorphism $\phi : \mathbb{Z}^3 \to \Gamma$ such that $\phi(1,0,0) = S$, $\phi(0,1,0) = P$ and $\phi(0,0,1) = Q$. Then $W_\phi(\mathbf{v}) = \Psi_{\mathbf{v}}(S,P,Q)$ for $\mathbf{v} \in \mathbb{Z}^3$ is an elliptic net. The Tate pairing is $\tau_m(P,Q) = f_P(D_Q)$. Therefore

$$\tau_m(P,Q) = \frac{W_\phi(1,0,0)W_\phi(1,m,1)}{W_\phi(1,m,0)W_\phi(1,0,1)} = \frac{V_\phi(s+mp+q)V_\phi(s)}{V_\phi(s+mp)V_\phi(s+q)} = T_m(P,Q).$$

□

Corollary 3.6. *Let n, E, K, P and Q be as above. Then*

$$\tau_m(P,Q) = \frac{W_{E,P,Q}(m+1,1)W_{E,P,Q}(1,0)}{W_{E,P,Q}(m+1,0)W_{E,P,Q}(1,1)}.$$

And if $W_{E,P}$ is the net associated to E, P, then we have

$$\tau_m(P,P) = \frac{W_{E,P}(m+2)W_{E,P}(1)}{W_{E,P}(m+1)W_{E,P}(2)}$$

Proof. For the first formula take $s = p$, obtaining

$$T_m(P,Q) = \frac{W((m+1)p+q)W(p)}{W((m+1)p)W(p+q)}.$$

For the second, take $p = q = s$, obtaining

$$T_m(P,Q) = \frac{W((m+2)p)W(p)}{W((m+1)p)W(2p)}.$$

□

3.3 Computation

Remark that we can choose several elliptic nets to compute the Tate pairing. This allows freedom for implementation considerations. For simplicity we only work with the net $W_{E,P,Q}$. Note that $W_{E,P,Q}(1,1)$ and $W_{E,P,Q}(1,0)$ are both 1. Consequently, in order to compute the Tate pairing as in corollary 3.6, it suffices to compute the terms $W_{E,P,Q}(m+1,1)$ and $W_{E,P,Q}(m+1,0)$. Denote by W the elliptic net $W_{E,P,Q}$. Stange adapts and generalises Shipsey's algorithm (section 4, chapter 1) to calculate terms $W(m,1)$ and $W(m,0)$ of an elliptic net. The algorithm is as follows. Stange obtains the block centred on m

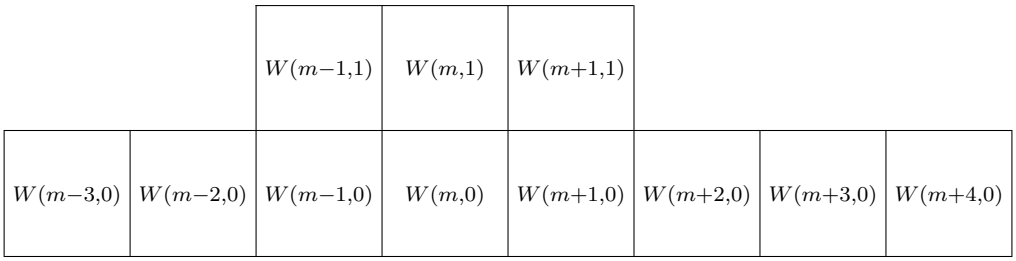


Figure 4.1

in $\log(m)$ steps by defining two functions:

1. **Double**(V): Given a block V centred on k, returns the block centred on $2k$.
2. **DoubleAdd**(V): Given a block V centred on k, returns the block centred on $2k+1$.

The block centred on 1 can easily be obtained, see [36, section 4.2] for the details. The formulae needed for calculating the terms of Double(V) and DoubleAdd(V) from the block V are

$$W(2i-1,0) = W(i+1,0)W(i-1,0)^3 - W(i-2,0)W(i,0)^3$$
$$W(2i,0) = \left(W(i,0)W(i+2,0)W(i-1,0)^2 - W(i,0)W(i-2,0)W(i+1,0)^2\right)/W(2,0)$$

and

$$W(2k-1,1) = \left(W(k+1,1)W(k-1,1)W(k-1,0)^2 - W(k,0)W(k-2,0)W(k,1)^2\right)/W(1,1)$$
$$W(2k,1) = W(-1,1)W(k+1,1)W(k,0)^2 - W(k-1,0)W(k+1,0)W(k,1)^2$$
$$W(2k+1,1) = \left(W(k-1,1)W(k+1,1)W(k+1,0)^2 - W(k,0)W(k+2,0)W(k,1)^2\right)/W(1,-1)$$
$$W(2k+2,1) = \left(W(k+1,0)W(k+3,0)W(k,1)^2 - W(k-1,1)W(k+1,1)W(k+2,0)^2\right)/W(2,-1).$$

The above formulae are instances of the elliptic net relation [36, section 4.1]. In this way we obtain the terms in figure 4.1 after $\log_2(m)$ steps and then compute

$$\tau_m(P,Q) = W(m+1,1)/W(m+1,0).$$

For a discussion about implementation considerations and complexity see [36, section 5]. The algorithm described above is of complexity $O(\log(m))$ and is comparable to Miller's algorithm in terms of efficiency.

4 Other Pairings via Elliptic Nets

Currently, the most suitable pairing for the efficient implementation of pairing-based cryptographic schemes is the Tate pairing. Therefore, many algorithms for efficient computation of the Tate pairings and some its variants have been proposed. The variants of the Tate pairing include $\eta_T[2]$, Duursma-Lee [9], Ate [19], Ate$_i$ [42], R-Ate [22], and optimal [39] Pairings. Naoki Ogura et al showed that all the above pairings can be computed using elliptic nets [27]. Their experimental results show that pairing computations using elliptic nets is comparable to those using Miller's Algorithm in terms of efficiency.

Chapter 5

The Discrete Logarithm Problem

Let $G, \cdot$ be a cyclic group with identity element 1 and generator g. Suppose that we have been given an element $h \in G$. *The discrete logarithm problem* asks for the smallest positive integer x such that

$$h = g^x.$$

Elliptic curve cryptography is based on the assumption that the discrete logarithm problem for elliptic curves is hard. In 1976, Diffie and Hellman published the first public key construction which is based on the discrete logarithm problem in $\mathbb{F}_p^*$ [10]. The DLP in $\mathbb{F}_q^*$ can be solved in subexponential time by index calculus methods [25, p. 129]. For elliptic curves there is no analogue algorithm. The best known algorithms to solve the ECDLP take exponential time. This fact is the primary attraction for using elliptic curves in cryptography. We will describe the well known MOV/Frey-Rück attack on the ECDLP. The sections in the end relate the ECDLP with elliptic nets.

1 Diffie-Hellman key exchange

We first state some closely related problems used in cryptography.

Problem 1.1 (Elliptic Curve Discrete Logarithm Problem (ECDLP))**.** *Let E be an elliptic curve over a finite field K. Suppose there are points $P, Q \in E(K)$ given such that $Q \in \langle P \rangle$. Determine k such that $Q = [k]P$.*

This problem is believed to be very hard since only exponential algorithms solve this problem in general.

Problem 1.2 (Computational Diffie-Hellman problem (CDH))**.** *Suppose that $g, g^a, g^b \in G$ are given. Determine g^{ab}. This problem is referred to as the computational Diffie-Hellman problem (CDHP).*

Problem 1.3 (Decisional Diffie-Hellman problem (DDH))**.** *Suppose that $g, g^a, g^b, h \in G$ are given. Decide whether $h = g^{ab}$. This problem is referred to as the computational Diffie-Helmman problem (CDHP).*

Obviously, if one can solve CDH in polynomial time then he can also solve DDH in polynomial time, notation $CDH \longrightarrow DDH$. It is also obvious that $DLP \longrightarrow CDH$. It is not known whether $CDH \longrightarrow DLP$.

One application of the hardness of CDH is the *Diffie-Hellman key exchange protocol* [10]. It solves the following problem. Two parties A (Alice) and B (Bob) want to share a secret key through an insecure channel such that no eavesdropper is able to find the secret key. Assume the two parties agreed on a cyclic group G with (large) prime order and generator g, and also the hardness of CDH in G. Then A and B can exchange a secret key in one round as follows:

1. Alice generates a random positive integer $a < |G|$. Then she sends to B the information
$$g^a.$$
2. Bob also generates a random positive integer $b < |G|$ and sends to A the element
$$g^b.$$

After these two steps A computes $(g^b)^a = g^{ab}$ and B computes $(g^a)^b = g^{ab}$. The secret key is $s = g^{ab}$. An eavesdropper watching the insecure channel knows only
$$G, g, g^a, g^b.$$
Therefore it is infeasible for him to find s. See [40, Chapter 6] for other applications in the same setting where G is a prime order subgroup of an elliptic curve E.

2 Attacks

A naive way to solve the DLP is by computing $g, g^2, g^3, \cdots$ until we encounter $h = g^x$. But this takes x steps and is very impractical when x is very large, say $x \approx 2^{60}$. The fastest algorithms which work for general groups G are the *Pollard-ρ* and *baby-step giant-step* methods. These algorithms are both exponential. The *index calculus method* can be addressed for the multiplicative group of a finite field $\mathbb{F}_q$. The index calculus method is a subexponential algorithm [25, p. 129]. Below we discuss a simplification of the DLP which clearly works for every abelian group G.

2.1 The Pohlig Hellman Simplificiation

In [28] Pohlig and Hellman noticed that it suffices to solve the logarithm problem for the case that $\langle P \rangle$ has prime order. To see this, denote by n the order of the point P. Let $p \mid n$ be a prime divisor and e the largest integer such that $p^e \mid n$. We wish to solve
$$Q = [m]P.$$
We can determine some information about m by solving the problem
$$Q' = [n']Q = [m_0]([n']P) = [m_0]P'$$
where $n' = n/p^{e-1}$ and P' is a point of order p. If we can solve this problem, then we find $m_0 \equiv m \bmod p$. Now suppose that the ECDLP can be solved (efficiently) in the case that $\mathrm{ord}(P)$ is a prime number. By the previous remark we immediately obtain

$m \bmod p$. Then we can ascertain m modulo $p^2, \cdots, p^e$ in the following way. Suppose we know $m \equiv m_i \bmod p^{i+1}$, hence $m = m_i + kp^{i+1}$ for some integer $k \in \mathbb{Z}$. Then

$$R = Q - [m_i]P = [m]P - [m_i]P = [k]([p^{i+1}]P) = [k]S,$$

where R and S are known and S has order $s = n/p^{i+1}$. Let $s' = s/p^{e-(i+1)-1}$, so $p \mid s'$ and $p^2 \nmid s'$. Therefore, the point

$$[s']S = S'$$

is a point of order p. Now we solve

$$R' = [s']R = [k]([s']S) = [k_0]S'$$

and find $k \equiv k_0 \bmod p$. We also acquire $m \bmod p^{i+2}$. We can continue in this fashion until we find $m \bmod p^e$. The same applies for the other prime divisors of

$$n = \prod_{i=1}^{l} p_i^{e_i}.$$

We deduce $m \bmod n$ by the chinese remainder theorem.

Ofcourse, for this method to be applicable we need to have some information about the factorisation of $|E(\mathbb{F}_q)|$. Even if it is *hard* to find the factorisation, for the above simplification to be infeasible it would be a good idea to ensure that $|E(\mathbb{F}_q)|$ has a large prime factor.

2.2 The MOV/Frey-Rück attack

An important application of pairings in elliptic curve cryptography is to transform an instance of the elliptic curve discrete logarithm problem to a discrete logarithm problem in a finite field. The motivation for this approach is that there are subexponential time algorithms which solve the discrete logarithm problem in a finite field. The first such approach was given by Menezes, Okamoto and Vanstone [24] by using the Weil pairing. An approach using the (modified) Tate pairing which generalized the MOV-attack was given by Frey and Rück [15].

The Frey-Rück attack is as follows:

Algorithm 2.1. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let $P \in E(\mathbb{F}_q)$ with prime order r coprime to q. Suppose that $Q = [k]P$ where $1 < k < r$. The following algorithm returns k. The map τ_r denotes the modified Tate pairing (equation (4.15), chapter 4).*

1. *Construct the field $\mathbb{F}_{q^k}$ such that r divides $(q^k - 1)$.*
2. *Find a point $S \in E(\mathbb{F}_{q^k})$ such that $e_r(P, S) \neq 1$*
3. *$\zeta_1 \leftarrow \tau_r(P, S)$*
4. *$\zeta_2 \leftarrow \tau_r(Q, S)$*
5. *Find λ such that $\zeta_1^\lambda = \zeta_2$ in $\mathbb{F}_{q^k}^*$.*

6. return λ

The first four steps require negligible computational resources. Does step 2 always work? Well, by theorem 2.2 of the previous chapter (and equation (4.15) after its proof) we have a surjective group morphism

$$f : S \mapsto \tau_r(P, S) \in \boldsymbol{\mu}_r,$$

because τ_r is non-degenerate and r is a prime. The size of its kernel is

$$\frac{|E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})|}{|\boldsymbol{\mu}_r|} = 1.$$

Therefore the probability that we choose a *wrong* S in step 2 is $\frac{1}{r}$, which is quite small when r is large. Consequently, we have that $\tau_r(P, S)$ is a primitive r-th root of 1 right from the start with a high probability. The running time is determined by step 5 which is subexponential.

2.3 Shipsey's attack

More relevant for our thesis is an attack given by Shipsey and Swart in [31]. The attack translates the problem to a DLP in the finite field $\mathbb{F}_q$, where we can use subexponential time algorithms. It concerns the case where E is an elliptic curve defined over a finite field field $\mathbb{F}_q$ with odd characteristic. We also assume that $|E(\mathbb{F}_q)| = q - 1$ has a large prime factor N. We can write $q - 1 = lN$ for a small even integer l. The attack is based on the following

Theorem 2.1. *For $P \in E$ the division polynomials satisfy*

$$\psi_{nk}(P) = \psi_k(P)^{n^2}\psi_n([k]P)$$

as long as $[k]P \neq \mathcal{O}$.

Proof. The proof is an easy application of the transformation formula (proposition 4.3, chapter 2) in the rank one case. □

We proceed with the notation $W(n) = W_{E,P}(n) = \psi_n(P)$. See theorem 3.4 in the next section where it is shown that for a point P with $\mathrm{ord}(P) \geq 4$, there exist constants $c, d \in \mathbb{F}_q$ such that

$$W(t + sN) = c^{st}d^{s^2}W(t) \quad \text{in } \mathbb{F}_q$$

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

By the above theorem we have that

$$W(kq) = W(k(lN + 1)) = c^{k^2l}d^{k^2l^2}W(k)$$

and

$$W((k + 1)q) = W((k + 1)(lN + 1)) = c^{(k+1)^2l}d^{(k+1)^2l^2}W(k + 1).$$

Use the fact that $c^l d^{l^2} = W(1+lN) = W(q)$ to deduce from the previous two equations that

$$W(q)^{2k+1} = \frac{W(q(k+1))}{W(qk)} \cdot \frac{W(k)}{W(k+1)}. \tag{5.1}$$

We want to get rid of the terms involving k in the right-hand side. We can assume that $[k]P \neq \mathcal{O} \neq [k+1]P$, else the problem would be trivial. Use theorem 2.1 twice:

$$W(qk) = W(k)^{q^2} W_{E,[k]P}(q)$$
$$W(q(k+1)) = W(k+1)^{q^2} W_{E,[k+1]P}(q).$$

Since $Q = [k]P$ we can write equation (5.1) as (using the previous two equations)

$$W(q)^{2k+1} = \left(\frac{W(k+1)}{W(k)}\right)^{q^2-1} \cdot \frac{W_{E,Q+P}(q)}{W_{E,Q}(q)}. \tag{5.2}$$

The term $\left(\frac{W(k+1)}{W(k)}\right)^{q^2-1}$ equals 1 since we work in the cyclic group $\mathbb{F}_q^*$. We are left with

$$\left(W(q)^2\right)^k = \frac{W_{E,Q+P}(q)}{W_{E,P}(q) W_{E,Q}(q)}. \tag{5.3}$$

We now have a discrete log $\alpha^k = \beta$ in $\mathbb{F}_q$, which would reveil nothing if $\alpha = 1$. Since $d^2 = c^N$ (theorem 3.4)and l is even, we find by theorem 2.1 that

$$W(q) = W(lN+1) = d^{l^2} c^l = c^{(lN)\frac{l}{2}} c^l = \left(c^{q-1}\right)^{l/2} c^l = c^l.$$

The order of c^l divides N because $q - 1 = lN$. We have two possibilities, because N is a prime number. If the order is 1, then the attack simply fails. In the second case the order must be N. Then it is clear that

$$\mathrm{ord}_{\mathbb{F}_q^*}(W(q)^2) = N.$$

The attack described above only works if $W(q) \neq 1$ in $\mathbb{F}_q$. The occasion $W(q) = 1$ should not cause a problem: Shipsey and Swart stated the following

Conjecture 2.2. *If P is a point of order N on an elliptic curve $E/\mathbb{F}_q$ and $|E(\mathbb{F}_q)| = q - 1 = lN$ where l is even, then*

$$W_{E,P}(q) = 1,$$

with probability $\frac{1}{N}$

3 ECDLP and equivalent hard problems for Elliptic Nets

In this section we explain the ideas of Lauter and Stange [21] in relating hard problems for elliptic divisibility sequences with the ECDLP. We assume that all elliptic divisibility sequences are of the form $W_{E,P}$. Throughout this section, the point $P \in E(K)$ will always be of prime order not dividing $q-1$ and greater than 3. Before going to the problems, we first study the important properties of elliptic nets over finite fields. We assume that the basic arithmetic in $\mathbb{F}_q$ can be executed in $O(\log(q)^2)$ steps [17, Chapter 2] since we are only concerned with polynomial vs. non-polynomial time algorithms.

3.1 Periodicity properties

Recall the definition of $\Psi_{\mathbf{v}}$ for an elliptic curve E defined over K described in chapter 2. We have also defined the elliptic net associated to an appropriate n-tuple of points $\boldsymbol{P} = (P_1, \cdots, P_n) \in E^n$ (definition 1.1, chapter 3) as the map

$$W_{E,P_1,\cdots,P_n} : \mathbb{Z}^n \to K$$

defined by

$$W_{E,P_1,\cdots,P_n}(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \cdots, P_n).$$

Recall also that for $\mathbf{v} \in \mathbb{Z}^n$ we have that $\Psi_{\mathbf{v}}(\boldsymbol{P}) = 0$ if and only if

$$v_1 P_1 + \cdots + v_n P_n = 0.$$

Hence the indices corresponding to the zero terms of an elliptic net form a sublattice.

Definition 3.1. *The lattice of zero-apparition of an elliptic net is the set of indices for which the elliptic net vanishes.*

Because the zeros of an elliptic net form a sublattice, for EDS the zeros are periodic and we know exactly the periodicity of these terms (the order of the point corresponding to W). If the EDS is periodic, this period must be a multiple of the period of the zeros. This leads to the following definition

Definition 3.2. *A perfectly periodic elliptic divisibility sequence is an EDS which has a finite period $n > 0$, and whose first positive index k such that $W(k) = 0$ is $k = n$. A non-perfectly periodic elliptic divisibility sequence is one which has a finite period $n > 0$, and whose first positive index k such that $W(k) = 0$ is $k < n$.*

Note that for the moment we do not know whether an EDS over a finite field is periodic.

Theorem 3.3. *Let $\mathbf{P} \in E^s$ and $\mathbf{v} \in \mathbb{Z}^t$. Suppose that T be any $t \times s$ integral matrix such that $T\mathbf{P}$ is an appropriate t-tuple. Then*

$$W_{E,\mathbf{P}}(T^{tr}(\mathbf{v})) = W_{E,T(\mathbf{P})}(\mathbf{v}) \times \prod_{i=1}^{t} W_{E,\mathbf{P}}(T^{tr}(\mathbf{e}_i))^{v_i^2 - v_i(\sum_{j \neq i} v_j)} \prod_{1 \leq i < j \leq t} W_{E,\mathbf{P}}(T^{tr}(\mathbf{e}_i + \mathbf{e}_j))^{v_i v_j}$$

The previous theorem is the key to the following theorems.

Theorem 3.4. *Suppose that $W_{E,P}(m) = 0$ for a non-degenerate elliptic divisibility sequence and* $\operatorname{ord}(P) \geq 4$. *Then for all $l, v \in \mathbb{Z}$, we have*

$$W_{E,P}(lm + v) = W_{E,P}(v)a^{vl}b^{l^2}$$

where

$$a = \frac{W_{E,P}(m+2)}{W_{E,P}(m+1)W_{E,P}(2)}, \qquad b = \frac{W_{E,P}(m+1)^2 W_{E,P}(2)}{W_{E,P}(m+2)}.$$

Furthermore, $a^m = b^2$. Therefore, there exists an $\alpha \in \bar{K}$, the algebraic closure of K, such that $\alpha^2 = a$ and $\alpha^m = b$, and so

$$W_{E,P}(lm + v) = W_{E,P}(v)\alpha^{(lm+v)^2 - v^2}.$$

Proof. The first equation was first proven by M. Ward for $K = \mathbb{F}_p$ [41, Theorem 8.1]. Stanges proof is based on theorem 3.3. In theorem 3.3, take successively the matrices

$$T = \begin{pmatrix} m+2 \\ 1 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

to obtain

$$W_{E,([m+2]P,P)}(s,t)W_{E,P}(m+2)^{s^2-st}W_{E,P}(m+3)^{st}W_{E,P}(1)^{t^2-st} = W_{E,P}(sm+2s+t). \tag{5.4}$$

and

$$W_{E,([2]P,P)}(s,t)W_{E,P}(2)^{s^2-st}W_{E,P}(3)^{st}W_{E,P}(1)^{t^2-st} = W_{E,P}(2s+t). \tag{5.5}$$

Note that $m | \operatorname{ord}(P)$, therefore $[m+2]P = 2P$. We also have that $W_{E,P}(1) = 1$. Set $t = v - 2l$ and rearrange equations (5.4) and (5.5) to find

$$W_{E,P}(lm + v) = W_{E,P}(v)a^{lv}b^{l^2}$$

for nonzero $a, b \in K$. The expressions for a and b can be derived from the above equation by setting $l = 1, k = 1, 2$. Finally we are left with proving that $a^m = b^2$. We calculate

$$W_{E,P}(k)a^{2v}b^4 = W_{2m+v} = W(m + (m + v)) = W_{E,P}(m + v)a^{m+v}b = W_{E,P}(v)a^{m+2v}b^2,$$

which gives the desired equation. □

For the rank two case, we have

Theorem 3.5. *Suppose $\mathbf{r} = (r_1, r_2) \in \mathbb{Z}^2$ is such that $W_{E,P,Q}(\mathbf{r}) = 0$. For $l \in \mathbb{Z}$ and $\mathbf{v} = (v_1, v_2) \in \mathbb{Z}^2$ we have*

$$W_{E,P,Q}(l\mathbf{r} + \mathbf{v}) = W_{E,P,Q}(\mathbf{v})a_{\mathbf{r}}^{lv_1}b_{\mathbf{r}}^{lv_2}c_{\mathbf{r}}^{l^2}$$

where

$$a_{\mathbf{r}} = \frac{W(r_1+2, r_2)}{W(r_1+1, r_2)w(2,0)},\ b_{\mathbf{r}} = \frac{W(r_1, r_2+2)}{W(r_1, r_2+1)W(0,2)},\ c_{\mathbf{r}} = \frac{W(r_1+1, r_2+1)}{a_{\mathbf{r}}b_{\mathbf{r}}W(1,1)}.$$

Proof. This is another application of theorem 3.3. The proof is quite lengthy, we refer to [37, Theorem 10.2.3]. □

Proposition 3.6. *Every (non-degenerate) EDS or EN over a finite field $K = \mathbb{F}_q$ is periodic.*

Proof. By theorem 3.4 we get

$$W(v + lm) = W(v)a^{vl}b^{l^2}$$

for all $v, l \in \mathbb{Z}$. Let l be the least common multiple of $\mathrm{ord}(a)$ and $\mathrm{ord}(b)$ in $\mathbb{F}_q^*$. Then we find that for all $v \in \mathbb{Z}$

$$W(v + lm) = W(v).$$

We conclude that W must be periodic and the period divides lm. Similarly, every (non-degenerate) elliptic net has a lattice of periodicity. □

3.2 Perfectly Periodic Elliptic Nets

The next proposition says that every non-degenerate EDS is equivalent with a perfect periodic EDS.

Proposition 3.7. *Let W be a non-degenerate elliptic divisibility sequence with rank of zero apparition m. There exists a perfectly periodic elliptic divisibility sequence W' such that $W \sim W'$.*

Proof. Let α be as in theorem 3.4. We first prove that the elliptic divisibility sequence defined by $W'(n) = \alpha^{1-n^2}W(n)$ is perfectly periodic with period m. Let $n \in \mathbb{Z}$, so by theorem 3.4 we have

$$\begin{aligned} W'(n+m) &= \alpha^{1-(n+m)^2}W(n+m) \\ &= \alpha^{1-(n+m)^2}\alpha^{(m+n)^2-n^2}W(n) \\ &= \alpha^{1-n^2}W(n) = W'(n). \end{aligned}$$

It is clear that the rank of zero apparition of W' equals m. We conclude that W' is perfectly periodic with period m. □

The last proposition shows that we can rescale any non-degenerate EDS to a perfectly period EDS. We have used the α of theorem 3.4. The practical problem is that we don't know α explicitely. The following theorem gives an explicit rescaling for certain elliptic divisibility sequences.

Theorem 3.8. *Let $K = \mathbb{F}_q$ be a finite field and E an elliptic curve defined over K. For all points $P \in E$ of order relatively prime to $q - 1$ and greater than 3, define*

$$\phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+\mathrm{ord}(P))}\right)^{\frac{1}{\mathrm{ord}(P)^2}}. \tag{5.6}$$

Set $\phi(\mathcal{O}) = 0$. Let m denote the order P. For all integers n where $\gcd(n, m) = 1$, it holds that

$$\phi([n]P) = \phi(P)^{n^2}W_{E,P}(n). \tag{5.7}$$

For a point P of prime order not dividing $q - 1$ and greater than 3, the sequence $\phi([n]P)$ is a perfectly periodic elliptic divisibility sequence equivalent to $W_{E,P}(n)$.

Proof. Note that the definition of ϕ makes sense. We have that $W_{E,P}(q-1+\mathrm{ord}(P)) \neq 0$ since m and $q-1$ are relatively prime. Now take $T = (l)$ in theorem 3.3, so

$$W_{E,[l]P}(n)W_{E,P}(l)^{n^2} = W_{E,P}(nl). \tag{5.8}$$

Changing the role of l and n yields

$$W_{E,[n]P}(l)W_{E,P}(n)^{l^2} = W_{E,P}(nl). \tag{5.9}$$

Taking $l = q-1$ in (5.8) and (5.9) gives

$$W_{E,[q-1]P}(n)W_{E,P}(q-1)^{n^2} = W_{E,P}(n(q-1))$$
$$W_{E,[n]P}(q-1)W_{E,P}(n)^{(q-1)^2} = W_{E,P}(n(q-1)).$$

Then

$$W_{E,[q-1]P}(n) = \frac{W_{E,P}(n(q-1))}{W_{E,P}(q-1)^{n^2}} = \frac{W_{E,[n]P}(q-1)W_{E,P}(n-1)^{(q-1)^2}}{W_{E,P}(q-1)^{n^2}}$$

Now take $l = q-1+m$, then

$$W_{E,[q-1+m]P}(n) = \frac{W_{E,P}((q-1+m)n)}{W_{E,P}(q-1+m)^{n^2}} = \frac{W_{E,[n]P}(q-1+m)W_{E,P}(n-1)^{(q-1+m)^2}}{W_{E,P}(q-1+m)^{n^2}},$$

and $W_{E,[q-1+m]P}(n) = W_{E,[q-1]P}(n)$. Therefore

$$\frac{W_{E,[n]P}(q-1)W_{E,P}(n)^{(q-1)^2}}{W_{E,P}(q-1)^{n^2}} = \frac{W_{E,[n]P}(q-1+m)W_{E,P}(n)^{(q-1+m)^2}}{W_{E,P}(q-1+m)^{n^2}}. \tag{5.10}$$

The terms live in $\mathbb{F}_q^*$, so we can rewrite equation (5.10) to the following form

$$\frac{W_{E,[n]P}(q-1)}{W_{E,[n]P}(q-1+m)} = \frac{W_{E,P}(q-1)^{n^2}}{W_{E,P}(q-1+m)^{n^2}}W_{E,P}(n)^{m^2}.$$

Let i be a positive integer such that $i \equiv m^{-1} \bmod (q-1)$. Taking the i^2-th power of both sides of the previous equation yields (5.7). It is an easy calculation to prove the last statement. □

In what follows, we will use the convenient notation

$$\tilde{W}_{E,P}(n) = \phi([n]P) \tag{5.11}$$

and call this the *perfectly periodic elliptic divisibility sequence associated to E and P*. We can illustrate the above theorem with an example.

Example 3.9. *Let E be the curve defined over $\mathbb{F}_{31}$ given by $y^2 = x^3 + 6x + 13$ and take the point $P = (2, 23)$ having order 13 . The sequence $W_{E,P}(n)$ starts with*

$$0, 1, 15, 3, 9, 30, 7, 12, 4, 22, 7, 1, 15, 0, 1, 27, 6, 20, 27, 7, 3, 8, 11, 28, 1, 27, 0, ...$$

We find that $\phi(P) = 4$. The sequence $\phi([n]P)$ is

$$0, 4, 27, 24, 5, 30, 28, 3, 1, 26, 7, 4, 27, 0, 4, 27, 24, 5, 30, 28, 3, 1, 26, 7, 4, 27, 0, ...$$

which has period 13. We have employed Stanges script (Sage) to compute the various terms of an EDS, see `http://math.stanford.edu/~stange/scripts/edstools.sage`.

More generally, we have the following result

Theorem 3.10 ([21, Theorem 6]). *Let $\mathbf{P} \in E(K)^n$ be a collection of nonzero points, no two equal or inverses, and all elements of a single cyclic group and having a fixed prime order greater than 3 not dividing $q-1$. The n-array $\phi(\mathbf{v}\cdot\mathbf{P})$ (as $\mathbf{v}$ ranges over $\mathbb{Z}^n$) forms a perfectly periodic elliptic net equivalent to $W_{E,\mathbf{P}}(\mathbf{v})$. Specifically,*

$$\phi(\mathbf{v}\cdot\mathbf{P}) = W_{E,\mathbf{P}}(\mathbf{v}) \prod_{i=1}^{n} \phi(P_i)^{v_i^2 - v_i\left(\sum_{j\neq i} v_j\right)} \prod_{1\leq i<j\leq n} \phi(P_i+P_j)^{v_i v_j}.$$

3.3 The problems

In the previous subsections we have covered the material which will be extensively used to explore the following problems and their relations.

Problem 3.1 (EDS Association). *Let E be an elliptic curve defined over a finite field K. Suppose there are points $P, Q \in E(K)$ given such that $Q \in \langle P\rangle$ and $\mathrm{ord}(P) \geq 4$ is prime. Determine $W_{E,P}(k)$ for $0 < k < \mathrm{ord}(P)$ such that $Q = [k]P$.*

Problem 3.2 (Width s EDS Discrete Log). *Given an elliptic divisibility sequence W whose rank of zero-apparition is prime, and given terms $W(k)$, $W(k+1)$, …, $W(k+s-1)$, determine k.*

Problem 3.3 (EDS Residue). *Let E be an elliptic curve over a finite field K. Suppose there are points $P, Q \in E(K)$ given such that $Q \in \langle P\rangle$, and $\mathrm{ord}(P) \geq 4$ is prime. Determine whether $W_{E,P}(k)$ is a square or not in K for $0 < k < \mathrm{ord}(P)$ such that $Q = [k]P$.*

Let us draw the attention to problem 3.1. It is trivial for perfectly periodic sequences $W_{E,P}$. This follows from the fact that if $m = \mathrm{ord}(P)$ is prime, we also have that the order of $Q = [k]P$ is equal to m. Theorem 3.8 implies

$$\phi(Q) = \left(\frac{W_{E,Q}(q-1)}{W_{E,Q}(q-1+\mathrm{ord}(Q))}\right)^{\frac{1}{\mathrm{ord}(Q)^2}}, \tag{5.12}$$

and clearly $\phi(P) = 1$, so we also have that

$$\phi(Q) = W_{E,P}(k).$$

Recall Shipsey's algorithm for computing the m-th term of an elliptic divisibility sequence $W_{E,P}(n)$ (section 4 of chapter 1). The loop runs $\log(m)$ times. Each step takes a bounded number of field operations in $\mathbb{F}_q$. Each field operations takes $O(loq(q)^2)$ steps. Hence the running time is $O(log(m)log(q)^2)$ steps. The terms involved in equation (5.12) can be computed in $O(\log(q)^3)$ time.

Lemma 3.11. *Let E be an elliptic curve defined over K, and $P \in E(K)$ be a point of prime order greater than 3 and not dividing $q-1$. The x-coordinate of $[n]P$, $x([n]P)$, can be calculated in $O((\log q)^2)$ time from the three terms $W_{E,P}(n-1)$, $W_{E,P}(n)$, and $W_{E,P}(n+1)$ or from the three terms $\widetilde{W}_{E,P}(n-1)$, $\widetilde{W}_{E,P}(n)$, and $\widetilde{W}_{E,P}(n+1)$.*

Proof. By lemma 2.4 in chapter 1 we have the identity

$$x([n]P) = x(P) - \frac{W_{E,P}(n-1)W_{E,P}(n+1)}{W_{E,P}(n)^2}. \tag{5.13}$$

To finish the proof, observe that

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

□

Theorem 3.12. *Let E be an elliptic curve over $\mathbb{F}_q$, and $P \in E(\mathbb{F}_q)$ a point of prime order not dividing $q-1$ and greater than 3. Given a point $Q = [k]P$, the term $\phi(Q) = \widetilde{W}_{E,P}(k)$ can be calculated in $O((\log q)^3)$ steps without requiring knowledge of k.*

Proof. Recall from theorem 3.8 the equation

$$\phi(Q) = \left(\frac{W_{E,Q}(q-1)}{W_{E,Q}(q-1+\mathrm{ord}(Q))}\right)^{\frac{1}{\mathrm{ord}(Q)^2}}$$

So, we need to find the terms $W_{E,Q}(q-1)$ and $W_{E,Q}(q-1+\mathrm{ord}(Q))$. Note that

$$\mathrm{ord}(P) = \mathrm{ord}(Q).$$

Hasse's theorem gives a bound for the number of points in $E(\mathbb{F}_q)$. We conclude that there is a constant C such that

$$|E(\mathbb{F}_q)| \leq Cq.$$

Therefore $\mathrm{ord}(Q)$ is on the order of q. Using Shipsey's algorithm we can find the necessary terms in $O(\log(q)^3)$ steps. We also need to find the inverse of $ord(Q)^2$ mod $q-1$ and raise the quotient to that power. Both of these operations take $O(\log(q))$ steps at worst. □

Theorem 3.13. *Let E be an elliptic curve over $\mathbb{F}_q$, and $P \in E(\mathbb{F}_q)$ a point of order relatively prime to $q-1$ and greater than 3. Given the terms $\widetilde{W}_{E,P}(k)$, $\widetilde{W}_{E,P}(k+1)$ and $\widetilde{W}_{E,P}(k+2)$, the point $Q = [k]P$ can be calculated with a probabilistic algorithm in time $O((\log q)^4)$ without requiring knowledge of k.*

Proof. By lemma 3.11 we can calculate $x([k+1]P)$ in $O(\log(q)^2)$ time. There are methods which can compute the corresponding y-values in probabilistic time $O((\log(q))^4)$ [1, 7.1-2]. We need to determine which of the points is actually $[k+1]P$. A way to determine the correct point is by choosing one of the two possible y-values and assume it is the correct one. Calculate $x([k+2]P)$ and $x([k+3]P)$ using the addition law on the elliptic curve. We use lemma 3.11 to determine $\widetilde{W}_{E,P}(k+3)$ and $\widetilde{W}_{E,P}(k+4)$ in turn. Then, if the terms $\widetilde{W}_{E,P}(k), \cdots, \widetilde{W}_{E,P}(k+4)$ also satisfy the recurrence instance

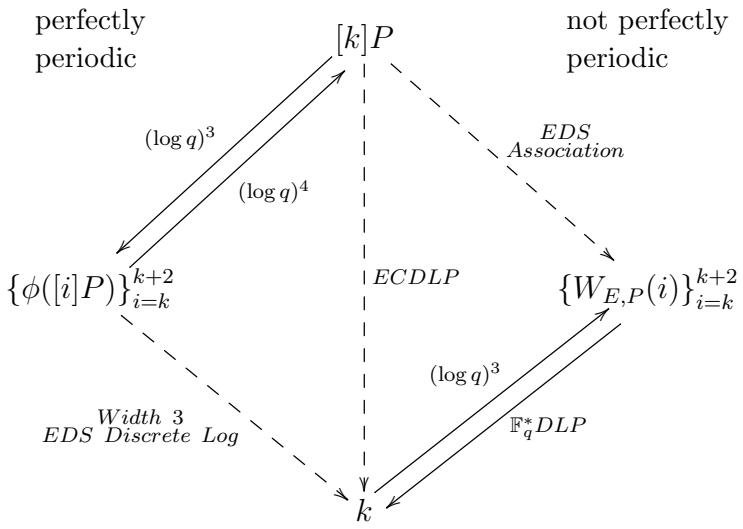
$$\widetilde{W}(k+4)\widetilde{W}(k) = \widetilde{W}(k+1)\widetilde{W}(k+3)\widetilde{W}(2)^2 - \widetilde{W}(3)\widetilde{W}(1)\widetilde{W}(k+2)^2,$$

our assumption about the point is correct. If not, our assumption was wrong and we choose the alternative. This follows from the fact that four consecutive terms of an elliptic divisibility sequence determine the sequence uniquely. □

We also have

Theorem 3.14 ([21, Theorem 10])**.** *Suppose P has order relatively prime to $q-1$ and greater than 3, and $\phi(P)$ is a primitive root in $\mathbb{F}_q^*$. Given $W_{E,P}(k), W_{E,P}(k+1), W_{E,P}(k+2)$, where it can be assumed that $0 < k < ord(P)$, calculating k can be reduced to a single discrete logarithm in $\mathbb{F}_q^*$ in probabilistic $O((\log q)^4)$ time.*

We can summarise with the diagram below. The dotted lines denote the hard problems which are proven to be equally hard in theorem 3.15



Theorem 3.15. *Let E be an elliptic curve defined over a finite field $K = \mathbb{F}_q$. Let $P \in E(\mathbb{F}_q)$ be a point of prime order not dividing $q-1$ and greater than 3. We work in the cyclic group generated by P. If any one of the following problems is solvable in sub-exponential time, then all of them are:*

1. *Problem 1.1: ECDLP*
2. *Problem 3.1: EDS Association for non-perfectly periodic sequences*
3. *Problem 3.2 ($s = 3$): Width 3 EDS Discrete Log for perfectly periodic sequences*

Proof.

- (1) $\implies$ (2)**:** Suppose that the ECDLP can be solven in subexponential time. Therefore, if $Q = [k]P$ is given, we obtain k in subexponential time. Then $W_{E,P}(k)$ can be calculated in $O((\log k)(\log q)^2) = O((\log q)^3)$ steps.
- (2) $\implies$ (1)**:** We have been given the points P and $Q = [k]P$. By hypothesis we obtain $W_{E,P}(k)$. By theorem 3.8 we have that

$$\frac{\phi(Q)}{W_{E,P}(k)} = \phi(P)^{k^2},$$

this is a discrete logarithm problem in $\mathbb{F}_q^*$ which we can solve in subexponential time.

- (1) $\implies$ (3)**:** Let $W_{E,P}(n)$ be a perfectly periodic elliptic divisibility sequence. Then $\widetilde{W} = W$. Suppose that the terms $W_{E,P}(k), W_{E,P}(k+1)$ and $W_{E,P}(k+2)$ are given. Theorem 3.13 computes the point $Q = [k]P$ in probabilistic $O(log(q)^4)$ time without requiring knowledge of k. By assumption the elliptic curve discrete logarithm problem can be solved in sub-exponential time. Therefore we can solve the Width 3 EDS Discrete Log in probabilistic sub-exponential time.

- (3) $\implies$ (1)**:** We have been given P and $Q = [k]P$. Theorem 3.12 allows calculation of $\phi([k]P)$, $\phi([k+1]P)$, and $\phi([k+2]P)$ in $O(log(q)^3)$ time. By hypothesis we can determine k in sub-exponential time. So we can solve the ECDLP in sub-exponential time.

□

3.4 Relating the EDS Residue problem

Lauter and Stange had the idea to study the residuosity of certain terms of an elliptic divisibility sequence. This led, as we will see, to some interesting insights concerning the discrete logarithm problem for elliptic curves.

Definition 3.16. *We call $x \in \mathbb{F}_q$ a quadratic residue if there exists an element $y \in \mathbb{F}_q$ such that $x = y^2$.*

A crucial fact is that the residuosity of an element of a finite field $\mathbb{F}_q$ can be determined in sub-exponential time [20].
The following proposition is an interesting hypothetical method for attacking the ECDLP.

Proposition 3.17. *Let P be a point of odd order relatively prime to $q-1$. Given an oracle which can determine the discrete logarithm of Q in $\langle P \rangle$ in time $O(T(q))$, the elliptic curve discrete logarithm for any such Q can be determined in time $O(T(q)\log q + (\log q)^2)$.*

Proof. Let k be such that $Q = [k]P$ and $0 \leq k < \operatorname{ord} P$. We work with the cyclic group $\langle P \rangle$. The basic algorithm is:

1. If $Q = P$, stop.
2. Call the oracle to determine the parity of k. If k is even, find Q' such that $[2]Q' = Q$. If k is odd, find Q' such that $[2]Q' = Q - P$.
3. Set $Q = Q'$ and return to step 1.

In Step 2, the point Q' is determined uniquely since the cyclic group $< P >$ has odd order. It can be found in $O(\log q)$ time (see [**?**] for methods). Furthermore, $Q' = [k']P$ where

$$k' = \begin{cases} k/2 & k \text{ even} \\ (k-1)/2 & k \text{ odd} \end{cases}.$$

Then k' is the minimal multiplier for Q' with respect to P. This process is repeated until $Q' = P$. The value of the original k can be deduced as follows:
For each even step, record a 0, and for each odd step a 1, writing from right to left, and adding a final 1. This will be the binary representation of k. Step 2 and 3 are executed

$log_2(k) = O(\log(q))$ times. Each time we go through step 2 we call the oracle and get an answer after $O(T(q))$ steps, and we need to determine Q' which is of complexity $O(\log(q))$. Therefore, the complexity is $O(\log(q)(T(q) + \log(q)))$. □

Proposition 3.18. *Let E be an elliptic curve over a field of characteristic not equal to two. Let P be a point of odd order such that $\phi(P)$ is a quadratic non-residue, and let k be the minimal multiplier of a multiple Q of P. Given P, Q and an oracle which can determine the quadratic residuosity of $W_{E,P}(k)$ in time $O(T(q))$, the elliptic curve discrete logarithm for any such Q can be determined in time $O((\log q)(T(q) + (\log q)^3))$.*

Proof. The oracle T determines the quadratic residuosity of $W_{E,P}(k)$ in time $O(T(q))$. Stange and Lauter argue that the parity of k can be determined by knowledge of the residuosity of $W_{E,P}(k)$ in time $O((\log q)^3)$ [21, Proposition 3]. So we have an oracle T' which determines the parity of k in time $O(T(q) + log(q)^3)$ given P, $Q = [k]P$ and $0 \leq k < \text{ord}(P)$. Use the oracle T' in proposition 3.17 to solve the elliptic curve discrete logarithm problem for Q in time

$$O\big((T(q) + log(q)^3)log(q) + log(q)^2\big) = O\big(log(q)(T(q) + log(q)^3)\big)$$

□

Theorem 3.19. *Let E be an elliptic curve defined over a finite field $K = \mathbb{F}_q$ with odd characteristic. Let $P \in E(\mathbb{F}_q)$ be a point of prime order not dividing $q - 1$ and greater than 3. We work with the cyclic group generated by P. Moreover, suppose that $|E(\mathbb{F}_q)|$ is odd. If any one of the following two problems is solvable in sub-exponential time, then both are:*

1. *Problem 1.1: ECDLP*
2. *Problem 3.3: EDS Residue for non-perfectly periodic sequences.*

The assumption that q is not a power of 2 is needed. If not then $x \mapsto x^2$ would be a group isomorphism, and every element would be a quadratic residue. If $\phi(P)$ is a quadratic residue, one solution to this obstacle is to replace the initial problem of $Q = [k]P$ with the equivalent problem of $[n]Q = [k]([n]P)$ for any n such that $\phi([n]P)$ is a quadratic non-residue. The sequence $W_{E,P}(n)$ can be calculated term-by-term until such an n is found. The existence of such an n is guaranteed when -1 is a quadratic non-residue in $\mathbb{F}_q$, in which case $\phi([m-1]P) = -\phi(P)$ suffices.

Proof.

(1) $\implies$ (2)**:** By hypothesis we obtain k from P and $Q = [k]Q$ in sub-exponential time. Then we compute $W_{E,P}(k)$ which takes $O((\log q)^3)$ time and determine the residuosity in sub-exponential time (see the comments after definition 3.16).

(2) $\implies$ (1)**:** This is proposition 3.18. □

Chapter 6

Rank Two Elliptic Nets Algorithm

There is already an algorithm for computing terms of elliptic divisibility sequences due to Shipsey. We have seen that it had relevance for cryptography. In this chapter we present an algorithm which computes a term $W(n,m)$ of (almost all) rank two elliptic nets in quadratic time. An overview of the algorithm is presented in section 3. An auxiliary algorithm of independent interest is presented in section 1, and one of the steps of the main algorithm is discussed in section 2.

1 First step

In this section we give an algorithm which computes $\dfrac{W(n,m)}{W(n,m+1)}$ in $O(x)$ steps if $W(n,-m) \neq 0$. Here x denotes the input size, i.e. the number of bits of $\max\{|n|,|m|\}$. We then prove an important consequence.

1.1 Efficient blocks

Let $W = W_{E,P,Q}$ be a non-degenerate elliptic net. For $k > 0$, Stange computes the block in Figure 6.1 in $\log(k)$ steps, see section 3.3 in chapter 4. Denote this horizontal block by $H(k)$. The idea of computing such blocks goes back to Shipsey as described in section 4 of chapter 1.

		$W(k-1,1)$	$W(k,1)$	$W(k+1,1)$			
$W(k-3,0)$	$W(k-2,0)$	$W(k-1,0)$	$W(k,0)$	$W(k+1,0)$	$W(k+2,0)$	$W(k+3,0)$	$W(k+4,0)$

Figure 6.1

Suppose we want to find the negative horizontal block in Figure 6.2 which we denote by $H(-k)$. Change the base to $-P, Q$ and let $W' = W_{E,-P,Q}$. For this base we efficiently

			$W(-k-1,1)$	$W(-k,1)$	$W(-k+1,1)$		
$W(-k-4,0)$	$W(-k-3,0)$	$W(-k-2,0)$	$W(-k-1,0)$	$W(-k,0)$	$W(-k+1,0)$	$W(-k+2,0)$	$W(-k+3,0)$

Figure 6.2

compute the block with center $-k$ as follows. We find that

$$\Psi_{v_1,v_2}(P,Q) = \frac{\Psi_{-v_1,v_2}(-P,Q)}{(-1)^{v_1^2-v_1v_2}\Psi_{-1,1}(-P,Q)^{v_1v_2}}$$

by the transformation formula where

$$T = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}.$$

The block centred on k and the transformation formula yield the block centred on $-k$ depicted in 6.2.
Clearly $W_{E,P,Q}(v,w) = W_{E,Q,P}(w,v)$ for $(v,w) \in \mathbb{Z}^2$. So in the same manner we obtain a block

$$W(0,k-3), W(0,k-2), \cdots, W(0,k+4), W(1,k-1), W(1,k), W(1,k+1).$$

Denote this vertical block by $V(k)$. We also obtain $V(-k)$.

1.2 Computing $W(n,m)/W(n,m+1)$

We seek an efficient algorithm for computing the value of a non degenerate elliptic net at a given index (n,m). By intuition we want to obtain this by using the blocks $H(-n), H(n), V(m)$ and $V(m)$. Recall the notation (2.10)

$$\begin{matrix} p_1 & q_1 & r_1 & s_1 \\ p_2 & q_2 & r_2 & s_2 \end{matrix} \left[\begin{matrix} p_1+q_1+s_1 & p_1-q_1 & r_1+s_1 & r_1 \\ p_2+q_2+s_2 & p_2-q_2 & r_2+s_2 & r_2 \end{matrix} \middle| \begin{matrix} q_1+r_1+s_1 & q_1-r_1 & p_1+s_1 & p_1 \\ q_2+r_2+s_2 & q_2-r_2 & p_2+s_2 & p_2 \end{matrix} \middle| \begin{matrix} r_1+p_1+s_1 & r_1-p_1 & q_1+s_1 & q_1 \\ r_2+p_2+s_2 & r_2-p_2 & q_2+s_2 & q_2 \end{matrix} \right].$$

Ideally we have one index (n,m) surrounded by $(\pm n+j,i)$ and $(t,\pm m+e)$ with small integers i,j,t,e such that the terms are contained in one of the blocks mentioned above.

Unfortunately, it *seems* that we cannot find $W(n,m)$ from these blocks. We could expect it though, else we would obtain an algorithm which is of the same complexity as the rank one case. Anyhow, we find that

$$W(n,-m)W(n,m) = W(n+1,0)W(0,m)^2W(n-1,0) \tag{6.1}$$
$$+ W(n,0)^2W(1,m)W(1,-m), \tag{6.2}$$

by

$$\begin{smallmatrix} n & n-1 & n & -n+1 \\ m & & 0 & 0 & & -m \end{smallmatrix} \left[\begin{smallmatrix} n & 1 & & 1 & n \\ 0 & m & -m & 0 \end{smallmatrix} \middle| \begin{smallmatrix} & n & -1 & 1 & n \\ -m & & 0 & 0 & m \end{smallmatrix} \middle| \begin{smallmatrix} n+1 & & 0 & & 0 & n-1 \\ & 0 & & -m & & -m \end{smallmatrix}\right],$$

and that

$$W(n,-m+1)W(n,m) = W(n+1,1)W(0,m)W(0,m-1)W(n-1,0) \tag{6.3}$$
$$+ W(n,1)W(1,m)W(1,1-m)W(n,0),$$

by

$$\begin{smallmatrix} n & n-1 & n & -n+1 \\ m & & 0 & 0 & & -m+1 \end{smallmatrix} \left[\begin{smallmatrix} n & 1 & & & 1 & n \\ 1 & m & -m+1 & 0 \end{smallmatrix} \middle| \begin{smallmatrix} & & n & -1 & 1 & n \\ -m+1 & & 0 & 1 & m \end{smallmatrix} \middle| \begin{smallmatrix} n+1 & & 0 & & & 0 & n-1 \\ & 1 & & -m & & -m+1 & \\ & & 0 & & & & \end{smallmatrix}\right].$$

So we can efficiently calculate the values $W(n,m)W(n,-m)$ and $W(n,m)W(n,-m+1)$. Note that $W(n,-m)$ and $W(n,-m+1)$ cannot be both zero (since $Q \neq \mathcal{O}$). Therefore we efficiently deduce whether $W(n,m)$ is zero or not. By dividing the LHS of (6.1) by the LHS of (6.3), we obtain $W(n,-m)/W(n,-m+1)$. Remark that this ratio is always useful. If it is zero or *not defined* then we know that $W(n,-m) = 0$ or $W(n,-m+1) = 0$. We can summarise the previous remarks with the following

Proposition 1.1. *Let W be a non-degenerate elliptic net. Let $n, m \in \mathbb{Z}$. Then we can determine*

- *whether $W(n,m)$ is zero or not,*
- *the ratios $W(n,m)/W(n,m+1)$ and $W(n,m)/W(n+1,m)$ if $W(n,-m) \neq 0$,*

in $O(\log(\max\{|n|,|m|\}))$ steps.

The following proposition is based on the previous proposition.

Proposition 1.2. *Let $W = W_{E,P,Q} : \mathbb{Z}^2 \to K$ be a non-degenerate elliptic net over a field K. Assume that*

$$2P \pm Q \neq \mathcal{O} \neq P \pm 2Q \qquad \text{and} \qquad 2P \pm 2Q \neq \mathcal{O}.$$

If a vertical block of length four is given

$$W(k,m), W(k,m+1), W(k,m+2), W(k,m+3)$$

then we can compute the adjacent vertical block

$$W(k+1,m), W(k+1,m+1), W(k+1,m+2), W(k+1,m+3)$$

in $O(\log(\max\{|k|,|m|\}))$.

Proof. The proof consists of five parts which cover all cases. We will often use expressions like $W(n,m) \longrightarrow W(n,m+1)$ to denote a (correct) application of proposition 1.1, that is, we can find $W(n,m)/W(n,m+1)$ only if $W(n,-m) \neq 0$.

A. The terms $W(k,m+3), W(k,m+2), W(k,m+1)$ and $W(k,m)$ are nonzero.

1. Suppose that $W(-k,m+i)$ is nonzero for $i \in \{0,1,2,3\}$. Then we find $W(k+1,m+i)$ for $i \in \{0,1,2,3\}$ by applying proposition 1.1 four times.

2. If $W(-k,m) = 0$, then both $W(-k,m+1)$ and $W(-k,m+2)$ are nonzero. We then find $W(k+1,m+1)$ and $W(k+1,m+2)$ by proposition 1.1. Two terms remain.

   (a) $W(k+1,m+1) \neq 0$:
   We directly acquire $W(k+1,m)$. We need to find $W(k+1,m+3)$. If $W(-k,m+3) \neq 0$, then we find $W(k+1,m+3)$. Else $W(-k,m+3) = 0$ and we consider two cases. The first case is $W(k+1,m+2) \neq 0$, then we find $W(k+1,m+3)$. The second case entails $W(k+1,m+2) = 0$. Then

   $$W(k+1,m+1) \longrightarrow W(k+2,m+1) \longrightarrow W(k+2,m+2) \longrightarrow W(k+2,m+3) \longrightarrow W(k+1,m+3),$$

   where each arrow is an application of proposition 1.1.

   (b) $W(k+1,m+1) = 0$:
   We have the sequence

   $$W(k,m+2) \longrightarrow W(k+1,m+2) \longrightarrow W(k+2,m+2) \longrightarrow W(k+2,m+1) \longrightarrow W(k+2,m) \longrightarrow W(k+1,m).$$

   So it remains to find $W(k+1,m+3)$. If $W(-k,m+3) \neq 0$, then we have that $W(k,m+3) \longrightarrow W(k+1,m+3)$. Else, we can do $W(k+1,m+2) \longrightarrow W(k+1,m+3)$.

3. If $W(-k,m+1) = 0$ we obtain the terms $W(k+1,m+3), W(k+1,m+2), W(k+1,m)$. In order to retrieve $W(k+1,m+1)$ we check whether $W(k+1,m)$ is zero or not (using proposition 1.1). If $W(k+1,m) = 0$ then

   $$W(k+1,m+2) \neq 0 \neq W(k+1,m+1).$$

   Then we find $W(k+1,m+1)$ because we acquire

   $$\frac{W(k+1,m+2)}{W(k+1,m+1)}.$$

   If $W(k+1,m) \neq 0$, then $W(k+1,m) \longrightarrow W(k+1,m+1)$.

4. The case $W(-k,m+2) = 0$ is analagous to **A**.3.

5. The case $W(-k,m+3) = 0$ is analagous to **A**.2.

This completes the first case.

B. $\boxed{W(k, m+3) = 0}$

1. $W(-k, m+2) = 0$:
   Then we have the sequence

$$W(k+1, m+1) \longrightarrow W(k+1, m+2) \longrightarrow W(k+1, m+3).$$

   The term $W(k+1, m)$ remains to be find. If $W(k, m) \neq 0$, then we find $W(k+1, m)$ because $W(-k, m+2) = 0$. Else we have the chain $W(k+1, m+1) \longrightarrow W(k+1, m)$, because the terms $W(k+1, m+1)$ and $W(-k-1, m)$ are nonzero.

2. $W(-k, m+1) = 0$:
   We find $W(k+1, m+3), W(k+1, m+2)$ and $W(k+1, m+2) \longrightarrow W(k+1, m+1)$. We also deduce that $W(-k-1, m) \neq 0$. The fact that $W(k, m+3)$ is zero implies $W(k+1, m+1) \neq 0$. By proposition 1.1 we obtain

$$\frac{W(k+1, m)}{W(k+1, m+1)}.$$

3. $W(-k, m) = 0$:
   By proposition 1.1 we obtain the nonzero terms

$$W(k+1, m+1) \qquad \text{and} \qquad W(k+1, m+2).$$

   We obtain $W(k+1, m)$ because $W(-k-1, m) \neq 0$. We also obtain $W(k+1, m+3)$ since $W(-k-1, m+2) \neq 0$ (recall that $P + 2Q \neq \mathcal{O}$).

4. $W(-k, m+3) = 0$:
   We obtain $W(k+1, m+1), W(k+1, m+2), W(k+1, m+3)$. The term $W(k+1, m)$ can be find by investigating two cases.

   (a) Suppose that $W(k, m) \neq 0$. If $W(-k, m) \neq 0$ then we find $W(k+1, m)$. Else, $W(-k-1, m) \neq 0$ and proposition 1.1 computes

$$\frac{W(k+1, m)}{W(k+1, m+1)}.$$

   (b) If $W(k, m) = 0$, then the terms $W(k+1, m), W(k+2, m), W(k+2, m+1)$ are nonzero. If $W(-k-1, m) \neq 0$, then one finds $W(k+1, m)$ by proposition 1.1. In the other case ($W(-k-1, m) = 0$) we obtain the chain

$$\begin{aligned} W(k+1, m+1) \longrightarrow W(k+2, m+1) \longrightarrow W(k+2, m) \longrightarrow W(k+2, m-1) \\ \longrightarrow W(k+1, m-1) \longrightarrow W(k+1, m). \end{aligned}$$

5. Consider the case where $W(-k, m) = 0 = W(-k, m+3)$. Then we obtain the nonzero terms $W(k+1, m+2), W(k+1, m+1)$. Finally, we execute $W(k+1, m+1) \longrightarrow W(k+1, m)$ and $W(k+1, m+2) \longrightarrow W(k+1, m+3)$.

6. We are left with the possibility $W(-k, m+i) \neq 0$ for $i \in \{0,1,2,3\}$.
We obtain the nonzero terms $W(k+1, m+2)$ and $W(k+1, m+1)$. Consider the following cases.

   (a) Suppose that $W(-k-1, m+2) = 0$. Then $W(-k-1, m) \neq 0$ and an application of proposition 1.1 yields $W(k+1, m)$. For the term $W(k+1, m+3)$ we use the chain (recall that $2P \pm 2Q \neq \mathcal{O}$)

$$W(k+1,m+1) \longrightarrow W(k+2,m+1) \longrightarrow W(k+2,m+2) \longrightarrow W(k+2,m+3) \longrightarrow W(k+1,m+3).$$

   (b) Now we have that $W(-k-1, m+2) \neq 0$. The term $W(k+1, m+3)$ is obtained by proposition 1.1. We are left with the term $W(k+1, m)$. If $W(k, m) \neq 0$, then we find $W(k+1, m)$. If $W(k, m) = 0$ we can use at least one of the chains

$$W(k+1,m+1) \longrightarrow W(k+1,m),$$

   or

$$W(k+1,m+1) \longrightarrow W(k+2,m+1) \longrightarrow W(k+2,m) \longrightarrow W(k+2,m-1) \longrightarrow W(k+1,m-1) \longrightarrow W(k+1,m).$$

Case **B** is completely proven.

C. $\boxed{W(k, m+2) = 0}$

1. If $W(-k, m+1) = 0$, then we find all the four adjacent terms as before.
2. If $W(-k, m+1) \neq 0$, then we immediately retrieve $W(k+1, m+1)$. We investigate two cases.

   (a) Suppose that $W(-k, m+3) = 0$. From the term $W(k+1, m+1)$ we obtain the terms $W(k+1, m+2)$ and $W(k+1, m+3)$. We retrieve $W(k+1, m)$ by

$$W(k,m) \longrightarrow W(k+1,m)$$

   if $W(-k, m) = 0$, else we apply

$$W(k+1,m+1) \longrightarrow W(k+1,m).$$

   (b) We obtain $W(k+1, m+3)$, since $W(-k, m+3)$ is nonzero. Inspect $W(-k, m)$. If it is zero we compute

$$W(k+1,m+1) \longrightarrow W(k+1,m) \quad \text{and} \quad W(k+1,m+1) \longrightarrow W(k+1,m+2).$$

   In the other case we find $W(k, m) \longrightarrow W(k+1, m)$. Then we can do at least one of the following

$$W(k+1,m+3) \to W(k+1,m+2) \quad \text{or} \quad W(k+1,m+1) \to W(k+1,m+2).$$

D. The case $\boxed{W(k, m+1) = 0}$ is analagous to case **C**.

E. The case $\boxed{W(k, m) = 0}$ is analogous to case **B**.

These five cases complete the proof of this proposition. The complexity is $O(\log(\max\{|n|, |m|\}))$: in the process of the (constructive) proof we call the algorithm in proposition 1.1 a bounded number of times. □

Remark that we can do exactly the same for a row of four vectors to find the adjacent row of four vectors.

1.3 Example

Let us put our hands on the computer. As mentioned earlier, we can determine quickly whether $W_{E,P,Q}(n, m)$ is zero or not. See the appendix for the Sage script which checks the latter. The code

```
sage:Fq=FiniteField(1847)
sage:E=EllipticCurve([Fq(1749),Fq(174)])
sage:P=E(531,1651);Q=5*P
```

creates a curve E defined over $\mathbb{F}_{1847}$ with two points P and $Q = [5]P$ of order 13 on it. Let us check if the script works correctly. By proposition 1.3 (chapter 3) we have that $W(5, -1) = 0, W(5, 1) \neq 0$ and $W(1681, 77) \neq 0$ since $1681 + 5 \cdot 77$ is not divisible by 13.

```
sage:ellipticnet_isZero(E,P,Q,5,-1,1847) # We ask whether W_{E,P,Q}(5,-1) is zero
     The term W(5,-1) is zero
sage:ellipticnet_isZero(E,P,Q,5,1,1847)
     The term W(5,1) is NOT zero.
sage:ellipticnet_isZero(E,P,Q,1681,77,1847)
     The term W(1681,77) is NOT zero.
```

2 Second step

In this section we construct an *S-block* around an index (k, n) which allows to go efficiently to an S block around $(k, 2n + \epsilon)$ with the understanding that $\epsilon \in \{0, 1\}$. We do the same for the first coordinate. For the second Suppose that we want to find $W(u, v)$. The idea is to first find a block centred on $(1, v)$ which will allow us to move to the final block around $W(u, v)$. See Figure 6.3 for the suitable block. We call it the (square) S-block around (k, n).

	$W(k-1,n+2)$	$W(k,n+2)$	$W(k+1,n+2)$	$W(k+2,n+2)$
$W(k-2,n+1)$	$W(k-1,n+1)$	$W(k,n+1)$	$W(k+1,n+1)$	$W(k+2,n+1)$
$W(k-2,n)$	$W(k-1,n)$	$W(k,n)$	$W(k+1,n)$	$W(k+2,n)$
$W(k-2,n-1)$	$W(k-1,n-1)$	$W(k,n-1)$	$W(k+1,n-1)$	$W(k+2,n-1)$

Figure 6.3: Square block around (k,n): $S(k,n)$.

2.1 Double and add going up

The following recurrences are needed to find the block around $W(k,2n)$ and $W(k,2n+1)$.

$$\begin{matrix} k & k-1 & -1 & -k+1 \\ n & n & -1(0) & 0 \end{matrix} \left[\begin{array}{cc|cc|cc} k & 1 & -k & -1 & -1 & k & 1 & k & 0 & -k-1 & 0 & k-1 \\ 2n & 0 & -1(0) & -1(0) & n-1(n) & n+1(n) & n & n & n-1(n) & -n-1(-n) & n & n \end{array}\right],$$

and

$$\begin{matrix} k & k-1 & -1 & -k+1 \\ n+1 & n & -1(0) & 0 \end{matrix} \left[\begin{array}{cc|cc|cc} k & 1 & -k & -1 & -1 & k & 1 & k & 0 & -k-1 & 0 & k-1 \\ 2n+1 & 1 & -1(0) & -1(0) & n-1(n) & n+1(n) & n+1 & n+1 & n(n+1) & -n-2(-n-1) & n & n \end{array}\right].$$

Notice that we consider four recurrence relations. This is to make sure that we do not divide by zero when we compute $W(k,2n)$ and $W(k,2n+1)$. Recall that we can compute the blocks described in section 6.1 in $O(log(x))$ steps where x denotes the input size. The indices appearing in the recurrences above and which are not contained in the block around (k,n) can be found in linear time as described in section 1.1. For the Double step (Figure 6.4) we already obtain 12 terms by varying k and n in the recurrences above. The unknown terms at the right side can be found in linear time by proposition 1.1. By using the same proposition, the three unknown terms at the left side can be found from the adjacent quadruple. This finishes the Double step.

	$W(k-1,2n+2)$	$W(k,2n+2)$	$W(k+1,2n+2)$	?
?	$W(k-1,2n+1)$	$W(k,2n+1)$	$W(k+1,2n+1)$	?
?	$W(k-1,2n)$	$W(k,2n)$	$W(k+1,2n)$	?
?	$W(k-1,2n-1)$	$W(k,2n-1)$	$W(k+1,2n-1)$	?

Figure 6.4: Square block around $(k, 2n)$.

For the Double and Add step we notice that we already have 9 terms (Figure 6.5). We also have the terms $W(k-1, 2n-1)$ and $W(k+1, 2n-1)$ at our disposal. Therefore we can find the three unknown terms at the left and right by proposition 1.2. Another application of proposition 1.2 yields the four terms at the top.

	?	?	?	?
?	$W(k-1,2n+2)$	$W(k,2n+2)$	$W(k+1,2n+2)$	?
?	$W(k-1,2n+1)$	$W(k,2n+1)$	$W(k+1,2n+1)$	?
?	$W(k-1,2n)$	$W(k,2n)$	$W(k+1,2n)$	?

Figure 6.5: Square block around $(k, 2n+1)$.

2.2 Initial S-block

Consider an elliptic curve E defined over a field K and points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on $E(K)$. Suppose that these points are appropriate cf. definition 1.1, chapter 3. We need to compute the square block around $(k, n) = (1, 1)$. So we start with a block with small indices which we already mostly know because the points are appropriate. Set $W = W_{E,P,Q}$. We obtain by theorems 2.5 (chapter 1), 2.7 (chapter 2) and the fact that

$$\begin{smallmatrix} 1 & 1 & -1 & 0 \\ 1 & 2 & 1 & -1 \end{smallmatrix} \left[\begin{smallmatrix} 2 & 0 & -1 & -1 \\ 2 & -1 & 0 & 1 \end{smallmatrix}\middle|\begin{smallmatrix} 0 & 2 & 1 & 1 \\ 2 & 1 & 0 & 1 \end{smallmatrix}\middle|\begin{smallmatrix} 0 & -2 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{smallmatrix}\right],$$

all terms of the initial block except some terms with supnorm three and one with supnorm two. We know the formula for $W_{E,P,Q}(1, 2)$ by theorem 2.7 (chapter 2). Use the transformation formula as in section 3 to find

$$W_{E,P,Q}(-1, 2) = -\frac{W_{E,-P,Q}(1, 2)}{(x_1 - x_2)^{-2}}.$$

Consider $([p, q, r, s] \leftarrow [(1, 2), (0, 1), (-1, 0), (0, 0)])$

$$W(1, 3) = \frac{(-W(-1, 1)W(1, 1)W(1, 2)W(1, 2) + W(0, 2)W(2, 2)W(0, 1)^2)}{(W(1, 1)W(-1, 0)^2)}.$$

We also obtain $W(-1, 3)$ and $W(3, 1)$ by the transformation formula. For the term $W(2, 3)$, use $([p, q, r, s] \leftarrow [(2, 3), (1, 1), (-1, 3), (0, -3)])$

$$W(2, 3) = \frac{(W(3, 1)W(1, 2)W(-1, 3) + W(1, 3)W(3, 0)W(1, -2))}{W(2, -2)W(2, 0)}, \tag{6.4}$$

or $([p, q, r, s] \leftarrow [(2, 3), (1, 0), (-1, 3), (0, -3)])$

$$W(2, 3) = \frac{(W(2, 1)W(2, 2)W(-1, 3) - W(1, 3)W(3, 0)W(0, 2))}{W(-1, 1)W(1, -2)W(2, 0)}. \tag{6.5}$$

Note that $W(1, -2)$ and $W(2, -2)$ cannot both be zero, therefore at least one of the equations (6.4) and (6.5) is defined. We also have that

$$W_{E,P,Q}(3, 3) = W_{E,P+Q}(3).$$

This follows from the transformation formula where

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

We find all the initial terms in this way.

2.3 Going to the right

We end up with a block centred at $(1, n)$. Simply change the role of k, n in section 2.1 to find the block centred at (k, n). This means that we consider the adjusted square block S_r as depicted below.

$W(0,n+2)$	$W(1,n+2)$	$W(2,n+2)$	$W(3,n+2)$
$W(0,n+1)$	$W(1,n+1)$	$W(2,n+1)$	$W(3,n+1)$
$W(0,n)$	$W(1,n)$	$W(2,n)$	$W(3,n)$
$W(0,n-1)$	$W(1,n-1)$	$W(2,n-1)$	$W(3,n-1)$
$W(0,n-2)$	$W(1,n-2)$	$W(2,n-2)$	

3 The algorithm

When moving up, we put the S-blocks in a 4×5 matrix with the understanding that the first entry is zero. When going right, we use the adjusted square blocks S_r which we put in a 5×4 matrix having last entry zero.

- Input: an elliptic curve E defined over K, points $P, Q \in E(K)$, nonnegative integers x and y.
- Output: The term $W_{E,P,Q}(x, y)$.

1. Compute the initial block as shown in section 2.2.
2. Compute the square block $S(1, B)$ centred at $(1, B)$ by a double and add algorithm as described in section 2.1.
3. After we have found the square block $S(1, B)$, we adjust this block to S_r as described in section 2.3.
4. Apply the double and add algorithm for the first coordinate starting with the adjusted block S_r found in the previous step.
5. Return $S_r[3, 2]$ which is equal to $W(x, y)$.

If x and y are both negative, then we apply the above algorithm to $-x$ and $-y$. Then $W(x, y)$ is equal to the (additive) inverse. For the other cases we employ the transforma-

tion formula for net polynomials (proposition 4.3)

$$\Psi_{v_1,v_2}(P,Q) = \frac{\Psi_{-v_1,v_2}(-P,Q)}{(-1)^{v_1^2-v_1v_2}\Psi_{-1,1}(-P,Q)^{v_1v_2}}$$
$$\Psi_{v_1,v_2}(P,Q) = \frac{\Psi_{v_1,-v_2}(P,-Q)}{(-1)^{v_2^2-v_1v_2}\Psi_{1,-1}(P,-Q)^{v_1v_2}}$$

The complexity of the algorithm is determined by step three and four. In step three we have a loop of lenght $\log_2(|y|)$. It takes at most $O(log_2(|y|))$ steps each time we pass the loop, because the most expensive calculations are done when we need to find the remaining terms for completing the square block. This is done by invoking proposition 1.1 a bounded (by a constant) number of times. The fourth step has the same complexity. We conclude that the algorithm is quadratic in the input size x.

4 Concluding remarks

We have presented an efficient algorithm for computing terms of a rank two elliptic net. This algorithm might be useful for several purposes. Division polynomials are important tools when studying elliptic curves. They provide a way to calculate multiples of points on elliptic curves (see the comments after lemma 2.4 in chapter 1). They also play a central role in Schoofs algorithm, which counts the number of points on elliptic curves defined over finite fields. We expect similar applications in higher rank, in particular rank two. One expects that linear combinations of points $P, Q \in E$ can be described in terms of net polynomials. Therefore we could improve on the arithmetic on elliptic curves by studying higher rank net polynomials. To our knowledge there is no such generalisation yet. Explicit examples of such an application are illustrated in propositions 1.3 (chapter 3) and 1.1.

We have seen in section 2.3 (chapter 5) that in a certain case the ECDLP boils down to the DLP in $\mathbb{F}_q^*$ using rank one elliptic nets. Let E be the curve defined over a finite field $\mathbb{F}_q$ and $Q = [k]P$ for a point $P \in E(\mathbb{F}_q)$ with order m. Lauter and Stange gave in [21], by using the periodicity property of a net (proposition 3.5, chapter 5), the equation

$$\left(\frac{W(m+1,0)W(2,0)}{W(m+2,0)}\right)^k = \left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)}\right)^m \left(-\frac{W(1,m)W(2,0)}{W(2,m)W(1,-1)^m}\right). \tag{6.6}$$

This equation is very much like equation (5.2) (chapter 5). If $m = q-1$ we obtain a DLP equation in $\mathbb{F}_q^*$. Note that equation (6.6) contains a term $W(2,m)$ which we now can compute efficiently. It is possible that more equations can be derived from the periodicity property resulting in other attacks of the ECDLP.

Another avenue could be the use of a perfectly periodic rank two elliptic net as it is given in proposition 3.10 (chapter 5):

$$\phi(v_1P_1 + v_2P_2) = W_{E,P_1,P_2}(v_1,v_2) \cdot \phi(P_1)^{v_1^2-v_1v_2} \cdot \phi(P_2)^{v_2^2-v_1v_2}\phi(P_1+P_2)^{v_1v_2}.$$

Recall that the formulation of the equivalences between the ECDLP and hard problems for elliptic divisibility sequences (see section 3 of chapter 5) were based on the construction of a perfectly periodic EDS denoted by $\phi([n]P)$. It is possible that, since there is an efficient algorithm for computing the terms of almost all rank two elliptic nets, we can select and employ a rank two perfectly periodic elliptic net to find other interesting connections with the ECDLP.

Summary

This is a thesis in the branch of mathematics which is called *algebraic geometry*. In the common understanding, geometry studies curves and surfaces and other objects which we can draw, while algebra is quite abstract and it deals with structures and operations. We study *elliptic curves*: they are curves in the plane (geometry) on which it is possible to sum points (algebra). Indeed, the sum of two points on an elliptic curve is still a point on the curve, whose coordinates are expressed by rational functions in the coordinates of the two points we are summing. We do not only consider the real numbers as possible coordinates, but also elements of other fields of arithmetic interest: this makes elliptic curves also a subject of *number theory*.

The most striking result in number theory that has been proven in the last decades is Fermat's Last Theorem: for every $n \geq 3$ the equation $x^n + y^n = z^n$ has no solutions in the non-zero integers (note, the case $n = 2$ has as solution the Pythagorean triples). And the proof is based on elliptic curves! A very rich theory for elliptic curves has been produced and is still growing. And yet another reason that makes these mathematical objects particularly interesting is their applications to *cryptography*.

Cryptography is what says that our passwords are secure, and it is always based on some computational problem that is lenghty for the computer to solve (as is, for example, factorizing large integers). One of the complicated problems we can use is about points on elliptic curves: if P, Q are given points on an elliptic curve (and if Q is a multiple of P) it is computationally hard to solve in n the equation $Q = nP$.

In this thesis, we focus on *elliptic nets*, which are functions that were recently introduced by Katherine Stange to generalise *elliptic divisibility sequences*. They are substantially related to the arithmetic of several points on an elliptic curve, while division polynomials were used to describe only one point. More precisely, division polynomials contain informations on the coordinates of the multiples of a point.

The main result in this thesis is producing an algorithm that lets us compute 'each term of (most) elliptic nets of rank 2'. Based on previous applications found by Stange, we consider research on elliptic nets necessary to ensure the security of cryptographic systems based on elliptic curves.

Appendix A

Sage code

Below is the Sage code for determining whether $W_{E,P,Q}(n,m)$ is zero or not. We make us of Stanges Pari/GP code (see `http://math.stanford.edu/~stange/scripts/tate_via_nets.gp`), adapt and expand it to compute the blocks mentioned in section 6.1.

```
def give_initialblock(EllipticCurve,point_a,point_b):

    #Given EllipticCurve in short Weierstrass form, so we only have a4 and a6.
    #We assume the points are on the curve and are appropriate
    #Output: starting block for the elliptic net, i.e. the block centred at 1
    #and creates the initial data

    initial_data=[0,0,0,0]
    V=matrix(2,8)

    #Set up the usual variable names for elliptic curves
    x1 = point_a[0]
    y1 = point_a[1]
    x2 = point_b[0]
    y2 = point_b[1]
    a4 = EllipticCurve.a4()
    a6 = EllipticCurve.a6()


    #Fill out the first vector of the initial_block
    V[0,3] = 1
    V[0,4] = 2*y1
    V[0,5] = 3*x1^4 + 6*a4*x1^2 + 12*a6*x1-a4^2
    V[0,6] = 4*y1*(x1^6 + 5*a4*x1^4 + 20*a6*x1^3 - 5*a4^2*x1^2- 4*a4*a6*x1 \
             - 8*a6^2 - a4^3)
    V[0,7] = -((V[0,5])^3 - (V[0,4])^3*(V[0,6]))
    V[0,2] = 0
    V[0,1] = - V[0,3]
    V[0,0] = - V[0,4]
```

```
    #Fill out the second vector of the initial_block
    V[1,0] = 1
    V[1,1] = 1
    V[1,2] = 2*x1+x2 - ((y2-y1)/(x2-x1))^2

    #Pre-compute the inverses
    initial_data[0] = 1/(2*y1)
    initial_data[1] = 1
    initial_data[2] = 1/(x1 - x2)
    initial_data[3] = 1/((y1+y2)^2 - (2*x1 + x2)*(x1-x2)^2)

    return V,initial_data


def double_or_add(V,initial_data,add):

    #Given a block V centred at k and the initial data
    #relevant to the elliptic net
    #Returns either a block centred at 2k or 2k+1
    #depending on whether "add" is 0 or 1


    doubleV=matrix(2,8)

    inverse_20 = initial_data[0]
    inverse_11 = initial_data[1]
    inverse_n1 = initial_data[2]
    inverse_2n = initial_data[3]


    #Fill out first vector of output block
    for j in range(-1,3): #j =-1,..,2
        i=j
        m=3 #index to middle of block


        doubleV[0,m + 2*i - add] = ((V[0,m+i])*(V[0,m+i+2])*(V[0,m+i-1])^2 \
                   -(V[0,m+i])*(V[0,m+i-2])*(V[0,m+i+1])^2)*inverse_20

        # when we hit j=-1, if add=1, calculate
        # W(2k+5,0) instead of W(2k-3,0)
        if i == -1 and add == 1:
            i=3

        doubleV[0,m + 2*i - 1 - add] = (V[0,m+i+1])*(V[0,m+i-1])^3  \
              - (V[0,m+i-2])*(V[0,m+i])^3 #deze zijn correct
```

```
    #Fill out second vector of output block
    m2=1
    m1=3

    if add==0 :
        doubleV[1,0] = ( V[1,m2+1]*V[1,m2-1]*V[0,m1-1]^2  \
                         - V[0,m1]*V[0,m1-2]*V[1,m2]^2 )*inverse_11

    doubleV[1,2-add-1] = ( V[1,m2-1]*V[1,m2+1]*V[0,m1]^2 \
                          - V[0,m1-1]*V[0,m1+1]*V[1,m2]^2)
    doubleV[1,3-add-1] = ( V[1,m2+1]*V[1,m2-1]*V[0,m1+1]^2 \
                         - V[0,m1]*V[0,m1+2]*V[1,m2]^2)*inverse_n1

    if add==1:
        doubleV[1,2] = ( V[0,m1+1]*V[0,m1+3]*V[1,m2]^2  \
                       - V[1,m2-1]*V[1,m2+1]*V[0,m1+2]^2)*inverse_2n


    return doubleV

def net_loop(EllipticCurve,point_a,point_b,m):
    #Given an EllipticCurve, two points on it an integer m >= 1.
    #Returns the block centred at m.

  E=EllipticCurve
  P=point_a
  Q=point_b

  V=give_initialblock(E,P,Q)[0]
  initial_data=give_initialblock(E,P,Q)[1]
  if m==1:
      return V
  else :
    #determine the number of steps in the double-and-add loop
    m_size=ceil(log(m+1)/log(2))

    #the variable storing the current block
    currentV=V

    #ignore the first "1" in the binary expansion of m
    m=m-2^(m_size-1)

    # step through the digits in the binary expansion of m
    for j in range(1,m_size): #j=1,...,m_size-1
        i = m_size - j #kludgy version of "down to"
```

```
        # determine if this is a double step or a
        # double-and-add step based on current digit
        # of m; set "add" accordingly
        if m - 2^(i-1) >= 0:
            add = 1
            m = m - 2^(i-1)
        else:
            add = 0




        # call the double or double-and-add function to
        # update the current block
        currentV = double_or_add(currentV, initial_data, add)

    return (currentV)

def hnet_loop_negative(EllipticCurve,point_a,point_b,n):

    #Given EllipticCurve, point_a ,point_b and an integer n < 0
    #Returns block centred at n, as in Figure 6.2 chapter 6


  if n>=0 :
      print "n is not negative!"
  else:
    nblock=matrix(2,8) #negative block

    E=EllipticCurve
    P= point_a
    Q= point_b

    pblock = net_loop(E,-P,Q,-n) #positive block


    #Fill out the first vectors of negative block using
    #the transformation formula, as given in section 3 chapter 6

    nblock[0,4]= pblock[0,3]*(-1)^((n)^2)
    nblock[0,3]= pblock[0,4]*(-1)^((n+1)^2)
    nblock[0,2]= pblock[0,5]*(-1)^((n+2)^2)
    nblock[0,1]= pblock[0,6]*(-1)^((n+3)^2)
    nblock[0,0]= pblock[0,7]*(-1)^((n+4)^2)
    nblock[0,7]= pblock[0,0]*(-1)^((n+5)^2)
    nblock[0,6]= pblock[0,1]*(-1)^((n+6)^2)
    nblock[0,5]= pblock[0,2]*(-1)^((n+7)^2)
```

```
    #Fill out the second vectors of negative block using transformation formula

    d= 1/(P[0]-Q[0])
    nblock[1,0]=pblock[1,2]*d^(n-1)
    nblock[1,1]=pblock[1,1]*d^(n)
    nblock[1,2]=pblock[1,0]*d^(n+1)

    return nblock

def vnet_loop_positive(EllipticCurve,point_a,point_b,m):
    #Given EllipticCurve, P=point_a,Q=point_b and m >= 1
    #Returns the vertical block:
    #W_{P,Q}(0,m-3),W(0,m-2),W(0,m-1),W(0,m),W(0,m+1),W(0,m+2),W(0,m+3),W(0,m+4)
    #W(1,m-1),W(1,m),W(1,m+1)

    #Because of the transformation formula we have W_P,Q(n,m)=W_Q,P(m,n),
    #therefore we just need to change the role of P and Q

    E=EllipticCurve
    P=point_a
    Q=point_b
    #interchange role of P and Q
    vblock= net_loop(E,Q,P,m)
    return vblock



def vnet_loop_negative(EllipticCurve,point_a,point_b,m):
    #Given EllipticCurve, P=point_a,Q=point_b and m =< -1
    #returns negative vertical block centered at m:
    #W_{P,Q}(0,m+3),W(0,m+2),W(0,m+1),W(0,m),W(0,m-1),W(0,m-2),W(0,m-3),W(0,m-4)
    #W(1,m+1),W(1,m),W(1,m-1)

    E=EllipticCurve
    P=point_a
    Q=point_b


    #Because of the transformation formula, we need the block in the
    #positive vertical direction, with base P,-Q

    pblock= vnet_loop_positive(E,P,-Q,-m)

    x1=P[0]
    x2=Q[0]
```

```
    nblock=matrix(2,8) #negative block

    #Fill first vectors of negative block

    nblock[0,4]= pblock[0,3]*(-1)^(m^2) #W_P,Q(0,m)=W_P,-Q(0,-m)*...
    nblock[0,3]= pblock[0,4]*(-1)^((m+1)^2) #W_P,Q(0,m-1)=W_P,-Q(0,-m+1)*...
    nblock[0,2]= pblock[0,5]*(-1)^(m^2)
    nblock[0,1]= pblock[0,6]*(-1)^((m+1)^2)
    nblock[0,0]= pblock[0,7]*(-1)^(m^2)

    nblock[0,5]= pblock[0,2]*(-1)^((m+1)^2) #W_P,Q(0,m+1)=W_P,-Q(0,-m-1)*...
    nblock[0,6]= pblock[0,1]*(-1)^((m)^2)
    nblock[0,7]= pblock[0,0]*(-1)^((m+1)^2) #W_P,Q(0,m+3)=W_P,-Q(0,-m-3)*....

    #Fill out the second vectors of negative block using transformation formula
    d= 1/(x2-x1)
    nblock[1,0]=pblock[1,2]*d^(m-1) #W_P,Q(1,m-1)=W_P,-Q(1,-m+1)
    nblock[1,1]=pblock[1,1]*d^(m)   #W_P,Q(1,m)=W_P,-Q(1,-m)
    nblock[1,2]=pblock[1,0]*d^(m+1) #W_P,Q(1,m+1)=W_P,-Q(1,-m-1)
    return nblock


def ellipticnet_isZero(EllipticCurve,point_a,point_b,n,m,char):

    #Function to determine whether W(n,m) is zero or not
    #Condition: n*m is not zero, else we just work with EDS
    #for which a wealth of Sage code is available
    #(see http://math.stanford.edu/~stange/scripts/edstools.sage)

    #Given EllipticCurve and points point_a, point_b which
    #determine the rank two elliptic net W
    #EllipticCurve is an elliptic curve defined over a field K and char
    #denotes the characteristic of this field
    #Return: true if W(n,m) is zero, else it returns false

    E=EllipticCurve
    P=point_a
    Q=point_b

    hblock=matrix(2,8)
    if n>0:
        hblock=net_loop(E,P,Q,n)
    else: #n<0
        hblock=hnet_loop_negative(E,P,Q,n)
    h=hblock

    v1=matrix(2,8)# vertical block around m
```

```
v2=matrix(2,8)# vertical block around -m

if m>0:
    v1=vnet_loop_positive(E,P,Q,m)
    v2=vnet_loop_negative(E,P,Q,-m)
else:
    v1=vnet_loop_negative(E,P,Q,m)
    v2=vnet_loop_positive(E,P,Q,-m)


#We need the quantities
#A=W(n,m)W(n,-m)
#B=W(n,m)*W(n,-m+1)
#Therefore we distinguish between four cases
if n>0 and m>0:      #case 1


  A=h[0,4]*v1[0,3]^2*h[0,2] + h[0,3]^2*v1[1,1]*v2[1,1]
  B=h[1,2]*v1[0,3]*v1[0,2]*h[0,2]+h[1,1]*v1[1,1]*v2[1,2]*h[0,3]


elif n>0 and m <0:   #case 2

  A= h[0,4]*h[0,2]*v1[0,4]^2 + h[0,3]^2*v1[1,1]*v2[1,1]
  B=h[1,2]*v1[0,3]*v1[0,4]*h[0,2] + h[1,1]*v1[1,1]*v2[1,2]*h[0,3]


elif  n<0 and m >0:  # case 3

  A=h[0,5]*v1[0,3]^2*h[0,3] + h[0,4]^2*v1[1,1]*v2[1,1]

  B=h[1,2]*v1[0,3]*v1[0,2]*h[0,3] + h[1,1]*v1[1,1]*v2[1,2]*h[0,4]



else :              # case 4 n<0 and m<0

  A=h[0,5]*v1[0,4]^2*h[0,3] + h[0,4]^2*v1[1,1]*v2[1,1]

  B=h[1,2]*v1[0,3]*v1[0,4]*h[0,3] + h[1,1]*v1[1,1]*v2[1,2]*h[0,4]

if A%char==0 and B%char==0:
    print "The term W("+str(n)+","+str(m)+") is zero."
else:
    print "The term W("+str(n)+","+str(m)+") is NOT zero."
```

Bibliography

[1] E. Bach and J. Shallit. *Algorithmic number theory, Efficient algorithms.* Foundations of computer series, vol. 1. MIT Press, Cambridge (1996).

[2] P.S.L.M. Barreto, S. D. Galbraith, C. ÓhÉigeartaigh, and M. Scott. *Efficient pairing computation on supersingular abelian varieties.* Designs, Codes and Cryptography, Vol. 42, No. 3, pp. 239271, Springer, 2007.

[3] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Advances in Elliptic Curve Cryptography.* Cambridge University Press, Cambridge, UK, 2005.

[4] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, Cambridge, UK, 1999.

[5] R. Balasubramian and N. Koblitz. *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm.* J. Cryptology, **11**, 141-145, 1998.

[6] J. Cheon and D. Lee. *Diffie-hellman problems and bilinear maps.* Cryptology ePrint Archive: Report 2002, 2002.

[7] K. Chandrasekharan. *Elliptic functions.* volume 281 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1986.

[8] L.S. Charlap and D.P. Robbins. *An elementary introduction to elliptic curves.* Technical Report 31, Institute for Defense Analysis, Princeton, December 1988.

[9] I. Duursma and H.S. Lee. *Tate Pairing Implementation for Hyperelliptic Curves* $y^2 = x^p - x + d$. Advances in Cryptology-ASIACRYPT 2003, LNCS 2894, pp. 111-123, Springer-Verlag, 2003.

[10] W. Diffie and M.E. Hellman. *New directions in cryptography.* IEEE Trans. Information Theory, IT-22(6):644-654, 1976.

[11] M. Einsiedler, G. Everest, and T. Ward. *Primes in elliptic divisibility sequences.* LMS J. Comput. Math., 4:113 (electronic), 2001.

[12] Andreas Enge. *Elliptic curves and their applications to cryptography.* Kluwer Academic Publishers, Boston, Second Printing, 1999.

[13] David Eisenbud and Joe Harris. *The geometry of schemes.* Springer-Verlag, New York, 1999.

[14] Graham Everest, Alf van der Poorten, Igor Shparlinski and Thomas Ward. *Recurrence Sequences.* American Mathematical Society ,2003, pp. 163-174.

[15] G. Frey and H.-G. Ruck. *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves.* Math. Comp., **62**, 865874, 1994.

[16] G. Frey, M. Müller, and H.-G. Rück. *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems.* IEEE Trans. Inform. Theory, 45(5):1717-1719, 1999.

[17] Darrel Hankerson, Alfred J. Menezes and Scott Vanstone. *Guide to elliptic curve cryptography.* Springer-Verlag, New York, 2004.

[18] F. Hess. *A note on the Tate pairing of curves over finite fields.* Arch. Math. **82**, 28-32, 2004.

[19] F. Hess, N.P. Smart, and F. Vercauteren. *The Eta pairing revisited.* IEEE Transaction on Information Theory, Vol. 52, No. 10, pp. 4595-4602, 2006.

[20] T. Itoh and S. Tsujii. *An efficient algorithm for deciding quadratic residuosity in finite fields GF(p^m).* Inform. Process. Lett. 30, 111-114 (1989).

[21] Kristin E. Lauter and Katherine E. Stange. *The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences.* Selected Areas in Cryptography,pages 309-327. 15th Annual International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, 2008.

[22] E. Lee, H.S. Lee, and C. M. Park. *Efficient and generalized pairing computation on abelian varieties.* IEEE Transactions on Information Theory, Vol. 55, No. 4, pp. 1793-1803, 2009.

[23] Alfred Menezes. *An introduction to Pairing-Based Cryptography.* Notes from lectures given in 2005. Available from `http://cacr.uwaterloo.ca/~ajmeneze/publications/pairings.pdf`.

[24] A.J. Menezes, T. Okamoto and S.A. Vanstone. *Reducing elliptic curve logarithms to a finite field.* IEEE Trans. Inf. Theory, **39**, 1639-1646, 1993.

[25] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. *Handbook of applied cryptography.* CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL,1997. With A foreword by R.L. Rivest.

[26] Victor S. Miller. *Short programs for functions on curves.* IBM Thomas J. Watson Research Center, 1986.

[27] Naoki Ogura, Naoki Kanayama, Shigenori Uchiyama, and Eiji Okamoto *Cryptographic Pairings Based on Elliptic Nets.* IACR Eprint archive, 2010.

[28] S. Pohlig and M. Hellman. *An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance.* IEEE Transactions on Information Theory 24, pp. 106-110, 1978.

[29] B. Poonen. *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers.* In Algorithmic number theory (Sydney, 2002), volume 2369 of Lecture Notes in Comput. Sci., pages 33-42. Springer, Berlin, 2002.

[30] Rachel Shipsey. *Elliptic Divisibility Sequences.* PhD thesis, Goldsmiths, University of London, 2001.

[31] Rachel Shipsey and Christine Swart. *Elliptic divisibility sequences and the elliptic curve discrete logarithm problem.* Cryptology ePrint Archive, 2008. Available from `http://eprint.iacr.org/2008/444.pdf`.

[32] Christine Swart. *Elliptic curves and related sequences.* Phd thesis, Royal Holloway and Bedford New College, University of London, 2003.

[33] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[34] Joseph H. Silverman. *Wieferich's criterion and the abc-conjecture.* J. Number Theory, 30(2): 226-237, 1988.

[35] Katherine Stange. *Elliptic nets and elliptic curves.* Algebra and Number Theory, 5(2): 197-229, 2011.

[36] K.E. Stange. *The Tate pairing via elliptic nets.* Pairing Conference 2007, LNCS 4575, pp.329-348, 2007.

[37] Katherine E. Stange. *Elliptic nets and elliptic curves.* Phd thesis, Brown University (May 2008).

[38] G. Taylor. *Stange's algorithm for elliptic nets.* Available from `http://aleph.straylight.co.uk/ellnet.pdf`

[39] F. Vercauteren. *Optimal pairings.* IEEE Transactions on Information Theory, Vol. 56, No. 1, pp. 455-461, 2010.

[40] Lawrence C. Washington. *Elliptic curves: number theory and cryptography.* Chapman & Hall/CRC, Boca Raton, 2003.

[41] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31-74, 1948.

[42] C.-A. Zhao, F. Zhang and J. Huang. *A note on the Ate pairing.* International Journal of Information Security, Vol. 6, No. 7, pp. 379-382, 2008.