

ELLIPTIC NETS AND ELLIPTIC CURVES

KATHERINE E. STANGE

ABSTRACT. An elliptic divisibility sequence is an integer recurrence sequence associated to an elliptic curve over the rationals together with a rational point on that curve. In this paper we present a higher-dimensional analogue over arbitrary base fields. Suppose E is an elliptic curve over a field K , and P_1, \dots, P_n are points on E defined over K . To this information we associate an n -dimensional array of values in K satisfying a nonlinear recurrence relation. Arrays satisfying this relation are called *elliptic nets*. We demonstrate an explicit bijection between the set of elliptic nets and the set of elliptic curves with specified points. We also obtain Laurentness/integrality results for elliptic nets.

CONTENTS

Introduction	2
1. Elliptic nets	4
2. Laurentness and integrality	5
3. Net polynomials over \mathbb{C}	15
4. Net polynomials over arbitrary fields	20
5. Elliptic nets from elliptic curves	24
6. Elliptic curves from elliptic nets	26
7. The curve-net theorem	30
References	33

Date: April 1, 2010.

1991 Mathematics Subject Classification. Primary 11G05, 11G07, 11B37, Secondary 11B39, 14H52.

Key words and phrases. elliptic curve, elliptic divisibility sequence, recurrence sequence.

This work was supported by NSERC Awards PGS D2 331379 and PDF 373333.

INTRODUCTION

An *elliptic divisibility sequence* is an integer sequence W_n satisfying

$$(1) \quad W_{n+m}W_{n-m} = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2.$$

This definition was introduced by Morgan Ward in 1948 [26]. Let $\Psi_n(x, y)$ denote the n -th division polynomial associated to an elliptic curve (the n -th division polynomial vanishes at the n torsion points). Ward showed that division polynomials satisfy the recurrence (1) and furthermore that all elliptic divisibility sequences have the form

$$W_n = \lambda^{n^2-1}\Psi_n(x, y)$$

for some constant λ , elliptic curve (or singular cubic) and point $P = (x, y)$ on the curve. This rich structure has led to number theoretic results [1, 6, 13, 18, 19, 23]; applications to Hilbert's 10th problem [4, 5, 15]; to integrable systems [12]; and to cryptography [3, 17, 21]. For a bibliography, see [8, Chapter 10].

There have been several attempts to generalise this theory. Van der Poorten and Swart study *translated elliptic divisibility sequences* [23, 24, 25]. Mazur and Tate generalise division polynomials to arbitrary endomorphisms in the p -adic setting [14], and Streng uses their definition to generalise to the endomorphism ring of an elliptic curve with complex multiplication [22]. Elliptic divisibility sequences are closely related to the denominators of the multiples $[n]P$ of a fixed point P ; questions have been asked about the collection of denominators of the linear combinations $[n]P + [m]Q$ by Everest, Miller and Stephens [7]. The hope of defining 'higher rank' elliptic divisibility sequences via a recurrence relation was discussed in correspondence by Elkies, Propp and Somos [16].

The primary purpose of this paper is to generalise from integer sequences to multi-dimensional arrays with values in any field, which we call *elliptic nets*. A substantial part of the difficulty lies in finding the correct recurrence and defining a generalised division polynomial.

We define an *elliptic net* to be a function $W : A \rightarrow R$ from a finite rank free abelian group A to an integral domain R satisfying the properties that $W(0) = 0$ and that

$$(2) \quad \begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &+ W(q+r+s)W(q-r)W(p+s)W(p) \\ &+ W(r+p+s)W(r-p)W(q+s)W(q) = 0 \end{aligned}$$

for all $p, q, r, s \in A$. If $A = R = \mathbb{Z}$, this is an equivalent definition of an elliptic divisibility sequence (this is not immediately obvious, but it is a consequence of results in this paper). By the *rank* of an elliptic net we shall mean the rank of A . Section 1 covers the basic definitions and gives examples.

Our primary interest is the relationship between elliptic curves and elliptic nets.

Theorem (Main Theorem - Introductory Version). *For each field K and integer n , there is an explicit bijection of sets*

$$\left\{ \begin{array}{l} \text{scale equivalence classes} \\ \text{of non-degenerate elliptic} \\ \text{nets } W : \mathbb{Z}^n \rightarrow K \end{array} \right\}$$

$$\updownarrow$$

$$\left\{ \begin{array}{l} \text{tuples } (C, P_1, \dots, P_n) \text{ where } C \text{ is a cubic} \\ \text{curve in Weierstrass form defined over } K, \\ \text{considered modulo unihomothetic changes} \\ \text{of variables, and such that } \{P_i\} \in C_{ns}(K)^n \\ \text{is appropriate} \end{array} \right\}$$

For a description of the relevant terminology, see Sections 5 (appropriate), 6.1 (scale equivalent, non-degenerate) and 7.1 (unihomothetic). See Theorem 7.4 for a more detailed statement. The isomorphism itself is described explicitly in Definition 5.1 (depending on Theorem 4.6) and Theorem 6.7. For ranks 1 and 2, explicit formulæ can be found in Propositions 3.8, 6.3 and 6.4. For an example, see Figure 1.

The other main aspect of elliptic nets studied in this paper is Laurentness. These results are needed for the proof of the main theorem, but are of independent interest. One property of elliptic divisibility sequences of particular interest is that they are integer sequences: if the sequence begins $1, a, b, ac, \dots$ ($a, b, c \in \mathbb{Z}$), then it will consist entirely of integers [26]. This result has been studied in the more general framework of the ‘Laurent phenomenon’ of Fomin and Zelevinsky [9].

Laurentness results are found in Section 2, which is devoted to the inductive structure of elliptic nets: how some terms are determined by others via the recurrence relation. We define a universal ring \mathcal{W}_A for elliptic nets on A , such that elliptic nets $W : A \rightarrow R$ are in bijection with homomorphisms $\mathcal{W}_A \rightarrow R$. We obtain results on the structure of this ring, and in turn, these imply integrality results. See Theorems 2.2

($n = 1$), 2.5 ($n = 2$) and 2.8 ($n \geq 3$). The proofs in this section are elementary but somewhat tedious.

Sections 3 and 4 define the higher rank generalisation of division polynomials called *net polynomials*: rational functions on the n -fold product E^n of an elliptic curve E , which vanish on tuples (P_1, \dots, P_n) satisfying a linear relation $[v_1]P_1 + \dots + [v_n]P_n = \mathcal{O}$ for fixed coefficients v_i . In Section 3, we work with the complex uniformization of an elliptic curve defined over \mathbb{C} . Section 4 generalises the definition to arbitrary fields by analysing the arithmetic properties of net polynomials. The main result here is Theorem 4.4.

The last three sections describe the bijection in the main theorem. Section 5 makes explicit the production of an elliptic net from any cubic Weierstrass curve using the net polynomials. Section 6 determines exactly those cubic curves which produce a given elliptic net. Finally, Section 7 puts together the results of the previous sections to prove the main theorem, stated in its full form as Theorem 7.4.

Computer software. The explicit isomorphism described in this paper has been implemented for Pari/GP in ranks 1 and 2. Scripts are available at <http://math.katestange.net>.

Acknowledgements. I would like to thank my thesis advisor, Joseph Silverman, for many patient hours. I would also like to thank Rafe Jones, Alf van der Poorten, and Jonathan Wise.

1. ELLIPTIC NETS

The following definition is the subject of the paper.

Definition 1.1. Let A be a free finitely-generated abelian group, and R be an integral domain. An *elliptic net* is any map $W : A \rightarrow R$ with

$$(3) \quad W(0) = 0,$$

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

$$(4) \quad \begin{aligned} &W(p + q + s)W(p - q)W(r + s)W(r) \\ &\quad + W(q + r + s)W(q - r)W(p + s)W(p) \\ &\quad + W(r + p + s)W(r - p)W(q + s)W(q) = 0. \end{aligned}$$

Functions $W : A \rightarrow R$ which satisfy (4) but not (3) can only appear in characteristic 3 (to see this, take $p = q = r = s = 0$ in (4)). Any constant function in characteristic 3 is an example. By definition, these are not elliptic nets.

We refer to the rank of A as the *rank* of the elliptic net. Suppose that $B \subset A$ is a subgroup of A . Then the restriction to B of an elliptic net $W : A \rightarrow R$ is also an elliptic net. We refer to this elliptic net as *the subnet associated to B* and write $W|_B : B \rightarrow R$.

Example 1.2. Let R be an integral domain. The following are elliptic nets.

- (1) The *zero net* $W : \mathbb{Z}^n \rightarrow R$ defined by $W(\mathbf{v}) = 0$ for all \mathbf{v} .
- (2) The identity map $W_{id} : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $W(v) = v$.
- (3) Let $W' : \mathbb{Z} \rightarrow R$ be an elliptic net. Then for each $1 \leq i \leq n$, we may define $W_i : \mathbb{Z}^n \rightarrow R$ by $W_i(v_1, \dots, v_n) = W'(v_i)$, and this will also be an elliptic net.
- (4) More generally, if $W : A \rightarrow R$ is an elliptic net and $f : B \rightarrow A$ is a homomorphism of finitely generated free abelian groups, then $W \circ f : B \rightarrow R$ is also an elliptic net.
- (5) If $W : A \rightarrow R$ is an elliptic net and $g : R \rightarrow S$ is a homomorphism of integral domains, then $g \circ W : A \rightarrow S$ is also an elliptic net.
- (6) $W_{Leg} : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $W(v) = \left(\frac{v}{3}\right)$, the Legendre symbol of v over 3. This can be verified by a finite examination of cases; observe that at least one of $p, q, r, p - q, q - r$, and $r - p$ is divisible by 3. See also [26, p. 31].
- (7) $W_{Fib} : \mathbb{Z} \rightarrow \mathbb{Z}$ given by

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

where F_{2v} is the $2v$ -th Fibonacci number. One may verify this example using the closed form for terms of the Fibonacci sequence. See also [26, p. 31].

- (8) Figure 1 shows a portion of an elliptic net of rank 2 displayed as an array. The origin is located at the term ‘0’. This elliptic net arises from a certain curve and two points as described in Section 5, Example 5.3. Each axis forms an elliptic divisibility sequence, e.g. $0, 1, 1, -3, 11, 38, 249, \dots$

2. LAURENTNESS AND INTEGRALITY

In this section we ask which terms of an elliptic net determine the others via the recurrence relation. In the case of $n = 1$, Ward showed that the terms $W(1), \dots, W(4)$ sufficed to determine the rest of the net (unless too many of these terms were zero) [26]. Our method also

FIGURE 1. Elliptic net associated to $y^2 + y = x^3 + x^2 - 2x$,
 $P = (0, 0)$, $Q = (1, 0)$ over \mathbb{Q} (origin is at '0')

3269	-2869	4335	5959	12016	-55287	23921	1587077	-7159461
-127	-299	94	479	919	-2591	13751	68428	424345
-44	-27	-31	53	-33	-350	493	6627	48191
-1	-7	-5	8	-19	-41	-151	989	-1466
3	-2	1	3	-1	-13	-36	181	-1535
1	-1	1	1	2	-5	7	89	-149
-1	-1	0	1	1	-3	11	38	249
↑ -2	-1	-1	1	-1	-4	1	47	185
Q 1	-3	-1	2	-3	-5	-17	63	-184
P →								

demonstrates Laurentness and integrality results. The main theorems of this section are used in Section 6.

2.1. Laurentness. Let I be a group, in additive notation, called the *indexing group*, whose elements are called *indices*. To each $i \in I$, we associate the symbol T_i . In what follows, the indexing group will be $I \cong \mathbb{Z}^n$ for some n .

Consider the ideal \mathcal{M} in the ring $\mathbb{Z}[T_i]_{i \in I}$ generated by T_0 and all polynomials

$$(5) \quad T_{p+q+s}T_{p-q}T_{r+s}T_r + T_{q+r+s}T_{q-r}T_{p+s}T_p + T_{r+p+s}T_{r-p}T_{q+s}T_q$$

(of the form (4)) as p, q, r, s range over I . Polynomials of the form (5) will be called *recurrence relations*. Consider the ring \mathcal{W}_I obtained from $\mathbb{Z}[T_i]_{i \in I}/\mathcal{M}$ as a quotient by its own nilradical. For each integral domain R , there is a bijection between elliptic nets $W : I \rightarrow R$ and homomorphisms $\mathcal{W}_I \rightarrow R$ (defined by taking $T_i \mapsto W(i)$).

Taking $p = q = i, r = s = 0$ shows that $T_i^3(T_i + T_{-i}) \in \mathcal{M}$ for each $i \in I$. In particular, $T_{-i}^3(T_i + T_{-i}) \in \mathcal{M}$ also. Therefore, any prime ideal containing \mathcal{M} contains $T_i + T_{-i}$; for if it did not, then it must contain T_i and T_{-i} , a contradiction. Therefore $T_{-i} = -T_i$ in \mathcal{W}_I . This implies the following.

Proposition 2.1. *Let $W : A \rightarrow R$ be an elliptic net. Then $W(-z) = -W(z)$ for all $z \in A$.*

The purpose of this section is to find a finite subset $0 \notin J \subset I$ such that the localisation $\mathcal{W}_I[T_i^{-1}]_{i \in J}$ is finitely generated as a \mathbb{Z} -algebra, and to give the generators. (The localisation is not the trivial ring ($1 = 0$) by the existence of a homomorphism from it to \mathbb{Q} given by Example 1.2, where one uses part (3) with $W' = W_{id}$ of part (2).) From

this we show that every T_i can be expressed as a Laurent polynomial in integer coefficients in a finite number of terms T_j . This implies that any elliptic net which does not take zero values at the T_j is entirely determined by those values.

To illustrate, consider the rank one case, which is essentially a result of Morgan Ward.

Theorem 2.2 (Ward, [26, Theorem 4.1]). *The ring $\mathcal{W}_{\mathbb{Z}}[T_1^{-1}, T_2^{-1}]$ is generated as a \mathbb{Z} -algebra by the six elements*

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

Furthermore, each T_i is expressible as a \mathbb{Z} -coefficient polynomial in

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

In particular, let $W : \mathbb{Z} \rightarrow \mathbb{Q}$ be an elliptic net. If $W(1) = 1$, $W(2) \neq 0$, $W(i)$ is an integer for $i = 2, 3, 4$, and $W(2)$ divides $W(4)$, then the elliptic net consists entirely of integers.

Proof. See [26], Theorem 4.1. Recall that $T_{-n} = -T_n$, so it suffices to prove the first two statements for positive n . Taking $(p, q, r, s) = (n+1, n, 1, 0)$ and $(n+1, n-1, 1, 0)$ respectively, in \mathcal{W}_I we have

$$(6) \quad T_{2n+1}T_1^3 + T_{n-1}T_{n+1}^3 + T_{n+2}T_{-n}T_n^2 = 0,$$

$$(7) \quad T_{2n}T_2T_1^2 + T_nT_{n-2}T_{n+1}^2 + T_{n+2}T_{-n}T_{n-1}^2 = 0.$$

The equations (6) and (7) prove the first statement by induction. The base case consists of $0 \leq n \leq 4$; for $n > 4$, we have $2n > n+2$.

For even i , it can be shown by induction on (7) that T_i is expressible as a \mathbb{Z} -coefficient polynomial in $T_1, T_1^{-1}, T_2, T_2^{-1}, T_3$, and T_4 in such a way that the combined degree of T_2 and T_4 in each monomial is positive. For $i = 2, 4$ this is clear. To complete the induction in general, observe that in (7), each of the rightmost two terms is divisible by at least two T_k where k is even and $k < 2n$.

For even i , the second statement of the theorem concerning the expressibility of all T_i in terms of T_1, T_1^{-1}, T_2, T_3 and $T_4 T_2^{-1}$ follows from the observation of the previous paragraph. The statement also holds for $i = 1, 3$. Consequently, it holds for odd i by induction on (6). \square

2.2. Proofs by induction. The inductive proofs in this section will be based on the following definitions. Consider finite sets $S, J \subset I$ where $0, i \notin S \cup J$. We say that an index $i \in I$ is *S-integrally implied by J* if there exists a \mathbb{Z} -coefficient monomial $P(T_s)$ (in variables indexed

by S) and \mathbb{Z} -coefficient polynomial $Q(T_j)$ (in variables indexed by J) such that

$$(8) \quad T_i P(T_s) = Q(T_j)$$

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

As an example (see Proposition 2.1 and the paragraph which precedes it), $-i$ is S -integrally implied by any J containing i (for any S). In what follows, this fact will often be used tacitly.

A set $B \subset I$ is an S -integral baseset for \mathcal{W}_I if all of I is S -integrally implied by B . If $B \subset I$ is an S -integral baseset, then each T_i can be expressed as a polynomial with integer coefficients in the set of variables $\{T_b\}_{b \in B} \cup \{T_s^{-1}\}_{s \in S}$ (when considered in the appropriate localisation).

It is straightforward to verify 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' . To show that B is an S -integral baseset for I , the proofs in this section show the following: for each index $i \in I$, there is a finite sequence $J_0 \subset J_1 \subset \dots \subset J_n$ such that $B = J_0$, $i \in J_n$ and for each $1 \leq k \leq n$, J_k is S -integrally implied by J_{k-1} . At each stage, we show that each index of J_i is S -integrally implied by J_{i-1} . Recall that implication is simply the existence of an relation of the form (8), and in fact we simply give a relevant element of the form (5).

These elements are cumbersome to write out. For example, taking in the case $n = 3$,

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

we obtain the element

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

For this information, let us instead use a more convenient notation

$$(9) \quad \begin{array}{ccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array} \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 \end{array} \right].$$

In this notation, the columns to the left of the square braces correspond to the columns of p , q , r and s , while the indices of the terms of the recurrence appear as the columns within the square braces.

To demonstrate that an index i is (S -integrally) implied by a set of indices J , it suffices to write down an appropriate such array. Notice

that any array of the form (9) is a recurrence if each row is a recurrence. Therefore we may construct examples row-by-row.

The following definition will be useful for ordering inductions.

Definition 2.3. Let

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

be the *sup-norm* of the vector \mathbf{v} .

2.3. Basesets for rank 2. For the rank two case, we require a lemma.

Lemma 2.4. *The ring $\mathcal{W}_{\mathbb{Z}^2}[T_{(1,0)}^{-1}, T_{(0,1)}^{-1}, T_{(1,1)}^{-1}]$ is generated as a \mathbb{Z} -algebra by the elements*

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

Proof. Let $S = \{(1, 0), (0, 1), (1, 1)\}$ and $B = \{\mathbf{v} \in \mathbb{Z}^2 : N(\mathbf{v}) \leq 4\}$. This proof proceeds by induction on the sup-norm. Trivially, any \mathbf{v} with $N(\mathbf{v}) \leq 4$ is S -integrally implied by B . Let $N_0 > 4$ and suppose that all terms with indices with sup-norm less than N_0 are S -integrally implied by B . Call the set of such indices K_{N_0} . Suppose \mathbf{v} is an index of sup-norm N_0 . We construct a recurrence demonstrating that \mathbf{v} is S -integrally implied by K_{N_0} row-by-row. For $i = 1, 2$, define $w_i = \lceil \frac{v_i}{2} \rceil$.

Case I: \mathbf{v} has one odd entry and one even entry. For the odd entry, we use the row

$$w_i \ w_{i-1} \ 0 \ 0 \ [\ 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} \]$$

For the even entry, we use the row

$$w_i \ w_i \ 1 \ 0 \ [\ v_i \ 0 \ 1 \ 1 \ | \ w_{i+1} \ w_{i-1} \ w_i \ w_i \ | \ w_{i+1} \ -w_{i+1} \ w_i \ w_i \]$$

Case II: \mathbf{v} has two odd entries. Use the rows

$$\begin{array}{c} w_1 \ w_{1-1} \ 0 \ 0 \ [\ v_1 \ 1 \ 0 \ 0 \ | \ w_{1-1} \ w_{1-1} \ w_1 \ w_1 \ | \ w_1 \ \ -w_1 \ w_{1-1} \ w_{1-1} \] \\ w_2 \ w_{2-1} \ 1 \ 0 \ [\ v_2 \ 1 \ 1 \ 1 \ | \ w_2 \ w_{2-2} \ w_2 \ w_2 \ | \ w_{2+1} \ -w_{2+1} \ w_{2-1} \ w_{2-1} \] \end{array}$$

Case III: \mathbf{v} has two even entries. Use the rows

$$\begin{array}{c} w_1 \ w_{1-1} \ 0 \ 1 \ [\ v_1 \ 1 \ 1 \ 0 \ | \ w_1 \ w_{1-1} \ w_{1+1} \ w_1 \ | \ w_{1+1} \ \ -w_1 \ w_1 \ w_{1-1} \] \\ w_2 \ w_2 \ 1 \ 0 \ [\ v_2 \ 0 \ 1 \ 1 \ | \ w_{2+1} \ w_{2-1} \ w_2 \ w_2 \ | \ w_{2+1} \ -w_{2+1} \ w_2 \ w_2 \] \end{array}$$

For even v_i , either $|v_i| \leq 2$ or $|v_i| > 3$. In the former case, $|w_i| + 1 \leq 2 < N_0$. In the latter case, we have $|w_i| + 1 \leq (|v_i| + 2)/2 < |v_i| \leq N_0$. For odd v_i , either $|v_i| \leq 3$ or $|v_i| > 4$. In the former case $|w_i| + 2 \leq 4 < N_0$. In the latter case, we have $|w_i| + 2 \leq (|v_i| + 5)/2 < |v_i| \leq N_0$.

Therefore all the vectors in the recurrence have sup-norm less than N_0 with the exception of \mathbf{v} . In the monomial of \mathbf{v} in the recurrence, the other indices are $(1, 0)$, $(0, 1)$ or $(1, 1)$. This demonstrates that \mathbf{v} is S -integrally implied by K_{N_0} and hence by B . \square

Theorem 2.5. *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 eleven elements*

$$T_{(1,1)}, T_{(1,0)}, T_{(0,1)}, T_{(1,1)}^{-1}, T_{(1,0)}^{-1}, T_{(0,1)}^{-1}, \\ T_{(2,1)}, T_{(1,2)}, T_{(2,0)}, T_{(0,2)}, T_{(2,2)},$$

and the following identities hold:

$$T_{(1,-1)}T_{(1,1)}^3 = T_{(1,0)}^3T_{(1,2)} - T_{(0,1)}^3T_{(2,1)}, \\ T_{(2,2)}T_{(1,-1)}T_{(1,0)}T_{(0,1)} = T_{(1,1)}(T_{(0,2)}T_{(2,1)}T_{(1,0)} - T_{(0,1)}T_{(2,0)}T_{(1,2)}).$$

In particular, if $W : \mathbb{Z}^2 \rightarrow \mathbb{Q}$ is 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. The first and second stated identities are the recurrences

$$(10) \quad \begin{array}{c} 1 \ 0 \ 1 \ 0 \\ 0 \ 1 \ 1 \ 0 \end{array} \left[\begin{array}{c|c|c} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{array} \left| \begin{array}{c|c|c} 1 & -1 & 1 & 1 \\ 2 & 0 & 0 & 0 \end{array} \right| \begin{array}{c|c|c} 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{array} \right], \\ \begin{array}{c} 1 \ 1 \ -1 \ 0 \\ 1 \ 2 \ 1 \ -1 \end{array} \left[\begin{array}{c|c|c} 2 & 0 & -1 & -1 \\ 2 & -1 & 0 & 1 \end{array} \left| \begin{array}{c|c|c} 0 & 2 & 1 & 1 \\ 2 & 1 & 0 & 1 \end{array} \right| \begin{array}{c|c|c} 0 & -2 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{array} \right].$$

Let $S = \{(1, 0), (0, 1), (1, 1)\}$, and $B = \{\mathbf{v} \in \mathbb{Z}^2 : N(\mathbf{v}) \leq 4\}$. By Lemma 2.4, it suffices to show that B is S -integrally implied by the set

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

We list the relevant recurrences in order. As each index is implied, it may be used to imply later indices. It is assumed that as (a, b) is implied, so is $(-a, -b)$. To begin, the index $(1, -1)$ is implied by (10).

$$(2, -1) : \begin{array}{c} -1 \ 0 \ 1 \ 1 \\ 1 \ 1 \ 0 \ 0 \end{array} \left[\begin{array}{c|c|c} 0 & -1 & 2 & 1 \\ 2 & 0 & 0 & 0 \end{array} \left| \begin{array}{c|c|c} 2 & -1 & 0 & -1 \\ 1 & 1 & 1 & 1 \end{array} \right| \begin{array}{c|c|c} 1 & 2 & 1 & 0 \\ 1 & -1 & 1 & 1 \end{array} \right]. \\ (-1, 2) : \begin{array}{c} 0 \ -1 \ -1 \ 0 \\ 1 \ 1 \ 0 \ 0 \end{array} \left[\begin{array}{c|c|c} -1 & 1 & -1 & -1 \\ 2 & 0 & 0 & 0 \end{array} \left| \begin{array}{c|c|c} -2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{array} \right| \begin{array}{c|c|c} -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 \end{array} \right]. \\ (2, -2) : \begin{array}{c} 1 \ 1 \ -1 \ 0 \\ -1 \ -2 \ -1 \ 1 \end{array} \left[\begin{array}{c|c|c} 2 & 0 & -1 & -1 \\ -2 & 1 & 0 & -1 \end{array} \left| \begin{array}{c|c|c} 0 & 2 & 1 & 1 \\ -2 & -1 & 0 & -1 \end{array} \right| \begin{array}{c|c|c} 0 & -2 & 1 & 1 \\ -1 & 0 & -1 & -2 \end{array} \right].$$

At this point we have implied all indices of sup-norm at most 2.

$$(3, 0) : \begin{array}{c} 2 \ 1 \ 0 \ 0 \\ 0 \ 0 \ 1 \ 0 \end{array} \left[\begin{array}{c|c|c} 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array} \left| \begin{array}{c|c|c} 1 & 1 & 2 & 2 \\ 1 & -1 & 0 & 0 \end{array} \right| \begin{array}{c|c|c} 2 & -2 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{array} \right]. \\ (3, 1) : \begin{array}{c} 2 \ 1 \ 0 \ 0 \\ 1 \ 0 \ 1 \ 0 \end{array} \left[\begin{array}{c|c|c} 3 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{array} \left| \begin{array}{c|c|c} 1 & 1 & 2 & 2 \\ 1 & -1 & 1 & 1 \end{array} \right| \begin{array}{c|c|c} 2 & -2 & 1 & 1 \\ 2 & 0 & 0 & 0 \end{array} \right]. \\ (11) \quad (3, 2) : \begin{array}{c} 2 \ 1 \ 0 \ 0 \\ 1 \ 1 \ 1 \ 0 \end{array} \left[\begin{array}{c|c|c} 3 & 1 & 0 & 0 \\ 2 & 0 & 1 & 1 \end{array} \left| \begin{array}{c|c|c} 1 & 1 & 2 & 2 \\ 2 & 0 & 1 & 1 \end{array} \right| \begin{array}{c|c|c} 2 & -2 & 1 & 1 \\ 2 & 0 & 1 & 1 \end{array} \right].$$

$$(3, 3) : \begin{array}{c} 2 \ 1 \ 1 \ 0 \\ 2 \ 1 \ 0 \ 0 \end{array} \left[\begin{array}{c|c|c} 3 \ 1 \ 1 \ 1 & 2 \ 0 \ 2 \ 2 & 3 \ -1 \ 1 \ 1 \\ 3 \ 1 \ 0 \ 0 & 1 \ 1 \ 2 \ 2 & 2 \ -2 \ 1 \ 1 \end{array} \right].$$

Simply by switching top rows with bottom rows, we similarly imply $(0, 3)$, $(1, 3)$, and $(2, 3)$. And by putting negatives on the second row of (11), we imply the index $(3, -2)$ (and $(-2, 3)$ by switching top and bottom).

$$(3, -1) : \begin{array}{c} 2 \ 1 \ 0 \ 0 \\ -1 \ -1 \ -2 \ 2 \end{array} \left[\begin{array}{c|c|c} 3 \ 1 \ 0 \ 0 & 1 \ 1 \ 2 \ 2 & 2 \ -2 \ 1 \ 1 \\ -1 \ 1 \ 1 \ -1 & -1 \ -1 \ 1 \ -1 & 0 \ 0 \ 0 \ -2 \end{array} \right].$$

$$(3, -3) : \begin{array}{c} 1 \ 2 \ 1 \ 0 \\ -2 \ -1 \ 0 \ 0 \end{array} \left[\begin{array}{c|c|c} 3 \ -1 \ 1 \ 1 & 3 \ 1 \ 1 \ 1 & 2 \ 0 \ 2 \ 2 \\ -3 \ -1 \ 0 \ 0 & -1 \ -1 \ -2 \ -2 & -2 \ 2 \ -1 \ -1 \end{array} \right].$$

Again by switching top and bottom we get $(-1, 3)$. We have now implied all indices with sup-norm at most 3.

$$(4, 0) : \begin{array}{c} 2 \ 1 \ 0 \ 1 \\ 0 \ 0 \ 1 \ 0 \end{array} \left[\begin{array}{c|c|c} 4 \ 1 \ 1 \ 0 & 2 \ 1 \ 3 \ 2 & 3 \ -2 \ 2 \ 1 \\ 0 \ 0 \ 1 \ 1 & 1 \ -1 \ 0 \ 0 & 1 \ 1 \ 0 \ 0 \end{array} \right].$$

$$(4, 1) : \begin{array}{c} 3 \ 2 \ 1 \ -1 \\ 0 \ 0 \ 0 \ 1 \end{array} \left[\begin{array}{c|c|c} 4 \ 1 \ 0 \ 1 & 2 \ 1 \ 2 \ 3 & 3 \ -2 \ 1 \ 1 \\ 1 \ 0 \ 1 \ 0 & 1 \ 0 \ 1 \ 0 & 1 \ 0 \ 1 \ 0 \end{array} \right].$$

$$(4, 2) : \begin{array}{c} 3 \ 2 \ 1 \ -1 \\ 1 \ 1 \ 1 \ 0 \end{array} \left[\begin{array}{c|c|c} 4 \ 1 \ 0 \ 1 & 2 \ 1 \ 2 \ 3 & 3 \ -2 \ 1 \ 2 \\ 2 \ 0 \ 1 \ 1 & 2 \ 0 \ 1 \ 1 & 2 \ 0 \ 1 \ 1 \end{array} \right].$$

$$(4, 3) : \begin{array}{c} 2 \ 2 \ 1 \ 0 \\ 2 \ 1 \ 0 \ 0 \end{array} \left[\begin{array}{c|c|c} 4 \ 0 \ 1 \ 1 & 3 \ 1 \ 2 \ 2 & 3 \ -1 \ 2 \ 2 \\ 3 \ 1 \ 0 \ 0 & 1 \ 1 \ 2 \ 2 & 2 \ -2 \ 1 \ 1 \end{array} \right].$$

$$(4, 4) : \begin{array}{c} 3 \ 2 \ 1 \ -1 \\ 2 \ 2 \ 1 \ 0 \end{array} \left[\begin{array}{c|c|c} 4 \ 1 \ 0 \ 1 & 2 \ 1 \ 2 \ 3 & 3 \ -2 \ 1 \ 2 \\ 4 \ 0 \ 1 \ 1 & 3 \ 1 \ 2 \ 2 & 3 \ -1 \ 2 \ 2 \end{array} \right].$$

Again by switching top rows with bottom rows, we similarly imply $(0, 4)$, $(1, 4)$, $(2, 4)$ and $(3, 4)$. And by putting negatives on the second rows, we imply the indices $(4, -1)$, $(-1, 4)$, $(4, -3)$ and $(-3, 4)$.

$$(4, -2) : \begin{array}{c} 2 \ 1 \ -1 \ 1 \\ -1 \ -1 \ -1 \ 0 \end{array} \left[\begin{array}{c|c|c} 4 \ 1 \ 0 \ -1 & 1 \ 2 \ 3 \ 2 & 2 \ -3 \ 2 \ 1 \\ -2 \ 0 \ -1 \ -1 & -2 \ 0 \ -1 \ -1 & -2 \ 0 \ -1 \ -1 \end{array} \right].$$

$$(4, -4) : \begin{array}{c} 2 \ 1 \ -1 \ 1 \\ -2 \ -2 \ -1 \ 0 \end{array} \left[\begin{array}{c|c|c} 4 \ 1 \ 0 \ -1 & 1 \ 2 \ 3 \ 2 & 2 \ -3 \ 2 \ 1 \\ -4 \ 0 \ -1 \ -1 & -3 \ -1 \ -2 \ -2 & -3 \ 1 \ -2 \ -2 \end{array} \right].$$

By switching rows, we imply $(-2, 4)$. We have now demonstrated the calculation of all terms of index with sup-norm at most 4. The second part of the statement follows immediately from the first. \square

2.4. Basesets for ranks $n \geq 3$. Let \mathbf{e}_i denote the standard basis vectors.

Lemma 2.6. *Define the followings subsets of \mathbb{Z}^3 .*

$$L_2 = \{\mathbf{e}_i\}_i \cup \{\mathbf{e}_i \pm \mathbf{e}_j\}_{i \neq j} \cup \{2\mathbf{e}_i\}_i$$

$$L'_2 = \{a_i \mathbf{e}_i + a_j \mathbf{e}_j : a_i \in \mathbb{Z}, 1 \leq i \leq j \leq 3\}.$$

Then all indices $\mathbf{v} \in \mathbb{Z}^3$ with $N(\mathbf{v}) \leq 2$ are L_2 -integrally implied by L'_2 .

Proof. We make use of the recurrences

$$(12) \quad \begin{array}{c} 1 \ 1 \ 0 \ -1 \\ 0 \ 0 \ -1 \ 1 \\ 1 \ 0 \ 1 \ 0 \end{array} \left[\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 \end{array} \right],$$

$$(13) \quad \begin{array}{c} 0 \ 0 \ 1 \ -1 \\ 1 \ 1 \ 0 \ -1 \\ 0 \ 1 \ 1 \ 0 \end{array} \left[\begin{array}{ccc|ccc} -1 & 0 & 0 & 0 & -1 & -1 \\ 1 & 0 & -1 & 0 & 1 & 0 \\ 1 & -1 & 1 & 1 & 2 & 0 \end{array} \right],$$

$$(14) \quad \begin{array}{c} 1 \ 0 \ 1 \ 0 \\ 0 \ 0 \ 0 \ 1 \\ 1 \ 1 \ 0 \ -1 \end{array} \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 \end{array} \right].$$

Permute the rows of (12) by the cyclic permutations (123) and (132), calling the results (12') and (12'') respectively (for example, the right-most column of (12') is $(0, 1, 0)$). Do the same for (13) and (14).

Consider the equation obtained by the combination

$$\begin{aligned} & (12) \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(1,-1,0)} T_{(0,1,0)}^2 + (12') \times T_{(1,1,1)} T_{(1,0,0)} T_{(0,1,-1)} T_{(0,1,0)}^2 T_{(0,0,1)} \\ & + (14) \times T_{(1,-1,0)} T_{(0,1,0)}^2 T_{(0,1,1)} T_{(0,0,1)} T_{(1,0,1)}^2 + (14') \times T_{(0,1,-1)} T_{(1,0,0)}^2 T_{(0,0,1)} T_{(1,0,1)} T_{(1,1,0)} \\ & + (13) \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(0,1,0)} T_{(1,1,0)} + (13') \times T_{(1,1,1)} T_{(0,1,0)}^2 T_{(1,0,0)} T_{(0,1,1)} T_{(0,0,1)} \\ & + (13'') \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(1,0,1)} T_{(0,1,0)} T_{(0,0,1)} \end{aligned}$$

The result has the form $aT_{(1,1,1)} + b = 0$ where a and b are polynomials in $T_{\mathbf{v}}$ where every \mathbf{v} has at least one zero coordinate. In particular,

$$a = T_{(1,0,0)}^3 T_{(0,1,0)} T_{(0,0,1)}^2 T_{(1,0,1)} T_{(0,2,0)} T_{(1,0,-1)}.$$

Thus $T_{(1,1,1)}$ is L_2 -integrally implied by L'_2 . To imply the terms $T_{(-1,1,1)}$, $T_{(1,-1,1)}$, and $T_{(1,1,-1)}$, use (12), (12'), and (12''). This covers all terms of sup-norm at most 1.

We have the following recurrence:

$$\begin{array}{c} 0 \ 0 \ 0 \ 1 \\ 0 \ 0 \ -1 \ 1 \\ 2 \ 1 \ 1 \ -1 \\ 0 \ 1 \ 0 \ 1 \\ 1 \ 1 \ 0 \ 0 \end{array} \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & 0 & 1 \\ 2 & 1 & 0 & 1 & 1 & 0 \\ 2 & -1 & 1 & 0 & 2 & 1 \\ 2 & 0 & 0 & 0 & 1 & 1 \end{array} \right].$$

If \mathbf{v} has exactly one coordinate of value ± 2 (the rest ± 1), then we imply \mathbf{v} by taking the first three rows in the recurrence above (possibly taking negatives and permutations of rows as necessary). If \mathbf{v} has exactly two ± 2 's, use the middle three rows in the same way. If \mathbf{v} has exactly three ± 2 's, use the last three rows (this relies on the previous cases). \square

Remark 2.7. The four equations (12), (12'), (12'') and (13) in the four unknowns $T_{(1,1,1)}$, $T_{(-1,1,1)}$, $T_{(1,-1,1)}$ and $T_{(1,1,-1)}$, are linear with coefficients consisting of monomials in $T_{\mathbf{v}}$ where \mathbf{v} has at least one zero coordinate. The determinant of the system is

$$2T_{(1,0,0)} T_{(0,1,0)} T_{(0,0,1)}^2 T_{(1,1,0)} T_{(1,0,1)}^2 T_{(0,1,1)} T_{(1,-1,0)} T_{(1,0,-1)} T_{(0,1,-1)}.$$

This observation is useful for calculations where 2 is invertible.

Theorem 2.8. *Let $n \geq 2$. For each ℓ in the set*

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

choose a vector \mathbf{x}_ℓ 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

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

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

Proof. The proof is by induction on n . The base case is $n = 2$, which is a consequence of Theorem 2.5.

If $\mathbf{v} \in \mathbb{Z}^n$ has one zero in the i -th position, and the theorem statement holds for $n - 1$, then \mathbf{v} is H_n -integrally implied by H'_n . This is because $H_{n-1} \subset H_n$ (and $H'_{n-1} \subset H'_n$), where the former is considered a subset of the latter by adding a zero between the $(i - 1)$ -th and i -th positions. Therefore it suffices to imply $\mathbf{v} \in \mathbb{Z}^n$ having no zero coordinate.

The inductive step is itself an induction on the sup-norm of \mathbf{v} . The base cases are $N(\mathbf{v}) = 1$ and $N(\mathbf{v}) = 2$. Both of these for $n = 3$ are provided by Lemma 2.6, so for the base cases, we may assume $n \geq 4$. To imply \mathbf{v} , we construct a recurrence row-by-row, so that the first column is exactly \mathbf{v} . For the first three rows, use the following, multiplied by -1 as necessary.

$$\begin{array}{c} 1 \ 0 \ 0 \ 0 \\ 0 \ 1 \ 0 \ 0 \\ 0 \ 0 \ 0 \ 1 \end{array} \left[\begin{array}{c|c|c} 1 & 1 & 0 \ 0 \\ 1 & -1 & 0 \ 0 \\ 1 & 0 & 1 \ 0 \end{array} \right].$$

For all subsequent rows, use one of the following two recurrences (shown together in an array), multiplied by -1 as appropriate:

$$\begin{array}{c} 1 \ 1 \ 1 \ -1 \\ 0 \ 0 \ -1 \ 1 \end{array} \left[\begin{array}{c|c|c} 1 & 0 & 0 \ 1 \\ 1 & 0 & 0 \ -1 \\ 1 & 0 & 0 \ 1 \\ 0 & 1 & 1 \ 0 \end{array} \right].$$

For each row, the choice between the two possibilities can be made in such a way that the fourth column of the recurrence lies in G_n . Columns two and three have at most two non-zero entries (which are ± 1) and so are in H_n . The other columns (5-12) have at least one zero entry, and so are already implied by the inductive step. This completes the case $N(\mathbf{v}) = 1$.

For the remainder of the proof, we will repeatedly use the following recurrences. Let $w_i = \lceil \frac{v_i}{2} \rceil$. If v_i is even, we call the following

recurrences (shown here in an array) ($E1$) through ($E4$):

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

If v_i is odd, we call the following recurrences ($O1$) through ($O5$).

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

The second base case is $N(\mathbf{v}) = 2$ ($n \geq 4$ still). Since we may assume $v_i \neq 0$ (this is covered by previous cases in the induction on n), the other v_i have $|v_i| = \pm 1$. There are three cases:

Case I: \mathbf{v} has at least three odd v_i . Use for the first three odd v_i the recurrences ($O1$), ($O4$) and ($O5$) respectively. Use ($E3$) for all the even v_i . In this case, all the columns besides the first contain only digits 0 and ± 1 and so were implied in the case $N(\mathbf{v}) = 1$. The columns 2-4 contain only one non-zero term each, and so are in H_n .

Case II: \mathbf{v} has one or two odd v_i . Use ($O3$) for one odd coordinate and ($O1$) for the other (if it exists). Use ($E3$) for all even coordinates. Then, the columns 2-4 contain one or two non-zero entries, and the columns 5-12 may contain at most one ± 2 , but such a column was implied in the Case I.

Case III: \mathbf{v} has no odd v_i . Use ($E1$) and ($E4$) for the first two rows, and ($E3$) for all others. Columns 2-4 contain one or two non-zero entries and 5-12 at most two ± 2 's, but such a column was implied in Case I or II.

This completes the $N(\mathbf{v}) = 2$ base case.

Now suppose $N(\mathbf{v}) = N_0 \geq 3$ and $n \geq 3$. This is the inductive step; we will assume we have implied all indices of sup-norm less than N_0 . As before, $v_i \neq 0$. For $|v_i| = 3$, ($O1$), ($O2$), ($O4$), and ($O5$) have entries less than N_0 in columns 5-12. For $1 \leq |v_i| \leq 2$, and $3 < |v_i| \leq N_0$, all applicable recurrences have entries less than N_0 in those columns. We have two cases:

Case I: \mathbf{v} has at least one even entry. Use ($E4$) for the first even coordinate, and choose from ($E1$) and ($E2$) for the second even coordinate (if it exists). We use ($E3$) for all other even coordinates. We will use ($O1$) or ($O2$) for all odd entries (and make the choice between ($E1$) and ($E2$) above) in such a way that the second column is in G_n .

Case II: \mathbf{v} has no even entry. Use (O4) and (O5) for the first two odd coordinates, and (O1) or (O2) for all others, according so that the second column is an element of G_n . \square

3. NET POLYNOMIALS OVER \mathbb{C}

Fix an elliptic curve E defined over \mathbb{C} . Our purpose is to define rational functions $\Omega_{\mathbf{v}} : E^n \rightarrow \mathbb{C}$ for all $\mathbf{v} \in \mathbb{Z}^n$ such that for each $\mathbf{P} \in E^n$, the map

$$W_{E, \mathbf{P}} : \mathbb{Z}^n \rightarrow \mathbb{C}, \quad \mathbf{v} \mapsto \Omega_{\mathbf{v}}(\mathbf{P})$$

is an elliptic net. In this section we associate a lattice $\Lambda \subset \mathbb{C}$ to the elliptic curve E and consider the complex uniformization \mathbb{C}/Λ .

3.1. Elliptic functions over \mathbb{C} . For a complex lattice Λ , let $\eta : \Lambda \rightarrow \mathbb{C}$ be the quasi-period homomorphism, and define a quadratic form $\lambda : \Lambda \rightarrow \{\pm 1\}$ by

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

Recall that the Weierstrass sigma function $\sigma : \mathbb{C}/\Lambda \rightarrow \mathbb{C}$ satisfies the following transformation formula for all $z \in \mathbb{C}$ and $\omega \in \Lambda$:

$$(15) \quad \sigma(z + \omega; \Lambda) = \lambda(\omega) e^{\eta(\omega)(z + \frac{1}{2}\omega)} \sigma(z; \Lambda)$$

Definition 3.1. Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E . For $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$, define a function $\Omega_{\mathbf{v}}$ on \mathbb{C}^n in variables $\mathbf{z} = (z_1, \dots, z_n)$ as follows:

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

(If $\mathbf{v} = \mathbf{0}$, we set $\Omega_{\mathbf{v}} \equiv 0$.) In particular, we have for each $n \in \mathbb{Z}$, a function Ω_n on \mathbb{C} in the variable z :

$$\Omega_n(z; \Lambda) = \frac{\sigma(nz; \Lambda)}{\sigma(z; \Lambda)^{n^2}},$$

and for each pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$, a function $\Omega_{m,n}$ on $\mathbb{C} \times \mathbb{C}$ in variables z and w :

$$\Omega_{m,n}(z, w; \Lambda) = \frac{\sigma(mz + nw; \Lambda)}{\sigma(z; \Lambda)^{m^2 - mn} \sigma(z + w; \Lambda)^{mn} \sigma(w; \Lambda)^{n^2 - mn}}.$$

Remark 3.2. Compare the proof of Lemma 4.5 to this definition.

Proposition 3.3. *Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E . The functions $\Omega_{\mathbf{v}}$ are elliptic functions in each variable.*

Proof. Let $\omega \in \Lambda$. We show the function is elliptic in the first variable. Let $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$ and $\mathbf{z} = (z_1, \dots, z_n)$, $\mathbf{w} = (\omega, 0, \dots, 0) \in \mathbb{C}^n$. Using (15), we calculate

$$\frac{\Omega_{\mathbf{v}}(\mathbf{z} + \mathbf{w}; \Lambda)}{\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)} = \frac{\lambda(v_1\omega)}{\lambda(\omega)^{v_1}} = 1$$

where the last equality holds because λ is a quadratic form. Thus $\Omega_{\mathbf{v}}$ is invariant under adding a period to the variable z_1 . Similarly $\Omega_{\mathbf{v}}$ is elliptic in each variable on $(\mathbb{C}/\Lambda)^n$. \square

Proposition 3.4. *Fix a lattice $\Lambda \in \mathbb{C}$. Let $\mathbf{v} \in \mathbb{Z}^m$ and $\mathbf{z} \in \mathbb{C}^n$. Let T be an $n \times m$ matrix with entries in \mathbb{Z} and transpose T^{tr} . Then*

$$\Omega_{\mathbf{v}}(T^{tr}(\mathbf{z}); \Lambda) = \frac{\Omega_{T(\mathbf{v})}(\mathbf{z}; \Lambda)}{\prod_{i=1}^n \Omega_{T(\mathbf{e}_i)}(\mathbf{z}; \Lambda)^{2v_i^2 - \sum_{j=1}^n v_i v_j} \prod_{1 \leq i < j \leq n} \Omega_{T(\mathbf{e}_i + \mathbf{e}_j)}(\mathbf{z}; \Lambda)^{v_i v_j}}.$$

Proof. A straightforward calculation using Definition 3.1. \square

Let \wp and ζ denote the usual Weierstrass functions.

Lemma 3.5.

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

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

Proof. The first statement is well-known (e.g. [2]). The second statement follows by direct calculation using Definition 3.1. \square

Lemma 3.6.

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

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

Proof. Denote by f and g the left and right side of the first equation respectively. Considered as functions of any one of x , a or b , these are elliptic functions. Suppose that $a, b \notin \Lambda$. Consider f and g as functions of x . The set of poles of f or g is $\{-a, -b\}$. The zeroes of g are at $-a - b$ and 0 . These are also zeroes of f , since ζ is an odd function. Hence $f = cg$ for some c not depending on x . Now define instead

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

We have $F = c'G$ for some constant c' independent of x . Taking derivatives and evaluating at $x = 0$, we have

$$(\wp(b) - \wp(a)) \sigma(a)\sigma(b) = c' \sigma(a+b) \sigma'(0)$$

We have $\sigma'(0) = 1$. By Lemma 3.5, we then have

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

which proves the first equation. The second is obtained by a change of variables $x \leftarrow a$, $a \leftarrow x+b$, $b \leftarrow x$. \square

3.2. Forming the elliptic net.

Theorem 3.7. *Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E . Fix $z_1, \dots, z_n \in \mathbb{C}$. Then the function $W : \mathbb{Z}^n \rightarrow \mathbb{C}$ defined by*

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

is an elliptic net.

Proof. For notational simplicity, we drop the arguments z_i , Λ on $\Omega_{\mathbf{v}}$ and also write $\sigma(\mathbf{v})$, $\wp(\mathbf{v})$ and $\zeta(\mathbf{v})$ for $\sigma(v_1 z_1 + \dots + v_n z_n)$, $\wp(v_1 z_1 + \dots + v_n z_n)$ and $\zeta(v_1 z_1 + \dots + v_n z_n)$. We observe that $\mathbf{v} = \mathbf{0}$ if and only if $\Omega_{\mathbf{v}} \equiv 0$.

We intend to show that (4) holds for W in \mathbf{p} , \mathbf{q} , \mathbf{r} and \mathbf{s} . If any one of \mathbf{p} , \mathbf{q} or \mathbf{r} are zero, then (4) holds trivially (note that σ is an odd function, so that $\Omega_{-\mathbf{v}} = -\Omega_{\mathbf{v}}$). Hence we may assume that none of $\Omega_{\mathbf{p}}$, $\Omega_{\mathbf{q}}$, or $\Omega_{\mathbf{r}}$ is identically zero. For any quadratic form f defined on \mathbb{Z}^n , we have the following relation for all $\mathbf{p}, \mathbf{q}, \mathbf{s} \in \mathbb{Z}^n$:

$$(16) \quad f(\mathbf{p}+\mathbf{q}+\mathbf{s}) + f(\mathbf{p}-\mathbf{q}) + f(\mathbf{s}) - f(\mathbf{p}+\mathbf{s}) - f(\mathbf{p}) - f(\mathbf{q}+\mathbf{s}) - f(\mathbf{q}) = 0.$$

First we address the case that $\mathbf{s} = \mathbf{0}$. By (16) and Lemma 3.5,

$$\frac{\Omega_{\mathbf{p}+\mathbf{q}}\Omega_{\mathbf{p}-\mathbf{q}}}{\Omega_{\mathbf{p}}^2\Omega_{\mathbf{q}}^2} = \frac{\sigma(\mathbf{p}+\mathbf{q})\sigma(\mathbf{p}-\mathbf{q})}{\sigma(\mathbf{p})^2\sigma(\mathbf{q})^2} = \wp(\mathbf{q}) - \wp(\mathbf{p}).$$

Therefore, we have

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

which gives the relation (4) for $\mathbf{s} = \mathbf{0}$, that is,

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

Now suppose that $\mathbf{s} \neq \mathbf{0}$ and so $\Omega_{\mathbf{s}} \neq 0$. By (16) and Lemma 3.6,

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

Therefore, we have

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

or, more simply,

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

which is what was required to prove. \square

The identity (4) for $\Omega_{\mathbf{v}}$ is similar to several identities known in complex function theory [11, 27].

3.3. Explicit rational functions. Elliptic functions for a lattice Λ of \mathbb{C} give rational functions on the associated elliptic curve (via complex uniformization). If we give a Weierstrass model for the same elliptic curve, we can give explicit expressions for the rational functions as elements of the usual field of rational functions associated to the model. In the following proposition, we do this for $\Omega_{\mathbf{v}}$ for some small $\mathbf{v} \in \mathbb{Z}^n$, for $n = 1, 2, 3$.

Proposition 3.8. *Consider an elliptic curve E , and a Weierstrass model for E given by*

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

As usual, let

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

To E we can also associate a complex uniformization and elliptic functions $\Omega_{\mathbf{v}}$ as above. As rational functions on E , we have the following equalities.

For $n = 1$:

$$\begin{aligned}\Omega_1 &= 1, & \Omega_2 &= 2y + a_1x + a_3, \\ \Omega_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\end{aligned}$$

$$\begin{aligned}\Omega_4 &= (2y + a_1x + a_3) \times \\ &(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2);\end{aligned}$$

For $n = 2$:

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

For $n = 3$:

$$\begin{aligned}\Omega_{(1,0,0)} &= \Omega_{(0,1,0)} = \Omega_{(0,0,1)} = \Omega_{(1,1,0)} = \Omega_{(0,1,1)} = \Omega_{(1,0,1)} = 1, \\ \Omega_{(1,-1,0)} &= x_2 - x_1, & \Omega_{(0,1,-1)} &= x_3 - x_2, & \Omega_{(-1,0,1)} &= x_1 - x_3, \\ \Omega_{(-1,1,0)} &= x_1 - x_2, & \Omega_{(0,-1,1)} &= x_2 - x_3, & \Omega_{(1,0,-1)} &= x_3 - x_1, \\ \Omega_{(1,1,1)} &= \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)}, \\ \Omega_{(-1,1,1)} &= \frac{y_1(x_2 - x_3) - y_2(x_3 - x_1) - y_3(x_1 - x_2)}{(x_2 - x_3)} + a_1x_1 + a_3, \\ \Omega_{(1,-1,1)} &= \frac{-y_1(x_2 - x_3) + y_2(x_3 - x_1) - y_3(x_1 - x_2)}{(x_3 - x_1)} + a_1x_2 + a_3, \\ \Omega_{(1,1,-1)} &= \frac{-y_1(x_2 - x_3) - y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)} + a_1x_3 + a_3.\end{aligned}$$

Proof. The division polynomial formulæ (the $n = 1$ case) are well-known [2] [10, p.80] [20, Exercise 3.7]. The formulæ for $n = 2$ and the related first dozen formulæ for $n = 3$ are immediate consequences of Lemma 3.5 and the addition law for elliptic curves [20, Algorithm 2.3]. Only the cases where $n = 3$, $v_i \neq 0$ for all $i = 1, 2, 3$ are not immediate: these formulæ are a result of the proof of Lemma 2.6. Note that using Remark 2.7 results in the same formulæ. \square

4. NET POLYNOMIALS OVER ARBITRARY FIELDS

In the last section, we defined elliptic functions $\Omega_{\mathbf{v}}$ in the case of \mathbb{C}/Λ . In this section we wish to define the same rational functions for any elliptic curve over any field, calling them $\Psi_{\mathbf{v}}$, the *net polynomials*. We will start from the results of the last section.

4.1. Defining net polynomials. 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 $f(x, y) \in R[x, y]$ by

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

Consider the affine scheme $\mathcal{E} : f(x, y) = 0$ over R . Let $\mathbf{a} = (a_i) \in \mathbb{C}^5$. The association $(\alpha_i) \mapsto (a_i)$ gives a map $\phi_{\mathbf{a}} : R \rightarrow \mathbb{C}$. Consider the affine variety over \mathbb{C} given by

$$C_{\mathbf{a}} : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Then $\phi_{\mathbf{a}}$ gives rise to a Cartesian diagram

$$\begin{array}{ccc} \mathcal{E}^n & \longleftarrow & C_{\mathbf{a}}^n \\ \downarrow & & \downarrow \\ \text{Spec}(R) & \longleftarrow & \text{Spec}(\mathbb{C}) \end{array}$$

where $\mathcal{E}^n = \mathcal{E} \times_{\text{Spec } R} \cdots \times_{\text{Spec } R} \mathcal{E}$ is the n -fold fibre product of \mathcal{E} with itself over R .

The rational functions $\Omega_{\mathbf{v}} \in \mathcal{K}(C_{\mathbf{a}}^n)$ have rational expressions in x , y and the a_i (in terms of the Weierstrass model, as in for example Proposition 3.8). These expressions have rational coefficients by construction and the general theory of sigma functions (the divisors are Galois invariant). So these same expressions (with a_i replaced with α_i) give rational functions $\Psi_{\mathbf{v}} \in \mathcal{K}(\mathcal{E}^n)$.

We obtain the following theorem.

Theorem 4.1. *Let $n \geq 1$. Denote by $\mathcal{K}(\mathcal{E}^n)$ the field of rational functions on \mathcal{E}^n . There exists a unique system of functions $\Psi_{\mathbf{v}} \in \mathcal{K}(\mathcal{E}^n)$ depending on $\mathbf{v} \in \mathbb{Z}^n$ such that*

- (1) *the map*

$$W : \mathbb{Z}^n \rightarrow \mathcal{K}(\mathcal{E}^n), \quad \mathbf{v} \mapsto \Psi_{\mathbf{v}}$$

is an elliptic net, and

- (2) *whenever $C_{\mathbf{a}}$ is elliptic, the restriction of $\Psi_{\mathbf{v}}$ to a fibre $C_{\mathbf{a}}^n$ is the rational function $\Omega_{\mathbf{v}}$.*

Proof. The union of the $C_{\mathbf{a}}^n$ for which $C_{\mathbf{a}}$ is an elliptic curve is Zariski dense, and so the $\Psi_{\mathbf{v}}$ are determined uniquely by their restrictions to these fibres. \square

We call these $\Psi_{\mathbf{v}}$ the *net polynomials*. Look ahead to Section 4.2 for the definition of the ‘polynomial’ ring \mathcal{R}_n in which they live.

We transfer some useful properties of the $\Omega_{\mathbf{v}}$ to properties of the $\Psi_{\mathbf{v}}$ on \mathcal{E}^n . Again, there are unique rational functions X and Y for \mathcal{E} whose restriction to elliptic $C_{\mathbf{a}}$ correspond to the Weierstrass functions \wp and \wp' . Each $\mathbf{v} \in \mathbb{Z}^n$ gives rise to a map $\mathbf{v} : \mathcal{E}^n \rightarrow \mathcal{E}$ which is the linear combination associated to the vector \mathbf{v} (e.g., $(1, 1)$ is the usual group law). Define rational functions $X_{\mathbf{v}} = X \circ \mathbf{v}$ and $Y_{\mathbf{v}} = Y \circ \mathbf{v}$ on \mathcal{E}^n .

The next lemma follows immediately from Lemma 3.5.

Lemma 4.2.

$$(17) \quad \Psi_{\mathbf{v}}^2 \Psi_{\mathbf{w}}^2 (X_{\mathbf{v}} - X_{\mathbf{w}}) = -\Psi_{\mathbf{v}+\mathbf{w}} \Psi_{\mathbf{v}-\mathbf{w}}.$$

More generally, there is a map $T : \mathcal{E}^m \rightarrow \mathcal{E}^n$ associated to any $T \in M_{n \times m}(\mathbb{Z})$. The next proposition follows from Proposition 3.4.

Proposition 4.3. *Let $\mathbf{v} \in \mathbb{Z}^n$. Let T be any $n \times m$ matrix with entries in \mathbb{Z} and transpose T^{tr} . Then*

$$(\Psi_{\mathbf{v}} \circ T) \prod_{i=1}^n \Psi_{T^{tr}(\mathbf{e}_i)}^{2v_i^2 - \sum_{j=1}^n v_i v_j} \prod_{1 \leq i < j \leq n} \Psi_{T^{tr}(\mathbf{e}_i + \mathbf{e}_j)}^{v_i v_j} = \Psi_{T^{tr}(\mathbf{v})}.$$

4.2. Net polynomials at primes. In this section we determine a little more about the exact nature of the elliptic net $\Psi_{\mathbf{v}}$. In particular, we wish to restrict the possible divisor of $\Psi_{\mathbf{v}}$, and show that it has zero valuation for certain primes.

Consider the ring $S = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6]$. Since $f(x, y)$ is defined over S , we may define $\mathcal{E}_S : f(x, y) = 0$ as a scheme over $\text{Spec } S$ whose fibre over $\text{Spec } R$ is \mathcal{E} . Then $\mathcal{E}_S^n = \mathcal{E}_S \times_{\text{Spec } S} \cdots \times_{\text{Spec } S} \mathcal{E}_S$ is a scheme over $\text{Spec } S$ whose fibre over $\text{Spec } R$ is \mathcal{E}^n . Define

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

The ring \mathcal{R}_n is the affine coordinate ring of the affine piece of \mathcal{E}_S^n obtained by removing all the coordinate hyperplanes, diagonals and anti-diagonals. There is a natural identification of \mathcal{R}_n with a subset of $\mathcal{K}(\mathcal{E}^n)$.

Theorem 4.4. *The functions $\Psi_{\mathbf{v}}$ are elements of \mathcal{R}_n . Let \mathfrak{p} be any prime of \mathcal{R}_n which is a lift of a prime of S . Then $\Psi_{\mathbf{v}} \notin \mathfrak{p}$.*

The lifted ideal $\mathfrak{p} = \mathfrak{q}\mathcal{R}_n$ is prime whenever \mathfrak{q} is a prime of S . The proof of the theorem will involve showing for all valuations v associated to such primes \mathfrak{p} that $v(\Psi_{\mathbf{v}})$ (slightly modified) is a quadratic form with certain vanishing. Then the following lemma will establish that this function is identically zero.

Let B and C be abelian groups written additively. The function $f : B \rightarrow C$ is a *quadratic form* if for all $x, y, z \in B$,

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

If f is a quadratic form, then for all $x, y \in B$,

$$f(x+y) + f(x-y) - 2f(x) - 2f(y) = 0.$$

The converse holds if C is 2-torsion free.

Lemma 4.5. *Let $M : \mathbb{Z}^n \rightarrow \mathbb{Z}$ be a quadratic form. Suppose that $M(\mathbf{v}) = 0$ for all $\mathbf{v} = \mathbf{e}_i$ and $\mathbf{v} = \mathbf{e}_i + \mathbf{e}_j$ (i.e. for standard basis vectors and their two-term sums). Then $M(\mathbf{v}) = 0$ for all \mathbf{v} .*

Proof. It is well-known that any value of a quadratic form can be given in terms of its value at a certain ‘base’ of vectors. In particular,

$$f\left(\sum_{i=1}^n a_i \mathbf{e}_i\right) = \sum_{i=1}^n \left(2a_i^2 - \sum_{j=1}^n a_i a_j\right) f(\mathbf{e}_i) + \sum_{1 \leq i < j \leq n} a_i a_j f(\mathbf{e}_i + \mathbf{e}_j).$$

□

Proof of Theorem 4.4. Each $\Psi_{\mathbf{v}} \in \mathcal{K}(\mathcal{E}^n)$ has a corresponding Weil divisor. Suppose a codimension-one subscheme X appears as a summand in this divisor, and let $\tilde{X} = X \cap C_{\mathbf{a}}^n$. If $C_{\mathbf{a}}$ is elliptic, $\tilde{X} \neq \emptyset$, and $\tilde{X} \neq C_{\mathbf{a}}^n$, then \tilde{X} is of codimension one in $C_{\mathbf{a}}^n$ and appears in the divisor of $\Omega_{\mathbf{v}}$ to the same order as X appears in the divisor of $\Psi_{\mathbf{v}}$. Definition 3.1 determines the divisors of $\Omega_{\mathbf{v}}$ and this restricts the possible divisors for $\Psi_{\mathbf{v}}$. In particular, it shows that $s\Psi_{\mathbf{v}} \in \mathcal{R}_n$, where $s \in S$.

Therefore, taking v to be a valuation of \mathcal{R}_n lifted from a valuation of S associated to a prime \mathfrak{q} of S , it will suffice to show that $v(\Psi_{\mathbf{v}}) = 0$ for all $\mathbf{v} \in \mathbb{Z}^n$.

Equation (17) of Lemma 4.2 implies

$$X_{\mathbf{v}} - X_{\mathbf{w}} = -\frac{\Psi_{\mathbf{v}+\mathbf{w}}\Psi_{\mathbf{v}-\mathbf{w}}}{\Psi_{\mathbf{v}}^2\Psi_{\mathbf{w}}^2}.$$

We claim that $v(X_{\mathbf{v}} - X_{\mathbf{w}}) = 0$ whenever $\mathbf{v} \neq \pm\mathbf{w}$, $\mathbf{v} \neq 0$, and $\mathbf{w} \neq 0$.

First we show that $v(X_{\mathbf{v}} - X_{\mathbf{w}}) < 0 \implies \mathbf{v} = 0$ or $\mathbf{w} = 0$. Suppose $v(X_{\mathbf{v}} - X_{\mathbf{w}}) < 0$. Then, $v(X_{\mathbf{v}}) < 0$ or $v(X_{\mathbf{w}}) < 0$. Suppose $v(X_{\mathbf{v}}) < 0$.

This implies that $\mathbf{v}(\mathbf{P}) = \mathcal{O}$ for all \mathbf{P} on the non-singular part of the fibre over \mathfrak{q} of \mathcal{E}_S . Since \mathbf{P} ranges over all possible values (e.g. $\mathbf{P} = (P, \mathcal{O}, \dots, \mathcal{O})$), we find that this implies that $[v_i] = [0]$ for all i . In turn, this shows that $\mathbf{v} = 0$. Similarly, if $v(X_{\mathbf{w}}) < 0$, then $\mathbf{w} = 0$.

Now we show that $v(X_{\mathbf{v}} - X_{\mathbf{w}}) > 0 \implies \mathbf{v} = \pm\mathbf{w}$. Suppose the valuation is positive. Then $\mathbf{v}(\mathbf{P}) = \pm\mathbf{w}(\mathbf{P})$ for all \mathbf{P} on the non-singular part of the fibre over \mathfrak{q} of \mathcal{E}_S . Since \mathbf{P} ranges over all possible values (e.g. $\mathbf{P} = (P, \mathcal{O}, \dots, \mathcal{O})$ or $\mathbf{P} = (P, P, \mathcal{O}, \dots, \mathcal{O})$), we find that this implies, in particular, that for all $0 \leq i \leq j \leq n$, we have $[v_i \pm w_i] = [0]$ and $[v_i + v_j \pm (w_i + w_j)] = [0]$ on \mathcal{E}_S . In turn, this gives $v_i = \pm w_i$ and $v_i + v_j = \pm(w_i + w_j)$. Together these imply that $\mathbf{v} = \pm\mathbf{w}$. This demonstrates the claim.

Define a function $M : \mathbb{Z}^n \rightarrow \mathbb{Z}$ by

$$M(\mathbf{v}) = \begin{cases} v(\Psi_{\mathbf{v}}) & \mathbf{v} \neq 0 \\ 0 & \mathbf{v} = 0 \end{cases}$$

Note that $M(-\mathbf{v}) = M(\mathbf{v})$, from which one can deduce that

$$(18) \quad M(\mathbf{v} + \mathbf{w}) + M(\mathbf{v} - \mathbf{w}) - 2M(\mathbf{v}) - 2M(\mathbf{w}) = 0$$

whenever $\mathbf{v} = 0$ or $\mathbf{w} = 0$. Our work up until now has shown that (18) holds in all other cases except $\mathbf{v} + \mathbf{w} = 0$ or $\mathbf{v} - \mathbf{w} = 0$. These remaining two cases reduce to the statement that for all \mathbf{u} , $M(2\mathbf{u}) = 4M(\mathbf{u})$. To obtain this, take the sum of the four instances of (18) with (\mathbf{v}, \mathbf{w}) respectively taking the values $(4\mathbf{u}, \mathbf{u})$, $(3\mathbf{u}, \mathbf{u})$, $(3\mathbf{u}, \mathbf{u})$ and $(2\mathbf{u}, \mathbf{u})$, and then subtract the instance of (18) with $(\mathbf{v}, \mathbf{w}) = (3\mathbf{u}, 2\mathbf{u})$.

We have shown that (18) holds for all \mathbf{v} and \mathbf{w} , and that therefore $M : \mathbb{Z}^n \rightarrow \mathbb{Z}$ is a quadratic form (since \mathbb{Z} is 2-torsion free). The other assumptions of Lemma 4.5 are verified by Proposition 3.8. Therefore, M is identically zero, which is what was required to prove. \square

4.3. Summary. Let $n \geq 1$. For any elliptic curve or scheme C , let \mathcal{O} denote the identity, $[m] : C \rightarrow C$ denote multiplication by m , $p_i : C^n \rightarrow C$ denote projection onto the i -th component, and $s : C^n \rightarrow C$ denote sum of all components. For $\mathbf{v} \in \mathbb{Z}^n$, define the expression

$$\begin{aligned} D_{C,\mathbf{v}} &= ([v_1] \times \dots \times [v_n])^* s^*(\mathcal{O}) - \sum_{1 \leq k < j \leq n} v_k v_j (p_k^* \times p_j^*) s^*(\mathcal{O}) \\ &\quad - \sum_{k=1}^n \left(2v_k^2 - \sum_{j=1}^n v_k v_j \right) p_k^*(\mathcal{O}), \end{aligned}$$

which is a divisor on the n -fold product C^n . Over the complex numbers, the functions $\Omega_{\mathbf{v}}$ have these divisors and satisfy the elliptic net recurrence (4) (see Section 3).

We now collect the results of the previous sections in one statement.

Theorem 4.6. *Let $n \geq 1$. There exists a unique collection of rational functions $\Psi_{\mathbf{v}} \in \mathcal{K}(\mathcal{E}_S^n)$ for each $\mathbf{v} \in \mathbb{Z}^n$ such that:*

- (1) *The map $\mathbf{v} \mapsto \Psi_{\mathbf{v}}$ gives an elliptic net $W : \mathbb{Z}^n \rightarrow \mathcal{R}_n$.*
- (2) *$\Psi_{\mathbf{v}} = 1$ whenever $\mathbf{v} = \mathbf{e}_i$ for some $1 \leq i \leq n$ or $\mathbf{v} = \mathbf{e}_i + \mathbf{e}_j$ for some $1 \leq i < j \leq n$.*
- (3) *$\text{Div}(\Psi_{\mathbf{v}}) = D_{\mathcal{E}_S, \mathbf{v}}$.*

Proof. Part (1) follows from Theorems 4.1 and 4.4. Part (2) follows from Proposition 3.8 and Theorem 4.1. Part (3) follows from Theorem 4.4. \square

5. ELLIPTIC NETS FROM ELLIPTIC CURVES

In light of Theorem 4.6, it is now natural to define an elliptic net associated to any cubic Weierstrass curve over any field.

Definition 5.1. Let K be any field. Let $a_1, a_2, a_3, a_4, a_6 \in K$. To this we associate a map

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

Let

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

and let C be a curve defined by $f(x, y) = 0$. Then we have a Cartesian diagram

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

under which we may pullback $\Psi_{\mathbf{v}}$ to obtain $\phi_{\mathbf{v}} \in \mathcal{K}(C^n)$ (this is possible since we know the open set on which $\Psi_{\mathbf{v}}$ is defined does not contain the fibre on the right, by Theorem 4.6).

The non-singular points of C defined over K , denoted $C_{ns}(K)$, form a group. We call a set of points $\{P_1, \dots, P_n\}$ on the non-singular part C_{ns} of a cubic curve *appropriate* if the following hold:

- (1) $P_i \neq 0$ for all i ;
- (2) $[2]P_i \neq 0$ for all i ;
- (3) $P_i \neq \pm P_j$ for any $i \neq j$; and

(4) $[3]P_1 \neq 0$ whenever $n = 1$.

If we have an appropriate n -tuple of points $\mathbf{P} \in C_{ns}(K)^n$, then we may define a map

$$W_{C,\mathbf{P}} : \mathbb{Z}^n \rightarrow K,$$

defined by $W_{C,\mathbf{P}}(\mathbf{v}) = \phi_{\mathbf{v}}(\mathbf{P})$. By Theorem 4.6, this will be an elliptic net. This will be called *the elliptic net associated to C and \mathbf{P}* .

We have the following additional corollary to Theorem 4.6.

Corollary 5.2. *For an elliptic net $W_{C,\mathbf{P}} : \mathbb{Z}^n \rightarrow K$ associated to a curve C and non-singular points \mathbf{P} , we have $W(\mathbf{v}) = 0$ if and only if $\mathbf{v}(\mathbf{P}) = \mathcal{O}$ on C_{ns} .*

Proof. This follows from the statement that $\Omega_{\mathbf{v}}(\mathbf{v} \cdot \mathbf{z}) = 0$ if and only if $\mathbf{v} \cdot \mathbf{z} \in \Lambda$ (see Section 3). \square

Example 5.3. Figure 1 (in Section 1) shows an example elliptic net associated to the elliptic curve and points

$$E : y^2 + y = x^3 + x^2 - 2x, \quad P = (0, 0), \quad Q = (1, 0)$$

Some of the smaller terms of the net $W_{E,(P,Q)}$ can be calculated using Proposition 3.8, for example,

$$W(0, 0) = 0, \quad W(1, 0) = W(0, 1) = W(1, 1) = 1,$$

$$W(2, 0) = 2y_1 + a_1x_1 + a_3 = 1, \quad W(0, 2) = 2y_2 + a_1x_2 + a_3 = 1,$$

$$W(1, -1) = x_2 - x_1 = 1,$$

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

$$W(2, -1) = (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 = -1.$$

More terms can be calculated using the recurrence relation (4). Since P and Q are independent non-torsion points, there are no zeroes in the array except the zero located at the origin ($W(0, 0) = 0$). The centre row is the elliptic divisibility sequence associated to E and P , which begins

$$1, 1, -3, 11, 38, 249, -2357, 8767, 496035, -3769372, -299154043, \\ -12064147359, 632926474117, -65604679199921, \dots$$

The centre column is the elliptic divisibility sequence associated to Q .

6. ELLIPTIC CURVES FROM ELLIPTIC NETS

We are now in a position to use the results of Section 2 to determine exactly which elliptic curves (or more generally cubic Weierstrass curves) give rise to any given elliptic net.

6.1. Scale equivalence and normalisation.

Proposition 6.1. *Let $W : A \rightarrow K$ be an elliptic net. Let $f : A \rightarrow K^*$ be a quadratic form. Define $W^f : A \rightarrow K$ by*

$$W^f(\mathbf{v}) = f(\mathbf{v})W(\mathbf{v}).$$

Then W^f is an elliptic net.

Proof. Let $p, q, r, s \in A$. We use multiplicative notation in K^* , so that f satisfies

$$(19) \quad f(p+q+s)f(p)f(q)f(s)f(p+q)^{-1}f(q+s)^{-1}f(p+s)^{-1} = 1.$$

The parallelogram law for quadratic forms (written multiplicatively) states that

$$(20) \quad f(p-q)f(p+q) = f(p)^2f(q)^2.$$

Multiplying $f(r)f(r+s)$ and equations (19) and (20) together,

$$\begin{aligned} f(p+q+s)f(p-q)f(r+s)f(r) &= \\ f(q+s)f(p+s)f(r+s)f(p)f(q)f(r)f(s)^{-1}, \end{aligned}$$

which is symmetric in p, q , and r , so

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

which shows that the recurrence (4) holds for W^f if it does for W . \square

If two elliptic nets are related in the manner of W and W^f for some quadratic form f , then we call them *scale equivalent*. This is clearly an equivalence relation.

Let $W : \mathbb{Z}^n \rightarrow K$ be an elliptic net. We say that W is *normalised* if $W(\mathbf{e}_i) = 1$ for all $1 \leq i \leq n$ and $W(\mathbf{e}_i + \mathbf{e}_j) = 1$ for all $1 \leq i < j \leq n$. An elliptic net arising from a curve and points is normalised. It should be emphasized that the concept of *normalised* is only defined for elliptic nets with a preferred basis.

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 $i \neq j$), or if $n = 1$ and any term of the form $W(3\mathbf{e}_1)$ is zero, then we say that W is *degenerate*. Compare the definition of *degenerate* to the definition of *appropriate* in Section 5.

Proposition 6.2. *Let $W : \mathbb{Z}^n \rightarrow K$ be a non-degenerate elliptic net. Then there is exactly one scaling W^f which is normalised.*

Proof. Define

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

Then W^f is normalised. Uniqueness is clear. \square

The proof demonstrates that scale equivalence has $\binom{n+1}{2}$ degrees of freedom. If $W : \mathbb{Z}^n \rightarrow K$ is an elliptic net, then its *normalisation* \widehat{W} is defined to be the unique normalised elliptic net which is a scaling of W . A *coordinate sublattice* of \mathbb{Z}^n is a sublattice of the form

$$\{\mathbf{v} \in \mathbb{Z}^n : v_i = 0 \text{ for } i \notin I\}$$

for some proper non-empty subset $I \subset \{1, 2, \dots, n\}$. The *rank* of the sublattice is $\#I$.

6.2. Curves from nets of ranks 1 and 2. Define a change of variables of a cubic curve in Weierstrass form to be *unihomothetic* if it is of the form

$$(21) \quad x' = x + r, \quad y' = y + sx + t,$$

for some r , s and t .

The rank-one result in the following form is due to Christine Swart.

Proposition 6.3 (Swart [23, Theorem 4.5.3]). *Let $W : \mathbb{Z} \rightarrow K$ 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

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

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

Proof. See [23, Theorem 4.5.3]. A normalised rank 1 non-degenerate elliptic net has $W(2) \neq 0$ and $W(3) \neq 0$. Any singular point $P = (x, y)$ on a cubic Weierstrass curve has vanishing partial derivatives, which implies $\Psi_2(P) = 2y + a_1x + a_3 = 0$ (see Proposition 3.8). Therefore, if any curve and singular point gives rise to W , then $W(2) = 0$, in contradiction to non-degeneracy. The division polynomials Ψ_1, Ψ_2, Ψ_3 and Ψ_4 are invariant under a change of coordinates of the form (21). Then, it is a simple calculation to check that $W_{C,P}$ agrees with W at the first four terms; hence $W_{C,P} = W$ by Theorem 2.2. Conversely, suppose $W = W_{C',P'}$. After applying a transformation of the form (21) taking P' to $(0, 0)$ and taking a_4 to 1, substitution of the division polynomials into the equations above verifies that $a'_i = a_i$ for all i . \square

Proposition 6.4. *Let $W : \mathbb{Z}^2 \rightarrow K$ be a normalised non-degenerate elliptic net. Then 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

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

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

Proof. In a normalised non-degenerate elliptic net,

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

(see Theorem 2.5). Thus (as in the previous theorem) if a curve and points give rise to W , then the points are non-singular. The formulæ for $W(2, 0)$, $W(0, 2)$, $W(2, 1)$ and $W(1, 2)$ are invariant under a change of coordinates of the form (21). The net W_{C,P_1,P_2} agrees with W at the terms $(2, 0)$, $(0, 2)$, $(2, 1)$ and $(1, 2)$; hence $W_{C,P_1,P_2} = W$ by Theorem 2.5. Conversely, suppose $W = W_{C',P'_1,P'_2}$. After applying a unihomothetic transformation taking P'_1 to $(0, 0)$ and P'_2 to $(W(1, 2) - W(2, 1), 0)$, substitution of the net polynomials into the equations above verifies that $a'_i = a_i$ for all i . \square

Example 6.5. Plugging in terms from the elliptic net of Figure 1 (in Section 1) to the formulæ in the statement of Proposition 6.4 we recover the curve and points stated in the figure caption.

Remark 6.6. A more symmetric set of equations in the case of characteristic not equal to 2 is as follows:

$$\begin{aligned} P_1 &= (v, 0), & P_2 &= (-v, 0), & 2v &= W(2, 1) - W(1, 2), \\ a_1 &= \frac{W(2, 0) - W(0, 2)}{W(2, 1) - W(1, 2)}, & 2a_2 &= W(2, 1) + W(1, 2), \\ 2a_3 &= W(2, 0) + W(0, 2), & 4a_4 &= -(W(2, 1) - W(1, 2))^2, \\ 8a_6 &= -(W(2, 1) - W(1, 2))^2(W(2, 1) + W(1, 2)). \end{aligned}$$

6.3. Curves from nets in general rank.

Theorem 6.7. *Let $n \geq 1$. Let $W : \mathbb{Z}^n \rightarrow K$ be a normalised non-degenerate elliptic net. Then the set of curves C and $\mathbf{P} \in C^n$ such that $W = W_{C, \mathbf{P}}$ forms a three-dimensional family of tuples (C, \mathbf{P}) . Further, none of the points $P \in \mathbf{P}$ are singular. In particular, the family consists of one such tuple and all its images under unihomothetic changes of coordinates.*

Proof. The proof is by strong induction on n , where 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 by Propositions 6.3 and 6.4; part (II) is by non-degeneracy, which implies $W(\mathbf{e}_1) \neq 0$ and $W(\mathbf{e}_1 + \mathbf{e}_2) \neq 0$.

Suppose $n \geq 3$ and the inductive statement holds for all $k < n$. Let W_1, W_2, \dots, W_n be the normalised elliptic subnets of W associated to the rank $n - 1$ coordinate sublattices $L_i = \{\mathbf{v} : v_i = 0\}$. These are defined as nets $W_i : L_i \rightarrow K$ but they can be identified with nets $W'_i : \mathbb{Z}^{n-1} \rightarrow K$ in the obvious way (by deleting the zero coordinate). They are 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 $W'_i = W_{C_i, \mathbf{P}_i}$ for some curves C_i and non-singular points $\mathbf{P}_i \in C_i^{n-1}$.

We observe a consequence of Proposition 4.3. Suppose $V_1 : \mathbb{Z}^m \rightarrow K$ is an elliptic net of rank m associated to C and \mathbf{P} . Also suppose

$$V_2 : \{\mathbf{v} \in \mathbb{Z}^m : v_m = 0\} \rightarrow K$$

is the elliptic subnet of V_1 associated to the coordinate sublattice of rank $m - 1$ which consists of vectors with last coordinate zero. Suppose $V'_2 : \mathbb{Z}^{m-1} \rightarrow K$ is naturally identified with V_2 by simply deleting the last coordinate of the domain. Then V'_2 is associated to C and \mathbf{P}' where \mathbf{P}' is simply \mathbf{P} with the last coordinate deleted. This statement, appropriately adjusted, holds for any coordinate hyperplane (not just the one with last coordinate zero).

Consider two of the rank $n - 1$ subnets, say W_i and W_j . Let $W_{ij} = W_i \cap W_j$ in W . Define $W'_{ij} : \mathbb{Z}^{n-2} \rightarrow K$ by the obvious identification. Then, $W'_{ij} = W_{C_{ij}, \mathbf{P}_{ij}}$ for some curve C_{ij} and $\mathbf{P}_{ij} \in C_{ij}^{n-2}$. By the foregoing, $C_i = C_j = C_{ij}$, \mathbf{P}_{ij} is just \mathbf{P}_j with the i -th coordinate deleted, and \mathbf{P}_{ij} is just \mathbf{P}_i with the $(j - 1)$ -th coordinate deleted.

Considering every such pair, we may define a candidate curve C by $C = C_i$ for all i and $\mathbf{P} \in C^n$ defined as the unique n -tuple which results in \mathbf{P}_i upon deleting the i -th coordinate. By the foregoing, this is well-defined. Now we see that W agrees with $W_{C, \mathbf{P}}$ on all coordinate sublattices of rank $n - 1$. By the inductive statement part (II) and Theorem 2.8, we see that W is determined by its sublattices of rank $n - 1$. Therefore $W = W_{C, \mathbf{P}}$.

To show part (II) of the inductive statement, we observe that if $W(\mathbf{v}) = 0$ for all $\mathbf{v} \in \{\pm 1\}^n$, then $\mathbf{v}(\mathbf{P}) = \mathcal{O}$ for all such \mathbf{v} (by Corollary 5.2). But this is impossible, since it would imply $[2]P_i = \mathcal{O}$ for $1 \leq i \leq n$, a contradiction to non-degeneracy (again Corollary 5.2).

A change of coordinates of the form (21) for C does not change the elliptic net, as it is determined by its values on its coordinate hyperplanes, where this is true. Further, if two tuples *not* related by such a change of coordinates generate the same net W , then the same would hold for some coordinate hyperplane, a contradiction. This demonstrates part (I) of the inductive statement. \square

7. THE CURVE-NET THEOREM

We set some remaining terminology, and then proceed to the statement and proof of the main theorem.

7.1. Homothety and singular elliptic nets. The only changes of coordinates of a Weierstrass equation into another are compositions of unihomothetic changes of coordinates and changes of coordinates of the form $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$, which we refer to as *homotheties* (since they correspond to homotheties of the lattice in the complex uniformization).

Proposition 7.1. *Consider the rank n elliptic net $W_{C, \mathbf{P}}$ associated to*

$$C : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

defined over K and $\mathbf{P} \in C(K)^n$. Let λ be a non-zero element of K . Suppose $\phi_\lambda : C \rightarrow C_\lambda$ is the isomorphism of curves taking C to

$$C_\lambda : y^2 + \lambda a_1 xy + \lambda^3 a_3 y = x^3 + \lambda^2 a_2 x^2 + \lambda^4 a_4 x + \lambda^6 a_6$$

under the change of coordinates $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$. Then

$$\widetilde{W}_{C_\lambda, \phi_\lambda(\mathbf{P})} = \lambda \widetilde{W}_{C, \mathbf{P}}$$

In particular, let δ_{ij} be the Kronecker delta, and define

$$g(\mathbf{v}) = -1 - \sum_{1 \leq i < j \leq n} (-1)^{\delta_{ij}} v_i v_j.$$

Then

$$W_{C_\lambda, \phi_\lambda(\mathbf{P})} = \lambda^{g(\mathbf{v})} W_{C, \mathbf{P}}.$$

Proof. The first statement is entailed by the second. From the general theory of Weierstrass sigma functions, $\sigma(\lambda z, \lambda \Lambda) = \lambda \sigma(z, \Lambda)$. Thus by Definition 3.1, we know that $\Omega_{\mathbf{v}}(\lambda \mathbf{z}; \lambda \Lambda) = \lambda^{g(\mathbf{v})} \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$. As in Section 4, this allows us to conclude that the same holds for $\Psi_{\mathbf{v}}$, so that

$$\Psi_{\mathbf{v}}(\lambda^2 x, \lambda^3 y, \lambda^i \alpha_i) = \lambda^{g(\mathbf{v})} \Psi_{\mathbf{v}}(x, y, \alpha_i),$$

from which the result follows. \square

Therefore we set the following definition

Definition 7.2. If $W : \mathbb{Z}^n \rightarrow K$ is an elliptic net, then with the notation of Proposition 7.1, we define

$$W^\lambda(\mathbf{v}) := \lambda^{g(\mathbf{v})} W(\mathbf{v}).$$

This gives an action of K on elliptic nets $W : \mathbb{Z}^n \rightarrow K$ called the *homothety action*. Two elliptic nets are *homothetic* if they are in the same orbit of the action of K .

The following proposition is immediate.

Proposition 7.3. *Let $W : \mathbb{Z}^n \rightarrow K$ be an elliptic net. Then for any non-zero $\lambda \in K$, W^λ is normalised if and only if W is.*

Let $W : \mathbb{Z}^n \rightarrow K$ be an elliptic net. If the curve C associated to its normalisation is a nodal or cuspidal cubic, then W is called *singular*. If, instead, C is an elliptic curve, then W is called *non-singular*. In either case, the discriminant Δ of W is defined to be the discriminant of the associated Weierstrass equation. Similarly, the j -invariant is the j -invariant of the associated Weierstrass equation. The discriminant of an elliptic net changes by a factor of λ^{12} under homothety, while the j -invariant remains unaltered.

7.2. The curve-net theorem. We may put a partial ordering on tuples (C, P_1, \dots, P_n) where C is a Weierstrass curve and P_i are non-singular points on the curve. We do this by defining

$$(C, P_1, \dots, P_n) \leq (D, Q_1, \dots, Q_m)$$

if and only if $C = D$ and the groups they generate satisfy a containment

$$\langle P_1, \dots, P_n \rangle \subseteq \langle Q_1, \dots, Q_m \rangle.$$

The collection of all elliptic nets is partially ordered by the subnet relation. Collecting our work up to this point, we have now shown:

Theorem 7.4. *For each field K , there is an explicit isomorphism of partially ordered sets*

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

$$\updownarrow$$

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

Non-singular nets correspond to elliptic curves. The action of K (by homothety) on the sets preserves the order and respects the isomorphism. The bijection takes an elliptic net of rank n to a tuple with n points. The elliptic net W associated to a tuple (C, P_1, \dots, P_n) satisfies the property that $W(v_1, \dots, v_n) = 0$ if and only if $v_1 P_1 + \dots + v_n P_n = 0$ on the curve C .

Proof. In the diagram in the statement of the theorem, call the upper set \mathcal{N} and the lower set \mathcal{C} . The first claim is that there is an injective map $\mathcal{N} \rightarrow \mathcal{C}$. Proposition 6.2 shows that each scale equivalence classes in \mathcal{N} contains a unique normalised elliptic net, so we can define the map by Theorem 6.7 (which also guarantees injectivity). Corollary 5.2 shows that the result is an element of \mathcal{C} . This shows the first claim.

The second claim is that there exists an inverse map $\mathcal{C} \rightarrow \mathcal{N}$. The map is given by Definition 5.1, which is well-defined as a result of Theorem 4.6. It is required to check that the resulting elliptic net is normalised (Proposition 3.8) and non-degenerate (Corollary 5.2).

Theorem 6.7 says that this map is indeed an inverse to the map of the first claim. This gives the second claim and the bijection of sets.

It is clear that the bijection associates an elliptic net of rank n to a tuple with n points, and that it preserves the partial ordering. The action of homothety is preserved by Proposition 7.1. And the final statement of the theorem is a result of Corollary 5.2. \square

Remark 7.5. The degenerate cases present several difficulties. One is that a degenerate elliptic net may not be determined by the usual initial set of terms as given in Section 2. For example, the sequence

$$W(n) = \begin{cases} 0 & n \neq k \\ 1 & n = k \end{cases} .$$

is an elliptic net for any integer k . However, some degenerate sequences can be thought of as arising from singular points on a singular cubic. For example, consider a sequence associated to an elliptic curve E and point P both defined over \mathbb{Q} such that P reduces to a singular point modulo some prime p . Then the sequence regarded modulo p as living in \mathbb{F}_p (which is necessarily a degenerate elliptic net) should be associated to a point on the special fibre of the Néron model. It is likely that Theorem 7.4 can be extended to include these cases (this is future work).

REFERENCES

- [1] Mohamed Ayad. Périodicité (mod q) des suites elliptiques et points S -entiers sur les courbes elliptiques. *Ann. Inst. Fourier (Grenoble)*, 43(3):585–618, 1993.
- [2] K. Chandrasekharan. *Elliptic functions*, volume 281 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.
- [3] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, 7(4):385–434, 1986.
- [4] Gunther Cornelissen and Karim Zahidi. Elliptic divisibility sequences and undecidable problems about rational points. *J. Reine Angew. Math.*, 613:1–33, 2007.
- [5] Kirsten Eisenträger and Graham Everest. Descent on elliptic curves and Hilbert’s tenth problem. *Proc. Amer. Math. Soc.*, 137(6):1951–1959, 2009.
- [6] Graham Everest, Gerard Mclaren, and Thomas Ward. Primitive divisors of elliptic divisibility sequences. *J. Number Theory*, 118(1):71–89, 2006.
- [7] Graham Everest, Victor Miller, and Nelson Stephens. Primes generated by elliptic curves. *Proc. Amer. Math. Soc.*, 132(4):955–963 (electronic), 2004.
- [8] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence Sequences*, chapter Elliptic Divisibility Sequences, pages 163–175. American Mathematical Society, Providence, 2003.

- [9] Sergey Fomin and Andrei Zelevinsky. The Laurent phenomenon. *Adv. Appl. Math.*, 28(2):119–144, 2002.
- [10] Gerhard Frey and Tanja Lange. Background on curves and Jacobians. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 45–85. Chapman & Hall/CRC, Boca Raton, FL, 2006.
- [11] George Gasper and Mizan Rahman. *Basic hypergeometric series*, volume 96 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 2004. With a foreword by Richard Askey.
- [12] A. N. W. Hone. Elliptic curves and quadratic recurrence sequences. *Bull. London Math. Soc.*, 37(2):161–171, 2005.
- [13] Patrick Ingram. Multiples of integral points on elliptic curves. *J. Number Theory*, 129(1):182–208, 2009.
- [14] B. Mazur and J. Tate. The p -adic sigma function. *Duke Math. J.*, 62(3):663–688, 1991.
- [15] Bjorn Poonen. Hilbert’s tenth problem and Mazur’s conjecture for large sub-rings of \mathbb{Q} . *J. Amer. Math. Soc.*, 16(4):981–990 (electronic), 2003.
- [16] James Propp. Robbins forum. <http://jamespropp.org/about-robbins>.
- [17] Rachel Shipsey. *Elliptic Divisibility Sequences*. PhD thesis, Goldsmiths, University of London, 2001.
- [18] Joseph H. Silverman. Common divisors of elliptic divisibility sequences over function fields. *Manuscripta Math.*, 114(4):431–446, 2004.
- [19] Joseph H. Silverman. p -adic properties of division polynomials and elliptic divisibility sequences. *Math. Ann.*, 332(2):443–471 (Addendum 473–474), 2005.
- [20] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [21] Katherine E. Stange. The Tate pairing via elliptic nets. In *Pairing-Based Cryptography - PAIRING 2007*, volume 4575 of *Lecture Notes in Comput. Sci.*, pages 329–348. Springer, Berlin, 2007.
- [22] Marco Streng. Divisibility sequences for elliptic curves with complex multiplication. *Algebra Number Theory*, 2(2):183–208, 2008.
- [23] Christine Swart. *Elliptic curves and related sequences*. PhD thesis, Royal Holloway and Bedford New College, University of London, 2003.
- [24] Alfred J. van der Poorten. Elliptic curves and continued fractions. *J. Integer Seq.*, 8(2):Article 05.2.5, 19 pp. (electronic), 2005.
- [25] Alfred J. van der Poorten and Christine S. Swart. Recurrence relations for elliptic sequences: every Somos 4 is a Somos k . *Bull. London Math. Soc.*, 38(4):546–554, 2006.
- [26] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.
- [27] Chu Wenchang, Shalosh B. Ekhad, and Robin J. Chapman. Problems and Solutions: Solutions: 10226. *Amer. Math. Monthly*, 103(2):175–177, 1996.

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, 8888 UNIVERSITY DRIVE, BURNABY, BC, CANADA V5A 1S6, AND PACIFIC INSTITUTE FOR THE MATHEMATICAL SCIENCES, 200 1933 WEST MALL, VANCOUVER, BC, CANADA V6T 1Z2

E-mail address: `kestange@pims.math.ca`