ON SYMMETRIES OF ELLIPTIC NETS AND VALUATIONS OF NET POLYNOMIALS

AMIR AKBARY, JEFF BLEANEY, AND SOROOSH YAZDANI

ABSTRACT. Under certain conditions, we prove that the set of zeros of an elliptic net forms an Abelian group. We present two applications of this fact. Firstly we give a generalization of a theorem of Ayad on valuations of division polynomials in the context of net polynomials. Secondly we generalize a theorem of Ward on symmetry of elliptic divisibility sequences to the case of elliptic nets.

CONTENTS

1. INTRODUCTION

Let E be an elliptic curve defined over a field K with the Weierstrass model $f(x,y)=0$, where

$$f(x,y) := y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6;\ a_i \in K. \tag{1.1}$$

It is known that there are polynomials $\phi_n,\ \psi_n$, and $\omega_n \in K[x,y]/\langle f(x,y)\rangle$ such that for any $P \in E(K)$, the group of K-rational points of E, we have

$$nP = \left(\frac{\phi_n(P)}{\psi_n^2(P)}, \frac{\omega_n(P)}{\psi_n^3(P)}\right). \tag{1.2}$$

Moreover, ψ_n satisfies the recursion

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2, \tag{1.3}$$

with initial conditions

$$\psi_1 = 1,\ \psi_2 = 2y + a_1x + a_3,\ \psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$
$$\psi_4 = \psi_2 \cdot \left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\right).$$

Date: August 29, 2014.
2010 *Mathematics Subject Classification.* 11G05, 11G07, 11B37.
Key words and phrases. elliptic divisibility sequences, division polynomials, elliptic nets, net polynomials.
Research of the authors is partially supported by NSERC.

Here

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

The polynomial ψ_n is called the *n-th division polynomial* associated to E. (See [3, Chapter 2] for the basic properties of division polynomials.)

Now let K be a field with a discrete valuation ν, let $\mathcal{O}_\nu = \{x \in K : \nu(x) \geq 0\}$ and $\mathfrak{p} = \{x \in K : \nu(x) > 0\}$. In [1, Theorem A], Ayad proved the following theorem on the valuation of $\psi_n(P)$.

Theorem 1.1 (Ayad). *Let E/K be an elliptic curve defined by the polynomial* (1.1) *with $a_i \in \mathcal{O}_\nu$ for $i = 1, 2, 3, 4, 6$. Let $P \in E(K)$ be a point in $E(K)$ such that $P \not\equiv \infty \pmod{\mathfrak{p}}$. Then the following assertions are equivalent:*

(a) $\nu(\psi_2(P))$ and $\nu(\psi_3(P)) > 0$.
(b) For all integers $n \geq 2$, we have $\nu(\psi_n(P)) > 0$.
(c) There exists an integer $n_0 \geq 2$ such that $\nu(\psi_{n_0}(P))$ and $\nu(\psi_{n_0+1}(P)) > 0$.
(d) There exists an integer $m_0 \geq 2$ such that $\nu(\psi_{m_0}(P))$ and $\nu(\phi_{m_0}(P)) > 0$.
(e) Reduction of P modulo $\mathfrak{p}$ is singular.

An important ingredient of the proof of the above theorem is the recursion (1.3). Generally, any solution over an arbitrary integral domain R of the recursion

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2, \tag{1.4}$$

where $m, n \in \mathbb{Z}$, is called an *elliptic sequence*. Hence the sequence $(\psi_n(P))$ is an example of an elliptic sequence. The theory of elliptic sequences was developed by Morgan Ward in 1948. An *elliptic divisibility sequence* (EDS) is an integer elliptic sequence (W_n), which is also a divisibility sequence (i.e. $W_m \mid W_n$ if $m \mid n$).

Theorem 1.1 has an immediate application to elliptic denominator sequences, which we will define now. Let $E/\mathbb{Q}$ be an elliptic curve defined by (1.1), with $a_i \in \mathbb{Z}$ for $i = 1, 2, 3, 4, 6$, and let $P \in E(\mathbb{Q})$ be a non-torsion point. It is known that

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

with $\gcd(A_P, D_P) = \gcd(B_P, D_P) = 1$ and $D_P \geq 1$ (see [2, Proposition 7.3.1]). Let (D_{nP}) be the sequence of denominators of the multiples of P. More precisely D_{nP} is given by the identity

$$nP = \left(\frac{A_{nP}}{D_{nP}^2}, \frac{B_{nP}}{D_{nP}^3}\right) \tag{1.5}$$

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

Comparing equations (1.5) and (1.2) we expect a close relation between $\psi_n(P)$ and D_{nP}. In particular, for any prime p we have that

$$\nu_p(x(nP)) = \nu_p(A_{nP}) - 2\nu_p(D_{nP}) = \nu_p(\phi_n(P)) - 2\nu_p(\psi_n(P)), \tag{1.6}$$

where ν_p is the p-adic valuation on $\mathbb{Q}$ and $x(nP)$ is the x coordinate of nP.

From construction of division polynomials we know that if $p \nmid D_p$ then $\nu_p(\psi_n(P)) \geq 0$ and $\nu_p(\phi_n(P)) \geq 0$. Now Theorem 1.1 tells us that if P reduces to a non-singular point and if P modulo p is different from ∞ (i.e. $p \nmid D_P$), then $\nu_p(\psi_n(P))\nu_p(\phi_n(P)) = 0$. Under these conditions if $\nu_p(x(nP)) \geq 0$ then by (1.6) and the fact that A_{nP} and D_{nP} are coprime to each other, we have $\nu_p(D_{nP}) = \nu_p(\psi_n(P)) = 0$. Similarly, if $\nu_p(x(nP)) < 0$ then $\nu_p(D_{nP}) = \nu_p(\psi_n(P)) = -\frac{1}{2}\nu_p(x(nP))$.

Therefore, we have the following proposition.

Proposition 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve over the rationals given by equation* (1.1)*, and assume that $a_i \in \mathbb{Z}$. Furthermore, let $P \in E(\mathbb{Q})$ be a point of infinite order such that $P \not\equiv \infty \pmod{p}$ and let (D_{nP}) be the elliptic denominator sequence associated to E and P. Then for a prime p if $P \pmod{p}$ is non-singular, we have*

$$\nu_p(D_{nP}) = \nu_p(\psi_n(P)).$$

Remark 1.3. (a) One can drop the condition $P \not\equiv \infty \pmod{p}$ in the previous proposition and prove a stronger result for an scaled version of $\psi_n(P)$. Let

$$\hat{\psi}_n(P) := D_P^{n^2}\psi_n(P).$$

Then if $P \pmod{p}$ is non-singular for all primes p, we have

$$D_{nP} = |\hat{\psi}_n(P)|.$$

(See [1]). For a proof of this fact (in more general case of elliptic nets) see Proposition 1.7.
(b) Formulas for explicit valuations of $\psi_n(P)$ at primes p (of good or bad reduction) are given in [8]. Also in [5] the sign of $\psi_n(P)$ is computed explicitly.

In [7], Stange generalized the concept of an elliptic sequence to an n-dimensional array, called an elliptic net. In this paper we give a generalization of Ayad's theorem for net polynomials.

Definition 1.4. *Let A be a free Abelian group of finite rank, and R be an integral domain. Let $\mathbf{0}$ and 0 be the additive identity elements of A and R respectively. An elliptic net is any map $W : A \to R$ for which $W(\mathbf{0}) = 0$, and that satisfies*

$$\begin{aligned} &W(\mathbf{p}+\mathbf{q}+\mathbf{s})W(\mathbf{p}-\mathbf{q})W(\mathbf{r}+\mathbf{s})W(\mathbf{r}) \\ &\qquad + W(\mathbf{q}+\mathbf{r}+\mathbf{s})W(\mathbf{q}-\mathbf{r})W(\mathbf{p}+\mathbf{s})W(\mathbf{p}) \\ &\qquad\qquad + W(\mathbf{r}+\mathbf{p}+\mathbf{s})W(\mathbf{r}-\mathbf{p})W(\mathbf{q}+\mathbf{s})W(\mathbf{q}) = 0, \quad (1.7)\end{aligned}$$

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

Note that if $A = \mathbb{Z}$ and $W : A \to R$ is an elliptic net, then by setting $\mathbf{p} = m$, $\mathbf{q} = n$, $\mathbf{r} = 1$, and $\mathbf{s} = 0$ in (1.7), and noting that W is an odd function, we get that $W(n)$ satisfies equation (1.4), hence $(W(n))$ is an elliptic sequence. Therefore elliptic nets are a generalization of elliptic sequences.

We can relate elliptic nets to elliptic curves in the following way. For an arbitrary field K, let

$$S = K[x_1, y_1, \cdots, x_r, y_r],$$

and consider the polynomial ring

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

where f is the defining polynomial (1.1) for E. Let $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$ and $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$. From [7, Section 4] follows that there exist "polynomials" $\Psi_{\mathbf{v}}, \Phi_{\mathbf{v}}, \overline{\Omega}_{\mathbf{v}} \in \mathcal{R}_r$ such that $\Psi_{\mathbf{v}}$ (as a function of $\mathbf{v} \in \mathbb{Z}^r$) is an elliptic net and

$$\mathbf{v} \cdot \mathbf{P} = v_1 P_1 + v_2 P_2 + \cdots + v_r P_r = \left(\frac{\Phi_{\mathbf{v}}(\mathbf{P})}{\Psi_{\mathbf{v}}^2(\mathbf{P})}, \frac{\overline{\Omega}_{\mathbf{v}}(\mathbf{P})}{\Psi_{\mathbf{v}}^3(\mathbf{P})} \right). \tag{1.8}$$

The "polynomial" $\Psi_{\mathbf{v}}$ is called the $\mathbf{v}$-*th net polynomial* associated to E. Also, the function $\mathbf{v} \mapsto \Psi_{\mathbf{v}}(\mathbf{P})$ is called *the elliptic net* associated to E and $\mathbf{P}$. In [7], Stange also proves that when $r > 1$, then we can compute $\Psi_{\mathbf{v}}$ using the recurrence relation (1.7) and the initial values $\Psi_{\mathbf{v}}$ for $\mathbf{v} = \mathbf{e}_i$, $\mathbf{v} = 2\mathbf{e}_i$, $\mathbf{v} = \mathbf{e}_i + \mathbf{e}_j$ and $\mathbf{v} = 2\mathbf{e}_i + \mathbf{e}_j$, where $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_r\}$ is the standard basis for $\mathbb{Z}^r$. (For $r = 1$ the recurrence (1.3) shows that ψ_n is uniquely determined by ψ_1, ψ_2, ψ_3, and ψ_4.) Note that the initial values of $\Psi_{\mathbf{v}}$ are defined as follows:

$$\begin{aligned} &\Psi_{\mathbf{e_i}} = 1, \ \Psi_{\mathbf{2e_i}} = 2y_i + a_1 x_i + a_3, \ \Psi_{\mathbf{e_i+e_j}} = 1, \\ &\Psi_{\mathbf{2e_i+e_j}} = 2x_i + x_j - \left(\frac{y_j - y_i}{x_j - x_i} \right)^2 - a_1 \left(\frac{y_j - y_i}{x_j - x_i} \right) + a_2. \end{aligned} \tag{1.9}$$

The above initial conditions define the $\mathbf{v}$-th net polynomials of rank $r > 1$ for any elliptic curves completely. We refer the reader to Theorem 2.5, Lemma 2.6, and Theorem 2.8 of [7] for the details of how this can be done.

In this paper, we prove the following generalization of Theorem 1.1 for net polynomials. Let K, ν, $\mathcal{O}_\nu$, and $\mathfrak{p}$ be defined as before.

Theorem 1.5. *Let E/K be an elliptic curve defined by the polynomial* (1.1) *with $a_i \in \mathcal{O}_\nu$ for $i = 1, 2, 3, 4, 6$. Let $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$ be such that $P_i \not\equiv \infty \pmod{\mathfrak{p}}$, for $1 \le i \le r$, and $P_i \pm P_j \not\equiv \infty \pmod{\mathfrak{p}}$, for $1 \le i < j \le r$. Then the following are equivalent:*

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

$$\nu(\Psi_{2\mathbf{e}_i}(\mathbf{P})) > 0 \text{ and } \nu(\Psi_{3\mathbf{e}_i}(\mathbf{P})) > 0.$$

(b) There exists $1 \le i \le r$ such that for all $n \ge 2$ we have

$$\nu(\Psi_{n\mathbf{e}_i}(\mathbf{P})) > 0.$$

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

$$\nu(\Psi_{\mathbf{v}}(\mathbf{P})) > 0 \text{ and } \nu(\Psi_{\mathbf{v}+\mathbf{e}_i}(\mathbf{P})) > 0.$$

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

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

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

To prove this, we first need to show that $\nu(\Psi_{\mathbf{v}}(\mathbf{P})) \ge 0$ in the cases we are dealing with. This result is of independent interest, so we record it in the following proposition.

Proposition 1.6. *Let E/K be an elliptic curve defined by the polynomial* (1.1) *with $a_i \in \mathcal{O}_\nu$ for $i = 1, 2, 3, 4, 6$, and let $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$. When $r = 1$, assume that $P_1 \not\equiv \infty \pmod{\mathfrak{p}}$. When $r > 1$, then assume that for all $1 \le i < j \le r$ we have $P_i \not\equiv \infty \pmod{\mathfrak{p}}$ and $P_i \pm P_j \not\equiv \infty \pmod{\mathfrak{p}}$. Then for all $\mathbf{v} \in \mathbb{Z}^r$ we have*

$$\nu(\Psi_{\mathbf{v}}(\mathbf{P})) \ge 0,$$

hence $\Psi_{\mathbf{v}}(\mathbf{P}) \in \mathcal{O}_\nu$.

Next we specialize to the case that E is defined over $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve, and let $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(\mathbb{Q})^r$ be r linearly independent points in $E(\mathbb{Q})$. For $\mathbf{v} = (v_1, v_2, \cdots, v_r) \in \mathbb{Z}^r$, let $\mathbf{v} \cdot \mathbf{P} = v_1P_1 + \cdots + v_rP_r$. We denote the *elliptic denominator net* associated to E and P by $(D_{\mathbf{v}\cdot\mathbf{P}})$, where $D_{\mathbf{v}\cdot\mathbf{P}}$ is the denominator of $\mathbf{v} \cdot \mathbf{P}$. More precisely,

$$\mathbf{v} \cdot \mathbf{P} = v_1P_1 + v_2P_2 + \cdots + v_rP_r = \left(\frac{A_{\mathbf{v}\cdot\mathbf{P}}}{D^2_{\mathbf{v}\cdot\mathbf{P}}}, \frac{B_{\mathbf{v}\cdot\mathbf{P}}}{D^3_{\mathbf{v}\cdot\mathbf{P}}}\right). \tag{1.10}$$

We are interested in the relation between the element $D_{\mathbf{v}\cdot\mathbf{P}}$ of the elliptic denominator net, and the value of the $\mathbf{v}$-th net polynomial $\Psi_{\mathbf{v}}$ at $\mathbf{P}$. An immediate corollary of Theorem 1.5 is that for all but finitely many primes p we have

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

where ν_p is the p-adic valuation. We extend this result, however similar to Remark 1.3 (a), we need to multiply $\Psi_{\mathbf{v}}$ at $\mathbf{P}$ with a quadratic form to obtain an equivalent net polynomial $\hat{\Psi}_{\mathbf{v}}$. More precisely, by using notation (1.10), let

$$F_{\mathbf{v}}(\mathbf{P}) = \prod_{1\leq i\leq j\leq r} A_{ij}^{v_iv_j}, \tag{1.11}$$

where

$$A_{ii} = D_{\mathbf{e}_i\cdot\mathbf{P}} = D_{P_i}, \text{ and } A_{ij} = \frac{D_{P_i+P_j}}{D_{P_i}D_{P_j}} \text{ for } i \neq j.$$

Then $F(\mathbf{P}) : \mathbb{Z}^r \to K^\times$ defined by $\mathbf{v} \mapsto F_{\mathbf{v}}(\mathbf{P})$ is a quadratic form. Define

$$\hat{\Psi}_{\mathbf{v}}(\mathbf{P}) = F_{\mathbf{v}}(\mathbf{P})\Psi_{\mathbf{v}}(\mathbf{P}),$$

for all $\mathbf{v} \in \mathbb{Z}^r$. Then $\hat{\Psi}(\mathbf{P})$ is an elliptic net that is scale equivalent to $\Psi(\mathbf{P})$ (see Section 2 for more explanation). Furthermore, notice that

$$\hat{\Psi}_{\mathbf{e}_i}(\mathbf{P}) = F_{\mathbf{e}_i}(\mathbf{P})\Psi_{\mathbf{e}_i}(\mathbf{P}) = A_{ii} = D_{\mathbf{e}_i\cdot\mathbf{P}},$$

and

$$\hat{\Psi}_{\mathbf{e}_i+\mathbf{e}_j}(\mathbf{P}) = F_{\mathbf{e}_i+\mathbf{e}_j}(\mathbf{P})\Psi_{\mathbf{e}_i+\mathbf{e}_j}(\mathbf{P}) = A_{ii}A_{jj}A_{ij} = D_{P_i+P_j} = D_{(\mathbf{e}_i+\mathbf{e}_j)\cdot\mathbf{P}}.$$

We will prove the following generalization of Proposition 1.2.

Proposition 1.7. *Let $E/\mathbb{Q}$ be an elliptic net defined by polynomial* (1.1) *with $a_i \in \mathbb{Z}$ for $i = 1, 2, 3, 4, 6$. Let $\mathbf{P} = (P_1, \ldots, P_r) \in E(\mathbb{Q})^r$ be an r-tuple consisting of r linearly independent points in $E(\mathbb{Q})$. Let p be a prime so that $P_i \pmod p$ is non-singular for $1 \leq i \leq r$. Then*

$$\nu_p(D_{\mathbf{v}\cdot\mathbf{P}}) = \nu_p(\hat{\Psi}_{\mathbf{v}}(\mathbf{P})),$$

for all $\mathbf{v} \in \mathbb{Z}^r$. In particular, if for all primes p and all integers $1 \leq i \leq r$ we have that $P_i \pmod p$ is nonsingular, then

$$D_{\mathbf{v}\cdot\mathbf{P}} = |\hat{\Psi}_{\mathbf{v}}(\mathbf{P})|.$$

Section 5 includes proofs of Propositions 1.6, 1.7, and Theorem 1.5. Also see Examples 5.1 and 5.2 for concrete descriptions of Proposition 1.7.

To prove Theorem 1.5, we need to study the behaviour of zeros of an elliptic net $W : \mathbb{Z}^r \to K$, where K is an arbitrary field. Recall that for the values of rank 1 elliptic nets (i.e. elliptic sequences), we have the concept of *rank of apparition*. More precisely, for any elliptic sequence (W_n) we say that a natural number ρ is a rank of apparition if $W_\rho = 0$ and $W_m \neq 0$ for any $m|\rho$. We say a sequence has *a unique rank of apparition* ρ (> 1) if $W_k = 0$ if and only if $\rho|k$. Motivated by this definition, we say an elliptic net $W : \mathbb{Z}^r \to K$ has a *unique rank of apparition with respect to the standard basis* if each sequence $(W(n\mathbf{e}_1)),\ (W(n\mathbf{e}_2)),\ \dots,\ (W(n\mathbf{e}_r))$ has a unique rank of apparition. In general, it is convenient to have a definition that works for a free finitely generated Abelian group A, rather than $\mathbb{Z}^r$.

Definition 1.8. *Let $W : A \to K$ be an elliptic net of rank r. Let $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_r\}$ be a basis for A. We say that W has a* unique rank of apparition with respect to $\mathcal{B}$ *if there exists an r-tuple $(\rho_1, \rho_2, \dots, \rho_r)$ of positive integers with $\rho_i > 1$ for $1 \le i \le r$, such that*

$$W(n\mathbf{b}_i) = 0 \iff \rho_i \mid n,$$

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

Note that an elliptic sequence (W_n) has a unique rank of apparition if its corresponding net $n \mapsto W_n$ has a unique rank of apparition with respect to $\{1\}$.

We remark here another possible generalization of a unique rank of apparition of a sequence. Namely, for a sequence $W : \mathbb{Z} \to K$, having a unique rank of apparition is the same as $\Lambda = \{v \in \mathbb{Z} :\ W(v) = 0\}$ being a subgroup of $\mathbb{Z}$. Therefore, a natural generalization of the concept of unique rank of apparition to elliptic nets $W : A \to K$ is that $\Lambda = W^{-1}(0) = \{\mathbf{v} \in A :\ W(\mathbf{v}) = 0\}$ to be a subgroup of A. The following theorem shows that our concept of unique rank of apparition implies that Λ is a subgroup of A.

Theorem 1.9. *Let $W : A \to K$ be an elliptic net, and let $\mathcal{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_r\}$ be a basis for A. Assume that W has a unique rank of apparition with respect to $\mathcal{B}$. Let*

$$\Lambda = W^{-1}(0) = \{\mathbf{v} \in A :\ W(\mathbf{v}) = 0\}$$

be the zero set of W. Then Λ is a full rank subgroup of A.

We prove Theorem 1.9 in Section 3.

The proof of Theorem 1.5 comes as a combination of Theorems 1.1, 1.9 and the following theorem.

Theorem 1.10 (Ward). *Let (W_n) be an elliptic sequence. A necessary and sufficient condition that (W_n) does not have a unique rank of apparition is that $W_3 = W_4 = 0$.*

The proof of Theorem 1.10 is analogous to [9, Theorem 6.2] where the case of an integer elliptic sequence modulo p has been considered.

Here we describe another application of Theorem 1.9. Let $W_n = \hat{\psi}_n(P)$ as defined in Remark 1.3 (a). Then Proposition 1.2 tells us that in many cases, we can think of W_n as the denominator of the point nP for some elliptic curve $E/\mathbb{Q}$ and some point $P \in E(\mathbb{Q})$. Now let p be a prime of good reduction and let n_p be the order of the point P in $E(\mathbb{F}_p)$, where $\mathbb{F}_p$ is the finite field of p elements. Then we have that $(n_p + k)P \equiv kP \pmod{p}$. Therefore, it is tempting to assume that $W_{n_p+k} \equiv W_k \pmod{p}$. More generally, let $W : \mathbb{Z} \to K$ be an elliptic sequence with ρ the unique rank of apparition of W. Then, one may speculate that $W_{\rho+k} = W_k$. This in fact is not true. However, in [9] the following is proved.

Theorem 1.11 (Ward's Symmetry Theorem). *Let (W_n) be an elliptic sequence and assume $W_2W_3 \neq 0$. Let $\rho > 1$ be the unique rank of apparition of W. Then there exists $a, b \in K$ such that*

$$W_{m\rho+n} = a^{m^2} b^{mn} W_n$$

for all $m, n \in \mathbb{Z}$.

See Theorem 9.2 of [9] for a proof and Theorem 8.2 of [9] for some properties of elements a and b, when $K = \mathbb{F}_p$. Note that the proofs also work for any field K.

The following theorem gives a generalization of Theorem 1.11.

Theorem 1.12. *Let $W : A \to K$ be an elliptic net with the property that $\Lambda = W^{-1}(0)$ is a subgroup of A and assume $|A/\Lambda| \geq 4$. Then, there exist well defined functions $\xi : \Lambda \to K^\times$ and $\chi : \Lambda \times A \to K^\times$ such that*

$$W(\boldsymbol{\lambda} + \mathbf{v}) = \xi(\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, \mathbf{v})W(\mathbf{v})\ for\ all\ \boldsymbol{\lambda} \in \Lambda\ and\ all\ \mathbf{v} \in A,$$

and the functions ξ and χ satisfy the following properties:

(i) χ *is bilinear,*
(ii) $\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2) = \chi(\boldsymbol{\lambda}_2, \boldsymbol{\lambda}_1)$,
(iii) $\xi(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2) = \xi(\boldsymbol{\lambda}_1)\xi(\boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2)$,
(iv) $\xi(-\boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})$*, and*
(v) $\xi(\boldsymbol{\lambda})^2 = \chi(\boldsymbol{\lambda}, \boldsymbol{\lambda})$.

Furthermore, the functions $\chi(\boldsymbol{\lambda}, \mathbf{p})$ and $\xi(\boldsymbol{\lambda})$, are defined by

$$\begin{array}{rccc} \delta : & \Lambda \times (A \setminus \Lambda) & \longrightarrow & K^\times \\ & (\boldsymbol{\lambda}, \mathbf{p}) & \longmapsto & \frac{W(\boldsymbol{\lambda}+\mathbf{p})}{W(\mathbf{p})}, \end{array}$$

and relations

$$\begin{array}{rccc} \chi : & \Lambda \times A & \longrightarrow & K^\times \\ & (\boldsymbol{\lambda}, \mathbf{p}) & \longmapsto & \frac{\delta(\boldsymbol{\lambda},\mathbf{p}+\mathbf{v})}{\delta(\boldsymbol{\lambda},\mathbf{v})}, \end{array}$$

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

$$\begin{array}{rccc} \xi : & \Lambda & \longrightarrow & K^\times \\ & \boldsymbol{\lambda} & \longmapsto & \frac{\delta(\boldsymbol{\lambda},\mathbf{v})}{\chi(\boldsymbol{\lambda},\mathbf{v})}, \end{array}$$

for any $\mathbf{v} \in A \setminus \Lambda$.

Note that under conditions of Theorem 1.11, by considering $\boldsymbol{\lambda} = m\rho$ and $\mathbf{v} = n$ in the previous theorem and applying the bilinearity of χ and Corollary 4.4, we obtain

$$W(m\rho + n) = \xi(m\rho)\chi(m\rho, n)W(n) = \xi(\rho)^{m^2}\chi(\rho, 1)^{mn}W(n).$$

Thus, by letting $a = \xi(\rho)$ and $b = \chi(\rho, 1)$ we have the assertion of Theorem 1.11.

We remark here that in [6], Stange relates some of the functions given in Theorem 1.12 to the Tate pairing on E. Furthermore, special cases of the above formula does show up in her thesis. However to the best of our knowledge, the statement of the above theorem is new.

Given the properties of χ and ξ, for any $r \in \mathbb{N}$, any $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \ldots, \boldsymbol{\lambda}_r \in \Lambda$, and any $n_1, n_2, \ldots, n_r \in \mathbb{Z}$, we get that

$$W\left(\left(\sum_{i=1}^{r} n_i\boldsymbol{\lambda}_i\right) + \mathbf{v}\right) = \left(\prod_{i=1}^{r} \xi(\boldsymbol{\lambda}_i)^{n_i^2}\chi(\boldsymbol{\lambda}_i, \mathbf{v})^{n_i}\left(\prod_{j=1}^{i-1} \chi(\boldsymbol{\lambda}_i, \boldsymbol{\lambda}_j)^{n_i n_j}\right)\right)W(\mathbf{v}). \tag{1.12}$$

As a simple corollary of the above identity, we have the following periodicity result.

Corollary 1.13. *Let $W : A \to \mathbb{F}_q$ be an elliptic net, and let $\Lambda = W^{-1}(0)$. Assume that Λ is a subgroup of A and $|A/\Lambda| \geq 4$. Then $W(\mathbf{v}_1) = W(\mathbf{v}_2)$ if $\mathbf{v}_1 \equiv \mathbf{v}_2 \pmod{(q-1)}$.*

We can also employ (1.12) in computing elliptic nets with values in finite fields (See Example 4.5 for a description). Section 4 is dedicated to proofs of Theorem 1.12 and its corollaries.

2. Review of Elliptic Nets

We will collect some basic facts about elliptic nets in this section for sake of completion. Recall that for a free Abelian group A and an integral domain R, we defined an elliptic net to be any map $W : A \to R$ with $W(\mathbf{0}) = 0$ and

$$W(\mathbf{p}+\mathbf{q}+\mathbf{s})W(\mathbf{p}-\mathbf{q})W(\mathbf{r}+\mathbf{s})W(\mathbf{r}) \\ + W(\mathbf{q}+\mathbf{r}+\mathbf{s})W(\mathbf{q}-\mathbf{r})W(\mathbf{p}+\mathbf{s})W(\mathbf{p}) \\ + W(\mathbf{r}+\mathbf{p}+\mathbf{s})W(\mathbf{r}-\mathbf{p})W(\mathbf{q}+\mathbf{s})W(\mathbf{q}) = 0,$$

for all $\mathbf{p}, \mathbf{q}, \mathbf{r}$, and $\mathbf{s} \in A$. Also recall that the rank of an elliptic net is defined to be the rank of its domain A.

Lemma 2.1. *Let $W : A \to R$ be an elliptic net.*

(a) For any integral domain R' and any morphism $\pi : R \to R'$, the function $\pi \circ W : A \to R'$ is an elliptic net,

(b) For any subgroup $A' \subset A$, the function $W|_{A'} : A' \to R$ is an elliptic net.

(c) For any $\mathbf{v} \in A$ we have $W(-\mathbf{v}) = -W(\mathbf{v})$,

Proof. To prove the first two parts of this lemma, note that both $W|_{A'}$ and $\pi \circ W$ satisfy the elliptic net recurrence (1.7). To prove $W(-\mathbf{v}) = -W(\mathbf{v})$, observe that if $W(\mathbf{v}) = W(-\mathbf{v}) = 0$, then we are done. Otherwise, assume without loss of generality that $W(\mathbf{v}) \neq 0$. Then by setting $\mathbf{p} = \mathbf{q} = \mathbf{v}$ and $\mathbf{r} = \mathbf{s} = \mathbf{0}$ in (1.7) we have

$$W(\mathbf{v})^3(W(\mathbf{v}) + W(-\mathbf{v})) = 0.$$

Since R is an integral domain, we get $W(-\mathbf{v}) = -W(\mathbf{v})$. □

We have already remarked that the values of an elliptic net of rank 1 form an elliptic sequence. Let $W : A \to R$ be any elliptic net, and let $\mathbf{v} \in A$. Then by part (b) of the above lemma, $W|_{\mathbf{v}\mathbb{Z}} : \mathbb{Z} \to R$ is an elliptic net of rank 1. Also, note that if R is an integral domain and $K = \mathrm{Frac}(R)$, the fraction field of R, then $i : R \to K$ is injective. Therefore $i \circ W : A \to K$ is an elliptic net, and $(i \circ W)^{-1}(0) = W^{-1}(0)$. Therefore we are not losing any generality in Theorems 1.9 and 1.12 by focusing on elliptic nets having entries in a field.

Next we are interested in relating elliptic nets with linear combination of points on elliptic curves. In order to do this we review some results of [7] on net polynomials.

For a complex lattice $\Lambda \subset \mathbb{C}$, let $\sigma : \mathbb{C} \to \mathbb{C}$ be the Weierstrass σ function

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

Fix an r-tuple $\mathbf{z} = (z_1, z_2, \ldots, z_r) \in \mathbb{C}^r$ with $z_i \notin \Lambda$ and $z_i + z_j \notin \Lambda$. For an r-tuple $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$ define

$$\Omega_{\mathbf{v}}(\mathbf{z}) = \Omega_{\mathbf{v}}(\mathbf{z};\Lambda) = (-1)^{\sum_{1\leq i\leq j\leq r} v_i v_j + 1} \frac{\sigma(v_1 z_1 + v_2 z_2 + \cdots + v_r z_r)}{\left(\prod_{i=1}^r \sigma(z_i)^{2v_i^2 - \sum_{j=1}^r v_i v_j}\right)\left(\prod_{1\leq i<j\leq r} \sigma(z_i + z_j)^{v_i v_j}\right)}.$$

Theorem 2.2 (Stange). *The function*

$$\begin{array}{rccc} \Omega = \Omega(\mathbf{z};\Lambda) : & \mathbb{Z}^r & \longrightarrow & \mathbb{C} \\ & \mathbf{v} & \longmapsto & \Omega_{\mathbf{v}}(\mathbf{z}), \end{array}$$

is an elliptic net.

Proof. See [7, Theorem 3.7]. □

Now let $E/\mathbb{C}$ be an elliptic curve, and let Λ_E be the lattice corresponding to E. Let $\mathbf{P} = (P_1, \ldots, P_r) \in E(\mathbb{C})^r$ with $P_i, P_i + P_j \neq \infty$ and let $\mathbf{z} = (z_1, \ldots, z_r) \in \mathbb{C}^r$ be such that z_i maps to P_i under the uniformization map

$$\mathbb{C} \to \mathbb{C}/\Lambda_E \simeq E(\mathbb{C}).$$

Then the function

$$\begin{array}{rccc} \Psi(\mathbf{P}; E): & \mathbb{Z}^r & \longrightarrow & \mathbb{C} \\ & \mathbf{v} & \longmapsto & \Omega_{\mathbf{v}}(\mathbf{z}), \end{array}$$

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

Let $S^{\text{univ}} = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6]$, and for any positive integer r let

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

where $f(x, y)$ is given by (1.1). Then for every elliptic curve E/K defined by the polynomial (1.1), and $\mathbf{P} \in E(K)^r$ with $P_i, P_i \pm P_j \neq \infty$, we can find a morphism

$$\pi = \pi_{\mathbf{P};E} : \mathcal{R}_r^{\text{univ}} \to K$$

so that $\pi(\alpha_i) = a_i$, and $(\pi(x_i), \pi(y_i)) = P_i$. The following result is proved in [7, section 4].

Theorem 2.3 (Stange). *For each $\mathbf{v} \in \mathbb{Z}^r$, there is $\Psi_{\mathbf{v}}^{univ} \in \mathcal{R}_r^{univ}$ so that $\Psi^{univ} : \mathbf{v} \mapsto \Psi_{\mathbf{v}}^{univ}$ is an elliptic net, and for any elliptic curve $E/\mathbb{C}$ and $\mathbf{P} \in E(\mathbb{C})^r$ with $P_i, P_i \pm P_j \neq \infty$ we have*

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

Let $\mathcal{R}_r^{\text{univ}}$, S^{univ}, and E/K be as before. Then, there exists a map $\pi_E : S^{\text{univ}} \to K$, so that $\pi_E(\alpha_i) = a_i$. This induces a map

$$(\pi_E)_* : \mathcal{R}_r^{\text{univ}} \to K[x_i, y_i]_{1 \leq i \leq r}[(x_i - x_j)^{-1}]_{1 \leq i < j \leq r} / \langle f(x_i, y_i) \rangle_{1 \leq i \leq r}.$$

Then part (a) of lemma 2.1 shows that $\Psi : \mathbf{v} \mapsto (\pi_E)_*(\Psi_{\mathbf{v}}^{\text{univ}})$ defines an elliptic net with values in

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

We call $\Psi_{\mathbf{v}} \in \mathcal{R}_r$ the $\mathbf{v}$*-th net polynomial* associated to E. Now let $\mathbf{P} \in E(K)^r$ with $P_i, P_i \pm P_j \neq \infty$. Then by part (a) of Lemma 2.1, $\Psi(\mathbf{P}; E) : \mathbf{v} \mapsto \Psi_{\mathbf{v}}(\mathbf{P})$ is an elliptic net with values in K. We call $\Psi(\mathbf{P}; E)$ the *elliptic net associated to* $E(\text{over } K)$ *and* $\mathbf{P}$.

Here we note that $\Psi_{n\mathbf{e}_i}(\mathbf{P}) = \psi_n(P_i)$. Moreover, we remark that for E/K defined by the polynomial (1.1), we can compute $\Psi_{\mathbf{v}}$ explicitly. In fact for $\mathbf{v} \in \{\mathbf{e}_i, 2\mathbf{e}_i, \mathbf{e}_i + \mathbf{e}_j, 2\mathbf{e}_i + \mathbf{e}_j : i \neq j\}$, the exact values of $\Psi_{\mathbf{v}}$ are given by (1.9). Furthermore, as we pointed out in the introduction, Theorem 2.5, Lemma 2.6, and Theorem 2.8 of [7] prove that these initial conditions are sufficient for computing $\Psi_{\mathbf{v}}$ for any $\mathbf{v} \in \mathbb{Z}^r$.

Example 2.4. If we let $(\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s}) = (\mathbf{e}_i + \mathbf{e}_j, \mathbf{e}_i \pm \mathbf{e}_k, -\mathbf{e}_i, -\mathbf{e}_i)$, then from (1.7) we get that

$$\Psi_{\mathbf{e}_i+\mathbf{e}_j\pm\mathbf{e}_k}\Psi_{\mathbf{e}_j\mp\mathbf{e}_k}\Psi_{-2\mathbf{e}_i}\Psi_{-\mathbf{e}_i} + \Psi_{-\mathbf{e}_i\pm\mathbf{e}_k}\Psi_{2\mathbf{e}_i\pm\mathbf{e}_k}\Psi_{\mathbf{e}_j}\Psi_{\mathbf{e}_i+\mathbf{e}_j} + \Psi_{-\mathbf{e}_i\pm\mathbf{e}_k}\Psi_{-2\mathbf{e}_i-\mathbf{e}_j}\Psi_{\pm\mathbf{e}_k}\Psi_{\mathbf{e}_i\pm\mathbf{e}_k} = 0.$$

We note that in [7, Theorem 2.5] it is shown that the terms $\Psi_{\mathbf{e}_i-\mathbf{e}_j}$, and $\Psi_{2\mathbf{e}_i-\mathbf{e}_j}$ can be computed explicitly in terms of $\Psi_{\mathbf{v}}$ for $\mathbf{v} \in \{\mathbf{e}_i, 2\mathbf{e}_i, \mathbf{e}_i + \mathbf{e}_j, 2\mathbf{e}_i + \mathbf{e}_j : i \neq j\}$. In particular, setting $(\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s}) = (\mathbf{e}_i, \mathbf{e}_j, \mathbf{0}, \mathbf{e}_i + \mathbf{e}_j)$ gives

$$\Psi_{\mathbf{e}_i-\mathbf{e}_j} = \Psi_{\mathbf{e}_i+2\mathbf{e}_j} - \Psi_{2\mathbf{e}_i+\mathbf{e}_j}.$$

Similarly, taking $(\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s}) = (-\mathbf{e}_i + \mathbf{e}_j, \mathbf{e}_j, \mathbf{e}_i, \mathbf{e}_i)$, we have

$$\Psi_{2\mathbf{e}_i - \mathbf{e}_j} = \psi_{2\mathbf{e}_i}\psi_{2\mathbf{e}_j} - \psi_{2\mathbf{e}_i+\mathbf{e}_j}\psi^2_{\mathbf{e}_i-\mathbf{e}_j}.$$

Thus $\Psi_{\mathbf{e}_i+\mathbf{e}_j\pm\mathbf{e}_k}$ can be computed using $\Psi_{\mathbf{v}}$ for $\mathbf{v} \in \{\mathbf{e}_i, 2\mathbf{e}_i, \mathbf{e}_i + \mathbf{e}_j, 2\mathbf{e}_i + \mathbf{e}_j : i \neq j\}$.

We are interested in relating $\Psi_{\mathbf{v}}(\mathbf{P})$ to the denominators of linear combinations of points on an elliptic curve. To do this, recall that for any E/K given by the polynomial (1.1), $\mathbf{P} \in E(K)^r$, and $\mathbf{v} \in \mathbb{Z}^r$ we can find rational functions (by repeated use of doubling and addition formulas for elliptic curves) $X_{\mathbf{v}}, Y_{\mathbf{v}} \in \mathrm{Frac}(\mathcal{R}_r)$, the fraction field of $\mathcal{R}_r$, such that

$$\mathbf{v} \cdot \mathbf{P} = v_1 P_1 + \cdots + v_r P_r = (X_{\mathbf{v}}(\mathbf{P}), Y_{\mathbf{v}}(\mathbf{P})).$$

The following lemma gives an explicit representation for $X_{\mathbf{v}}$ in terms of net polynomials.

Lemma 2.5. *Let E/K be an elliptic net, and let $\mathbf{P} \in E(K)^r$ be such that $P_i \neq \infty$ and $P_i \pm P_j \neq \infty$. Then For any $\mathbf{v} \in \mathbb{Z}^r$, there is $\Phi_{\mathbf{v}} \in \mathcal{R}_r$ such that*

$$X_{\mathbf{v}} = \frac{\Phi_{\mathbf{v}}}{\Psi^2_{\mathbf{v}}}.$$

In particular for any $1 \leq i \leq r$ we have

$$\Phi_{\mathbf{v}}(\mathbf{P}) = \Psi^2_{\mathbf{v}}(\mathbf{P})x(P_i) - \Psi_{\mathbf{v}+\mathbf{e}_i}(\mathbf{P})\Psi_{\mathbf{v}-\mathbf{e}_i}(\mathbf{P}).$$

Proof. In [7, Lemma 4.2], it is proved that for any $\mathbf{v}, \mathbf{u} \in \mathbb{Z}^r$ we have

$$\Psi^2_{\mathbf{v}}\Psi^2_{\mathbf{u}}(X_{\mathbf{v}} - X_{\mathbf{u}}) = -\Psi_{\mathbf{v}+\mathbf{u}}\Psi_{\mathbf{v}-\mathbf{u}}.$$

If we let $\mathbf{u} = \mathbf{e}_i$, then $X_{\mathbf{u}}(\mathbf{P}) = x(P_i)$. Thus we have

$$(\Psi^2_{\mathbf{v}}X_{\mathbf{v}})(\mathbf{P}) = \Psi^2_{\mathbf{v}}(\mathbf{P})x(P_i) - \Psi_{\mathbf{v}+\mathbf{e}_i}(\mathbf{P})\Psi_{\mathbf{v}-\mathbf{e}_i}(\mathbf{P}),$$

which gives us the desired result. □

Definition 2.6. *Let B and C be Abelian groups written additively. Furthermore, assume that C is 2-torsion free. Then a function $F : B \to C$ is a quadratic form if*

$$F(x + y) + F(x - y) = 2F(x) + 2F(y), \tag{2.1}$$

for all $x, y \in B$.

Equation (2.1) is sometimes called the *parallelogram law*.

Example 2.7. (a) Let $a_i, c_{ij} \in \mathbb{Q}$ and consider $F : \mathbb{Z}^r \to \mathbb{Q}$ defined by

$$F(v_1, v_2, \ldots, v_r) = \sum_{i=1}^{r} a_i v_i^2 + \sum_{1\leq i<j\leq r} c_{ij}v_iv_j.$$

Then we can check that F satisfies the parallelogram law (2.1).

(b) Let $p_i, q_{ij} \in \mathbb{Q}^\times$. Then the function $G : \mathbb{Z}^r \to \mathbb{Q}^\times$ defined by

$$G(v_1, v_2, \ldots, v_r) = \prod_{i=1}^{r} p_i^{v_i^2} \cdot \prod_{1\leq i<j\leq r} q_{ij}^{v_iv_j}$$

is a quadratic form.

(c) Let $F_1, F_2 : B \to C$ be two quadratic forms. Then their difference, $F_1 - F_2$, is again a quadratic form.

The main reason we are interested in quadratic forms is the following result.

Proposition 2.8. *Let K be a field and let $W : A \to K$ be an elliptic net. Let $F : A \to K^\times$ be a quadratic form. Then*

$$\begin{array}{rccc} W^F : & A & \longrightarrow & K \\ & \mathbf{v} & \longmapsto & W(\mathbf{v})F(\mathbf{v}) \end{array} \tag{2.2}$$

is an elliptic net.

Proof. See [7, Proposition 6.1]. □

Definition 2.9. *We say that two elliptic nets W and W' are scale equivalent, if there is a quadratic form $F : A \to K$ such that $W' = W^F$.*

Let λ_p be the *(local) Néron height function on E associated to the prime p*. (See [4, Chapter VI, Theorem1.1] for properties of λ_p.) An important property of Néron height is that it satisfies the *quasi-parallelogram law*.

Lemma 2.10. *Assume that P, $Q \in E(\mathbb{Q})$ are two points such that P, Q, $P \pm Q \neq \infty$. Then we have*

$$\lambda_p(P+Q) + \lambda_p(P-Q) = 2\lambda_p(P) + 2\lambda_p(Q) + \nu_p(x(P) - x(Q)) - \frac{1}{6}\nu_p(\Delta_E).$$

Proof. See [4, Page 476, Exercise 6.3]. □

Lemma 2.11. *Let $E/\mathbb{Q}$ defined by the polynomial* (1.1), *and assume a_i's are all integers. Let Δ_E be the discriminant of E. Let $\mathbf{P} = (P_1, \dots, P_r) \in E(\mathbb{Q})^r$ be an r-tuple consisting of r linearly independent points on $E(\mathbb{Q})$. Define*

$$\varepsilon(\mathbf{v}) = \begin{cases} \lambda_p(\mathbf{v} \cdot \mathbf{P}) - \frac{1}{12}\nu_p(\Delta_E) - \nu_p(\Psi_{\mathbf{v}}(\mathbf{P})) & \textit{if } \mathbf{v} \neq \mathbf{0}, \\ 0 & \textit{otherwise.} \end{cases}$$

Then ε is a quadratic form from $\mathbb{Z}^r$ to $\mathbb{Z}$.

Proof. From Lemma 2.5, we know that

$$\nu_p(\Psi_{\mathbf{v}+\mathbf{w}}(\mathbf{P})) + \nu_p(\Psi_{\mathbf{v}-\mathbf{w}}(\mathbf{P})) = 2\nu_p(\Psi_{\mathbf{v}}(\mathbf{P})) + 2\nu_p(\Psi_{\mathbf{w}}(\mathbf{P})) + \nu_p(X_{\mathbf{v}}(\mathbf{P}) - X_{\mathbf{w}}(\mathbf{P})). \tag{2.3}$$

Now assume that $\mathbf{v}, \mathbf{w}, \mathbf{v} \pm \mathbf{w} \neq \mathbf{0}$. Then substituting $\mathbf{v} \cdot \mathbf{P}$ and $\mathbf{w} \cdot \mathbf{P}$ in Lemma 2.10, we get

$$\lambda_p(\mathbf{v}\cdot\mathbf{P}+\mathbf{w}\cdot\mathbf{P})+\lambda_p(\mathbf{v}\cdot\mathbf{P}-\mathbf{w}\cdot\mathbf{P}) = 2\lambda_p(\mathbf{v}\cdot\mathbf{P})+2\lambda_p(\mathbf{w}\cdot\mathbf{P})+\nu_p(X_{\mathbf{v}}(\mathbf{P})-X_{\mathbf{w}}(\mathbf{P}))-\frac{1}{6}\nu_p(\Delta_E). \tag{2.4}$$

Subtracting (2.3) from (2.4) we have

$$\varepsilon(\mathbf{v}+\mathbf{w}) + \varepsilon(\mathbf{v}-\mathbf{w}) = 2\varepsilon(\mathbf{v}) + 2\varepsilon(\mathbf{w}), \tag{2.5}$$

where $\mathbf{v}, \mathbf{w}, \mathbf{v} \pm \mathbf{w} \neq \mathbf{0}$. The identity (2.5) also holds if $\mathbf{v}$ or $\mathbf{w} = \mathbf{0}$. So to complete the proof it is enough to show that $\varepsilon(2\mathbf{v}) = 4\varepsilon(\mathbf{v})$. In order to establish this we add copies of (2.5) for $(\mathbf{v}, \mathbf{w}) = (4\mathbf{u}, \mathbf{u}), (3\mathbf{u}, \mathbf{u}), (3\mathbf{u}, \mathbf{u}), (2\mathbf{u}, \mathbf{u})$ to obtain

$$\varepsilon(5\mathbf{u}) + \varepsilon(\mathbf{u}) = 2\varepsilon(3\mathbf{u}) + 8\varepsilon(\mathbf{u}) \tag{2.6}$$

Also letting $(\mathbf{v}, \mathbf{w}) = (3\mathbf{u}, 2\mathbf{u})$ in (2.5) yields

$$\varepsilon(5\mathbf{u}) + \varepsilon(\mathbf{u}) = 2\varepsilon(3\mathbf{u}) + 2\varepsilon(2\mathbf{u}). \tag{2.7}$$

Now subtracting (2.7) from (2.6) gives $\varepsilon(2\mathbf{u}) = 4\varepsilon(\mathbf{u})$. Thus ε is a quadratic form as desired. □

3. Proof of Theorem 1.9

Let K be any field and assume that $W : A \to K$ is an elliptic net of rank r. Theorem 1.9 claims that if W has a unique rank of apparition then $\Lambda = W^{-1}(0)$ will be a subgroup of A. The goal of this section is to prove this claim.

Throughout this section assume that W has a unique rank of apparition and let $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_r\}$ be a basis for A such that W has a unique rank of apparition with respect to $\mathcal{B}$. Therefore, there exists $(\rho_1, \rho_2, \dots, \rho_r) \in \mathbb{Z}^r$ with $\rho_i > 1$ for $1 \leq i \leq r$ such that $W(n\mathbf{b}_i) = 0$ if and only if $n|\rho_i$.

Let A_i be the subgroup of A generated by $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_i\}$ for $1 \leq i \leq r$ and let

$$\Lambda_i = \Lambda \cap A_i = \{\mathbf{v} \in A_i : W(\mathbf{v}) = 0\}.$$

Note that Λ_i is the zero set of the elliptic net $W|_{A_i} : A_i \to K$. By induction on i, we will prove that Λ_i is a subgroup of A_i. Note that the base case, $i = 1$, is true by definition of unique rank of apparition.

We will prove the inductive step by proving three lemmas.

Lemma 3.1. *Let $n \in \mathbb{Z}$, and let $1 \leq i \leq r$. If $\rho_i \mid n$, then we have*

$$W(\mathbf{v} + n\mathbf{b}_i) = 0 \Longleftrightarrow \mathbf{v} \in \Lambda.$$

Proof. First let $\mathbf{v} \in \Lambda$. Taking $\mathbf{p} = \mathbf{v}$, $\mathbf{q} = -n\mathbf{b}_i$, $\mathbf{r} = \mathbf{b}_i$, and $\mathbf{s} = 2n\mathbf{b}_i$ in (1.7) yields

$$W(\mathbf{v} + n\mathbf{b}_i)^2 W((2n+1)\mathbf{b}_i) W(\mathbf{b}_i) = 0. \tag{3.1}$$

Note that since $\rho_i \mid n$ and $\rho_i > 1$, we have $\rho_i \nmid (2n+1)$ and so $W((2n+1)\mathbf{b}_i) \neq 0$. Thus, from (3.1), we have $W(\mathbf{v} + n\mathbf{b}_i) = 0$ for all $\mathbf{v} \in \Lambda$.

Conversely assume that $\mathbf{v} \notin \Lambda$. Then taking $\mathbf{p} = \mathbf{v}$, $\mathbf{q} = n\mathbf{b}_i$, $\mathbf{r} = \mathbf{b}_i$, and $\mathbf{s} = \mathbf{0}$ in (1.7) yields

$$W(\mathbf{v} + n\mathbf{b}_i) W(\mathbf{v} - n\mathbf{b}_i) W(\mathbf{b}_i)^2 + W((n+1)\mathbf{b}_i) W((n-1)\mathbf{b}_i) W(\mathbf{v})^2 = 0. \tag{3.2}$$

Since $\mathbf{v} \notin \Lambda$ and $\rho_i \mid n$, we have $W((n+1)\mathbf{b}_i) W((n-1)\mathbf{b}_i) W(\mathbf{v})^2 \neq 0$. It therefore follows, from (3.2), that $W(\mathbf{v} + n\mathbf{b}_i) \neq 0$ for all $\mathbf{v} \notin \Lambda$. □

The following is a straightforward consequence of Lemma 3.1.

Corollary 3.2. *We have*

$$\{n_1\mathbf{b}_1 + n_2\mathbf{b}_2 + \cdots + n_r\mathbf{b}_r : \rho_i \mid n_i \textit{ for } 1 \leq i \leq r\} \subseteq \Lambda.$$

Lemma 3.3. *Suppose that for a fixed $i > 1$ we have that Λ_{i-1} is a subgroup of A. Then for all $\mathbf{v} \in \Lambda_{i-1}$, we have*

$$W(\mathbf{v} + n\mathbf{b}_i) = 0 \Longleftrightarrow \rho_i \mid n.$$

Proof. Choose $\mathbf{v} \in \Lambda_{i-1}$. Since $\mathbf{v} \in \Lambda_{i-1} \subset \Lambda$, it follows from Lemma 3.1 that if $\rho_i \mid n$ then $W(\mathbf{v} + n\mathbf{b}_i) = 0$. Conversely, let $\rho_i \nmid n$, taking $\mathbf{p} = \mathbf{v}$, $\mathbf{q} = n\mathbf{b}_i$, $\mathbf{r} \in A_{i-1} \setminus \Lambda_{i-1}$, and $\mathbf{s} = \mathbf{0}$ in (1.7) yields

$$W(\mathbf{v} + n\mathbf{b}_i) W(\mathbf{v} - n\mathbf{b}_i) W(\mathbf{r})^2 + W(\mathbf{r} + \mathbf{v}) W(\mathbf{r} - \mathbf{v}) W(n\mathbf{b}_i)^2 = 0. \tag{3.3}$$

Since $\mathbf{v} \in \Lambda_{i-1}$, $\mathbf{r} \in A_{i-1} \setminus \Lambda_{i-1}$, and Λ_{i-1} is a subgroup, it follows that $\mathbf{v} \pm \mathbf{r} \in A_{i-1} \setminus \Lambda_{i-1}$, hence $W(\mathbf{v} \pm \mathbf{r}) \neq 0$. It therefore follows from (3.3) that $W(\mathbf{v} + n\mathbf{b}_i) \neq 0$. □

Lemma 3.4. *Suppose that Λ_{i-1} is a subgroup of A for a fixed $i > 1$ and $\rho_i > 2$. Let $\mathbf{u}, \mathbf{v} \in \Lambda_i$ such that $\mathbf{u} = \mathbf{u}_0 + n\mathbf{b}_i$, and $\mathbf{v} = \mathbf{v}_0 + n\mathbf{b}_i$ for $\mathbf{u}_0, \mathbf{v}_0 \in A_{i-1}$. Then $\mathbf{u} - \mathbf{v} = \mathbf{u}_0 - \mathbf{v}_0 \in \Lambda_{i-1}$.*

Proof. Setting $\mathbf{p} = \mathbf{u}_0 + n\mathbf{b}_i$, $\mathbf{q} = \mathbf{v}_0 + n\mathbf{b}_i$, $\mathbf{r} = m\mathbf{b}_i$, and $\mathbf{s} = -2n\mathbf{b}_i$ in (1.7) gives

$$W(\mathbf{u}_0 + \mathbf{v}_0)W(\mathbf{u}_0 - \mathbf{v}_0)W((2n - m)\mathbf{b}_i)W(m\mathbf{b}_i) = 0. \tag{3.4}$$

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

$$W((2n - m)\mathbf{b}_i)W(m\mathbf{b}_i) \neq 0.$$

Thus from (3.4) we conclude that $W(\mathbf{u}_0 + \mathbf{v}_0)W(\mathbf{u}_0 - \mathbf{v}_0) = 0$. Now if $W(\mathbf{u}_0 - \mathbf{v}_0) = 0$ we are done. Otherwise we assume that $W(\mathbf{u}_0 - \mathbf{v}_0) \neq 0$, hence $W(\mathbf{u}_0 + \mathbf{v}_0) = 0$, and show that this gives a contradiction.

Setting $\mathbf{p} = \mathbf{u}_0 + n\mathbf{b}_i$, $\mathbf{q} = \mathbf{v}_0 + n\mathbf{b}_i$, $\mathbf{r} = \mathbf{b}_i$, and $\mathbf{s} = \mathbf{0}$ in (1.7) gives

$$W(\mathbf{u}_0 + \mathbf{v}_0 + 2n\mathbf{b}_i)W(\mathbf{u}_0 - \mathbf{v}_0)W(\mathbf{b}_i)^2 = 0,$$

hence $W(\mathbf{u}_0 + \mathbf{v}_0 + 2n\mathbf{b}_i) = 0$ (recall that $W(\mathbf{u}_0 - \mathbf{v}_0) \neq 0$). Since $\mathbf{u}_0 + \mathbf{v}_0 \in \Lambda_{i-1}$ it follows from Lemma 3.3 that $\rho_i \mid 2n$. Now we consider two cases.

Case 1: If $\rho_i \mid n$, then since $\mathbf{u} = \mathbf{u}_0 + n\mathbf{b}_i, \mathbf{v} = \mathbf{v}_0 + n\mathbf{b}_i \in \Lambda_i$, it follows from Lemma 3.1 that $\mathbf{u}_0, \mathbf{v}_0 \in \Lambda_{i-1}$, hence $\mathbf{u}_0 - \mathbf{v}_0 \in \Lambda_{i-1}$, contradicting our assumption that $W(\mathbf{u}_0 - \mathbf{v}_0) \neq 0$.

Case 2: If $\rho_i \nmid n$, then $W(\mathbf{u}_0 + \mathbf{v}_0 + n\mathbf{b}_i) \neq 0$ by Lemma 3.3. Setting $\mathbf{p} = \mathbf{u}_0 + n\mathbf{b}_i$, $\mathbf{q} = \mathbf{v}_0 + n\mathbf{b}_i$, $\mathbf{r} = \mathbf{b}_i$, and $\mathbf{s} = -n\mathbf{b}_i$ in (1.7) gives

$$W(\mathbf{u}_0 + \mathbf{v}_0 + n\mathbf{b}_i)W(\mathbf{u}_0 - \mathbf{v}_0)W((n - 1)\mathbf{b}_i)W(\mathbf{b}_i) = 0,$$

hence $W((n - 1)\mathbf{b}_i) = 0$ and so $\rho_i \mid n - 1$. Similarly by setting $\mathbf{p} = \mathbf{u}_0 + n\mathbf{b}_i$, $\mathbf{q} = \mathbf{v}_0 + n\mathbf{b}_i$, $\mathbf{r} = -\mathbf{b}_i$, and $\mathbf{s} = -n\mathbf{b}_i$ in (1.7) we find that $W((n + 1)\mathbf{b}_i) = 0$ and so $\rho_i \mid n + 1$. Since $\rho_i \mid n - 1$ and $\rho_i \mid n + 1$, we have $\rho_i = 2$. This is a contradiction. □

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

Proof of Theorem 1.9. We proceed by induction on i. Note that Λ_1 is a subgroup of $\mathbf{b}_1\mathbb{Z}$, since $W(n\mathbf{b}_1) = 0$ if and only if $\rho_1 | n$. Assume that Λ_{i-1} is a subgroup. We want to prove that Λ_i is a subgroup, that is for any $\mathbf{u}, \mathbf{v} \in \Lambda_i$ that $\mathbf{u} - \mathbf{v} \in \Lambda_i$. We will prove this by contradiction, so assume that $\mathbf{u} - \mathbf{v} \notin \Lambda_i$. Let $\mathbf{u} = \mathbf{u}_0 + n\mathbf{b}_i,\ \mathbf{v} = \mathbf{v}_0 + m\mathbf{b}_i \in \Lambda_i$, where $\mathbf{u}_0, \mathbf{v}_0 \in A_{i-1}$. It follows from (1.7), for $\mathbf{p} = \mathbf{u}$, $\mathbf{q} = \mathbf{v}$, $\mathbf{r} = \mathbf{u} + \mathbf{w}$, and $\mathbf{s} = -2\mathbf{u}$, that $W(\mathbf{u} - \mathbf{v})^2 W(\mathbf{u} - \mathbf{w})W(\mathbf{u} + \mathbf{w}) = 0$. Since $W(\mathbf{u} - \mathbf{v}) \neq 0$ and $\mathbf{u} = \mathbf{u}_0 + n\mathbf{b}_i$, we conclude that

$$W(\mathbf{u}_0 + n\mathbf{b}_i - \mathbf{w})W(\mathbf{u}_0 + n\mathbf{b}_i + \mathbf{w}) = 0 \tag{3.5}$$

for any $\mathbf{w} \in A_i$. We claim that (3.5) implies that $\rho_i \mid n$. To show this assume otherwise that $\rho_i \nmid n$. Then, since $\mathbf{u} = \mathbf{u}_0 + n\mathbf{b}_i \in \Lambda_i$ it follows from Lemma 3.3 that $\mathbf{u}_0 \notin \Lambda_{i-1}$. We consider two cases.

Case 1: If $\rho_i > 2$, then setting $\mathbf{w} = \mathbf{u}_0$ in (3.5) yields

$$W(2\mathbf{u}_0 + n\mathbf{b}_i)W(n\mathbf{b}_i) = 0.$$

Then we have that $W(2\mathbf{u}_0 + n\mathbf{b}_i) = 0$ since $\rho_i \nmid n$. Since $W(\mathbf{u}_0 + n\mathbf{b}_i) = W(2\mathbf{u}_0 + n\mathbf{b}_i) = 0$, it follows from Lemma 3.4 that $\mathbf{u}_0 \in \Lambda_{i-1}$. This is a contradiction.

Case 2: If $\rho_i = 2$, then setting $\mathbf{w} = \mathbf{b}_i$ in (3.5) yields

$$W(\mathbf{u}_0 + (n + 1)\mathbf{b}_i)W(\mathbf{u}_0 + (n - 1)\mathbf{b}_i) = 0,$$

from which it follows that $\mathbf{u}_0 \in \Lambda_{i-1}$ (since both $n - 1$ and $n + 1$ are even). This is a contradiction.

In either case, the assumption $\rho_i \nmid n$ leads to a contradiction. Thus, we have $\mathbf{u} = \mathbf{u}_0 + n\mathbf{b}_i$ with $\mathbf{u}_0 \in \Lambda_{i-1}$, and $\rho_i \mid n$. Similarly we have $\mathbf{v} = \mathbf{v}_0 + m\mathbf{b}_i$, with $\mathbf{v}_0 \in \Lambda_{i-1}$ and $\rho_i | m$. Then, $\mathbf{u} - \mathbf{v} = \mathbf{u}_0 - \mathbf{v}_0 + (n - m)\mathbf{b}_i$ with $\mathbf{u}_0 - \mathbf{v}_0 \in \Lambda_{i-1}$, and $\rho_i \mid (n - m)$. Thus it follows from Lemma 3.3 that $W(\mathbf{u} - \mathbf{v}) = 0$. This is a contradiction as we assumed that $W(\mathbf{u} - \mathbf{v}) \neq 0$.

Since the assumption $\mathbf{u}-\mathbf{v}\notin\Lambda_i$ leads to a contradiction, we conclude that $\mathbf{u}-\mathbf{v}\in\Lambda_i$ and so Λ_i is a subgroup of A. □

4. Proofs of Theorem 1.12 and Corollary 1.13

Theorem 1.9 shows that for a given elliptic net $W:A\to K$, in favorable conditions, if $W(\boldsymbol{\lambda}_1)=W(\boldsymbol{\lambda}_2)=0$ then $W(\boldsymbol{\lambda}_1+\boldsymbol{\lambda}_2)=0$. In this section we study the relation between $W(\mathbf{v}+\boldsymbol{\lambda})$ and $W(\mathbf{v})$ when $W(\boldsymbol{\lambda})=0$ but $W(\mathbf{v})$ is non-zero. Throughout this section we assume that $\Lambda=W^{-1}(0)$ is a subgroup of A. We also assume that $|A/\Lambda|\geq 4$. The results of this section generalizes Theorem 1.11 to Elliptic nets. In order to do this, we first define the auxiliary function

$$\begin{array}{rccc}\delta: & \Lambda\times(A\setminus\Lambda) & \longrightarrow & K^\times\\ & (\boldsymbol{\lambda},\mathbf{v}) & \longmapsto & \frac{W(\boldsymbol{\lambda}+\mathbf{v})}{W(\mathbf{v})},\end{array}$$

and explore the properties of δ. Notice that for $\boldsymbol{\lambda}\in\Lambda$ and $\mathbf{v}\notin\Lambda$ we get that $\delta(\boldsymbol{\lambda},\mathbf{v})\neq 0$. We have the following lemma.

Lemma 4.1. *For all $\boldsymbol{\lambda}\in\Lambda$, and $\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}\in A\backslash\Lambda$ with $\mathbf{a}+\mathbf{b}=\mathbf{c}+\mathbf{d}$, we have*

$$\delta(\boldsymbol{\lambda},\mathbf{a})\delta(\boldsymbol{\lambda},\mathbf{b})=\delta(\boldsymbol{\lambda},\mathbf{c})\delta(\boldsymbol{\lambda},\mathbf{d}).$$

Proof. Assume that $\mathbf{p}+\mathbf{s},\mathbf{p},\mathbf{q}+\mathbf{s},\mathbf{q}\notin\Lambda$. Then, setting $\mathbf{r}=\boldsymbol{\lambda}$ in (1.7) gives

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

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

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

Thus

$$\delta(\boldsymbol{\lambda},\mathbf{q}+\mathbf{s})\delta(\boldsymbol{\lambda},-\mathbf{q})=\delta(\boldsymbol{\lambda},\mathbf{p}+\mathbf{s})\delta(\boldsymbol{\lambda},-\mathbf{p}).$$

Taking

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

yields the result. □

Note that if $\mathbf{v},\mathbf{p}_1,\mathbf{p}_2\in A$ and $\mathbf{p}_1,\mathbf{p}_2,\mathbf{v}+\mathbf{p}_1,\mathbf{v}+\mathbf{p}_2\notin\Lambda$, then

$$\delta(\boldsymbol{\lambda},\mathbf{v}+\mathbf{p}_1)\delta(\boldsymbol{\lambda},\mathbf{p}_2)=\delta(\boldsymbol{\lambda},\mathbf{v}+\mathbf{p}_2)\delta(\boldsymbol{\lambda},\mathbf{p}_1).$$

Since δ is nonzero, we get

$$\frac{\delta(\boldsymbol{\lambda},\mathbf{v}+\mathbf{p}_1)}{\delta(\boldsymbol{\lambda},\mathbf{p}_1)}=\frac{\delta(\boldsymbol{\lambda},\mathbf{v}+\mathbf{p}_2)}{\delta(\boldsymbol{\lambda},\mathbf{p}_2)}. \tag{4.1}$$

Since we are assuming that $|A/\Lambda|\geq 4$, we get that for any $\mathbf{v}\in A$ there is an an element $\mathbf{p}\in A$ so that $\mathbf{p}$ and $\mathbf{v}+\mathbf{p}$ are in $A\setminus\Lambda$. In light of this observation, we define the function χ by

$$\begin{array}{rccc}\chi: & \Lambda\times A & \longrightarrow & K^\times\\ & (\boldsymbol{\lambda},\mathbf{v}) & \longmapsto & \frac{\delta(\boldsymbol{\lambda},\mathbf{v}+\mathbf{p})}{\delta(\boldsymbol{\lambda},\mathbf{p})},\end{array} \tag{4.2}$$

for any choice of $\mathbf{p}$ with $\mathbf{p},\mathbf{v}+\mathbf{p}\notin\Lambda$. Equation (4.1) shows that this definition is independent of the choice of $\mathbf{p}$. Furthermore, note that δ is non-zero, so χ maps to $K^\times$.

We now show that χ is a bilinear map.

Lemma 4.2. *Let $W : A \to K$ be an elliptic net, and $\Lambda = W^{-1}(0)$ be a subgroup of A such that $|A/\Lambda| \geq 4$. Let $\chi : \Lambda \times A \to K^\times$ be defined as before. Then for $\boldsymbol{\lambda}, \boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \Lambda$, and $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2 \in A$, we have the following:*

(i) $\chi(\boldsymbol{\lambda}, \mathbf{v}_1 + \mathbf{v}_2) = \chi(\boldsymbol{\lambda}, \mathbf{v}_1)\chi(\boldsymbol{\lambda}, \mathbf{v}_2)$.
(ii) $\chi(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2, \mathbf{v}) = \chi(\boldsymbol{\lambda}_1, \mathbf{v})\chi(\boldsymbol{\lambda}_2, \mathbf{v})$.
(iii) $\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2) = \chi(\boldsymbol{\lambda}_2, \boldsymbol{\lambda}_1)$.
(iv) $\chi(\boldsymbol{\lambda}, -\mathbf{v}) = \chi(\boldsymbol{\lambda}, \mathbf{v})^{-1}$.

Proof. First we note that if $|A/\Lambda| \geq 4$, then for any choice of $\mathbf{v}_1, \mathbf{v}_2 \in A$, we can find $\mathbf{p} \in A$ so that $\mathbf{p}, \mathbf{p} + \mathbf{v}_2$, and $\mathbf{p} + \mathbf{v}_1 + \mathbf{v}_2$ are not in Λ. In particular, by pigeonhole principle, we can find $\overline{\mathbf{u}} \in A/\Lambda$ so that the image of $\mathbf{0}, \mathbf{v}_2$ and $\mathbf{v}_1 + \mathbf{v}_2$ will miss $\overline{\mathbf{u}}$ in A/Λ. Letting $\mathbf{p}$ be any element in A that reduces to $-\overline{\mathbf{u}}$ we get the desired result. Given this $\mathbf{p}$ we have,

$$\begin{aligned}
\chi(\boldsymbol{\lambda}, \mathbf{v}_1)\chi(\boldsymbol{\lambda}, \mathbf{v}_2) &= \frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{p})}{\delta(\boldsymbol{\lambda}, \mathbf{v}_2 + \mathbf{p})} \frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_2 + \mathbf{p})}{\delta(\boldsymbol{\lambda}, \mathbf{p})} \\
&= \frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{p})}{\delta(\boldsymbol{\lambda}, \mathbf{p})} \\
&= \chi(\boldsymbol{\lambda}, \mathbf{v}_1 + \mathbf{v}_2).
\end{aligned}$$

This proves the first statement.

For the second statement, we let $\mathbf{p} \in A \backslash \Lambda$ be such that $\mathbf{v} + \mathbf{p} \notin \Lambda$ (Again, by pigeonhole principle, such an element exists). Since Λ is a subgroup of A, it follows that $\mathbf{v}+\mathbf{p}+\boldsymbol{\lambda}_2, \mathbf{p}+\boldsymbol{\lambda}_2 \notin \Lambda$. Hence, we have

$$\begin{aligned}
\chi(\boldsymbol{\lambda}_1, \mathbf{v})\chi(\boldsymbol{\lambda}_2, \mathbf{v}) &= \frac{\delta(\boldsymbol{\lambda}_1, \mathbf{v} + \mathbf{p} + \boldsymbol{\lambda}_2)\delta(\boldsymbol{\lambda}_2, \mathbf{v} + \mathbf{p})}{\delta(\boldsymbol{\lambda}_1, \mathbf{p} + \boldsymbol{\lambda}_2)\delta(\boldsymbol{\lambda}_2, \mathbf{p})} \\
&= \frac{W(\mathbf{v} + \mathbf{p} + \boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)W(\mathbf{p} + \boldsymbol{\lambda}_2)W(\mathbf{v} + \mathbf{p} + \boldsymbol{\lambda}_2)W(\mathbf{p})}{W(\mathbf{v} + \mathbf{p} + \boldsymbol{\lambda}_2)W(\mathbf{p} + \boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)W(\mathbf{v} + \mathbf{p})W(\mathbf{p} + \boldsymbol{\lambda}_2)} \\
&= \frac{W(\mathbf{v} + \mathbf{p} + \boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)W(\mathbf{p})}{W(\mathbf{v} + \mathbf{p})W(\mathbf{p} + \boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)} \\
&= \frac{\delta(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2, \mathbf{v} + \mathbf{p})}{\delta(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2, \mathbf{p})} \\
&= \chi(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2, \mathbf{v}).
\end{aligned}$$

For the third statement, taking $\mathbf{p} \in A \setminus \Lambda$, we have

$$\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2) = \frac{\delta(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 + \mathbf{p})}{\delta(\boldsymbol{\lambda}_1, \mathbf{p})} = \frac{W(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2 + \mathbf{p})W(\mathbf{p})}{W(\boldsymbol{\lambda}_2 + \mathbf{p})W(\boldsymbol{\lambda}_1 + \mathbf{p})} = \frac{\delta(\boldsymbol{\lambda}_2, \boldsymbol{\lambda}_1 + \mathbf{p})}{\delta(\boldsymbol{\lambda}_2, \mathbf{p})} = \chi(\boldsymbol{\lambda}_2, \boldsymbol{\lambda}_1).$$

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

Note that for $\boldsymbol{\lambda} \in \Lambda$ and $\mathbf{v} \notin \Lambda$ we have

$$W(\mathbf{v} + \boldsymbol{\lambda}) = \delta(\boldsymbol{\lambda}, \mathbf{v})W(\mathbf{v}) = \frac{\delta(\boldsymbol{\lambda}, \mathbf{v})}{\chi(\boldsymbol{\lambda}, \mathbf{v})}\chi(\boldsymbol{\lambda}, \mathbf{v})W(\mathbf{v}).$$

We now show that $\delta(\boldsymbol{\lambda}, \mathbf{v})/\chi(\boldsymbol{\lambda}, \mathbf{v})$ is independent of choice of $\mathbf{v}$.

Lemma 4.3. *For all* $\mathbf{v}_1, \mathbf{v}_2 \in A\backslash\Lambda$ *we have*

$$\frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_1)}{\chi(\boldsymbol{\lambda}, \mathbf{v}_1)} = \frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_2)}{\chi(\boldsymbol{\lambda}, \mathbf{v}_2)}.$$

Proof. First, if $\mathbf{v}_1 + \mathbf{v}_2 \notin \Lambda$ we have

$$\frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_1)}{\chi(\boldsymbol{\lambda}, \mathbf{v}_1)} = \frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_1)\delta(\boldsymbol{\lambda}, \mathbf{v}_2)}{\delta(\boldsymbol{\lambda}, \mathbf{v}_1 + \mathbf{v}_2)} = \frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_2)}{\chi(\boldsymbol{\lambda}, \mathbf{v}_2)}. \tag{4.3}$$

Next, we suppose that $\mathbf{v}_1 + \mathbf{v}_2 \in \Lambda$. Then, since $|A/\Lambda| \geq 4$, we can find $\mathbf{p} \in A \setminus \Lambda$ such that $\mathbf{p} \not\equiv -\mathbf{v}_1, -\mathbf{v}_2 \pmod{\Lambda}$. Then, we have

$$\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{p}, 2\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{p}, \mathbf{v}_1 + 2\mathbf{v}_2 + \mathbf{p} \notin \Lambda.$$

It then follows from (4.3), that

$$\frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_1)}{\chi(\boldsymbol{\lambda}, \mathbf{v}_1)} = \frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{p})}{\chi(\boldsymbol{\lambda}, \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{p})} = \frac{\delta(\boldsymbol{\lambda}, \mathbf{v}_2)}{\chi(\boldsymbol{\lambda}, \mathbf{v}_2)}.$$

□

Now in light of Lemma 4.3, we define

$$\begin{array}{rccc} \xi : & \Lambda & \longrightarrow & K^\times \\ & \boldsymbol{\lambda} & \longmapsto & \frac{\delta(\boldsymbol{\lambda}, \mathbf{v})}{\chi(\boldsymbol{\lambda}, \mathbf{v})}, \end{array} \tag{4.4}$$

for any choice of $\mathbf{v} \in A \setminus \Lambda$. Lemma 4.3 shows that ξ is a well defined function.

We are now in a position to give a generalization of Theorem 1.11.

Theorem 1.12. *Let* $W : A \to K$ *be an elliptic net with the property that* $\Lambda = W^{-1}(0)$ *is a subgroup of* A *and assume* $|A/\Lambda| \geq 4$. *Then, there exist well defined functions* $\xi : \Lambda \to K^\times$ *and* $\chi : \Lambda \times A \to K^\times$ *such that*

$$W(\boldsymbol{\lambda} + \mathbf{v}) = \xi(\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, \mathbf{v})W(\mathbf{v}) \; for \; all \; \boldsymbol{\lambda} \in \Lambda \; and \; all \; \mathbf{v} \in A,$$

and the functions ξ *and* χ *satisfy the following properties:*

(i) χ *is bilinear,*
(ii) $\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2) = \chi(\boldsymbol{\lambda}_2, \boldsymbol{\lambda}_1)$,
(iii) $\xi(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2) = \xi(\boldsymbol{\lambda}_1)\xi(\boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2)$,
(iv) $\xi(-\boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})$, *and*
(v) $\xi(\boldsymbol{\lambda})^2 = \chi(\boldsymbol{\lambda}, \boldsymbol{\lambda})$.

Proof. Recall that we have defined the functions $\delta(\boldsymbol{\lambda}, \mathbf{v}) = \frac{W(\mathbf{v}+\boldsymbol{\lambda})}{W(\mathbf{v})}$, $\chi(\boldsymbol{\lambda}, \mathbf{v}) = \frac{\delta(\boldsymbol{\lambda}, \mathbf{v}+\mathbf{p})}{\delta(\boldsymbol{\lambda}, \mathbf{p})}$, $\xi(\boldsymbol{\lambda}) = \frac{\delta(\boldsymbol{\lambda}, \mathbf{v})}{\chi(\boldsymbol{\lambda}, \mathbf{v})}$ for any choice of $\mathbf{v}, \mathbf{p} \in A$ so that the fractions make sense. Note that

$$W(\mathbf{v} + \boldsymbol{\lambda}) = \delta(\boldsymbol{\lambda}, \mathbf{v})W(\mathbf{v}) = \xi(\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, \mathbf{v})W(\mathbf{v}),$$

for any $\mathbf{v} \notin \Lambda$. If $\mathbf{v} \in \Lambda$ then both sides are 0. Therefore, for any $\mathbf{v} \in A$ and any $\boldsymbol{\lambda} \in \Lambda$ we have

$$W(\mathbf{v} + \boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, \mathbf{v})W(\mathbf{v}) \tag{4.5}$$

Furthermore, Lemma 4.2 shows that χ is bilinear and $\chi|_{\Lambda \times \Lambda}$ is symmetric.

Therefore, all we have to do is to show that

$$\xi(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2) = \xi(\boldsymbol{\lambda}_1)\xi(\boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2), \tag{4.6}$$

that $\xi(-\boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})$, and

$$\xi(\boldsymbol{\lambda})^2 = \chi(\boldsymbol{\lambda}, \boldsymbol{\lambda}). \tag{4.7}$$

Let $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \Lambda$ and $\mathbf{v} \notin \Lambda$. Note that by (4.5) and (i) we get

$$W(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2 + \mathbf{v}) = \xi(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2, \mathbf{v})W(\mathbf{v}) = \xi(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \mathbf{v})\chi(\boldsymbol{\lambda}_2, \mathbf{v})W(\mathbf{v}).$$

On the other hand

$$\begin{aligned} W(\boldsymbol{\lambda}_1 + (\boldsymbol{\lambda}_2 + \mathbf{v})) =& \xi(\boldsymbol{\lambda}_1)\chi(\boldsymbol{\lambda}_1, \mathbf{v} + \boldsymbol{\lambda}_2)W(\mathbf{v} + \boldsymbol{\lambda}_2) \\ =& \xi(\boldsymbol{\lambda}_1)\xi(\boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \mathbf{v} + \boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_2, \mathbf{v})W(\mathbf{v}) \\ =& \xi(\boldsymbol{\lambda}_1)\xi(\boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \mathbf{v})\chi(\boldsymbol{\lambda}_2, \mathbf{v})W(\mathbf{v}). \end{aligned}$$

Equating the above two equations for $W(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda_2} + \mathbf{v})$ yields

$$\xi(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \mathbf{v})\chi(\boldsymbol{\lambda}_2, \mathbf{v}) = \xi(\boldsymbol{\lambda}_1)\xi(\boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2)\chi(\boldsymbol{\lambda}_1, \mathbf{v})\chi(\boldsymbol{\lambda}_2, \mathbf{v}),$$

which gives us (4.6).

Now note that $\xi(\mathbf{0}) = 1$, since $W(\mathbf{v} + \mathbf{0}) = \xi(\mathbf{0})\chi(\mathbf{0}, \mathbf{v})W(\mathbf{v}) = W(\mathbf{v})$. Similarly,

$$\begin{aligned} W(-\mathbf{v} - \boldsymbol{\lambda}) &= \xi(-\boldsymbol{\lambda})\chi(-\boldsymbol{\lambda}, -\mathbf{v})W(-\mathbf{v}) \\ &= \xi(-\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, \mathbf{v})W(-\mathbf{v}) \\ &= -\xi(-\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, \mathbf{v})W(\mathbf{v}) \end{aligned}$$

while

$$\begin{aligned} W(-\mathbf{v} - \boldsymbol{\lambda}) &= -W(\mathbf{v} + \boldsymbol{\lambda}) \\ &= -\xi(\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, \mathbf{v})W(\mathbf{v}) \end{aligned}$$

which implies $\xi(-\boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})$. Therefore

$$1 = \xi(\mathbf{0}) = \xi(\boldsymbol{\lambda} - \boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})\xi(-\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, -\boldsymbol{\lambda}),$$

which by employing part (iv) of Lemma 4.2 results in $\xi(\boldsymbol{\lambda})^2 = \chi(\boldsymbol{\lambda}, \boldsymbol{\lambda})$. This completes the proof of our theorem. □

As an immediate corollary of the above theorem we have

Corollary 4.4. *Let $W : A \to K$ be an elliptic net with $\Lambda = W^{-1}(0)$ be a subgroup of A and $|A/\Lambda| \geq 4$. Then for all $\boldsymbol{\lambda} \in \Lambda$ and $n \in \mathbb{Z}$ we have*

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

Proof. We already showed that $\xi(\mathbf{0}) = 1$, so the statement holds for $n = 0$. It also trivially holds for $n = 1$. We proceed by induction. Assume the statement is true for some $n \geq 1$. From part (4) of Theorem 1.12 and Lemma 4.2, we have

$$\xi((n+1)\boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})\xi(n\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, n\boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})\xi(n\boldsymbol{\lambda})\chi(\boldsymbol{\lambda}, \boldsymbol{\lambda})^n.$$

From the induction hypothesis and part (v) of Theorem 1.12, it follows that

$$\xi((n+1)\boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})^{n^2+1}\xi(\boldsymbol{\lambda})^{2n} = \xi(\boldsymbol{\lambda})^{(n+1)^2}.$$

Therefore the statement holds for all $n \geq 0$. Finally note that $\xi(-n\boldsymbol{\lambda}) = \xi(n\boldsymbol{\lambda}) = \xi(\boldsymbol{\lambda})^{n^2}$ from part (5) of Theorem 1.12. Thus the statement holds for all $n \in \mathbb{Z}$. □

Note that Theorem 1.12 allows us to compute $W : A \to K$ by knowing the values of W on a set of representatives of A/Λ and by computing certain values of χ and ξ. In particular if Λ is a full rank subgroup of A, then we can choose $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \ldots, \boldsymbol{\lambda}_r$ as a basis of Λ. Then

$$\begin{aligned} W\left(\left(\sum_{i=1}^{r} n_i\boldsymbol{\lambda}_i\right) + \mathbf{v}\right) &= \xi\left(\sum_{i=1}^{r} n_i\boldsymbol{\lambda}_i\right)\chi\left(\sum_{i=1}^{r} n_i\boldsymbol{\lambda}_i, \mathbf{v}\right)W(\mathbf{v}) \\ &= \xi\left(\sum_{i=1}^{r} n_i\boldsymbol{\lambda}_i\right)\prod_{i=1}^{r}\chi\left(\boldsymbol{\lambda}_i, \mathbf{v}\right)^{n_i} W(\mathbf{v}) \end{aligned}$$

and

$$\begin{aligned} \xi\left(\sum_{i=1}^{r} n_i\boldsymbol{\lambda}_i\right) &= \prod_{i=1}^{r}\xi(n_i\boldsymbol{\lambda}_i)\left(\prod_{j=i+1}^{r}\chi(\boldsymbol{\lambda}_i, \boldsymbol{\lambda}_j)^{n_in_j}\right) \\ &= \prod_{i=1}^{r}\xi(\boldsymbol{\lambda}_i)^{n_i^2}\left(\prod_{j=i+1}^{r}\chi(\boldsymbol{\lambda}_i, \boldsymbol{\lambda}_j)^{n_in_j}\right). \end{aligned}$$

Combining the above two identities yields (1.12).

Proof of Corollary 1.13. If $K = \mathbb{F}_q$, a finite field with q elements, and if $(q-1)|n_i$ for all i, then we get $\xi(\sum_{i=1}^{r} n_i\boldsymbol{\lambda}_i) = 1$, since every term is raised to a power divisible by n_i for some i. Similarly, $\chi(\boldsymbol{\lambda}_i, \mathbf{v})^{n_i} = 1$. □

Example 4.5. Here by an example we show that how one can use the identity (1.12) to calculate an arbitrary term of an elliptic net over a finite field. To illustrate the method we consider a rank 2 elliptic net associated to an elliptic curve over $\mathbb{Q}$ and compute a specific term of its associated p-reduced nets as p varies over certain primes.

For a prime p let $W : \mathbb{Z}^2 \to \mathbb{F}_p$ be the elliptic net associated to the rank 2 elliptic curve $y^2 = x^3 - 11$ and generators $P = (3, 4)$, and $Q = (15, 58)$. The net W has a unique rank of apparition respect to the standard basis $\{\mathbf{e}_1, \mathbf{e}_2\}$ and so its zero set forms a subgroup of rank 2 of $\mathbb{Z}^2$. We choose a basis $\{\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2\}$ for this subgroup and by using definitions of functions ξ and χ we compute $\xi(\boldsymbol{\lambda}_1)$, $\xi(\boldsymbol{\lambda}_2)$, $\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2)$, $\chi(\boldsymbol{\lambda}_1, \mathbf{e}_1)$, $\chi(\boldsymbol{\lambda}_1, \mathbf{e}_2)$, $\chi_{(}\boldsymbol{\lambda}_2, \mathbf{e}_1)$, and $\chi(\boldsymbol{\lambda}_2, \mathbf{e}_2)$. The following table summarizes the result of our computations for five values of p (i.e. $p = 7, 11, 19, 61, 89$).

p	$\boldsymbol{\lambda}_1$	$\boldsymbol{\lambda}_2$	$\xi(\boldsymbol{\lambda}_1)$	$\xi(\boldsymbol{\lambda}_2)$	$\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2)$	$\chi(\boldsymbol{\lambda}_1, \mathbf{e}_1)$	$\chi(\boldsymbol{\lambda}_1, \mathbf{e}_2)$	$\chi_{(}\boldsymbol{\lambda}_2, \mathbf{e}_1)$	$\chi(\boldsymbol{\lambda}_2, \mathbf{e}_2)$
7	(1,5)	(0,13)	1	4	3	3	3	6	2
11	(1,7)	(0,11)	4	9	9	4	9	9	6
19	(1,6)	(0,14)	8	5	4	1	3	6	2
61	(2,8)	(0,38)	39	60	19	34	6	43	41
89	(9,3)	(0,10)	87	43	80	62	58	52	33

Let D be a fixed set of representatives for $\mathbb{Z}^2/\Lambda$. Then any point (r, s) in $\mathbb{Z}^2$ can be uniquely written as $(r, s) = n_1\boldsymbol{\lambda}_1 + n_2\boldsymbol{\lambda}_2 + m_1\mathbf{e}_1 + m_2\mathbf{e}_2$ with $(m_1, m_2) \in D$. Now by computing values for $W(m_1\mathbf{e}_1 + m_2\mathbf{e}_2)$ (by using the defining recursion of our net), the above table, and employing the rank 2 version of (1.12),

$$\begin{aligned} W(n_1\boldsymbol{\lambda}_1 + n_2\boldsymbol{\lambda}_2 + m_1\mathbf{e}_1 + m_2\mathbf{e}_2) = \xi(\boldsymbol{\lambda}_1)^{n_1^2}\xi(\boldsymbol{\lambda}_2)^{n_2^2}\chi(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2)^{n_1n_2}\chi(\boldsymbol{\lambda}_1, \mathbf{e}_1)^{n_1m_1}\chi(\boldsymbol{\lambda}_1, \mathbf{e}_2)^{n_1m_2} \\ \times\ \chi(\boldsymbol{\lambda}_2, \mathbf{e}_1)^{n_2m_1}\chi(\boldsymbol{\lambda}_2, \mathbf{e}_2)^{n_2m_2}W(m_1\mathbf{e}_1 + m_2\mathbf{e}_2), \end{aligned}$$

we can compute $W(r,s)$.

Here by using the above formula and table we compute the term $W(101,100)$ modulo p.

p	n_1	n_2	m_1	m_2	$W(m_1\mathbf{e}_1+m_2\mathbf{e}_2)$	W(101, 100)
7	101	-32	0	11	3	1
11	101	-56	0	9	6	5
19	101	-37	0	12	12	12
61	50	-8	1	4	21	28
89	11	6	2	7	44	52

5. Proofs of Proposition 1.6, Theorem 1.5, and Proposition 1.7

Recall that K is a field with a discrete valuation $\nu : K^\times \to \mathbb{Z}$. We have $\mathcal{O}_\nu$, $\mathfrak{p}$, and K defined as before. An application of the fact that $\Psi_{\mathbf{v}}^{\text{univ}} \in \mathcal{R}_r^{\text{univ}}$ is the following proof of proposition 1.6.

Proof of Proposition 1.6. Recall that $\pi_E : S^{\text{univ}} \to K$ is defined by $\pi_E(\alpha_i) = a_i$. Then the image of π_E lies in $\mathcal{O}_\nu$, so we can think of π_E as a function from S^{univ} into $\mathcal{O}_\nu$. In particular for any $\mathbf{v} \in \mathbb{Z}^r$ we get that

$$\Psi_{\mathbf{v}} = (\pi_E)_*(\Psi_{\mathbf{v}}^{\text{univ}}) \in \mathcal{O}_\nu[x_i, y_i]_{1\le i\le r}[(x_i - x_j)^{-1}]_{1\le i<j\le r}/\langle f(x_i,y_i)\rangle_{1\le i\le r}. \tag{5.1}$$

Now assume that $P_i \not\equiv \infty \pmod{\mathfrak{p}}$ and $P_i \pm P_j \not\equiv \infty \pmod{\mathfrak{p}}$ for all $i \neq j$. Then, since $P_i \not\equiv \infty \pmod{\mathfrak{p}}$, we have $\nu(x(P_i)) \ge 0$ and $\nu(y(P_i)) \ge 0$ and so $\nu(x(P_i) - x(P_j)) \ge 0$. On the other hand, since $P_i, P_j, P_i \pm P_j \not\equiv \infty \pmod{\mathfrak{p}}$ we conclude that $x(P_i) \not\equiv x(P_j) \pmod{\mathfrak{p}}$, and thus $\nu(x(P_i) - x(P_j)) \le 0$. Therefore, $\nu(x(P_i) - x(P_j)) = 0$. This together with (5.1) give $\nu(\Psi_{\mathbf{v}}(\mathbf{P})) \ge 0$, as desired. □

Proof of Theorem 1.5. $(a) \Longrightarrow (b)$. Observe that $\Psi_{ne_i}(\mathbf{P}) = \psi_n(P_i)$. So the result follows from Theorem 1.1.

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

$(c) \Longleftrightarrow (d)$. From Lemma 2.5, we have

$$\Phi_{\mathbf{v}}(\mathbf{P}) = \Psi_{\mathbf{v}}^2(\mathbf{P})x(P_i) - \Psi_{\mathbf{v}+\mathbf{e}_i}(\mathbf{P})\Psi_{\mathbf{v}-\mathbf{e}_i}(\mathbf{P}),$$

which implies the (c) and (d) are equivalent.

$(c) \Longrightarrow (e)$. First note that by proposition 1.6, we have $\nu(\Psi_{\mathbf{v}}(\mathbf{P})) \ge 0$, hence $\nu(\Psi_{\mathbf{v}}(\mathbf{P})) \in \mathcal{O}_\nu$ and therefore the reduction mod $\mathfrak{p}$ is well defined. We let $\Psi_{\mathbf{v}}(\mathbf{P}) \pmod{\mathfrak{p}}$ be the image of $\Psi_{\mathbf{v}}(\mathbf{P})$ in the corresponding residue field under this reduction map. By part (a) of Lemma 2.1 we get that $\Psi_{\mathbf{v}}(\mathbf{P}) \pmod{\mathfrak{p}}$ is an elliptic net. Under the assumptions of (c) we have $\Psi_{\mathbf{v}}(\mathbf{P}) \pmod{\mathfrak{p}} = 0$ and $\Psi_{\mathbf{v}+\mathbf{e}_i}(\mathbf{P}) \pmod{\mathfrak{p}} = 0$. Now if the zero set of $\Psi_{\mathbf{v}}(\mathbf{P}) \pmod{\mathfrak{p}}$ forms a subgroup then we have $\Psi_{\mathbf{e}_i}(\mathbf{P}) \pmod{\mathfrak{p}} = \psi_1(P_i) \pmod{\mathfrak{p}} = 0$ which is a contradiction, since $\psi_1 = 1$. So the zero set of $\Psi_{\mathbf{v}}(\mathbf{P}) \pmod{\mathfrak{p}}$ does not form a subgroup of $\mathbb{Z}^r$ and thus by Theorem 1.9 we conclude that $\Psi_{\mathbf{v}}(\mathbf{P}) \pmod{\mathfrak{p}}$ does not have a unique rank of apparition (with respect to $\{\mathbf{e}_1, \cdots, \mathbf{e}_r\}$). So there exists $1 \le i \le r$ such that $\Psi_{n\mathbf{e}_i}(\mathbf{P}) \pmod{\mathfrak{p}}$ does not have a unique rank of apparition. By Theorem 1.10 we get that $\Psi_{3\mathbf{e}_i} \pmod{\mathfrak{p}} = \Psi_{4\mathbf{e}_i} \pmod{\mathfrak{p}} = 0$, which means $\nu(\Psi_{3\mathbf{e}_i})$ and $\nu(\Psi_{4\mathbf{e}_i}) > 0$. Therefore from Theorem 1.1 we conclude that $P_i \pmod{\mathfrak{p}}$ is singular.

$(e) \Longrightarrow (a)$ Since $P_i \pmod{\mathfrak{p}}$ is singular, then from Theorem 1.1 we know that $\nu(\psi_2(P_i)) > 0$ and $\nu(\psi_3(P_i)) > 0$. Now the result follows since $\psi_n(P_i) = \Psi_{ne_i}(\mathbf{P})$ for $n \in \mathbb{Z}$. □

Proof of Proposition 1.7. First of all by [4, Theorem 4.1] if P is a point such that $P \pmod p$ is non-singular then we have the following expression for the local Néron height of P,

$$\lambda_p(P) = \max\left\{-\frac{1}{2}\nu_p(x(P)), 0\right\} + \frac{1}{12}\nu_p(\Delta_E).$$

Observe that

$$\nu_p(D_P) = \max\left\{-\frac{1}{2}\nu_p(x(P)), 0\right\}.$$

Under our assumptions since $P_i \pmod p$ is non-singular for $1 \leq i \leq r$, we conclude that the quadratic form $\varepsilon(\mathbf{v})$ in Lemma 2.11, can be written as

$$\varepsilon(\mathbf{v}) = \nu_p(D_{\mathbf{v}\cdot\mathbf{P}}) - \nu_p(\Psi_{\mathbf{v}}(\mathbf{P}))$$

for $\mathbf{v} \neq \mathbf{0}$. We also note that $\mathbf{v} \mapsto \nu_p(F_{\mathbf{v}}((P))$ is a quadratic form, where $F_{\mathbf{v}}(\mathbf{P})$ is given in (1.11). Define $\hat{\varepsilon} : \mathbb{Z}^r \to \mathbb{Z}$ by

$$\hat{\varepsilon}(\mathbf{v}) = \varepsilon(\mathbf{v}) - \nu_p(F_{\mathbf{v}}(\mathbf{P})) = \nu_p(D_{\mathbf{v}\cdot\mathbf{P}}) - \nu_p(\hat{\Psi}_{\mathbf{v}}(\mathbf{P})).$$

Since $\hat{\varepsilon}$ is the difference of two quadratic forms, we conclude that $\hat{\varepsilon}$ is also a quadratic form. Furthermore, we have

$$\hat{\varepsilon}(\mathbf{e}_i) = \nu_p(D_{P_i}) - \nu_p(\hat{\Psi}_{\mathbf{e}_i}(\mathbf{P})) = 0,$$

for all $1 \leq i \leq r$, and

$$\hat{\varepsilon}(\mathbf{e}_i + \mathbf{e}_j) = \nu_p(D_{P_i+P_j}) - \nu_p(\hat{\Psi}_{\mathbf{e}_i+\mathbf{e}_j}(\mathbf{P})) = 0,$$

for all $1 \leq i < j \leq r$. Thus by [7, Lemma 4.5] we have $\hat{\varepsilon}(\mathbf{v}) = 0$ for all $\mathbf{v} \in \mathbb{Z}^r$. This shows that, for all $\mathbf{v} \in \mathbb{Z}^r$, we have

$$\nu_p(D_{\mathbf{v}\cdot\mathbf{P}}) = \nu_p(\hat{\Psi}_{\mathbf{v}}(\mathbf{P})),$$

as desired. □

The following two examples give illustrations of Proposition 1.7.

Example 5.1. We consider the elliptic curve $E : y^2 = x^3 - 11$. Then the group of rational points of E over $\mathbb{Q}$ is generated by two points $P = (3, 4)$ and $Q = (15, 58)$. We observe that $P, Q \not\equiv \infty \pmod p$ for all primes p and $P + Q \not\equiv \infty \pmod p$ for all primes p except $p = 2$. In Table 5.1 we provide some values of the elliptic denominator net associated to E and the points P and Q as a two dimensional array with lower left corner D_{0Q+0P}, lower right corner D_{4Q+0P}, upper left corner D_{0Q+9P}, and upper right corner D_{4Q+9P}. Table 5.2 provides the corresponding values for the elliptic net associated to net polynomials $\Psi_{(v_1,v_2)}(P, Q)$. As predicted in Proposition 1.7 the valuations of these two nets at all primes p (except $p = 2$) coincide.

Example 5.2. We consider the elliptic curve $E : y^2 + 7y = x^3 + x^2 + 28x$ with $E(\mathbb{Q})$ generated by two independent points $P = (0, 0)$ and $Q = (1, 3)$. Then $P, Q, P + Q \not\equiv \infty \pmod p$ for any prime p. However P reduces to a singular point modulo 7. Thus as predicted in Proposition 1.7 the valuations of the elliptic denominator net (given in Table 5.3) and the elliptic net (given in Table 5.4) are the same for all primes $p \neq 7$.

$3^3 \cdot 17 \cdot 861139 \cdot 638022143238323743$	$2 \cdot 31 \cdot 227 \cdot 32114101 \cdot 2233563433631$	$13 \cdot 97 \cdot 967 \cdot 2333 \cdot 899531 \cdot 20086489$	$2 \cdot 3^2 \cdot 67 \cdot 89 \cdot 379 \cdot 1078019 \cdot 724929587$	$23 \cdot 103 \cdot 340789 \cdot 175849593114259$
$2^5 \cdot 37 \cdot 167 \cdot 245519 \cdot 3048674017$	$3 \cdot 7^2 \cdot 11 \cdot 1567 \cdot 634026250609$	$2^2 \cdot 5^2 \cdot 43 \cdot 293 \cdot 349 \cdot 631 \cdot 1670527$	$41 \cdot 227 \cdot 4051 \cdot 32279374297$	$2^3 \cdot 3 \cdot 17 \cdot 37 \cdot 47 \cdot 149 \cdot 263 \cdot 2003 \cdot 714947$
$19 \cdot 433 \cdot 2689 \cdot 8819 \cdot 40487$	$2 \cdot 131 \cdot 179 \cdot 2103080101$	$3 \cdot 17 \cdot 101 \cdot 15641 \cdot 150379$	$2 \cdot 71 \cdot 83 \cdot 107 \cdot 751 \cdot 22613$	$77711 \cdot 82149276767$
$2^3 \cdot 3^2 \cdot 5 \cdot 17 \cdot 23 \cdot 1737017$	$163 \cdot 1877 \cdot 42797$	$2^2 \cdot 67 \cdot 317 \cdot 98377$	$3^2 \cdot 5 \cdot 59 \cdot 25640299$	$2^6 \cdot 7 \cdot 41 \cdot 157 \cdot 229 \cdot 9437$
$449 \cdot 104759$	$2 \cdot 3 \cdot 29 \cdot 809$	$11 \cdot 19 \cdot 31 \cdot 677$	$2 \cdot 29 \cdot 569 \cdot 4987$	$3 \cdot 17 \cdot 1439 \cdot 925741$
$2^4 \cdot 37 \cdot 167$	$5^2 \cdot 631$	$2^2 \cdot 3 \cdot 17 \cdot 149$	$13 \cdot 30557$	$2^3 \cdot 5 \cdot 37 \cdot 239 \cdot 1549$
$3^2 \cdot 17$	$2 \cdot 67$	$7 \cdot 157$	$2 \cdot 3^3 \cdot 2087$	$19 \cdot 23 \cdot 503 \cdot 659$
2^3	3	$2^2 \cdot 5$	$11 \cdot 1553$	$2^4 \cdot 3 \cdot 17 \cdot 199 \cdot 577$
1	2	$3 \cdot 17$	$2 \cdot 31 \cdot 233$	$631 \cdot 1753$
0	1	$2^2 \cdot 29$	$3^2 \cdot 5 \cdot 3331$	$2^3 \cdot 29 \cdot 37 \cdot 83 \cdot 3467$

TABLE 5.1. Elliptic denominator net associated to $E : y^2 = x^3 - 11$ and the points $Q = (15, 58)$ and $P = (3, 4)$

$-3^3 \cdot 17 \cdot 861139 \cdot 638022143238323743$	$-2^{-8} \cdot 31 \cdot 227 \cdot 32114101 \cdot 2233563433631$	$-2^{-18} \cdot 13 \cdot 97 \cdot 967 \cdot 2333 \cdot 899531 \cdot 20086489$	$-2^{-26} \cdot 3^2 \cdot 67 \cdot 89 \cdot 379 \cdot 1078019 \cdot 724929587$	$-2^{-36} \cdot 23 \cdot 103 \cdot 340789 \cdot 175849593114259$
$2^5 \cdot 37 \cdot 167 \cdot 245519 \cdot 3048674017$	$-2^{-8} \cdot 3 \cdot 7^2 \cdot 11 \cdot 1567 \cdot 634026250609$	$-2^{-14} \cdot 5^2 \cdot 43 \cdot 293 \cdot 349 \cdot 631 \cdot 1670527$	$-2^{-24} \cdot 41 \cdot 227 \cdot 4051 \cdot 32279374297$	$-2^{-29} \cdot 3 \cdot 17 \cdot 37 \cdot 47 \cdot 149 \cdot 263 \cdot 2003 \cdot 714947$
$19 \cdot 433 \cdot 2689 \cdot 8819 \cdot 40487$	$2^{-6} \cdot 131 \cdot 179 \cdot 2103080101$	$2^{-14} \cdot 3 \cdot 17 \cdot 101 \cdot 15641 \cdot 150379$	$-2^{-20} \cdot 71 \cdot 83 \cdot 107 \cdot 751 \cdot 22613$	$-2^{-28} \cdot 77711 \cdot 82149276767$
$2^3 \cdot 3^2 \cdot 5 \cdot 17 \cdot 23 \cdot 1737017$	$2^{-6} \cdot 163 \cdot 1877 \cdot 42797$	$2^{-10} \cdot 67 \cdot 317 \cdot 98377$	$2^{-18} \cdot 3^2 \cdot 5 \cdot 59 \cdot 25640299$	$2^{-18} \cdot 7 \cdot 41 \cdot 157 \cdot 229 \cdot 9437$
$-449 \cdot 104759$	$-2^{-4} \cdot 3 \cdot 29 \cdot 809$	$2^{-10} \cdot 11 \cdot 19 \cdot 31 \cdot 677$	$2^{-14} \cdot 29 \cdot 569 \cdot 4987$	$2^{-20} \cdot 3 \cdot 17 \cdot 1439 \cdot 925741$
$-2^4 \cdot 37 \cdot 167$	$-2^{-4} \cdot 5^2 \cdot 631$	$-2^{-6} \cdot 3 \cdot 17 \cdot 149$	$-2^{-12} \cdot 13 \cdot 30557$	$2^{-13} \cdot 5 \cdot 37 \cdot 239 \cdot 1549$
$-3^2 \cdot 17$	$-2^{-2} \cdot 67$	$-2^{-6} \cdot 7 \cdot 157$	$-2^{-8} \cdot 3^3 \cdot 2087$	$-2^{-12} \cdot 19 \cdot 23 \cdot 503 \cdot 659$
2^3	$2^{-2} \cdot 3$	$-2^{-2} \cdot 5$	$-2^{-6} \cdot 11 \cdot 1553$	$-2^{-4} \cdot 3 \cdot 17 \cdot 199 \cdot 577$
1	1	$2^{-2} \cdot 3 \cdot 17$	$2^{-2} \cdot 31 \cdot 233$	$-2^{-4} \cdot 631 \cdot 1753$
0	1	$2^2 \cdot 29$	$3^2 \cdot 5 \cdot 3331$	$2^3 \cdot 29 \cdot 37 \cdot 83 \cdot 3467$

TABLE 5.2. Elliptic net associated to $E : y^2 = x^3 - 11$ and the points $Q = (15, 58)$ and $P = (3, 4)$.

$3^2 \cdot 5 \cdot 8243 \cdot 7289363$	$59 \cdot 523 \cdot 1170779$	$2803 \cdot 2163467$	$2^3 \cdot 23 \cdot 7758139$	$59 \cdot 149837011$	$31 \cdot 229 \cdot 32045369$	$3 \cdot 11 \cdot 733 \cdot 154099559$
$13 \cdot 127 \cdot 3066533$	$2 \cdot 41 \cdot 53 \cdot 26627$	$7 \cdot 13 \cdot 17 \cdot 5653$	$5^2 \cdot 29 \cdot 67 \cdot 487$	$3 \cdot 13 \cdot 19 \cdot 89 \cdot 1291$	$7 \cdot 109 \cdot 1427 \cdot 2833$	$2^2 \cdot 13 \cdot 167 \cdot 199 \cdot 617887$
5948431	$181 \cdot 8819$	$3^2 \cdot 47 \cdot 1097$	$11 \cdot 11779$	$2 \cdot 61 \cdot 74377$	$17 \cdot 25967671$	$5 \cdot 56479 \cdot 333271$
$3 \cdot 5 \cdot 7 \cdot 1949$	6553	$2^4 \cdot 431$	$7^2 \cdot 521$	42181	$47 \cdot 71 \cdot 14557$	$3 \cdot 7 \cdot 127 \cdot 349 \cdot 32537$
$2 \cdot 11 \cdot 113$	911	463	$5 \cdot 557$	$3^3 \cdot 37 \cdot 137$	$2^2 \cdot 2059769$	25084117199
127	7	$3 \cdot 19$	$2 \cdot 199$	$7 \cdot 2039$	$653 \cdot 15767$	$5 \cdot 11 \cdot 293 \cdot 662327$
$3 \cdot 5$	2^3	1	349	$53 \cdot 593$	5624039	$2 \cdot 3^2 \cdot 41 \cdot 73 \cdot 661 \cdot 2141$
1	1	7	$5 \cdot 11$	$2^2 \cdot 3 \cdot 23 \cdot 107$	$7 \cdot 4812433$	$19 \cdot 127 \cdot 601 \cdot 4637$
1	1	$2 \cdot 3$	601	$277 \cdot 313$	$1987 \cdot 119321$	$5^2 \cdot 139843540153$
0	1	13	$7 \cdot 59$	$13 \cdot 55819$	$2 \cdot 29 \cdot 26272439$	$3 \cdot 7 \cdot 13 \cdot 59 \cdot 263 \cdot 5880307$

TABLE 5.3. Elliptic denominator net associated to $E : y^2 + 7y = x^3 + x^2 + 28x$ and the points $Q = (1, 3)$ and $P = (0, 0)$

$-3^2 \cdot 5 \cdot 7^{20} \cdot 8243 \cdot 7289363$	$7^{20} \cdot 59 \cdot 523 \cdot 1170779$	$7^{20} \cdot 2803 \cdot 2163467$	$2^3 \cdot 7^{20} \cdot 23 \cdot 7758139$	$-7^{20} \cdot 59 \cdot 149837011$	$-7^{20} \cdot 31 \cdot 229 \cdot 32045369$	$-3 \cdot 7^{20} \cdot 11 \cdot 733 \cdot 154099559$
$-7^{16} \cdot 13 \cdot 127 \cdot 3066533$	$-2 \cdot 7^{16} \cdot 41 \cdot 53 \cdot 26627$	$7^{17} \cdot 13 \cdot 17 \cdot 5653$	$5^2 \cdot 7^{16} \cdot 29 \cdot 67 \cdot 487$	$3 \cdot 7^{16} \cdot 13 \cdot 19 \cdot 89 \cdot 1291$	$-7^{17} \cdot 109 \cdot 1427 \cdot 2833$	$-2^2 \cdot 7^{16} \cdot 13 \cdot 167 \cdot 199 \cdot 617887$
$7^{12} \cdot 5948431$	$-7^{12} \cdot 181 \cdot 8819$	$-3^2 \cdot 7^{12} \cdot 47 \cdot 1097$	$7^{12} \cdot 11 \cdot 11779$	$2 \cdot 7^{12} \cdot 61 \cdot 74377$	$7^{12} \cdot 17 \cdot 25967671$	$-5 \cdot 7^{12} \cdot 56479 \cdot 333271$
$3 \cdot 5 \cdot 7^{10} \cdot 1949$	$7^9 \cdot 6553$	$-2^4 \cdot 7^9 \cdot 431$	$-7^{11} \cdot 521$	$-7^9 \cdot 42181$	$7^9 \cdot 47 \cdot 71 \cdot 14557$	$3 \cdot 7^{10} \cdot 127 \cdot 349 \cdot 32537$
$2 \cdot 7^6 \cdot 11 \cdot 113$	$7^6 \cdot 911$	$7^6 \cdot 463$	$-5 \cdot 7^6 \cdot 557$	$-3^3 \cdot 7^6 \cdot 37 \cdot 137$	$-2^2 \cdot 7^6 \cdot 2059769$	$7^6 \cdot 25084117199$
$-7^4 \cdot 127$	7^5	$3 \cdot 7^4 \cdot 19$	$2 \cdot 7^4 \cdot 199$	$-7^5 \cdot 2039$	$-7^4 \cdot 653 \cdot 15767$	$-5 \cdot 7^4 \cdot 11 \cdot 293 \cdot 662327$
$-3 \cdot 5 \cdot 7^2$	$-2^3 \cdot 7^2$	-7^2	$7^2 \cdot 349$	$7^2 \cdot 53 \cdot 593$	$-7^2 \cdot 5624039$	$-2 \cdot 3^2 \cdot 7^2 \cdot 41 \cdot 73 \cdot 661 \cdot 2141$
7	-7	-7^2	$-5 \cdot 7 \cdot 11$	$2^2 \cdot 3 \cdot 7 \cdot 23 \cdot 107$	$7^2 \cdot 4812433$	$-7 \cdot 19 \cdot 127 \cdot 601 \cdot 4637$
1	1	$-2 \cdot 3$	-601	$-277 \cdot 313$	$1987 \cdot 119321$	$5^2 \cdot 139843540153$
0	1	13	$-7 \cdot 59$	$-13 \cdot 55819$	$-2 \cdot 29 \cdot 26272439$	$3 \cdot 7 \cdot 13 \cdot 59 \cdot 263 \cdot 5880307$

TABLE 5.4. Elliptic nets associated to $E : y^2 + 7y = x^3 + x^2 + 28x$ and the points $Q = (1, 3)$ and $P = (0, 0)$

References

[1] M. Ayad, Points S-entiers des courbes elliptiques, *manuscripta math.* **76** (1992), 305–324.

[2] H. Cohen, Number Theory Volume 1: Tools and Diophantine Equations, Springer, 2007.

[3] S. Lang, Elliptic Curves Diophantine Analysis, Springer-Verlag, 1978.

[4] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, 1994.

[5] J. H. Silverman and N. Stephens, The sign of an elliptic divisibility sequence, *J. Ramanujan Math. Soc.* **21** (2006), 1–17.

[6] K. Stange, The Tate pairing via elliptic nets Pairing-Based Cryptography – PAIRING 2007, *Springer LNCS*, **4575** (2007), 329-348.

[7] K. Stange, Elliptic nets and elliptic curves, *Algebra and Number Theory* **5** (2011), 197-229.

[8] K. Stange, Integral points on elliptic curves and explicit valuations of division polynomials, *arXiv: 1108.3051*, 37 pages.

[9] M. Ward, Memoir on elliptic divisibility sequences, *Amer. J. Math.* **70** (1948), 31–74.

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada

E-mail address: amir.akbary@uleth.ca
E-mail address: jeff.bleaney@uleth.ca
E-mail address: syazdani@gmail.com