The signs in elliptic nets

Amir Akbary, Manoj Kumar and Soroosh Yazdani

ABSTRACT. We give a generalization of a theorem of Silverman and Stephens regarding the signs in an elliptic divisibility sequence to the case of an elliptic net. We also describe applications of this theorem in the study of the distribution of the signs in elliptic nets and generating elliptic nets using the denominators of the linear combination of points on elliptic curves.

CONTENTS

1. Introduction

Definition 1.1. An elliptic sequence (W_n) over a field K is a sequence of elements of K satisfying the nonlinear recurrence

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

for all $m, n \in \mathbb{Z}$. An elliptic sequence is said to be nondegenerate if

$$W_1 W_2 W_3 \neq 0.$$

Furthermore, if $W_1 = 1$, we call it a normalized elliptic sequence.

We can show that for a nondegenerate elliptic sequence $W_0 = 0$ (let $m = n = 1$ in (1.1)), $W_1 = \pm 1$ (let $m = 2$, $n = 1$ in (1.1)), and $W_{-n} = -W_n$. The nontrivial examples of elliptic sequences can be obtained by addition of

---

points on cubics. Let E be a cubic curve, defined over a field K, given by the Weierstrass equation $f(x, y) = 0$, where

$$(1.2) \qquad f(x, y) := y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6; \ a_i \in K.$$

Let $E^{\mathrm{ns}}(K)$ be the collection of nonsingular K-rational points of E. It is known that $E^{\mathrm{ns}}(K)$ forms a group. Moreover, there are polynomials ϕ_n, ψ_n, and $\omega_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x, y]$ such that for any $P \in E^{\mathrm{ns}}(K)$ we have

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

In addition, ψ_n satisfies the recursion

$$(1.3) \qquad \psi_{m+n} \psi_{m-n} = \psi_{m+1} \psi_{m-1} \psi_n^2 - \psi_{n+1} \psi_{n-1} \psi_m^2.$$

The polynomial ψ_n is called the *n-th division polynomial* associated to E. (See [4, Chapter 2] for the basic properties of division polynomials.) The equation (1.3) shows that $(\psi_n(P))$ is an elliptic sequence over K. A remarkable fact, first observed by Ward for integral (integer-valued) elliptic sequences, is that any normalized nondegenerate elliptic sequence can be realized as a sequence $(\psi_n(P))$. A concrete version of this statement is given in the following proposition (See [12, Theorem 4.5.3]).

Proposition 1.2 (Swart)**.** *Let (W_n) be a normalized nondegenerate elliptic sequence. Then there is a cubic curve E with equation $f(x, y) = 0$, where $f(x, y)$ is given by (1.2) and with*

$$a_1 = \frac{W_4 + W_2^5 - 2W_2 W_3}{W_2^2 W_3}, \quad a_2 = \frac{W_2 W_3^2 + W_4 + W_2^5 - W_2 W_3}{W_2^3 W_3},$$
$$a_3 = W_2, \quad a_4 = 1, \quad a_6 = 0,$$

such that $W_n = \psi_n((0, 0))$, where ψ_n is the n-th division polynomial associated to E.

We call the pair $(E, (0, 0))$ in the above proposition a *curve-point* pair associated with the elliptic sequence (W_n). Any two curve-point pairs associated to an elliptic sequence (W_n) are *uni-homothetic* (see [11, Section 6.2] for definition). A normalized nondegenerate elliptic sequence (W_n) is called *nonsingular* if the cubic curve E in a curve-point pair (E, P) associated to (W_n) is an elliptic curve (a nonsingular cubic).

Ward's version of the above proposition is stated for normalized, nondegenerate, integral elliptic divisibility sequences (i.e. an integer-valued elliptic sequence with the property that $W_m \mid W_n$ if $m \mid n$). However, examining its proof reveals that in fact it is a theorem for any normalized, nondegenerate, elliptic sequence defined over a subfield of $\mathbb{C}$. Moreover Ward represents the terms of such elliptic sequences as values of certain elliptic functions at certain complex numbers. To explain Ward's representation, one observes that

for the n-th division polynomial ψ_n of an elliptic curve E, defined over a subfield K of $\mathbb{C}$, we have

$$\psi_n(P) = (-1)^{n^2-1} \frac{\sigma(nz; \Lambda)}{\sigma(z; \Lambda)^{n^2}}$$

for a complex number z and a lattice Λ (See [8, Chapter VI, Exercise 6.15] and [3, Theorem 2.3.5] for a proof). The lattice Λ is the lattice associated to E over $\mathbb{C}$ and $\sigma(z; \Lambda)$ is the Weierstrass σ-function associated to Λ defined as

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

More precisely, Ward proved the following assertion.

Theorem 1.3 (Ward). *Let (W_n) be a normalized, nondegenerate, nonsingular elliptic divisibility sequence defined over a subfield K of complex numbers. Then there is a lattice $\Lambda \subset \mathbb{C}$ and a complex number $z \in \mathbb{C}$ such that*

$$(1.4) \qquad\qquad W_n = \frac{\sigma(nz; \Lambda)}{\sigma(z; \Lambda)^{n^2}} \quad \text{for all } n \geq 1.$$

Further, the Eisenstein series $g_2(\Lambda)$ and $g_3(\Lambda)$ associated to the lattice Λ and the Weierstrass values $\wp(z; \Lambda)$ and $\wp'(z; \Lambda)$ associated to the point z on the elliptic curve $\mathbb{C}/\Lambda$ are in the field $\mathbb{Q}(W_2, W_3, W_4)$. In other words $g_2(\Lambda), g_3(\Lambda), \wp(z; \Lambda), \wp'(z; \Lambda)$ are all defined over K.

The above version of Ward's theorem is [9, Theorem 3]. In [9] Silverman and Stephens proved a formula regarding signs in an unbounded, normalized, nondegenerate, nonsingular, real elliptic sequence. (The results of [9] are stated for integral elliptic divisibility sequences. However, their results hold more generally for real elliptic sequences.) In order to describe Silverman–Stephens's theorem we need to set up some notation.

Notation 1.4. For an elliptic curve E defined over $\mathbb{R}$, we let $\Lambda \subset \mathbb{C}$ be its corresponding lattice. Let $E(\mathbb{R})$ be the group of $\mathbb{R}$-rational points of E. For a point $P \in E(\mathbb{R})$ we let z be the corresponding complex number under the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. From the theory of elliptic curves we know that there exists a unique $q = e^{2\pi i \tau}$, where τ is in the upper half-plane, such that $\mathbb{R}^*/q^{\mathbb{Z}} \cong E(\mathbb{R})$ (see Theorem 2.4). Let $u \in \mathbb{R}^*$ be the corresponding real number to the point $P \in E(\mathbb{R})$, where $P \neq \mathcal{O}$ (the point at infinity).We assume that u is normalized such that it satisfies $q < |u| < 1$ if $q > 0$ and $q^2 < u < 1$ if $q < 0$ (see Lemma 2.1). Finally, for any nonzero real number x, we define the parity of x by

$$\text{Sign}[x] = (-1)^{\text{Parity}[x]}, \text{ where } \text{Parity}[x] \in \mathbb{Z}/2\mathbb{Z}.$$

The following is [9, Theorem 1].

Theorem 1.5 (Silverman–Stephens). *Let (W_n) be an unbounded, normalized, nonsingular, nondegenerate (integral) elliptic divisibility sequence. Let (E, P) be a curve-point pair corresponding to (W_n). Assume conventions given in Notation 1.4. Then possibly after replacing (W_n) by the related sequence $((-1)^{n^2-1} W_n)$, there is an irrational number $\beta \in \mathbb{R}$, given in Table 1.1, so that if $q < 0$, or $q > 0$ and $u > 0$,*

$$\mathrm{Parity}[W_n] \equiv \lfloor n\beta \rfloor \pmod 2,$$

and if $q > 0$ and $u < 0$,

$$\mathrm{Parity}[W_n] \equiv \begin{cases} \lfloor n\beta \rfloor + n/2 \pmod 2 & \text{if } n \text{ is even,} \\ (n-1)/2 \pmod 2 & \text{if } n \text{ is odd.} \end{cases}$$

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

q	u	β
$q > 0$	$u > 0$	$\log_q u$
	$u < 0$	$\log_q |u|$
$q < 0$	$u > 0$	$\dfrac{1}{2} \log_{|q|} u$

TABLE 1.1. Explicit expressions for β

In this paper we give a generalization of Silverman–Stephens's theorem in the context of elliptic nets.

Definition 1.6. Let $\Lambda \subset \mathbb{C}$ be a fixed lattice corresponding to an elliptic curve $E/\mathbb{C}$. For an n-tuple $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$, define a function $\Omega_{\mathbf{v}}$ (with respect to Λ) on $\mathbb{C}^n$ in variable $\mathbf{z} = (z_1, z_2, \ldots, z_n)$ as follows:

$$(1.5) \qquad \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) = (-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \leq i < j \leq n} v_i v_j - 1}$$
$$\cdot \frac{\sigma(v_1 z_1 + v_2 z_2 + \cdots + v_n z_n; \Lambda)}{\prod_{i=1}^{n} \sigma(z_i; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \leq i < j \leq n} \sigma(z_i + z_j; \Lambda)^{v_i v_j}},$$

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

In [11, Theorem 3.7] it is shown that if $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ is an n-tuple consisting of n points in $E(\mathbb{C})$ such that $P_i \neq \mathcal{O}$ for each i and $P_i \pm P_j \neq \mathcal{O}$ for $1 \leq i < j \leq n$, and $\mathbf{z} = (z_1, z_2, \ldots, z_n)$ in $\mathbb{C}^n$ be such that each z_i

corresponds to P_i under the isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, then $\Omega_{\mathbf{v}} := \Omega_{\mathbf{v}}(z; \Lambda)$ satisfies the recursion

(1.6)
$$\Omega_{\mathbf{p}+\mathbf{q}+\mathbf{s}}\Omega_{\mathbf{p}-\mathbf{q}}\Omega_{\mathbf{r}+\mathbf{s}}\Omega_{\mathbf{r}} + \Omega_{\mathbf{q}+\mathbf{r}+\mathbf{s}}\Omega_{\mathbf{q}-\mathbf{r}}\Omega_{\mathbf{p}+\mathbf{s}}\Omega_{\mathbf{p}} + \Omega_{\mathbf{r}+\mathbf{p}+\mathbf{s}}\Omega_{\mathbf{r}-\mathbf{p}}\Omega_{\mathbf{q}+\mathbf{s}}\Omega_{\mathbf{q}} = 0,$$

for all $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s} \in \mathbb{Z}^n$. In [11], Stange generalized the concept of an elliptic sequence to an n-dimensional array, called an elliptic net.

Definition 1.7. 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

$$(1.7) \quad W(\mathbf{p} + \mathbf{q} + \mathbf{s})W(\mathbf{p} - \mathbf{q})W(\mathbf{r} + \mathbf{s})W(\mathbf{r})$$
$$+ W(\mathbf{q} + \mathbf{r} + \mathbf{s})W(\mathbf{q} - \mathbf{r})W(\mathbf{p} + \mathbf{s})W(\mathbf{p})$$
$$+ W(\mathbf{r} + \mathbf{p} + \mathbf{s})W(\mathbf{r} - \mathbf{p})W(\mathbf{q} + \mathbf{s})W(\mathbf{q}) = 0,$$

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

Note that for $A = \mathbb{Z}$, $\mathbf{s} = 0$, $\mathbf{r} = 1$, and $W(1) = 1$ the recursion (1.7) reduces to (1.1). Also it is known that the solutions of (1.1) also satisfy the recurrence (1.7). Thus elliptic nets are generalizations of elliptic sequences. Moreover, in light of (1.6) the function

$$\Psi(\mathbf{P}; E) : \mathbb{Z}^n \quad \longrightarrow \quad \mathbb{C}$$
$$\mathbf{v} \quad \longmapsto \quad \Psi_{\mathbf{v}}(\mathbf{P}; E) = \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$$

is an elliptic net with values in $\mathbb{C}$. Observe that $\Psi_{n\mathbf{e_i}}(\mathbf{P}) = \psi_n(P_i)$, where $\mathbf{e_i}$ denotes the ith standard basis vector for $\mathbb{Z}^n$.

Definition 1.8. The function $\Psi(\mathbf{P}; E)$ is called the elliptic net associated to E (over $\mathbb{C}$) and $\mathbf{P}$. The value $\Psi_{\mathbf{v}}(\mathbf{P}; E) = \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ is called the $\mathbf{v}$-th net polynomial associated to E and $\mathbf{P}$.

We note that if $P_1, P_2, \ldots, P_n$ are n linearly independent points in $E(\mathbb{R})$ then by [11, Theorem 7.4] we have $\Psi_{\mathbf{v}}(\mathbf{P}; E) \neq 0$ for $\mathbf{v} \neq \mathbf{0}$. We prove the following generalization of Theorem 1.5 regarding the signs in $\Psi(\mathbf{P}, E)$.

Theorem 1.9. *Let E be an elliptic curve defined over $\mathbb{R}$ and*

$$\mathbf{P} = (P_1, P_2, \ldots, P_n)$$

be an n-tuple consisting of n linearly independent points in $E(\mathbb{R})$. Let Λ, q, z_i, and u_i be as defined in Notation 1.4. Assume that $u_1, u_2, \ldots, u_n > 0$ or there exists a nonnegative integer k such that $u_1, u_2, \ldots, u_k < 0$ and $u_{k+1}, u_{k+2}, \ldots, u_n > 0$. Then there are n irrational numbers $\beta_1, \beta_2, \ldots, \beta_n$, which are $\mathbb{Q}$-linearly independent, given by rules similar to Table 1.1, such that the parity of $\Psi_{\mathbf{v}}(\mathbf{P}; E) (= \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda))$, possibly after replacing $\Psi_{\mathbf{v}}(\mathbf{P}; E)$

with $(-1)^{\sum\limits_{i=1}^{n} v_i^2 - \sum\limits_{1 \le i < j \le n} v_i v_j - 1} \Psi_{\mathbf{v}}(\mathbf{P}; E)$, is given by

$$(1.8) \quad \mathrm{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] \equiv \left\lfloor \sum_{i=1}^{n} v_i \beta_i \right\rfloor + \sum_{1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \quad (\mathrm{mod}\ 2),$$

if all $u_i > 0$, but if $u_1, u_2, \ldots, u_k < 0$ and $u_{k+1}, u_{k+2}, \ldots, u_n > 0$, we have two cases:

(1) If $\sum\limits_{i=1}^{k} v_i$ is even, we have

$$(1.9\mathrm{a}) \quad \mathrm{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] \equiv \sum_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j$$

$$+ \left\lfloor \sum_{i=1}^{n} v_i \beta_i \right\rfloor + \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \quad (\mathrm{mod}\ 2).$$

(2) If $\sum\limits_{i=1}^{k} v_i$ is odd, we have

$$(1.9\mathrm{b}) \quad \mathrm{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] \equiv \sum_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j$$

$$+ \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \quad (\mathrm{mod}\ 2).$$

Note that in the above theorem all $u_i > 0$ is the same as $k = 0$, which leads to $\sum_{i=1}^{k} v_i = 0$ always being even. Thus (1.9a) for $k = 0$ reduces to (1.8). The method of the proof of the above theorem follows closely the techniques devised in the proof of Theorem 1 of [9] for the case $n = 1$, however the proof of Theorem 1.9 involves analyzing more cases since the expression (1.5), for $n > 1$, includes some new terms.

We also prove a generalization of Theorem 1.5 for sign of certain elliptic nets that are not necessarily given as values of net polynomials. In order to describe our result, we need to review some concepts from the theory of elliptic nets as developed in [11].

Definition 1.10. Let $W : \mathbb{Z}^n \to R$ be an elliptic net. Let

$$\mathcal{B} = \{\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}\}$$

be the standard basis of $\mathbb{Z}^n$. We say W is nondegenerate if

$$W(\mathbf{e_i}),\ W(2\mathbf{e_i}) \ne 0$$

for all $1 \le i \le n$, and

$$W(\mathbf{e_i} \pm \mathbf{e_j}) \ne 0$$

for $1 \leq i, j \leq n$, $i \neq j$. If $n = 1$, we need an additional condition that $W(\mathbf{3e_i}) \neq 0$. If any of the above conditions is not satisfied we say that W is degenerate.

Definition 1.11. Let $W : \mathbb{Z}^n \longrightarrow R$ be an elliptic net. Then we say that W is normalized if $W(\mathbf{e_i}) = 1$ for all $1 \leq i \leq n$ and $W(\mathbf{e_i} + \mathbf{e_j}) = 1$ for all $1 \leq i < j \leq n$.

In [11, Theorem 7.4] a generalization of Theorem 1.3 in the context of elliptic nets is given. More precisely it is proved that for a normalized and nondegenerate elliptic net $W : \mathbb{Z}^n \longrightarrow K$ there exists a cubic curve E and a collection of points $\mathbf{P}$ on E such that W can be realized as an elliptic net associated to E and $\mathbf{P}$. (Theorem 7.4 of [11] is also applicable to elliptic nets over a field K that is not contained in $\mathbb{C}$.) We call W *nonsingular* if E in the curve-point pair $(E, \mathbf{P})$ associated to W is an elliptic curve. We also need the following concept for our second generalization of Theorem 1.5.

Definition 1.12. A function $f : \mathbb{Z}^n \longrightarrow \mathbb{R}^*$ is called a quadratic form if

$$(1.10) \quad f(\mathbf{a} + \mathbf{b} + \mathbf{c})f(\mathbf{a} + \mathbf{b})^{-1}f(\mathbf{b} + \mathbf{c})^{-1}f(\mathbf{c} + \mathbf{a})^{-1}f(\mathbf{a})f(\mathbf{b})f(\mathbf{c}) = 1,$$

for $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{Z}^n$.

An example of a quadratic form is the function

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

where $p_i, q_{ij} \in \mathbb{R}^*$. As we mentioned before, Theorem 1.9 can be stated as a theorem for the sign of certain elliptic nets. Our next theorem establishes such a result for nonsingular, nondegenerate elliptic nets.

Theorem 1.13. *Let* $W : \mathbb{Z}^n \longrightarrow \mathbb{R}$ *be a nonsingular, nondegenerate elliptic net. Assume that* $W(\mathbf{v}) \neq 0$ *for* $\mathbf{v} \neq \mathbf{0}$*. Then, possibly after replacing* $W(\mathbf{v})$ *with either* $g(\mathbf{v})W(\mathbf{v})$ *or* $-g(\mathbf{v})W(\mathbf{v})$ *for a quadratic form* $g : \mathbb{Z}^n \to \mathbb{R}^*$*, there are* n *irrational numbers* $\beta_1, \beta_2, \ldots, \beta_n$*, given by rules similar to Table* 1.1*, that can be calculated using an elliptic curve associated to* W *and points on it, such that*

$$(1.11) \qquad \mathrm{Parity}[W(\mathbf{v})] \equiv \left\lfloor \sum_{i=1}^{n} v_i \beta_i \right\rfloor \pmod{2},$$

$$(1.12) \qquad \mathrm{Parity}[W(\mathbf{v})]$$

$$\equiv \begin{cases} \left\lfloor \sum_{i=1}^{n} v_i \beta_i \right\rfloor + \sum_{i=1}^{k} \left\lfloor \dfrac{v_i}{2} \right\rfloor \pmod{2} & \text{if } \sum_{i=1}^{k} v_i \text{ is even,} \\[4mm] \sum_{i=1}^{k} \left\lfloor \dfrac{v_i}{2} \right\rfloor \pmod{2} & \text{if } \sum_{i=1}^{k} v_i \text{ is odd.} \end{cases}$$

Here (1.11) *is applicable when all* $u_i > 0$ *and* (1.12) *is applicable if*

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

Again note that for $k = 0$ the formula (1.12) reduces to (1.11). Next we describe some applications of Theorem 1.9 and Theorem 1.13.

Definition 1.14. For $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{N}^n$, let $(S(\mathbf{v}))$ be an n-dimensional array of integers. For $j \in \{0, 1, \ldots, m-1\}$ and $m \geq 2$ denote

$$C(m, j; V_1, V_2, \ldots, V_n)$$
$$= \#\big\{\mathbf{v}; \ 1 \leq v_i \leq V_i \ for \ 1 \leq i \leq n \ and \ S(\mathbf{v}) \equiv j \pmod{m}\big\}.$$

The array $(S(\mathbf{v}))$ is said to be uniformly distributed mod m if

$$\lim_{V_1, V_2, \ldots, V_n \to \infty} \frac{C(m, j; V_1, V_2, \ldots, V_n)}{V_1 V_2 \ldots V_n} = \frac{1}{m},$$

for $j = 0, 1, \ldots, m-1$. We say that the signs in an n-dimensional array $S : \mathbb{Z}^n \to \mathbb{R}^*$ are uniformly distributed if the array $(\mathrm{Parity}[S(\mathbf{v})])$ is uniformly distributed mod 2.

Note that here the restriction to $\mathbf{v} \in \mathbb{N}^n$ is for the simplicity of presentation and similar results will hold for $\mathbf{v} \in \mathbb{Z}^n$. By employing formulas in Theorem 1.9 and Theorem 1.13 we establish the following result.

Theorem 1.15. *Let* $\Psi(\mathbf{P}; E)$ *and* $W(\mathbf{v})$ *be as in Theorem* 1.9 *and Theorem* 1.13. *Then the signs in* $\Psi(\mathbf{P}; E)$ *and* $W(\mathbf{v})$ *are uniformly distributed.*

In order to explain the second application of our results we first introduce the concept of a *denominator net*. Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation with integer coefficients. If $P \in E(\mathbb{Q})$ is a nontorsion point (i.e., $nP \neq \mathcal{O}$ for any n) then we have that

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

where A_{nP}, B_{nP}, and $D_{nP} > 0$ are integers (See [10, Chapter III, Section 2]). The sequence (D_{nP}) is called an *elliptic denominator sequence* associated to the curve E and the point P. It can be shown that (D_{nP}) is a divisibility sequence. Several authors have studied the sequence (D_{nP}). In fact, Shipsey [6, Section 4.4] has shown a way of assigning signs to the sequence (D_{nP}) so that the resulting sequence becomes an elliptic divisibility sequence (Note that $D_{nP} > 0$ for all n by our definition). The concept of an elliptic denominator sequence has been generalized to higher ranks and it is called an *elliptic denominator net*. If $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ is an n-tuple of linearly independent points in $E(\mathbb{Q})$. Then for $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$ we can write

$$\mathbf{v} \cdot \mathbf{P} = v_1 P_1 + v_2 P_2 + \cdots + v_n P_n = \left(\frac{A_{\mathbf{v} \cdot \mathbf{P}}}{D_{\mathbf{v} \cdot \mathbf{P}}^2}, \frac{B_{\mathbf{v} \cdot \mathbf{P}}}{D_{\mathbf{v} \cdot \mathbf{P}}^3} \right),$$

where $A_{\mathbf{v} \cdot \mathbf{P}}, B_{\mathbf{v} \cdot \mathbf{P}}$, and $D_{\mathbf{v} \cdot \mathbf{P}} > 0$ are integers. Then $(D_{\mathbf{v} \cdot \mathbf{P}})$ is called the *elliptic denominator net* associated to an elliptic curve E and a collection of points $\mathbf{P}$. As a consequence of Theorem 1.9 and Proposition 1.7 of [1], we describe how in certain cases one can assign signs to a denominator net in order to obtain an elliptic net. We first need to establish a connection between the denominator sequence $(D_{\mathbf{v} \cdot \mathbf{P}})$ and an scaled version of the elliptic net $\Psi_{\mathbf{v}}(\mathbf{P}; E)$. For $\mathbf{v} \in \mathbb{Z}^n$, let

$$(1.13) \qquad \hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E) = F_{\mathbf{v}}(\mathbf{P}) \Psi_{\mathbf{v}}(\mathbf{P}; E),$$

where $F(\mathbf{P}) : \mathbb{Z}^n \longrightarrow \mathbb{Q}^*$ is the quadratic form given by

$$(1.14) \qquad F_{\mathbf{v}}(\mathbf{P}) = \prod_{1 \leq i \leq j \leq n} \gamma_{ij}^{v_i v_j},$$

with

$$\gamma_{ii} = D_{\mathbf{e_i} \cdot \mathbf{P}} = D_{P_i}, \quad \text{and} \quad \gamma_{ij} = \frac{D_{P_i + P_j}}{D_{P_i} D_{P_j}} \text{ for } i \neq j.$$

The following assertion is proved in [1, Proposition 1.7].

Proposition 1.16. *Let E be an elliptic curve defined over $\mathbb{Q}$ given by the Weierstrass equation*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \qquad a_i \in \mathbb{Z}.$$

Let $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ be an n-tuple of linearly independent points in $E(\mathbb{Q})$ so that each $P_i \pmod{\ell}$ is nonsingular for every prime ℓ. Then we have

$$(1.15) \qquad D_{\mathbf{v} \cdot P} = |\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)|$$

for all $\mathbf{v} \in \mathbb{Z}^n$.

By employing Theorem 1.9, we have the following direct corollary of Proposition 1.16, which gives a way for generating elliptic nets from denominator nets.

Corollary 1.17. *Assume the conditions of Proposition 1.16. Define a map $W : \mathbb{Z}^n \longrightarrow \mathbb{Q}$ by*

$$(1.16) \qquad W(\mathbf{v}) = (-1)^{\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)]} D_{\mathbf{v} \cdot P},$$

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

In the next section we will review preliminaries needed in the proofs and in Sections 3 and 4 we prove our main results on the signs in elliptic nets. In Section 5 we illustrate our results by providing several examples. Finally in Sections 6 and 7 we give proofs of our results on uniform distribution of signs and on relation with denominator sequences.

2. Preliminaries

We will follow the conventions described in Notation 1.4. We first show that the claimed normalization in Notation 1.4 is possible.

Lemma 2.1. *Let $q \in \mathbb{R}$ be such that $0 < |q| < 1$ and $u_0 \in \mathbb{R}^{>0} \setminus q^{\mathbb{Z}}$. Then the following statements hold:*

(i) *For $0 < q < 1$ there exists an integer k such that $0 < q < q^k u_0 < 1$.*
(ii) *For $-1 < q < 0$ there exists an integer k with $0 < q^2 < q^k u_0 < 1$.*

Proof. (i) Let $k_0 = \min\{k \in \mathbb{Z} \mid q^k u_0 < 1\}$. Then

$$q^{k_0} u_0 < 1 \quad \text{and} \quad q^{k_0-1} u_0 > 1.$$

We claim that $q < q^{k_0} u_0 < 1$. Clearly $q^{k_0} u_0 < 1$. If $q^{k_0} u_0 \leq q$ then

$$q^{k_0-1} u_0 \leq 1$$

which contradicts the minimality of k_0. So the claim holds.

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

Thus, letting $u = q^k u_0$ in the above lemma will result in the desired normalization.

Let Λ_τ be the normalized lattice with basis $[\tau, 1]$, where τ is in the upper half-plane. From [7, Chapter I, Theorem 6.4] we know that, the q-expansion of the σ-function $\sigma(z; \Lambda_\tau)$ is given by

$$(2.1) \quad \sigma(z; \Lambda_\tau) = -\frac{1}{2\pi i} e^{\frac{1}{2} z^2 \eta(1) - \pi i z} (1-w) \prod_{m \geq 1} \frac{(1 - q^m w)(1 - q^m w^{-1})}{(1 - q^m)^2},$$

where $w = e^{2\pi i z}$, $q = e^{2\pi i \tau}$, and $\eta(1)$ is the quasi-period associated to the period 1 in the lattice Λ_τ. The next proposition gives the q-expansion for the numerator in the expression for $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda_\tau)$ in (1.5).

Proposition 2.2. *Let*

$$\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n,$$
$$\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n.$$

Let $w_j = e^{2\pi i z_j}$ for $j = 1, 2, \ldots n$ and $q = e^{2\pi i \tau}$. Then

$$(2.2) \quad \sigma(\mathbf{v} \cdot \mathbf{z}; \Lambda_\tau) = -\frac{1}{2\pi i} e^{\frac{1}{2}(\mathbf{v} \cdot \mathbf{z})^2 \eta(1) - \pi i (\mathbf{v} \cdot \mathbf{z})} \left(1 - \prod_{j=1}^{n} w_j^{v_j}\right)$$

$$\cdot \prod_{m \geq 1} \frac{(1 - q^m \prod_{j=1}^{n} w_j^{v_j})(1 - q^m \prod_{j=1}^{n} w_j^{-v_j})}{(1 - q^m)^2},$$

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

Proof. The result is obtained by replacing z with

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

in (2.1). Observe that the map $z \longmapsto v_1 z_1 + v_2 z_2 + + \cdots v_n z_n$, corresponds to $w \longmapsto \prod_{j=1}^{n} w_j^{v_j}$. $\qquad\square$

The next proposition provides a q-expansion for $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda_\tau)$ defined in Definition 1.6.

Proposition 2.3. *Let*

$$\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n,$$
$$\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n.$$

Let $w_j = e^{2\pi i z_j}$ *for* $j = 1, 2, \ldots n$ *and* $q = e^{2\pi i \tau}$. *Then we have*

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

$$\cdot \frac{\theta\left(\prod_{j=1}^{n} w_j^{v_j}, q\right)}{\displaystyle \prod_{j=1}^{n} \theta(w_j, q)^{2v_j^2 - \sum_{k=1}^{n} v_j v_k} \prod_{1 \le j < k \le n} \theta(w_j w_k, q)^{v_j v_k}},$$

where

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

Proof. The proof is computational and follows by substituting the q-expansions (2.1) and (2.2) in (1.5). The one thing to note is that the product expansion of $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda_\tau)$ is independent of $\eta(1)$. It disappears after substituting the q-expansions and simplifying the terms. $\qquad\square$

For $q = e^{2\pi i \tau}$ with τ in the upper half-plane, let E_q be the elliptic curve defined as

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

where

$$a_4(q) = -5 \sum_{n \ge 1} \frac{n^3 q^n}{1 - q^n}$$

and

$$a_6(q) = -\frac{5}{12} \sum_{n \ge 1} \frac{n^3 q^n}{1 - q^n} - \frac{7}{12} \sum_{n \ge 1} \frac{n^5 q^n}{1 - q^n}.$$

Let

$$(2.3) \qquad \phi : \mathbb{C}^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(\mathbb{C})$$

be the $\mathbb{C}$-analytic isomorphism given in [7, Chapter V, Theorem 1.1]. We are only concerned with elliptic nets with values in $\mathbb{R}$. By [11, Theorem 7.4] we know that such elliptic nets come from elliptic curves defined over $\mathbb{R}$. So from now on we assume that our elliptic curves are defined over $\mathbb{R}$. The following theorem will play an important role in our investigations.

Theorem 2.4. *Let $E/\mathbb{R}$ be an elliptic curve. Then the following assertions hold:*

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

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

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

(b) *The composition of the isomorphism in part* (a) *with the isomorphism ϕ defined in* (2.3), *yields an isomorphism*

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

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

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

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

Proof. See [7, Chapter V, Theorem 2.3]. □

Let $E/\mathbb{R}$ be an elliptic curve and let Λ be the lattice associated with E such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. We denote by $\pi : E_q \to E$ the isomorphism in Theorem 2.4(a). Let τ be a complex number associated to q such that $q = e^{2\pi i \tau}$ and let Λ_τ be the lattice generated by $[\tau, 1]$. Since $E \cong E_q$, there exists an $\alpha \in \mathbb{C}^*$ such that $\Lambda = \alpha \Lambda_\tau$. Then the multiplication by α carries $\mathbb{C}/\Lambda_\tau$ isomorphically to $\mathbb{C}/\Lambda$. If we let z_i to be the corresponding complex number to $P_i \in E(\mathbb{R})$ under the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, then z_i/α will be the corresponding complex number to $\pi^{-1}(P_i) \in E_q(\mathbb{R})$ under the isomorphism $E_q(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$. From part (b) of Theorem 2.4, the map

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

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

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

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

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

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

Here we have used the fact that for a nonzero $\alpha \in \mathbb{C}^*$ we have $\sigma(\alpha z; \alpha\Lambda) = \alpha\sigma(z; \Lambda)$. Now substituting the value of $\Omega_{\mathbf{v}}\left(\alpha^{-1}\mathbf{z}; \Lambda_\tau\right)$ from Proposition 2.3 yields

$$(2.4) \quad \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) = \left(\frac{2\pi i}{\alpha}\right)^{\displaystyle\sum_{j=1}^{n} v_j^2 - \sum_{1 \leq j < k \leq n} v_j v_k - 1}$$

$$\cdot \prod_{j=1}^{n} u_j^{\frac{v_j^2 - v_j}{2}} \frac{\theta\left(\prod_{j=1}^{n} u_j^{v_j}, q\right)}{\prod_{j=1}^{n} \theta(u_j, q)^{2v_j^2 - \sum_{k=1}^{n} v_j v_k} \prod_{1 \leq j < k \leq n} \theta(u_j u_k, q)^{v_j v_k}},$$

where

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

In the following two sections, we compute the parity of terms in the right hand side of (2.4).

3. Proof of Theorem 1.13

Proposition 3.1. *Assume the assumptions of Theorem* 1.9 *and let*

$$\theta\left(\prod_{j=1}^{n} u_j^{v_j}, q\right)$$

be as defined in (2.4). *Then if there exists a nonnegative integer k such that $u_1, u_2, \ldots, u_k < 0$ and $u_{k+1}, u_{k+2}, \ldots, u_n > 0$, we have*

$$\text{Parity}\left[\theta\left(\prod_{j=1}^{n} u_j^{v_j}, q\right)\right] \equiv \begin{cases} \lfloor \sum_{i=1}^{n} v_i \beta_i \rfloor \pmod{2} & \text{if } \sum_{i=1}^{k} v_i \text{ is even,} \\ 0 \pmod{2} & \text{if } \sum_{i=1}^{k} v_i \text{ is odd,} \end{cases}$$

where β_i is given in Table 1.1.

Proof. Let $u_1, u_2, u_3, \ldots, u_k < 0$ and $u_{k+1}, u_{k+2}, u_{k+3}, \ldots, u_n > 0$. (Note that for $k = 0$, this reduces to $u_i > 0$ for $1 \leq i \leq n$.) For all $u_i < 0$ we can

write $u_i = (-1)|u_i|$. Thus the expansion for $\theta\left(\prod_{i=1}^{n} u_i^{v_i}, q\right)$ can be rewritten as

$$(3.1) \quad \left(1 - (-1)^{\sum_{i=1}^{k} v_i} \prod_{i=1}^{n} |u_i|^{v_i}\right)$$

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

We consider cases according to the sign of q.

Case I. Suppose that $q > 0$. Then from the above expression we deduce that if $\sum_{i=1}^{k} v_i$ is odd then $\theta\left(\prod_{i=1}^{n} u_i^{v_i}, q\right)$ is positive. For the case that $\sum_{i=1}^{k} v_i$ is even, the factor $1 - \prod_{i=1}^{n} |u_i|^{v_i}$ may be positive or negative. Thus we further split into two cases.

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

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

Hence for this case there are $\left\lfloor \sum_{i=1}^{n} v_i \log_q |u_i| \right\rfloor$ negative signs in the expression (3.1) for $\theta\left(\prod_{i=1}^{n} u_i^{v_i}, q\right)$.

Subcase II. Assume that $1 - \prod_{i=1}^{n} |u_i|^{v_i} < 0$. Following a similar argument to that used in Subcase I we have that,

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

Observe that since $1 - \prod_{i=1}^{n} |u_i|^{v_i} < 0$, we have $\sum_{i=1}^{n} (-v_i) \log_q |u_i| > 0$. Hence there are in total $\left\lfloor -\sum_{i=1}^{n} v_i \log_q |u_i| \right\rfloor + 1$ negative signs in expression (3.1) for $\theta\left(\prod_{i=1}^{n} u_i^{v_i}, q\right)$. (The addition of 1 in the count of negative signs comes from the factor $1 - \prod_{i=1}^{n} |u_i|^{v_i}$.)

Note that since $P_1, P_2, \ldots, P_n$ are linearly independent in $E(\mathbb{R})$, then by [11, Theorem 7.4] we have $\theta\left(\prod_{j=1}^{n} u_j^{v_j}, q\right) \neq 0$. Thus the subcase

$$1 - \prod_{i=1}^{n} |u_i|^{v_i} = 0$$

does not occur.

Now we claim that $\sum_{i=1}^{n} v_i \log_q |u_i|$ is not an integer. More generally, we claim that $\log_q |u_1|, \log_q |u_2|, \ldots, \log_q |u_n|$, and 1 are linearly independent over $\mathbb{Q}$. To see this suppose that there are integers $k_0, k_1, k_2, \ldots, k_n$ not all zero such that the sum $\sum_{i=1}^{n} k_i \log_q |u_i| + k_0 = 0$. Equivalently we have that

$\sum_{i=1}^n k_i z_i = -k_0$. Note that $1 \in \Lambda_\tau$, so under the isomorphism $\mathbb{C}/\Lambda_\tau \cong E(\mathbb{C})$ integers are mapped to the identity element of $E(\mathbb{C})$. Thus $\sum_{i=1}^n k_i z_i = -k_0$ under the isomorphism $\mathbb{C}/\Lambda_\tau \cong E(\mathbb{C})$ leads to $\sum_{i=1}^n k_i P_i = \mathcal{O}$. This contradicts our assumption that the points $P_1, P_2, \ldots, P_n$ are linearly independent in $E(\mathbb{R})$. Hence we have that $\log_q |u_1|, \log_q |u_2|, \ldots, \log_q |u_n|$, and 1 are linearly independent over $\mathbb{Q}$. (This also shows that each number $\log_q |u_i|$ is irrational.) Therefore the number $\sum_{i=1}^n v_i \log_q |u_i|$ can not be an integer. Using this fact and the property of the greatest integer function that

$$(3.2) \qquad \lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0 & \text{if } x \in \mathbb{Z}, \\ -1 & \text{if } x \notin \mathbb{Z}, \end{cases}$$

we see that the number of negative signs in Subcase II is

$$- \left\lfloor \sum_{i=1}^n v_i \log_q |u_i| \right\rfloor.$$

Therefore we can combine the results from these two subcases to get that

$$(3.3) \quad \text{Parity} \left[\theta \left(\prod_{i=1}^n u_i^{v_i}, q \right) \right] \equiv \left\lfloor \sum_{i=1}^n v_i \beta_i \right\rfloor \pmod 2 \quad \text{if } \sum_{i=1}^k v_i \text{ is even,}$$

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

Case II. Suppose that $q < 0$. Let $x = \prod_{i=1}^n u_i^{v_i}$. Note that in this case $u_i > 0$ for $1 \le i \le n$, hence $x > 0$. From definition of θ we have

$$\theta \left(\prod_{i=1}^n u_i^{v_i}, q \right) = \theta(x, q)$$

$$= (1 - x) \prod_{m \ge 1} \frac{(1 - xq^m)(1 - xq^{-m})}{(1 - q^m)^2}$$

$$= (1 - x) \left(\prod_{m \ge 1} \frac{(1 - xq^{2m})(1 - xq^{-2m})}{(1 - q^{2m})^2} \right)$$

$$\cdot \left(\prod_{m \ge 1} \frac{(1 - xq^{2m+1})(1 - xq^{-2m-1})}{(1 - q^{2m+1})^2} \right)$$

$$= \theta(x, q^2) \prod_{m \ge 1} \frac{(1 - xq^{2m+1})(1 - xq^{-2m-1})}{(1 - q^{2m+1})^2}.$$

Note that $1 - xq^{2m+1}$ and $1 - xq^{-2m-1}$ are both positive, since q is assumed to be negative. As a result

$$\prod_{m \ge 1} \frac{(1 - xq^{2m+1})(1 - xq^{-2m-1})}{(1 - q^{2m+1})^2} > 0,$$

and we get $\mathrm{Sign}\,[\theta(x,q)] = \mathrm{Sign}\,[\theta(x,q^2)]$. Since $q^2 > 0$ and $u_i > 0$, applying (3.3) we get

(3.4)
$$\mathrm{Parity}\left[\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q\Big)\right] \equiv \mathrm{Parity}\left[\theta\Big(\prod_{i=1}^{n} u_i^{v_i}, q^2\Big)\right] \equiv \left\lfloor \sum_{i=1}^{n} v_i\beta_i \right\rfloor \pmod{2},$$

where $\beta_i = \log_{q^2} u_i = \frac{1}{2}\log_{|q|} u_i$. □

We record two immediate corollaries from this proposition, which we will use in the next section.

Corollary 3.2. *Assume that u_i and q are normalized so that if $q > 0$ then $q < |u_i| < 1$, and for $q < 0$ we have $q^2 < u_i < 1$. Then $\theta(u_i, q) > 0$.*

Proof. If $q > 0$ and $u_i < 0$, then by Proposition 3.1 for $v_i = 1$ (odd) we have
$$\mathrm{Parity}\,[\theta(u_i, q)] \equiv 0 \pmod{2}.$$
Also if $q > 0$ and $u_i > 0$ or $q < 0$, then by Proposition 3.1 for $k = 0$ (even), we have
$$\mathrm{Parity}\,[\theta(u_i, q)] \equiv \lfloor \beta_i \rfloor = 0 \pmod{2},$$
since $0 < \beta_i < 1$. Thus in both cases $\theta(u_i, q)$ is positive. □

Corollary 3.3. *Assume that u_i, q, and β_i are defined as in Proposition* 3.1. *Then*
$$\mathrm{Parity}\,[\theta(u_i u_j, q)] \equiv \begin{cases} \lfloor \beta_i + \beta_j \rfloor \pmod{2} & \text{if } u_i u_j > 0, \\ 0 \pmod{2} & \text{if } u_i u_j < 0. \end{cases}$$

Proof. It follows from the result of Proposition 3.1. □

We now proceed with the main proof of this section.

Proof of Theorem 1.13. First of all note that for a nonsingular nondegenerate elliptic net $W : \mathbb{Z}^n \longrightarrow \mathbb{R}$ there exists an elliptic curve E defined over $\mathbb{R}$ and a collection $\mathbf{P} = (P_1, P_2, \ldots, P_n)$ of points in $E(\mathbb{R})$, such that
$$W(\mathbf{v}) = f(\mathbf{v})\Psi_{\mathbf{v}}(\mathbf{P}; E)$$
for any $\mathbf{v} \in \mathbb{Z}^n$. Here $f : \mathbb{Z}^n \longrightarrow \mathbb{R}^*$ is a quadratic form and $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ is the elliptic net associated to $\mathbf{P}$ and E. Moreover, since $W(\mathbf{v}) \neq 0$ for $\mathbf{v} \neq \mathbf{0}$ we have that $P_1, P_2, \ldots, P_n$ are n linearly independent points in $E(\mathbb{R})$ (see [11, Theorem 7.4]). Next observe that in the expression (2.4) the numbers u_j and q are in $\mathbb{R}^*$. Therefore the products containing u_j and q are also in $\mathbb{R}$. Also by [11, Theorem 4.4], since E is defined over $\mathbb{R}$ then $\Psi_{\mathbf{v}}(\mathbf{P}; E) \in \mathbb{R}$. Hence from (2.4) we conclude that $(2\pi i/\alpha)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \leq i < j \leq n} v_i v_j - 1} \in \mathbb{R}^*$. Note that this statement is true for all $\mathbf{v} \in \mathbb{Z}^n$, therefore for $n \geq 2$, taking $v_1 = 1, v_2 = 2$ and $v_i = 0$ for all $3 \leq i \leq n$, we get that $(2\pi i/\alpha)^2 \in \mathbb{R}^*$. Furthermore, taking $v_1 = 2$ and $v_i = 0$ for all $2 \leq i \leq n$ shows that $(2\pi i/\alpha)^3 \in \mathbb{R}^*$. Since

$(2\pi i/\alpha)^2$ and $(2\pi i/\alpha)^3 \in \mathbb{R}^*$, we have that $2\pi i/\alpha \in \mathbb{R}^*$. A similar result also holds if $n = 1$, by choosing $v_1 = 2$ and 3. Hence $2\pi i/\alpha$ is either a positive real number or a negative real number. Thus, after possibly replacing $W(\mathbf{v})$ with $(-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \le i < j \le n} v_i v_j - 1} W(\mathbf{v})$, we have

(3.5)
$$\mathrm{Sign}[W(\mathbf{v})] = \mathrm{Sign}\left[g(\mathbf{v})\right] \mathrm{Sign}\left[\prod_{i=1}^{n} u_i^{(v_i^2 - v_i)/2}\right] \mathrm{Sign}\left[\theta\left(\prod_{j=1}^{n} u_j^{v_j}, q\right)\right],$$

where
$$g(\mathbf{v}) = \frac{f_1(\mathbf{v})}{\displaystyle\prod_{j=1}^{n} \theta(u_j, q)^{2v_j^2 - \sum_{k=1}^{n} v_j v_k} \prod_{1 \le j < k \le n} \theta(u_j u_k, q)^{v_j v_k}}.$$

Here, if $\varepsilon = (-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \le i < j \le n} v_i v_j - 1}$ and if $W(\mathbf{v})$ was replaced by $\varepsilon W(\mathbf{v})$, then $f_1(\mathbf{v}) = \varepsilon f(\mathbf{v})$. Otherwise $f_1(\mathbf{v}) = f(\mathbf{v})$. Observe that $g(\mathbf{v})$ is a quadratic form. From (3.5) we have

(3.6) $\mathrm{Parity}[W(\mathbf{v})]$

$$= \mathrm{Parity}\left[g(\mathbf{v})\right] + \mathrm{Parity}\left[\prod_{i=1}^{n} u_i^{(v_i^2 - v_i)/2}\right] + \mathrm{Parity}\left[\theta\left(\prod_{j=1}^{n} u_j^{v_j}, q\right)\right].$$

We next deal with $\mathrm{Parity}\left[\prod_{i=1}^{n} u_i^{(v_i^2 - v_i)/2}\right]$. If all $u_i > 0$ this value is zero. Now assume that $u_1, u_2, u_3, \ldots, u_k < 0$ and $u_{k+1}, u_{k+2}, u_{k+3} \ldots u_n > 0$. Looking at values of v_i modulo 4, we get that

(3.7) $$\mathrm{Parity}\left[\prod_{i=1}^{n} u_i^{(v_i^2 - v_i)/2}\right] \equiv \sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor \pmod{2}.$$

Next we define $H : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ as follows. If $u_1, u_2, u_3, \ldots, u_k < 0$ and $u_{k+1}, u_{k+2}, u_{k+3} \ldots u_n > 0$, we set

$$H(\mathbf{v}) = \begin{cases} \left\lfloor \displaystyle\sum_{i=1}^{n} v_i \beta_i \right\rfloor + \displaystyle\sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor & \text{if } \displaystyle\sum_{i=1}^{k} v_i \text{ is even,} \\ \displaystyle\sum_{i=1}^{k} \left\lfloor \frac{v_i}{2} \right\rfloor & \text{if } \displaystyle\sum_{i=1}^{k} v_i \text{ is odd.} \end{cases}$$

From (3.6), Proposition 3.1, (3.7), and the expressions for $H(\mathbf{v})$, we conclude that
$$\mathrm{Parity}[g(\mathbf{v})W(\mathbf{v})] \equiv H(\mathbf{v}) \pmod{2}.$$

The proof is complete. □

4. Proof of Theorem 1.9

Proof of Theorem 1.9. First, note that in the proof of Proposition 3.1 we showed that $\beta_1, \ldots, \beta_n$ are n irrational numbers that are linearly independent over $\mathbb{Q}$. Moreover, as described in the proof of Theorem 1.13, $2\pi i/\alpha$ in (2.4) is a nonzero real number. From now on, without loss of generality, we will assume that $2\pi i/\alpha > 0$. (Note that if $2\pi i/\alpha < 0$ we can compute the sign of $\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$ by considering $(-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \leq i < j \leq n} v_i v_j - 1} \Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)$.) Since $2\pi i \alpha^{-1} > 0$, it does not play any role in determining the sign of (2.4). Thus from (2.4) we have that $\text{Parity}\big[\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)\big]$ in $\mathbb{Z}/2\mathbb{Z}$ is equal to

(4.1)

$$
\text{Parity}\left[\prod_{i=1}^{n} u_i^{(v_i^2 - v_i)/2}\right] + \text{Parity}\left[\theta\left(\prod_{i=1}^{n} u_i^{v_i}, q\right)\right]
$$

$$
+ \text{Parity}\left[\prod_{i=1}^{n} \theta(u_i, q)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j}\right] + \text{Parity}\left[\prod_{1 \leq i < j \leq n} \theta(u_i u_j, q)^{v_i v_j}\right].
$$

The first two terms of the above sum were computed in (3.7) and Proposition 3.1 respectively. By Corollary 3.2, we get that $\theta(u_i, q) > 0$, so the third summand is even. Thus,

(4.2)
$$
\text{Parity}\left[\prod_{i=1}^{n} \theta(u_i, q)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j}\right] \equiv 0 \pmod 2.
$$

Finally, for the last summand we have

$$
\text{Parity}\left[\prod_{1 \leq i < j \leq n} \theta(u_i u_j, q)^{v_i v_j}\right] \equiv \sum_{1 \leq i < j \leq n} v_i v_j \, \text{Parity}\left[\theta(u_i u_j, q)\right] \pmod 2.
$$

Note that in the range $1 \leq i < j \leq n$, we have $u_i u_j < 0$ only when $1 \leq i \leq k < j \leq n$. (That is, $u_i u_j > 0$ when $1 \leq i < j \leq k$ or $k + 1 \leq i < j \leq n$.) By Corollary 3.3 we have

$$
\text{Parity}\left[\theta(u_i u_j, q)\right] \equiv
\begin{cases}
0 \pmod 2 & \text{if } 1 \leq i \leq k < j \leq n, \\
\lfloor \beta_i + \beta_j \rfloor \pmod 2 & \text{otherwise.}
\end{cases}
$$

Therefore we get

(4.3)
$$
\text{Parity}\left[\prod_{1 \leq i < j \leq n} \theta(u_i u_j, q)^{v_i v_j}\right]
$$

$$
\equiv \sum_{1 \leq i < j \leq n} v_i v_j \, \text{Parity}\left[\theta(u_i u_j, q)\right]
$$

$$
\equiv \sum_{1 \leq i < j \leq k} v_i v_j \lfloor \beta_i + \beta_j \rfloor + \sum_{k+1 \leq i < j \leq n} v_i v_j \lfloor \beta_i + \beta_j \rfloor \pmod 2.
$$

Now applying (3.7), Proposition 3.1, (4.2), and (4.3) in (4.1) yield

$\text{Parity}[\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)]$

$$\equiv \begin{cases} \sum\limits_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum\limits_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \\ \quad + \left\lfloor \sum\limits_{i=1}^{n} v_i \beta_i \right\rfloor + \sum\limits_{i=1}^{k} \left\lfloor \dfrac{v_i}{2} \right\rfloor \pmod 2 \qquad \text{if } \sum_{i=1}^{k} v_i \text{ is even}, \\ \\ \sum\limits_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum\limits_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \\ \quad + \sum\limits_{i=1}^{k} \left\lfloor \dfrac{v_i}{2} \right\rfloor \pmod 2 \qquad\qquad \text{if } \sum_{i=1}^{k} v_i \text{ is odd}. \quad \square \end{cases}$$

5. Numerical Examples

We now give illustrations of various cases of Theorem 1.9 with the help of some examples. For sake of simplicity we only give examples for rank 2 elliptic nets. All the computations were done using mathematical software SAGE.

Keeping the assumptions and notations used in Theorem 1.9, for the case $n = 2$, the sign of either $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ or $(-1)^{v_1^2 + v_2^2 - v_1 v_2 - 1} \Psi_{\mathbf{v}}(\mathbf{P}; E)$, can be computed using one of the following parity formulas:

(5.1) $\text{Parity}[\Psi_{\mathbf{v}}(P; E)]$

$$\equiv \left\lfloor v_1 \beta_1 + v_2 \beta_2 \right\rfloor + \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 \pmod 2$$

(5.2) $\text{Parity}[\Psi_{\mathbf{v}}(P; E)]$

$$\equiv \begin{cases} \left\lfloor v_1 \beta_1 + v_2 \beta_2 \right\rfloor + \left\lfloor \dfrac{v_1}{2} \right\rfloor \pmod 2 & \text{if } v_1 \text{ is even}, \\ \left\lfloor \dfrac{v_1}{2} \right\rfloor \pmod 2 & \text{if } v_1 \text{ is odd}. \end{cases}$$

(5.3) $\text{Parity}[\Psi_{\mathbf{v}}(P; E)]$

$$\equiv \begin{cases} \left\lfloor v_1 \beta_1 + v_2 \beta_2 \right\rfloor + \left\lfloor \dfrac{v_2}{2} \right\rfloor \pmod 2 & \text{if } v_2 \text{ is even}, \\ \left\lfloor \dfrac{v_2}{2} \right\rfloor \pmod 2 & \text{if } v_2 \text{ is odd}. \end{cases}$$

(5.4) $\text{Parity}[\Psi_{\mathbf{v}}(P; E)]$

$$\equiv \begin{cases} \left\lfloor v_1 \beta_1 + v_2 \beta_2 \right\rfloor + \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 \\ \quad + \left\lfloor \dfrac{v_1}{2} \right\rfloor + \left\lfloor \dfrac{v_2}{2} \right\rfloor \pmod 2 & \text{if } v_1 + v_2 \text{ is even}, \\ \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 + \left\lfloor \dfrac{v_1}{2} \right\rfloor + \left\lfloor \dfrac{v_2}{2} \right\rfloor \pmod 2 & \text{if } v_1 + v_2 \text{ is odd}. \end{cases}$$

Here the two irrational numbers β_1 and β_2 are given by the rules in Table 1.1. The formula (5.1) is used when $u_1 > 0$ and $u_2 > 0$ and formula (5.2) is used for the case when $u_1 < 0$ and $u_2 > 0$. We use the formula (5.3) when $u_1 > 0$ and $u_2 < 0$. Finally the formula (5.4) is used when both $u_1 < 0$ and $u_2 < 0$.

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

Example 5.1. Let E be the elliptic curve defined over $\mathbb{R}$ given by the Weierstrass equation $y^2 + xy = x^3 - x^2 - 4x + 4$. Let $P_1 = (69/25, -532/125)$ and $P_2 = (2, -2)$ be two points in $E(\mathbb{R})$. Let $\mathbf{P} = (P_1, P_2)$. The following table presents the values of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ for $\mathbf{v} = (v_1, v_2)$ in the range $0 \leq v_1 \leq 3$ and $0 \leq v_2 \leq 5$.

$$\vdots$$

	-832	1232600000	430685595625000000	$33305696363315761718750000000$	
	112	-12560000	-18772893750000	$121093285553785156250000000$	
$\cdots$	-4	-165500	-141878687500	-1754232556789062500	$\cdots$
	-2	-150	196317500	-1270400610718750	
	1	95	152725	-181061702375	
	$\mathbf{0}$	5	-3595	63803440	

$$\vdots$$

TABLE 5.1. Elliptic net $\Psi(\mathbf{P}; E)$ associated to elliptic curve $E : y^2 + xy = x^3 - x^2 - 4x + 4$ and points $P_1 = (69/25, -532/125)$, $P_2 = (2, -2)$.

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

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

$$q = 0.00011996329444927815129854801426436678 40\ldots\ldots,$$
$$u_1 = 0.08032857195868687779619226593992649096 08\ldots\ldots,$$
$$u_2 = 0.03600942542966326797848808049477306988 456\ldots\ldots$$

Since $u_1, u_2 > 0$, by employing Theorem 1.9, the sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ up to a factor of $(-1)^{v_1^2 + v_2^2 - v_1 v_2 - 1}$ can be calculated by (5.1). Since Theorem 1.9 gives either sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ or $(-1)^{v_1^2 + v_2^2 - v_1 v_2 - 1}\Psi_{\mathbf{v}}(\mathbf{P}; E)$.

By computing the sign of $\Psi_{(2,2)}(\mathbf{P}; E)$ using (5.1) we conclude that in this case the parity is given by the formula

$$\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)]$$
$$\equiv \left\lfloor v_1 \beta_1 + v_2 \beta_2 \right\rfloor + \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 + (v_1 + v_2 + v_1 v_2 + 1) \pmod 2$$

with

$$\beta_1 = 0.2793020829801927957749331343976812416467\dots,$$
$$\beta_2 = 0.3681717984734797193981452826601334954064\dots.$$

Next we illustrate the truth of our formula using two special cases.

$$\mathrm{Sign}[\Psi_{(1,3)}(\mathbf{P};E)] = (-1)^{\lfloor \beta_1 + 3\beta_2 \rfloor + 3\lfloor \beta_1 + \beta_2 \rfloor + 8} = -1$$

and

$$\mathrm{Sign}[\Psi_{(3,4)}(\mathbf{P};E)] = (-1)^{\lfloor 3\beta_1 + 4\beta_2 \rfloor + 12\lfloor \beta_1 + \beta_2 \rfloor + 20} = 1,$$

which agree with the signs from the above table.

Example 5.2. Let E be the elliptic curve defined over $\mathbb{R}$ given by the Weierstrass equation $y^2 + xy = x^3 - x^2 - 4x + 4$. Let $P_1 = (-1, 3)$ and $P_2 = (3, 2)$ be two points in $E(\mathbb{R})$ so that $\mathbf{P} = (P_1, P_2)$. The following table presents the values of $\Psi_{\mathbf{v}}(\mathbf{P};E)$ for $\mathbf{v} = (v_1, v_2)$ in the range $0 \le v_1 \le 3$ and $0 \le v_2 \le 6$.

		$\vdots$	
-219900856	71486913947	48178148140103	-112925826309806338
-495235	58762243	3246745150	-20471103308793
-749	170718	-24093133	-16532329817
62	2291	-154139	-28273396
7	67	-1256	-101083
1	4	3	-1579
$\mathbf{0}$	1	5	-94
		$\vdots$	

TABLE 5.2. Elliptic net $\Psi(\mathbf{P};E)$ associated to elliptic curve $E : y^2 + xy = x^3 - x^2 - 4x + 4$ and points $P_1 = (-1, 3)$, $P_2 = (3, -2)$.

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

$$q = 0.00011996329444927815129854801426436678 40\dots\dots,$$
$$u_1 = -0.28342295594867907205363849972450866 3516\dots\dots,$$
$$u_2 = 0.0012966787197744796316630601458950482 3338\dots\dots$$

Observe that q is the same as in the previous example. Further since $u_1 < 0$ and $u_2 > 0$, by using Theorem 1.9, parity of $\Psi_{\mathbf{v}}(\mathbf{P};E)$ is either given by (5.2) or

$$(5.5) \qquad \mathrm{Parity}[\Psi_{\mathbf{v}}(\mathbf{P};E)]$$
$$\equiv \begin{cases} \left\lfloor v_1\beta_1 + v_2\beta_2 \right\rfloor + \left\lfloor \dfrac{v_1}{2} \right\rfloor + v_2 + 1 \pmod 2 & \text{if } v_1 \text{ is even} \\ \left\lfloor \dfrac{v_1}{2} \right\rfloor \pmod 2 & \text{if } v_1 \text{ is odd} \end{cases}$$

with

$$\beta_1 = 0.1396510414900963978874665671988406208233\ldots,$$
$$\beta_2 = 0.7363435969469594387962905653202669908128\ldots.$$

By computing the sign of $\Psi_{(2,2)}(\mathbf{P}; E)$ using (5.2) and (5.5) we conclude that in this case the parity is given by formula (5.5). Next we illustrate the truth of our formula using two special cases.

$$\mathrm{Sign}[\Psi_{(2,3)}(\mathbf{P}; E)] = (-1)^{\mathrm{Parity}[\Psi_{(2,3)}(\mathbf{P};E)]} = (-1)^{\lfloor 2\beta_1 + 3\beta_2 \rfloor + \lfloor 1 \rfloor + 3 + 1} = -1$$

and

$$\mathrm{Sign}[\Psi_{(1,5)}(\mathbf{P}; E)] = (-1)^{\lfloor \frac{1}{2} \rfloor} = 1$$

Again these agree with the signs from the above table.

Example 5.3. Let E be the elliptic curve defined over $\mathbb{R}$ given by the Weierstrass equation $y^2 + y = x^3 + x^2 - 2x$. Let $P_1 = (-1, 1)$ and $P_2 = (0, -1)$ be two points in $E(\mathbb{R})$. Let $\mathbf{P} = (P_1, P_2)$. The following table presents the values of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ for $\mathbf{v} = (v_1, v_2)$ in the range $-5 \le v_1 \le 5$ and $-2 \le v_2 \le 2$.

						⋮					
	535	44	-7	-1	1	-1	-4	17	151	-55	-106201
	1187	67	1	-2	-1	1	1	-5	26	709	-19061
$\cdots$	-3376	129	19	-3	-1	**0**	1	3	-19	-129	3376	$\cdots$
	19061	-709	-26	5	-1	-1	1	2	-1	-67	-1187
	106201	55	-151	-17	4	1	-1	1	7	-44	-535
						⋮					

TABLE 5.3. Elliptic net $\Psi(\mathbf{P}; E)$ associated to elliptic curve $E : y^2 + y = x^3 + x^2 - 2x$ and points $P_1 = (-1, 1)$, $P_2 = (0, -1)$.

The above array is centered at $\Psi_{(0,0)}(\mathbf{P}; E) = 0$. The bottom left corner represent the value $\Psi_{(-5,-2)}(\mathbf{P}; E)$ and the upper right corner represents $\Psi_{(5,2)}(\mathbf{P}; E)$. For this example we have the isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ such that $P_1 \longleftrightarrow u_1$ and $P_2 \longleftrightarrow u_2$ with the explicit values

$$q = 0.0003578597615372348081828089670285622329 2 \ldots \ldots,$$
$$u_1 = -0.2170771835085414203450101536155224134341 \ldots \ldots,$$
$$u_2 = -0.0077622720300518161218942441500824493219 \ldots \ldots.$$

Since $u_1 < 0$ and $u_2 < 0$, by using Theorem 1.9, sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ is given by either (5.4) or

$$(5.6) \quad \text{Parity}[\Psi_{\mathbf{v}}(P; E)]$$

$$\equiv \begin{cases} \left\lfloor v_1\beta_1 + v_2\beta_2 \right\rfloor + \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 + \\ \quad \left\lfloor \dfrac{v_1}{2} \right\rfloor + \left\lfloor \dfrac{v_2}{2} \right\rfloor + v_1 v_2 + 1 \quad (\bmod\ 2) \quad \text{if } v_1 + v_2 \text{ is even} \\[2mm] \left\lfloor \beta_1 + \beta_2 \right\rfloor v_1 v_2 + \left\lfloor \dfrac{v_1}{2} \right\rfloor + \left\lfloor \dfrac{v_2}{2} \right\rfloor \quad (\bmod\ 2) \quad \text{if } v_1 + v_2 \text{ is odd} \end{cases}$$

with

$$\beta_1 = 0.19249290511394232281737656529730009963007\ldots\ldots,$$
$$\beta_2 = 0.61225633869594764202204647455919443449939\ldots\ldots$$

By computing the sign of $\Psi_{(2,2)}(\mathbf{P}; E)$ using (5.4) and (5.6) we conclude that in this case the parity is given by formula (5.6).

Example 5.4. Let E be the elliptic curve defined over $\mathbb{R}$ given by Weierstrass equation $y^2 = x^3 - 7x + 10$. Let $P_1 = (-2, 4)$ and $P_2 = (1, 2)$ be two linear independent points in $E(\mathbb{R})$. Let $\mathbf{P} = (P_1, P_2)$. The following table presents the values of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ for $\mathbf{v} = (v_1, v_2)$ in the range $0 \leq v_1 \leq 4$ and $0 \leq v_2 \leq 6$.

			$\vdots$			
	-54525952	1086324736	81340137472	-15800157077504	-29481936481157120	
	-163840	-950272	131956736	30954979328	-31977195339776	
	-2048	-17408	280576	85124096	30585993216	
$\cdots$	32	-352	-9440	979488	449423648	$\cdots$
	4	-4	-276	-16028	8814788	
	1	3	-31	-1697	67225	
	$\mathbf{0}$	1	8	-409	-65488	
			$\vdots$			

TABLE 5.4. Elliptic net $\Psi(\mathbf{P}; E)$ associated to elliptic curve $E : y^2 = x^3 - 7x + 10$ and points $P_1 = (-2, 4)$, $P_2 = (1, 2)$.

In the above array the bottom left corner represents the value $\Psi_{(0,0)}(\mathbf{P}; E)$ and the upper right corner represents $\Psi_{(4,6)}(\mathbf{P}; E)$. In this case there is an isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ such that $P_1 \longleftrightarrow u_1$ and $P_2 \longleftrightarrow u_2$ with explicit values

$$q = -0.00040774898223432390576678547418175491 72\ldots\ldots,$$
$$u_1 = 0.0012019363489838374293496967354004186015 19\ldots\ldots,$$
$$u_2 = 0.0089929799179066516646207809697264983128 14\ldots\ldots$$

Since $u_1, u_2 > 0$, by using Theorem 1.9 and calculating the sign of

$$\Psi_{(2,2)}(\mathbf{P}; E),$$

we observe that the sign of $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ in this case is given by (5.1) with

$$\beta_1 = 0.4307458699792390794239197192204249668246\ldots\ldots,$$
$$\beta_2 = 0.3018191057841811111031361738974315389666\ldots\ldots.$$

6. Uniform distribution of signs

Definition 6.1. Let $(S(\mathbf{v}))$ be an n-dimensional array of real numbers. For any a and b with $0 \le a < b \le 1$ and for any positive integers $V_1, V_2, \ldots, V_n$ denote

$$C\big([a, b);\ V_1, V_2, \ldots, V_n\big)$$
$$= \#\Big\{\mathbf{v} = (v_1, v_2, \ldots, v_n); 1 \le v_i \le V_i \text{ for } 1 \le i \le n \text{ and } \{S(\mathbf{v})\} \in [a, b)\Big\},$$

where $\{S(\mathbf{v})\}$ is the fractional part of $S(\mathbf{v})$. Then the array $(S(\mathbf{v}))$ is said to be uniformly distributed mod 1 if

$$\lim_{V_1, V_2, \ldots, V_n \to \infty} \frac{C([a, b); V_1, V_2, \ldots, V_n)}{V_1 V_2 \ldots V_n} = b - a.$$

Lemma 6.2 (Weyl Criterion). *The array $(S(\mathbf{v}))$ is uniformly distributed mod 1 if and only if*

$$\lim_{V_1, V_2, \ldots, V_n \to \infty} \frac{1}{V_1 V_2 \ldots V_n} \sum_{1 \le v_1 \le V_1} \sum_{1 \le v_2 \le V_2} \cdots \sum_{1 \le v_n \le V_n} e^{2\pi i h S(\mathbf{v})} = 0$$

for all integers $h \ne 0$.

Proof. The proof follows along the same lines as the proof for 2-dimensional case. See [2, Chapter 1, Theorem 2.9]. □

Proposition 6.3. *Let θ_1 be an irrational number and let $\theta_2, \theta_3, \ldots, \theta_n$, and θ_0 be arbitrary real numbers. Then the array $(v_1\theta_1 + v_2\theta_2 + \cdots + v_n\theta_n + \theta_0)$ is uniformly distributed mod 1.*

Proof. This is a direct consequence of Theorem 6.2. See also [2, Example 2.9]. □

The following proposition is a generalization of a part of Theorem 3.1 of [5] for sequences to arrays.

Proposition 6.4. *For an irrational number θ_1 and real numbers $\theta_2, \ldots \theta_n$, θ_0, the array*

(6.1)
$$\left(\Big\lfloor v_1\theta_1 + v_2\theta_2 + \cdots + v_n\theta_n + \theta_0 \Big\rfloor\right)$$

is uniformly distributed mod m.

Proof. Proposition 6.3 for the irrational number θ_1/m and real numbers $\theta_2/m, \ldots, \theta_n/m, \theta_0/m$ yields that the array of real numbers $(v_1\frac{\theta_1}{m} + v_2\frac{\theta_2}{m} +$

$\cdots + v_n \frac{\theta_n}{m} + \frac{\theta_0}{m})$ is uniformly distributed mod 1. Thus we conclude that the array of fractional part

$$\left\{ v_1 \frac{\theta_1}{m} + v_2 \frac{\theta_2}{m} + \cdots + v_n \frac{\theta_n}{m} + \frac{\theta_0}{m} \right\}$$
$$= v_1 \frac{\theta_1}{m} + v_2 \frac{\theta_2}{m} + \cdots + v_n \frac{\theta_n}{m} + \frac{\theta_0}{m} - \left\lfloor v_1 \frac{\theta_1}{m} + v_2 \frac{\theta_2}{m} + \cdots + v_n \frac{\theta_n}{m} + \frac{\theta_0}{m} \right\rfloor$$

is uniformly distributed in the unit interval $[0, 1)$. By multiplying the terms of the array $(\{v_1\theta_1/m + v_2\theta_2/m + \cdots + v_n\theta_n/m + \theta_0/m\})$ with m we see that the array of real numbers

$$v_1\theta_1 + v_2\theta_2 + \cdots + v_n\theta_n + \theta_0 - m \left\lfloor v_1 \frac{\theta_1}{m} + v_2 \frac{\theta_2}{m} + \cdots + v_n \frac{\theta_n}{m} + \frac{\theta_0}{m} \right\rfloor$$

is uniformly distributed over the interval $[0, m)$ on the real line. Hence by taking the integer parts of the terms of the above array we conclude that the terms of the array

(6.2)
$$\left\lfloor v_1\theta_1 + v_2\theta_2 + \cdots + v_n\theta_n + \theta_0 - m \left\lfloor v_1 \frac{\theta_1}{m} + v_2 \frac{\theta_2}{m} + \cdots + v_n \frac{\theta_n}{m} + \frac{\theta_0}{m} \right\rfloor \right\rfloor$$
$$= \left\lfloor v_1\theta_1 + v_2\theta_2 + \cdots + v_n\theta_n + \theta_0 \right\rfloor - m \left\lfloor v_1 \frac{\theta_1}{m} + v_2 \frac{\theta_2}{m} + \cdots + v_n \frac{\theta_n}{m} + \frac{\theta_0}{m} \right\rfloor$$

are uniformly distributed modulo m. Furthermore, the removal of the terms $m \lfloor v_1\theta_1/m + v_2\theta_2/m + \cdots + v_n\theta_n/m + \theta_0/m \rfloor$, from the array (6.2), does not effect the uniform distribution mod m. □

Corollary 6.5. *Let $(S(\mathbf{v}))$ be an array of integers that is uniformly distributed mod m. Let $(c(\mathbf{v}))$ be an integer array which is constant mod m. Then the array $(S(\mathbf{v}) + c(\mathbf{v}))$ is uniformly distributed mod m. In particular, under the assumptions of Theorem 6.4, the sequence*

(6.3)
$$\left(\left\lfloor v_1\theta_1 + v_2\theta_2 + \cdots + v_n\theta_n + \theta_0 \right\rfloor + c(\mathbf{v}) \right)$$

is uniformly distributed mod m for a fixed real number θ_0.

Proof. The first assertion follows from Definition 1.14. The second one follows from Proposition 6.4 and the first assertion. □

Proof of Theorem 1.15. Let $(S(\mathbf{v}))$ be the n-dimensional array given by the formulas at the right-hand side of the congruences (1.8), (1.9a), and (1.9b). We show that $(S(\mathbf{v}))$ is uniformly distributed mod 2. In order to do this, we consider $(S(\mathbf{v}))$ as union of 2^n subarrays $(S_\ell(\mathbf{v}))$ $(1 \le \ell \le 2^n)$ according to the parity of v_i's. It is enough to prove that $(S_\ell(\mathbf{v}))$ is uniformly distributed mod 2.

For fixed ℓ, the expression for $S_\ell(\mathbf{v})$ is one of the three formulas given in the right-hand side of the congruences (1.8), (1.9a), and (1.9b). We consider three cases.

Case I. From (1.8) we have

$$S_\ell(\mathbf{v}) = \left\lfloor \sum_{i=1}^n v_i \beta_i \right\rfloor + \sum_{1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j.$$

Since β_i's are fixed irrational numbers and the parity of v_i's are fixed, $\left(\sum_{1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \right)$ is a fixed array $(c(\mathbf{v}))$ mod 2 and thus, by Corollary 6.5, $(S_\ell(\mathbf{v}))$ is uniformly distributed mod 2.

Case II. Similar to Case I,

$$\left(\sum_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \right)$$

is a fixed array $(c(\mathbf{v}))$ mod 2. Thus, from (1.9a), we have

$$S_\ell(\mathbf{v}) \equiv \left\lfloor \sum_{i=1}^n v_i \beta_i \right\rfloor + \sum_{i=1}^k \left\lfloor \frac{v_i}{2} \right\rfloor + c(\mathbf{v}) \pmod 2$$

$$\equiv \left\lfloor \sum_{i=1}^k \left\lfloor \frac{v_i}{2} \right\rfloor (2\beta_i + 1) + \sum_{i=k+1}^n \left\lfloor \frac{v_i}{2} \right\rfloor (2\beta_i) + \sum_{i=1}^n \eta_i \beta_i \right\rfloor + c(\mathbf{v}) \pmod 2,$$

where $\eta_i \in \{0, 1\}$ according to the parity of v_i. Since β_i's are fixed irrational numbers and the parity of v_i's are fixed, $\sum_{i=1}^n \eta_i \beta_i$ is a fixed real number θ_0 and thus, by Corollary 6.5, $(S_\ell(\mathbf{v}))$ is uniformly distributed mod 2.

Case III. Similar to Case II,

$$\left(\sum_{1 \le i < j \le k} \lfloor \beta_i + \beta_j \rfloor v_i v_j + \sum_{k+1 \le i < j \le n} \lfloor \beta_i + \beta_j \rfloor v_i v_j \right)$$

is a fixed array $(c(\mathbf{v}))$ mod 2. Thus, from (1.9b), we have

$$S_\ell(\mathbf{v}) \equiv \sum_{i=1}^k \left\lfloor \frac{v_i}{2} \right\rfloor + c(\mathbf{v}) \pmod 2,$$

which is uniformly distributed mod 2 by Corollary 6.5 and the fact that $\left(\sum_{i=1}^k \left\lfloor \frac{v_i}{2} \right\rfloor \right)$ is uniformly distributed mod m. This completes the proof. $\square$

Remark 6.6. We remark that inclusion of the factor

$$(-1)^{\sum_{i=1}^n v_i^2 - \sum_{1 \le i < j \le n} v_i v_j - 1}$$

does not affect the result of Theorem 1.15. Note that

$$\text{Parity}\left[(-1)^{\sum_{i=1}^{n} v_i^2 - \sum_{1 \leq i < j \leq n} v_i v_j - 1}\right] \equiv \sum_{1 \leq i \leq j \leq n} v_i v_j + 1 \pmod{2},$$

which is a constant for v_i's with fixed parities. Thus, we can apply Corollary 6.5.

7. Relation with denominator sequences

Proof of Corollary 1.17. First of all observe that since all the terms of a denominator net is positive hence the quadratic form given by (1.14) is also positive. Therefore from (1.13) it follows that

$$(7.1) \qquad \text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)] = \text{Parity}[\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)].$$

Now consider $W(\mathbf{v}) : \mathbb{Z}^n \longrightarrow \mathbb{Q}$ such that

$$|W(\mathbf{v})| = D_{\mathbf{v} \cdot \mathbf{P}} \qquad \text{for all } \mathbf{v} \in \mathbb{Z}^n,$$

and define

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

where the $\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)]$ is given in Theorem 1.9. Thus,

$$(7.2) \qquad W(\mathbf{v}) = (-1)^{\text{Parity}[\Psi_{\mathbf{v}}(\mathbf{P}; E)]} D_{\mathbf{v} \cdot \mathbf{P}}.$$

By employing (1.15) and (7.1) we rewrite (7.2) as

$$W(\mathbf{v}) = (-1)^{\text{Parity}[\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)]} |\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)|$$
$$= \text{Sign}[\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)] |\hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E)|$$
$$= \hat{\Psi}_{\mathbf{v}}(\mathbf{P}; E).$$

Hence $W(\mathbf{v})$ is an elliptic net by [11, Proposition 6.1] and the fact that $\Psi_{\mathbf{v}}(\mathbf{P}; E)$ is an elliptic net. $\square$

References

[1] AKBARY, AMIR; BLEANEY, JEFF; YAZDANI, SOROOSH. On symmetries of elliptic nets and valuations of net polynomials. *J. Number Theory* **158** (2016), 185–216. MR3393547, Zbl 06479846, arXiv:1408.6623, doi: 10.1016/j.jnt.2015.06.005.

[2] KUIPERS, LAUWERENS; NIEDERREITER, HARALD. Uniform distribution of sequences. *Dover Publications*, 2006. xviii, 390 p.

[3] KUMAR, MANOJ. The signs in an elliptic net. M.Sc. Thesis, *University of Lethbridge*, 2014. http://hdl.handle.net/10133/3625.

[4] LANG, SERGE. Elliptic curves: Diophantine analysis. Grundlehren der Mathematischen Wissenschaften, 231. *Springer-Verlag, Berlin-New York*, 1978. xi+261 pp. ISBN: 3-540-08489-4. MR0518817, Zbl 0388.10001, doi: 10.1007/978-3-662-07010-9.

[5] NIVEN, IVAN. Uniform distribution of sequences of integers. *Trans. Amer. Math. Soc.* **98** (1961), 52–61. MR0120214, Zbl 0096.03102, doi: 10.2307/1993512.

[6] Shipsey, Rachel. Elliptic divisibility sequences. Ph.D. Thesis, *Goldsmith's College, University of London*, 2000. `http://homepages.gold.ac.uk/rachel/`.

[7] Silverman, Joseph H. Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. *Springer-Verlag, New York*, 1994. xiv+525 pp. ISBN: 0-387-94328-5. MR1312368, Zbl 0911.14015, doi: 10.1007/978-1-4612-0851-8.

[8] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Text in Mathematics, 106. *Springer, Dordrecht*, 2009. xx+513 pp. ISBN: 978-0-387-09493-9. MR2514094, Zbl 1194.11005, doi: 10.1007/978-0-387-09494-6.

[9] Silverman, Joseph H.; Stephens, Nelson. The sign of an elliptic divisibility sequence. *J. Ramanujan Math. Soc.* **21** (2006), no. 1, 1–17. MR2226354, Zbl 1148.11013, arXiv:math/0402415.

[10] Silverman, Joseph H.; Tate, John T. Rational points on elliptic curves. Undergraduate Texts in Mathematics. *Springer-Verlag, New York*, 1992. MR1171452, Zbl 0752.14034, doi: 10.1007/978-1-4757-4252-7.

[11] Stange, Katherine. Elliptic nets and elliptic curves. *Algebra and Number Theory* **5** (2011), no. 2, 197–229. MR2833790, Zbl 1277.11063, arXiv:0710.1316, doi: 10.2140/ant.2011.5.197.

[12] Swart, Christine S. Elliptic curves and related sequences. PhD Thesis, *Royal Holloway and Bedford New College, University of London*, 2003. `https://www.researchgate.net/publication/238223247_Elliptic_curves_and_related_sequences`.

[13] Ward, Morgan. Memoir on elliptic divisibility sequences. *Amer. J. Math.* **70** (1948), 31–74. MR0023275, Zbl 0035.03702, doi: 10.2307/2371930.

(Amir Akbary) Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada
`amir.akbary@uleth.ca`

(Manoj Kumar) Pure Mathematics, University of Waterloo, 200 University Ave W, Waterloo, Ontario, N2L3G1, Canada
`m29kumar@uwaterloo.ca`

(Soroosh Yazdani) Pure Mathematics, University of Waterloo, 200 University Ave W, Waterloo, Ontario, N2L3G1, Canada
`syazdani@gmail.com`

This paper is available via `http://nyjm.albany.edu/j/2017/23-54.html`.