Bull. Aust. Math. Soc. (First published online 2024), page 1 of 14*
doi:10.1017/S0004972724000583
*Provisional—final page numbers to be inserted when paper edition is published

THEOREM OF WARD ON SYMMETRIES OF ELLIPTIC NETS

L. DEWAGHE

(Received 16 March 2024; accepted 29 May 2024)

Abstract

We present a new version of a generalisation to elliptic nets of a theorem of Ward ['Memoir on elliptic divisibility sequences', *Amer. J. Math.* **70** (1948), 31–74] on symmetry of elliptic divisibility sequences. Our results cover all that is known today.

2020 *Mathematics subject classification*: primary 14H52; secondary 11B50, 11B83, 11G05.

Keywords and phrases: elliptic curve, elliptic divisibility sequences, division polynomials, elliptic nets.

1. Introduction

This paper concerns a generalisation of a theorem of Ward [7] on symmetry of elliptic sequences to the case of nondegenerate elliptic nets of rank d ($d \in \mathbb{N}$) associated to an elliptic curve E and points on E. In our opinion, it is the most comprehensive form that we can hope to achieve.

Symmetries of such elliptic nets written explicitly in a form similar to Ward's theorem [7] are only known for the cases $d = 1$ [6] and $d = 2$ [4, 6]. To get the right shape for all d, an essential point of our demonstration consists of showing that appropriate quotients of two elliptic nets follow a geometric progression. This new approach allows us to obtain a simple proof of the generalisation of the symmetry theorem in Ward's form. In this way, we unify all the results known to date: for $d = 1$, Ward [7, Theorem 8.1], Stange [4, Theorem 10.2.2] and [6, Theorem 4], and the author [2, Theorem 1]; for $d = 2$, [4, Lemma 10.2.5] and [6, Theorem 5]; and for $d > 2$, [4, Theorem 10.2.3] and Akbary *et al.* [1, Theorems 1.12 and 1.13].

Let E be an elliptic curve over a field $\mathbb{K}$ (see [3]). To simplify, we assume that the characteristic is different from 2 and 3. Then

$$E(\mathbb{K}) = \{[X : Y : Z] \in \mathbb{P}^2(\mathbb{K}) \mid \mathcal{F}(X, Y, Z) = 0\} = \{(x, y) \in \mathbb{K}^2 \mid \mathcal{F}(x, y, 1) = 0\} \cup \{0_E\},$$

with $\mathcal{F}(X,Y,Z) = Y^2Z - (X^3 + aXZ^2 + bZ^3)$, $a, b \in \mathbb{K}$ such that $4a^3 + 27b^2 \neq 0$ and 0_E the unique point at infinity of the curve. The group structure of $E(\mathbb{K})$ is defined by the chord and tangent method with the neutral element 0_E.

We introduce division polynomials $\psi_m(x,y), m \in \mathbb{Z}$, of an elliptic curve E over the field $\mathbb{K}$ with an affine equation $y^2 = x^3 + ax + b$ (see [8]) by

$$\psi_0(x,y) = 0, \quad \psi_1(x,y) = 1, \quad \psi_2(x,y) = 2y \quad \psi_3(x,y) = 3x^4 + 6ax^2 + 12bx - a^2,$$
$$\psi_4(x,y) = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),$$

and for n a natural integer, $\psi_{-n} = -\psi_n$. Then, for all (m,n) in $\mathbb{Z}^2$,

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2. \tag{1.1}$$

This equality can be used for the product $\psi_\imath\psi_\jmath$ when the integers $\imath$ and $\jmath$ have the same parity. Any solution over an arbitrary integral domain of (1.1) is called an *elliptic sequence*. Also,

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1} \quad \text{and} \quad \psi_{2n}\psi_2 = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$$

for n in $\mathbb{Z}$. Note also Stephen Nelson's form (see [4, page 22]): for all $(\alpha,\beta,\gamma,\delta) \in \mathbb{Z}^4$,

$$\psi_{\alpha+\beta}\psi_{\alpha-\beta}\psi_{\gamma+\delta}\psi_{\gamma-\delta} + \psi_{\alpha+\gamma}\psi_{\alpha-\gamma}\psi_{\delta+\beta}\psi_{\delta-\beta} + \psi_{\alpha+\delta}\psi_{\alpha-\delta}\psi_{\beta+\gamma}\psi_{\beta-\gamma} = 0. \tag{1.2}$$

Division polynomials have partial periodicity, called symmetry.

THEOREM 1.1 [2]. *Let $\mathbb{F}_q$ be a finite field, let $E/\mathbb{F}_q$ be an elliptic curve and let $P \in E(\bar{\mathbb{F}}_q)$ be a point of exact order $u \geq 2$. Then there exists $\omega \in \bar{\mathbb{F}}_q$, depending on P, such that the following hold.*

(1) *If $u \geq 3$, then for all k and v in $\mathbb{Z}$:*

- *if $u = 2m$, we have $\psi_{ku+v}(P) = (-\omega^m)^{k^2}\omega^{kv}\psi_v(P)$;*
- *if $u = 2m+1$, we have $\psi_{ku+v}(P) = (-\omega^{2m+1})^{k^2}(\omega^2)^{kv}\psi_v(P)$.*

(2) *If $u = 2$, then for all $k \in \mathbb{Z}$,*

$$\psi_{4k+1}(P) = (-1)^k\psi_3^{k(2k+1)}, \quad \psi_{4k+3}(P) = (-1)^k\psi_3^{(k+1)(2k+1)}.$$

Note that the proof works for any field $\mathbb{K}$ and that $\psi_u(P) = 0$. Furthermore, if $u = 2m$, then $\omega = (\psi_{m+1}/\psi_{m-1})(P)$; otherwise $\omega = (\psi_{m+1}/\psi_m)(P)$. This result will become a particular case of our generalisation and is already a precision of Ward's symmetry theorem for the elliptic sequence (ψ_n).

THEOREM 1.2 [7]. *Let W be an integer elliptic sequence such that $W(1) = 1$ and $W(2) \mid W(4)$. Let p be an odd prime and suppose that $W(2)W(3) \not\equiv 0 \bmod p$. Let u be the rank of apparition of W with respect to p (that is, $W(u) \equiv 0$ and $W(m) \not\equiv 0$ for any $m \mid u$). Then there exist integers $\mathcal{A}$ and C such that*

$$W(ku+v) = \mathcal{A}^{kv}C^{k^2}W(v) \quad \textit{for all } k, v \in \mathbb{N}. \tag{1.3}$$

https://doi.org/10.1017/S0004972724000583 Published online by Cambridge University Press

We usually call the smallest positive index of a vanishing term the *rank of zero-apparition*. If we consider the elliptic sequence $W = \psi(P)$, the rank of zero-apparition is the order of P on E.

In [5], Stange generalised the concept of an elliptic sequence to a d-dimensional array, called an elliptic net. An elliptic net in this article is a map $W : \mathbb{Z}^d \to \mathbb{K}$ such that, for all $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s}$ in $\mathbb{Z}^d$,

$$W(\mathbf{p}+\mathbf{q}+\mathbf{s})W(\mathbf{p}-\mathbf{q})W(\mathbf{r}+\mathbf{s})W(\mathbf{r}) + W(\mathbf{q}+\mathbf{r}+\mathbf{s})W(\mathbf{q}-\mathbf{r})W(\mathbf{p}+\mathbf{s})W(\mathbf{p}) + W(\mathbf{r}+\mathbf{p}+\mathbf{s})W(\mathbf{r}-\mathbf{p})W(\mathbf{q}+\mathbf{s})W(\mathbf{q}) = 0. \quad (1.4)$$

We have $W(\mathbf{0}) = 0$, where $\mathbf{0}$ is the additive identity element of $\mathbb{Z}^d$, since $\mathrm{char}(\mathbb{K}) \neq 3$. Stange proved that we can compute $W(\mathbf{v})$ for all $\mathbf{v}$ in $\mathbb{Z}^d$ from (1.4) and initial values $W(\mathbf{v})$ with $\mathbf{v} = \mathbf{e}_i$, $\mathbf{v} = 2\mathbf{e}_i$, $\mathbf{v} = \mathbf{e}_i + \mathbf{e}_j$ and $\mathbf{v} = 2\mathbf{e}_i + \mathbf{e}_j$ with $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d\}$ the standard basis of $\mathbb{Z}^d$. For $\mathbf{s} = \mathbf{0}$, we deduce that

$$W(\mathbf{p}+\mathbf{q})W(\mathbf{p}-\mathbf{q})W(\mathbf{r})^2 = W(\mathbf{p}+\mathbf{r})W(\mathbf{p}-\mathbf{r})W(\mathbf{q})^2 - W(\mathbf{q}+\mathbf{r})W(\mathbf{q}-\mathbf{r})W(\mathbf{p})^2. \quad (1.5)$$

An elliptic net W is called degenerate if one of the terms $W(\mathbf{e}_i)$, $W(2\mathbf{e}_i)$, $W(\mathbf{e}_i \pm \mathbf{e}_j)$ (where $i \neq j$) is zero, and $W(3\mathbf{e}_1)$ is zero if $d = 1$. As shown in [5], we can define an elliptic net $\mathcal{W} = W_{E,\mathbf{P}}$ associated to the elliptic curve E and a d-tuple of fixed points $\mathbf{P} = (P_1, P_2, \ldots, P_d)$ on E^d with $P_i = (x_i, y_i) \neq 0_E$ for $1 \leq i \leq d$ and $P_i \pm P_j \neq 0_E$ for $i \neq j$, using the recurrence relation (1.4) and initial values

$$\mathcal{W}(\mathbf{e}_i) = 1, \quad \mathcal{W}(2\mathbf{e}_i) = 2y_i, \quad \mathcal{W}(\mathbf{e}_i+\mathbf{e}_j) = 1, \quad \mathcal{W}(2\mathbf{e}_i+\mathbf{e}_j) = 2x_i + x_j - \left(\frac{y_j - y_i}{x_j - x_i}\right).$$

From [1, Example 2.4], $W(\mathbf{e}_i - \mathbf{e}_j) = W(\mathbf{e}_i + 2\mathbf{e}_j) - W(2\mathbf{e}_i + \mathbf{e}_j)$, so $\mathcal{W}(\mathbf{e}_i - \mathbf{e}_j) = x_j - x_i$. The nondegenerate case therefore reduces to $\mathcal{W}(2\mathbf{e}_i) \neq 0$ $(1 \leq i \leq d)$ with $\mathcal{W}(3\mathbf{e}_1) \neq 0$ when $d = 1$.

From (1.5) with $\mathbf{r} = \mathbf{e}_r$, we obtain (1.1) when $d = 1$ (note that, in general, $W_1 = 1$ [7, Ch. VIII]). Therefore, elliptic nets are effectively a generalisation of elliptic sequences.

Even though it is not essential for our purpose, we take the opportunity to show the converse, that is, that (1.1) implies (1.4) for $d = 1$, by giving the missing elementary proof reported in [4, Ch. 3, page 22].

PROPOSITION 1.3. *For all* $(p, q, r, s) \in \mathbb{Z}^4$,

$$\psi_{p+q+s}\psi_{p-q}\psi_{r+s}\psi_r + \psi_{q+r+s}\psi_{q-r}\psi_{p+s}\psi_p + \psi_{r+p+s}\psi_{r-p}\psi_{q+s}\psi_q = 0. \quad (1.6)$$

PROOF. For any $(\alpha, \beta) \in \mathbb{Z}^2$, the integers $\alpha + \beta + 1$ and $\alpha - \beta$ have different parities. Thus, we obtain $\psi_{\alpha+\beta+1}\psi_{\alpha-\beta}\psi_2\psi_1 = \psi_{\beta+2}\psi_{\beta-1}\psi_{\alpha+1}\psi_\alpha - \psi_{\alpha+2}\psi_{\alpha-1}\psi_{\beta+1}\psi_\beta$ from the expressions for $\psi_{2k+1}\psi_1$ and $\psi_{2k'}\psi_2$ for the left-hand side and from (1.1) for the right-hand side, since the terms on each side of the subtraction can be coupled in pairs of products $\psi_\iota\psi_\jmath$ whose indexes have the same parity, which can be written in terms of

https://doi.org/10.1017/S0004972724000583 Published online by Cambridge University Press

k and k'. Accordingly, we deduce a modified version of Stephen Nelson's form: for all $(\alpha, \beta, \gamma, \delta) \in \mathbb{Z}^4$,

$$\psi_{\alpha+\beta+1}\psi_{\alpha-\beta}\psi_{\gamma+\delta+1}\psi_{\gamma-\delta} + \psi_{\alpha+\gamma+1}\psi_{\alpha-\gamma}\psi_{\delta+\beta+1}\psi_{\delta-\beta} + \psi_{\alpha+\delta+1}\psi_{\alpha-\delta}\psi_{\beta+\gamma+1}\psi_{\beta-\gamma} = 0. \quad (1.7)$$

The equality (1.6) follows by setting $r = \beta - \alpha, p = \gamma - \alpha, q = \delta - \alpha$ and, according to the parity, $s = 2\alpha$ in (1.2) or $s = 2\alpha + 1$ in (1.7). □

For the symmetries, for the case $d = 1$ [4, Theorem 10.2.2], with $\mathcal{W}(u) = 0$ ($u \in \mathbb{Z}$) at a point P of E, we have, for all $k \in \mathbb{Z}$,

$$\mathcal{W}(ku + v) = \mathcal{A}^{kv} C^{k^2} \mathcal{W}(v) \quad \text{with } \mathcal{A} = \frac{\mathcal{W}(u+2)}{\mathcal{W}(u+1)\mathcal{W}(2)} \text{ and } C = \frac{\mathcal{W}(u+1)}{\mathcal{A}}.$$

For the case $d = 2$ [4, Lemma 10.2.5], with $\mathcal{W}(\mathbf{u}) = \mathcal{W}(u_1, u_2) = 0$ ($\mathbf{u} = (u_1, u_2) \in \mathbb{Z}^2$), $\mathbf{P} = (P_1, P_2) \in E^2$ and $\mathbf{v} = (v_1, v_2) \in \mathbb{Z}^2$, we have, for all $k \in \mathbb{Z}$,

$$\mathcal{W}(k\mathbf{u} + \mathbf{v}) = \mathcal{A}_1^{kv_1} \mathcal{A}_2^{kv_2} C^{k^2} \mathcal{W}(\mathbf{v}) \quad \text{with } \mathcal{A}_1 = \frac{\mathcal{W}(u_1+2, u_2)}{\mathcal{W}(u_1+1, u_2)\mathcal{W}(2,0)},$$
$$\mathcal{A}_2 = \frac{\mathcal{W}(u_1, u_2+2)}{\mathcal{W}(u_1, u_2+1)\mathcal{W}(0,2)}, \; C = \frac{\mathcal{W}(u_1+1, u_2+1)}{\mathcal{A}_1\mathcal{A}_2\mathcal{W}(1,1)}.$$

There are some general results in the literature [4, Theorem 10.2.3] and [1, Theorem 1.13] for any natural integer d, presented as a generalisation of Ward's theorem (1.3), which we give here in a succinct form to avoid overloading the presentation. For the version ([4], [1, Theorem 1.12]), which deals with nondegenerate elliptic nets associated with an elliptic curve and a d-tuple of points on it,

$$\mathcal{W}(\mathbf{u} + \mathbf{v}) = \delta(\mathbf{u}, \mathbf{v})\mathcal{W}(\mathbf{v}) \quad \text{for all } \mathbf{v} \in \mathbb{Z}^d, \quad (1.8)$$

where $\mathcal{W}(\mathbf{u}) = 0$ and δ is a quadratic function that is linear in the second factor. Stange's version has a rather complicated proof [4, Theorem 10.2.3, page 62] and a simplified version of its proof with 'general' elliptic nets W can be found in [1, Theorem 1.13] with a factorised form of δ into linear and quadratic forms: that is,

$$W(\mathbf{u} + \mathbf{v}) = \xi(\mathbf{u})\chi(\mathbf{u}, \mathbf{v})W(\mathbf{v}) \quad \text{for all } \mathbf{v} \in \mathbb{Z}^d. \quad (1.9)$$

To obtain their results, Ward and Stange use complex analysis, which requires the nondegeneracy hypothesis. The authors in [1] use the recurrence (1.4), which allows them to remove the nondegeneracy condition and deal with elliptic nets that do not necessarily come from elliptic curves but with the property that $\Lambda = W^{-1}(0)$ is a subgroup of $\mathbb{Z}^d$ and $|\mathbb{Z}^d/\Lambda| \geq 4$. The result (1.9) is presented as a generalisation of (1.3) by letting $\mathcal{A} = \chi(v, 1)$ and $C = \xi(u)$ (see [1] for more details).

The purpose of this article is to prove the following result that unifies [7, Theorem 9.2], [2, Theorem 1], [4, Theorem 10.2.3] and [1, Theorem 1.13].

https://doi.org/10.1017/S0004972724000583 Published online by Cambridge University Press

THEOREM 1.4. *For a nondegenerate elliptic net $\mathcal{W} = W_{E,\mathbf{P}}$ associated to an elliptic curve E and a d-tuple of fixed points $\mathbf{P} = (P_1, P_2, \dots, P_d)$ on E^d such that $\mathcal{W}(\mathbf{u}) = 0$ with $\mathbf{u} \in (\mathbb{Z}^*)^d$ ($d \in \mathbb{N}$), we have, for all $k \in \mathbb{Z}$ and $\mathbf{v} = (v_1, v_2, \dots, v_d) \in \mathbb{Z}^d$,*

$$\mathcal{W}(k\mathbf{u} + \mathbf{v}) = C^{k^2}\Big(\prod_{r=1}^{d} \mathcal{A}_r^{v_r}\Big)^k \times \mathcal{W}(\mathbf{v}) \tag{1.10}$$

with

$$\mathcal{A}_r = \frac{\mathcal{W}(\mathbf{u} + 2\mathbf{e}_r)}{\mathcal{W}(\mathbf{u} + \mathbf{e}_r)\mathcal{W}(2\mathbf{e}_r)} \quad \text{for all } r \in \{1, 2, \dots, d\},$$

$$C = \begin{cases} \dfrac{\mathcal{W}(\mathbf{u} + \mathbf{1})}{\mathcal{W}(\mathbf{1}) \times \prod_{r=1}^{d} \mathcal{A}_r} & \text{if } \mathbf{u} \neq \mathbf{1}, \\ -\mathcal{A}_s \mathcal{W}(\mathbf{u} - \mathbf{e}_s) \ \ (s \in \{1, 2, \dots, d\}) & \text{if } \mathbf{u} = \pm\mathbf{1}. \end{cases}$$

We limit ourselves to elliptic nets of the form $\mathcal{W}$. Indeed, Ward [7] showed that almost all elliptic divisibility sequences are of the form $\mathcal{W} = W_{E,P} = \psi_n(P)$ and Stange [6] reports that 'nearly all elliptic nets arise in this way', and are hence of the form $\mathcal{W} = W_{E,\mathbf{P}}$. On the other hand, in [1], to ensure that Λ is a group, the authors use the hypothesis that each elliptic sequence $W(ne_i)$ ($n \in \{1, 2, \dots, d\}$) has a unique rank of zero-apparition. In our context, this means that all points P_i are of finite order on E, which seems to be very restrictive in a field of characteristic different from zero.

Note that, from [5, Corollary 5.2], we have the equivalence between $\mathcal{W}(\mathbf{u}) = 0$ and $\mathbf{u}.\mathbf{P} = 0_E$. The zeros of an elliptic net then appear as a sublattice of $\mathbb{Z}^d$, called the lattice of zero-apparition [6, Definition 3].

2. Periodicity

2.1. Generalities. In this paragraph, we consider, for d in $\mathbb{N}_{\geq 2}$ and $\boldsymbol{\ell} = (\ell_1, \ell_2, \dots, \ell_d)$ in $\mathbb{Z}^d$, a multi-index sequence denoted by $G_{\boldsymbol{\ell}} = G_{\ell_1,\ell_2,\dots,\ell_d}$ of elements in the field $\mathbb{K}$. We say that the sequence $G_{\boldsymbol{\ell}}$ is $\mathbb{Z}$-geometric if, for all k fixed in $\{1, 2, \dots, d\}$ and $\boldsymbol{\ell}$ fixed in $\mathbb{Z}^d$, the sequence $G_{\ell_1,\ell_2,\dots,\ell_{k-1},\ell,\ell_{k+1},\dots,\ell_d} = \mathcal{G}_\ell$ is geometric. To be more explicit, for all k in $\{1, 2, \dots, d\}$ we set $\boldsymbol{\ell}_k = (\ell_1, \ell_2, \dots, \ell_{k-1}, \ell_{k+1}, \dots, \ell_d)$ in $\mathbb{Z}^{d-1}$ and define the ratios $q^{(k)}_{\boldsymbol{\ell}_k}$ in $\mathbb{K}$ such that $G_{\boldsymbol{\ell}+\mathbf{e}_k} = q^{(k)}_{\boldsymbol{\ell}_k} G_{\boldsymbol{\ell}}$.

We prove the following lemma, which is useful for obtaining our final result.

LEMMA 2.1. *Consider a $\mathbb{Z}$-geometric sequence $(G_{\boldsymbol{\ell}})_{\boldsymbol{\ell}\in\mathbb{Z}^d}$ of elements in the field $\mathbb{K}$ such that*

$$\text{for all } u \neq v \in \{1, 2, \dots, d\}, \quad G_{\boldsymbol{\ell}+\mathbf{e}_u+\mathbf{e}_v} G_{\boldsymbol{\ell}} = G_{\boldsymbol{\ell}+\mathbf{e}_u} G_{\boldsymbol{\ell}+\mathbf{e}_v}.$$

Then, the sequence $G_{\boldsymbol{\ell}}$ is geometric in each direction $\mathbf{e}_k$ for $k \in \{1, 2, \dots, d\}$, namely,

$$\text{for all } k \in \{1, 2, \dots, d\} \text{ there exists } q_k \in \mathbb{K}, \quad G_{\boldsymbol{\ell}+\mathbf{e}_k} = q_k G_{\boldsymbol{\ell}}.$$

https://doi.org/10.1017/S0004972724000583 Published online by Cambridge University Press

PROOF. We show this result by induction on the integer d.

In the case $d = 2$, for $i \neq j$ in $\{1, 2\}$, from $G_{\boldsymbol{\ell}+\mathbf{e}_j} G_{\boldsymbol{\ell}-\mathbf{e}_j} = G_{\boldsymbol{\ell}}^2$ since $G_{\boldsymbol{\ell}}$ is $\mathbb{Z}$-geometric, we deduce that $q^{(i)}_{\ell_j+1} G_{\boldsymbol{\ell}-\mathbf{e}_i+\mathbf{e}_j} q^{(i)}_{\ell_j-1} G_{\boldsymbol{\ell}-\mathbf{e}_i-\mathbf{e}_j} = (q^{(i)}_{\ell_j} G_{\boldsymbol{\ell}-\mathbf{e}_i})^2$ so $q^{(i)}_{\ell_j}$ is a geometric sequence whose ratio is denoted r_j. So, we have $q^{(i)}_{\ell_j} = r_j^{\ell_j} q^{(i)}_0$. Expressing $G_{1,1}$ in terms of $G_{0,0}$ gives $r_1 = r_2$ and, from $G_{1,1} G_{0,0} = G_{1,0} G_{0,1}$, we find that $r_1 = r_2 = 1$. Finally, we obtain $G_{\boldsymbol{\ell}+\mathbf{e}_i} = q^{(i)}_{\ell_j} G_{\boldsymbol{\ell}} = r_j^{\ell_j} q^{(i)}_0 G_{\boldsymbol{\ell}} = q^{(i)}_0 G_{\boldsymbol{\ell}} = q_i G_{\boldsymbol{\ell}}$ with $q^{(i)}_0 = q_i$.

For the case $d > 2$, in the same way, we deduce, for k in $\{1, 2, \ldots, d\}$, that $q^{(k)}_{\boldsymbol{\ell}_k}$ is $\mathbb{Z}$-geometric. On the other hand, for $u \neq v$, $q^{(k)}_{\boldsymbol{\ell}_k}$ satisfies $q^{(k)}_{\boldsymbol{\ell}_k+\mathbf{e}_u+\mathbf{e}_v} q^{(k)}_{\boldsymbol{\ell}_k} = q^{(k)}_{\boldsymbol{\ell}_k+\mathbf{e}_u} q^{(k)}_{\boldsymbol{\ell}_k+\mathbf{e}_v}$. Therefore, by the inductive hypothesis,

$$\text{for all } k \in \{1, 2, \ldots, d\} \text{ and for all } j \neq k, \text{ there exists } r_{k,j} \in \mathbb{K}, \quad q^{(k)}_{\boldsymbol{\ell}_k+\bar{\mathbf{e}}_j} = r_{k,j} q^{(k)}_{\boldsymbol{\ell}_k},$$

where $\bar{\mathbf{e}}_j$ is the projection of $\mathbf{e}_j$ over $\mathrm{span}_{\mathbb{Z}}(\mathbf{e}_1, \ldots, \mathbf{e}_{k-1}, \mathbf{e}_{k+1}, \ldots, \mathbf{e}_d)$. It follows that $q^{(k)}_{\boldsymbol{\ell}_k} = \prod_{1 \leq j \leq d, j \neq k} r_{k,j}^{\ell_j} q^{(k)}_{\mathbf{0}_{d-1}}$ with $\mathbf{0}_{d-1} = (0, 0, \ldots, 0)$ in $\mathbb{Z}^{d-1}$ and thus we have $G_{\boldsymbol{\ell}+\mathbf{e}_k} = \prod_{1 \leq j \leq d, j \neq k} r_{k,j}^{\ell_j} q^{(k)}_{\mathbf{0}_{d-1}} G_{\boldsymbol{\ell}}$. So, for $u \neq v$ in $\{1, 2, \ldots, d\}$, we can write $G_{\mathbf{e}_u+\mathbf{e}_v} = r_{v,u} q^{(v)}_{\mathbf{0}_{d-1}} q^{(u)}_{\mathbf{0}_{d-1}} G_{\mathbf{0}} = G_{\mathbf{e}_v+\mathbf{e}_u}$. Hence, $r_{u,v} = r_{v,u}$. Finally, from $G_{\mathbf{e}_u+\mathbf{e}_v} G_{\mathbf{0}} = G_{\mathbf{e}_u} G_{\mathbf{e}_v}$, we obtain $r_{u,v} = 1$ and so, for all k in $\{1, 2, \ldots, d\}$, we have $G_{\boldsymbol{\ell}+\mathbf{e}_k} = q^{(k)}_{\mathbf{0}_{d-1}} G_{\boldsymbol{\ell}} = q_k G_{\boldsymbol{\ell}}$. □

2.2. Geometric sequence of quotient of elliptic nets. We consider a nondegenerate elliptic net $\mathcal{W} = W_{E,\mathbf{P}}$ associated to the elliptic curve E and the d-tuple of fixed points $\mathbf{P} = (P_1, P_2, \ldots, P_d)$ on E^d. We assume that there is $\mathbf{u} = (u_1, \ldots, u_d)$ in $\mathbb{Z}^d$ with $\mathcal{W}(\mathbf{u}) = \mathcal{W}_{E,\mathbf{P}} = 0$. In other words, $\mathbf{u}.\mathbf{P} = u_1 P_1 + \cdots + u_d P_d = 0_E$ [5, Corollary 5.2].

In equation (1.5), we set $\mathbf{r} = \mathbf{e}_r$ $(r \in \{1, 2, \ldots, d\})$, $\mathbf{p} = \mathbf{i} - \boldsymbol{\ell}$ and $\mathbf{q} = \mathbf{j} + \boldsymbol{\ell}$ with $\boldsymbol{\ell}, \mathbf{i}, \mathbf{j} \in \mathbb{Z}^d$ and we consider $\mathbf{i} + \mathbf{j} = \mathbf{u}$. We obtain, for all r in $\{1, 2, \ldots, d\}$,

$$\mathcal{W}(\mathbf{i} - \boldsymbol{\ell} + \mathbf{e}_r)\mathcal{W}(\mathbf{i} - \boldsymbol{\ell} - \mathbf{e}_r)\mathcal{W}(\mathbf{j} + \boldsymbol{\ell})^2 - \mathcal{W}(\mathbf{j} + \boldsymbol{\ell} + \mathbf{e}_r)\mathcal{W}(\mathbf{j} + \boldsymbol{\ell} - \mathbf{e}_r)\mathcal{W}(\mathbf{i} - \boldsymbol{\ell})^2 = 0. \tag{2.1}$$

This equation does not provide any information in certain cases, for example, for $\boldsymbol{\ell} = \mathbf{i} \pm \mathbf{e}_r, \mathbf{i}$. We now define

$$G_{\boldsymbol{\ell}} = \frac{\mathcal{W}(\mathbf{j} + \boldsymbol{\ell})}{\mathcal{W}(\mathbf{i} - \boldsymbol{\ell})},$$

which depends on $\mathbf{i}$ and $\mathbf{j}$ but we will fix them later. Note also that $G_{\boldsymbol{\ell}}$ is not defined for some $\boldsymbol{\ell}$, for example, for $\boldsymbol{\ell} = \mathbf{i}, \boldsymbol{\ell} = -\mathbf{j}$. From (2.1),

$$\text{for all } r \in \{1, 2, \ldots, d\}, \quad G_{\boldsymbol{\ell}+\mathbf{e}_r} \times G_{\boldsymbol{\ell}-\mathbf{e}_r} = G_{\boldsymbol{\ell}}^2. \tag{2.2}$$

Again, (2.2) does not make sense for some values of $\boldsymbol{\ell}$. We will come back later to all these problematic cases (see Section 2.3) and we provisionally assume that $G_{\boldsymbol{\ell}}$ is well defined for all $\boldsymbol{\ell}$ in $\mathbb{Z}^d$.

So, the sequence $G_{\boldsymbol{\ell}}$ is $\mathbb{Z}$-geometric. Furthermore, from (1.4) with $\mathbf{p} = -\mathbf{e}_u$, $\mathbf{q} = \mathbf{j} + \boldsymbol{\ell} + \mathbf{e}_v$, $\mathbf{r} = \mathbf{i} - \boldsymbol{\ell} - \mathbf{e}_u$ and $\mathbf{s} = \mathbf{e}_u - \mathbf{e}_v$, we obtain

$$\text{for all } u \neq v \in \{1, 2, \ldots, d\}, \quad G_{\boldsymbol{\ell}+\mathbf{e}_u+\mathbf{e}_v} G_{\boldsymbol{\ell}} = G_{\boldsymbol{\ell}+\mathbf{e}_u} G_{\boldsymbol{\ell}+\mathbf{e}_v}.$$

https://doi.org/10.1017/S0004972724000583 Published online by Cambridge University Press

From the previous section, with $q_r = G_{\mathbf{e}_r}/G_{\mathbf{0}}$, we deduce that

$$\text{for all } r \in \{1,\dots,d\}, \text{ there exists } q_r \in \mathbb{K}, \quad G_{\boldsymbol{\ell}+\mathbf{e}_r} = q_r G_{\boldsymbol{\ell}}.$$

Finally,

$$\text{for all } \boldsymbol{\ell} = (\ell_1, \ell_2, \dots, \ell_d) \in \mathbb{Z}^d, \quad G_{\boldsymbol{\ell}} = \prod_{r=1}^{d} q_r^{\ell_r} G_{\mathbf{0}}. \tag{2.3}$$

However, this result omits the problematic cases mentioned, which does not guarantee the existence of $G_{\boldsymbol{\ell}}$ for some $\boldsymbol{\ell}$ in $\mathbb{Z}^d$. Thus, we do not know whether we are keeping the same ratio through certain points of $\mathbb{Z}^d$ in a given direction. We deal with these questions in the following section.

Before doing so, we fix $\mathbf{i}$ and $\mathbf{j}$ with $\mathbf{u} = \mathbf{i} + \mathbf{j}$. For that, for all r in $\{1, 2, \dots, d\}$, if $u_r = 2w_r$ ($\overline{u_r} \equiv u_r \bmod 2 = 0$), we set $i_r = w_r - 1$; but if $u_r = 2w_r + 1$ ($\overline{u_r} = 1$), we set $i_r = w_r$ and, in all cases, $j_r = w_r + 1$. Thus, if $\mathbf{i} = (i_1, i_2, \dots, i_d)$ and $\mathbf{j} = (j_1, j_2, \dots, j_d)$, writing $\bar{\mathbf{u}} \equiv \mathbf{u} \bmod 2$ and $\mathbf{1} = (1, 1, \dots, 1)$ in $\mathbb{Z}^d$, we have

$$\mathbf{i} = \frac{\mathbf{u} + \bar{\mathbf{u}}}{2} - \mathbf{1} \quad \text{and} \quad \mathbf{j} = \frac{\mathbf{u} - \bar{\mathbf{u}}}{2} + \mathbf{1}.$$

It can be observed that $G'_{\boldsymbol{\ell}} = G_{\boldsymbol{\ell}}^{-1}$ with $\boldsymbol{\ell}' = \bar{\mathbf{u}} - 2 \times \mathbf{1} - \boldsymbol{\ell}$.

2.3. Problematic cases. First, if $\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2$ in $\mathbb{Z}^d$ with $\mathcal{W}_{\mathbf{u}} = 0$, then $\mathcal{W}_{\mathbf{u}_1} = 0 \Leftrightarrow \mathcal{W}_{\mathbf{u}_2} = 0$. Thus, the quantities $G_{\boldsymbol{\ell}}$ do not cancel, but are not defined at some points of $\mathbb{Z}^d$. Moreover, the nondegeneracy hypothesis tells us that a problematic case can only occur on one of three (four if $d = 1$) consecutive terms of the sequence $G_{\boldsymbol{\ell}}$ in one direction. We will come back to the special cases of points of order two or three in Section 2.6. On the other hand, if $G_{\boldsymbol{\ell}}$ and $G'_{\boldsymbol{\ell}}$ are not defined, then $(\boldsymbol{\ell} - \boldsymbol{\ell}').\mathbf{P} = 0_E$. We deduce that, if $G_{\boldsymbol{\ell}}$ is not defined, then this is not the case for the $G_{\boldsymbol{\ell}+\delta\mathbf{e}_r}$ such that δ is in $\{\pm 1, \pm 2\}$ for r in $\{1, 2, \dots, d\}$ or even for $G_{\boldsymbol{\ell}\pm\mathbf{e}_r\pm\mathbf{e}_s}$ ($r \neq s$).

We show that we keep the same ratio q_r ($r \in \{1, 2, \dots, d\}$) through a problematic case of index $\boldsymbol{\ell}$ in the direction $\mathbf{e}_r$. This means that $\mathcal{W}(\mathbf{j} + \boldsymbol{\ell}) = \mathcal{W}(\mathbf{i} - \boldsymbol{\ell}) = 0$. We define the value of $G_{\boldsymbol{\ell}}$ by the expression $G^2_{\boldsymbol{\ell}-\mathbf{e}_r}/G_{\boldsymbol{\ell}-2\mathbf{e}_r} = q_r G_{\boldsymbol{\ell}-\mathbf{e}_r}$. Then, from the addition formula on an elliptic curve expressing $x((\mathbf{r} + \mathbf{s}).\mathbf{P})$ and $x((\mathbf{r} - \mathbf{s}).\mathbf{P})$ for $\mathbf{r} \neq \mathbf{s}$ in $(\mathbb{Z}^d)^*$ such that $x(\mathbf{r}.\mathbf{P}) \neq x(\mathbf{s}.\mathbf{P})$ and [5, Lemma 4.2], we obtain $\mathcal{W}(2\mathbf{r})\mathcal{W}(2\mathbf{s}) = 4y(\mathbf{r}.\mathbf{P})y(\mathbf{s}.\mathbf{P})\mathcal{W}(\mathbf{r})^4\mathcal{W}(\mathbf{s})^4$. Hence, if $\mathbf{s} = \mathbf{e}_s$ for $s \neq r$ in $\{1, 2, \dots, d\}$ with $x(\mathbf{r}.\mathbf{P}) \neq x(P_s)$, we deduce that

$$\mathcal{W}(2\mathbf{r}) = 2y(\mathbf{r}.\mathbf{P})\mathcal{W}(\mathbf{r})^4, \tag{2.4}$$

for r in $\{1, 2, \dots, d\}$. With $\mathbf{r} = \mathbf{j} + \boldsymbol{\ell} - \mathbf{e}_r$, so that $y(\mathbf{r}.\mathbf{P}) = -y_r$ in (2.4), we obtain $\mathcal{W}(2(\mathbf{j} + \boldsymbol{\ell} - \mathbf{e}_r)) = -\mathcal{W}(2\mathbf{e}_r)\mathcal{W}(\mathbf{j} + \boldsymbol{\ell} - \mathbf{e}_r)^4$. Combining this with (1.5) for $\mathbf{p} = \mathbf{j} + \boldsymbol{\ell}$, $\mathbf{q} = \mathbf{j} + \boldsymbol{\ell} - 2\mathbf{e}_r$ and $\mathbf{r} = \mathbf{e}_r$ gives

$$\mathcal{W}(\mathbf{j} + \boldsymbol{\ell} + \mathbf{e}_r)\mathcal{W}(\mathbf{j} + \boldsymbol{\ell} - 2\mathbf{e}_r)^2 = -\mathcal{W}(2\mathbf{e}_r)^2\mathcal{W}(\mathbf{j} + \boldsymbol{\ell} - \mathbf{e}_r)^3. \tag{2.5}$$

https://doi.org/10.1017/S0004972724000583 Published online by Cambridge University Press

In the same way, with $\mathbf{r} = \mathbf{i} - \boldsymbol{\ell} + \mathbf{e}_r$ in (2.4) and $\mathbf{p} = \mathbf{i} - \boldsymbol{\ell}$, $\mathbf{q} = \mathbf{i} - \boldsymbol{\ell} + 2\mathbf{e}_r$ and $\mathbf{r} = \mathbf{e}_r$ in (1.5), we obtain

$$\mathcal{W}(\mathbf{i} - \boldsymbol{\ell} - \mathbf{e}_r)\mathcal{W}(\mathbf{i} - \boldsymbol{\ell} + 2\mathbf{e}_r)^2 = -\mathcal{W}(2\mathbf{e}_r)^2\mathcal{W}(\mathbf{i} - \boldsymbol{\ell} + \mathbf{e}_r)^3. \tag{2.6}$$

From (2.5) and (2.6), we deduce that

$$\begin{aligned}\mathcal{W}(\mathbf{j} + \boldsymbol{\ell} + \mathbf{e}_r)&\mathcal{W}(\mathbf{j} + \boldsymbol{\ell} - 2\mathbf{e}_r)^2\mathcal{W}(\mathbf{i} - \boldsymbol{\ell} + \mathbf{e}_r)^3\\ &= \mathcal{W}(\mathbf{i} - \boldsymbol{\ell} - \mathbf{e}_r)\mathcal{W}(\mathbf{i} - \boldsymbol{\ell} + 2\mathbf{e}_r)^2\mathcal{W}(\mathbf{j} + \boldsymbol{\ell} - \mathbf{e}_r)^3,\end{aligned}$$

and, therefore, $G_{\boldsymbol{\ell}+\mathbf{e}_r} = G_{\boldsymbol{\ell}}^2/G_{\boldsymbol{\ell}-\mathbf{e}_r} = q_r G_{\boldsymbol{\ell}}$ with the new definition of $G_{\boldsymbol{\ell}}$.

Next, for all λ and μ in $\mathbb{Z}^*$, we set $\mathbf{p} = \mathbf{i} - \boldsymbol{\ell} + \lambda\mathbf{e}_r$, $\mathbf{q} = \lambda\mathbf{e}_r + \mu\mathbf{e}_r$, $\mathbf{r} = \mathbf{j} + \boldsymbol{\ell} + \lambda\mathbf{e}_r$ and $\mathbf{s} = -2\lambda\mathbf{e}_r$ with $r \in \{1, 2, \dots, d\}$ in (1.4). We obtain $G_{\boldsymbol{\ell}+\lambda\mathbf{e}_r}G_{\boldsymbol{\ell}-\lambda\mathbf{e}_r} = G_{\boldsymbol{\ell}+\mu\mathbf{e}_r}G_{\boldsymbol{\ell}+\mu\mathbf{e}_r}$, and, therefore, $G_{\boldsymbol{\ell}+2\mathbf{e}_r}/G_{\boldsymbol{\ell}+\mathbf{e}_r} = G_{\boldsymbol{\ell}-\mathbf{e}_r}/G_{\boldsymbol{\ell}-2\mathbf{e}_r} = q_r$.

Finally, we show that the definition of $G_{\boldsymbol{\ell}}$ in the direction $\mathbf{e}_r$ is consistent with that in another direction $\mathbf{e}_s$, which we denote by $\widetilde{G}_{\boldsymbol{\ell}}$. For that, we set $\mathbf{p} = \mathbf{j} + \boldsymbol{\ell} - \mathbf{e}_r - \mathbf{e}_s$, $\mathbf{q} = \mathbf{i} - \boldsymbol{\ell} + \mathbf{e}_r + \mathbf{e}_s$ and $\mathbf{r} = \mathbf{e}_r - \mathbf{e}_s$ in (1.5) to obtain $G^2_{\boldsymbol{\ell}-\mathbf{e}_r-\mathbf{e}_s} = G_{\boldsymbol{\ell}-2\mathbf{e}_s}G_{\boldsymbol{\ell}-2\mathbf{e}_r}$, and so $G^2_{\boldsymbol{\ell}-\mathbf{e}_r}G_{\boldsymbol{\ell}-2\mathbf{e}_s} = G^2_{\boldsymbol{\ell}-\mathbf{e}_s}G_{\boldsymbol{\ell}-2\mathbf{e}_r}$, that is, $G_{\boldsymbol{\ell}} = \widetilde{G}_{\boldsymbol{\ell}}$. So, for a problematic index $\boldsymbol{\ell}$, we can set $G_{\boldsymbol{\ell}} = q_r G_{\boldsymbol{\ell}-\mathbf{e}_r}$ to ensure that $G_{\boldsymbol{\ell}}$ is geometric in each direction.

EXAMPLE 2.2. For the curve $y^2 = x^3 + 2x - 4$ over $\mathbb{F}_{73}$ and the points $P_1 = (36, 71)$, $P_2 = (51, 53)$, $P_3 = (7, 34)$, we have $U = (3, 5, 7)$ and $(q_1, q_2, q_3) = (22, 71, 58)$. The values $G_{\mathbf{i}}$ and $G_{-\mathbf{j}}$ are not defined. We set $G_{\mathbf{i}} = q_r G_{\mathbf{i}-\mathbf{e}_r} = 47$ and $G_{-\mathbf{j}} = q_r G_{-\mathbf{j}-\mathbf{e}_r} = 14$. The values of $G_{\mathbf{i}+k\mathbf{e}_r}$ $(k \in \{-3; 3\})$ are, for $r = 1, 2, 3$ successively,

$$\{61, 28, 32, \mathbf{47}, 12, 45, 45\}, \quad \{58, 30, 13, \mathbf{47}, 52, 42, 62\}, \quad \{23, 20, 65, \mathbf{47}, 25, 63, 4\},$$

and for $G_{-\mathbf{j}+k\mathbf{e}_r}$,

$$\{57, 13, 67, \mathbf{14}, 16, 60, 6\}, \quad \{53, 40, 66, \mathbf{14}, 45, 56, 34\}, \quad \{55, 51, 38, \mathbf{14}, 9, 11, 54\}.$$

We can give a harmonious formulation of the ratios q_r in terms of G and, therefore, of $\mathcal{W}$, if the quantities involved are well defined. Indeed, from (2.2) for $\boldsymbol{\ell} = \mathbf{e}_r - \mathbf{1}$, we obtain $G_{2\mathbf{e}_r-\mathbf{1}}G_{-\mathbf{1}} = G^2_{\mathbf{e}_r-\mathbf{1}}$ for all r in $\{1, 2, \dots, d\}$. With $G_{2\mathbf{e}_r-\mathbf{1}} = q_r G_{\mathbf{e}_r-\mathbf{1}}$ and $G_{-\mathbf{1}} = G^{-1}_{\bar{\mathbf{u}}-\mathbf{1}}$, we deduce that

$$\text{for all } r \in \{1, 2, \dots, d\}, \quad q_r = G_{\bar{\mathbf{u}}-\mathbf{1}} \times G_{\mathbf{e}_r-\mathbf{1}} = \frac{\mathcal{W}(\frac{\mathbf{u}+\bar{\mathbf{u}}}{2})}{\mathcal{W}(\frac{\mathbf{u}-\bar{\mathbf{u}}}{2})} \times \frac{\mathcal{W}(\frac{\mathbf{u}-\bar{\mathbf{u}}}{2} + \mathbf{e}_r)}{\mathcal{W}(\frac{\mathbf{u}+\bar{\mathbf{u}}}{2} - \mathbf{e}_r)}. \tag{2.7}$$

EXAMPLE 2.3. For the curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_{11}$, we consider the points of order seven, that is, $P_1 = (6, 5)$ and $P_2 = (3, 3)$. We have $3P_1 + P_2 = 0_E = 2P_1 + 3P_2 = 5P_1 + 4P_2$, so $\mathbf{u} = (5, 4) = (3, 1) + (2, 3) = \mathbf{u}_1 + \mathbf{u}_2$. In this case, $G_{(-1,0)}$ and $G_{(0,-2)}$ are not defined since $\mathcal{W}_{2,3} = \mathcal{W}_{3,1} = 0$ and so q_2 is not defined. We define $G_{(0,-2)} = q_1 G_{(-1,-2)} = 4 * 5 = 9$ and $G_{(-1,0)} = G_{(0,0)}/q_1 = 9/4 = 5 = 9^{-1}$. We also set $q_2 = G_{(0,-1)}G_{(-1,0)} = 2 * 5 = 10$. Note that, at the end of the article, we show that $q_r(\mathbf{u}) = q_r(\mathbf{u}_1) * q_r(\mathbf{u}_2)$ $(r \in \{1, 2\})$. Indeed, $q(\mathbf{u}) = (4, 10)$, $q(\mathbf{u}_1) = (6, 6)$ and $q(\mathbf{u}_2) = (8, 9)$.

If we now consider $\mathbf{u} = 2(3,1) = (6,2)$, then $G_{-\mathbf{1}}$ is not defined, nor are the quantities q_1 and q_2. We have $q_1 = G_{(1,0)}/G_{(0,0)} = 3$, $q_2 = G_{(0,1)}/G_{(0,0)} = 3$ and $G_{(-1,-1)} = G_{(0,0)}/(q_1 q_2) = -1$. Once again, we see that $q_r(2\mathbf{u}) = q_r(\mathbf{u})^2$. Indeed, $q((6,2)) = (3,3); q((3,1)) = (6,6)$.

For the case $\mathbf{u} = \mathbf{1}$, the quantities $G_{-\mathbf{1}}$, $G_{\mathbf{0}}$, and thus the ratios q_k, are not defined. But, we can set

$$\text{for all } k \in \{1,2,\ldots,n\}, \quad q_k \overset{k' \neq k}{=} \frac{G_{\mathbf{e}_{k'}}}{G_{\mathbf{e}_{k'}-\mathbf{e}_k}},$$

and $G_{-\mathbf{1}} = G_{-\mathbf{1}+\mathbf{e}_k}/q_k$, $G_{\mathbf{0}} = q_k G_{-\mathbf{e}_k}$.

For the curve $y^2 = x^3 + 17x - 53$ over $\mathbb{F}_{229}$, we consider the points $P_1 = (217,63)$, $P_2 = (153,59)$, $P_3 = (42,211)$, $P_4 = (40,222)$ and $P_5 = (13,126)$. We have $\mathbf{u} = \mathbf{1}$. We can write $q_1 = G_{\mathbf{e}_2}/G_{\mathbf{e}_2-\mathbf{e}_1} = 211$ and so $q_2 = 55, q_3 = 221, q_4 = 13, q_5 = 227$ and $G_{-\mathbf{1}} = G_{\mathbf{e}_1-\mathbf{1}}/q_1 = 181$.

So we can have cases where the definition $q_r = G_{\bar{\mathbf{u}}-\mathbf{1}} \times G_{\mathbf{e}_r-\mathbf{1}}$ is problematic. However, we can always find $\boldsymbol{\ell}$ in $\mathbb{Z}^d$ so that the ratio $q_r = G_{\boldsymbol{\ell}+\mathbf{e}_r}/G_{\boldsymbol{\ell}}$ is well defined. Nevertheless, the expression (2.7) needs some $\mathcal{W}$ whose indexes are in the neighbourhood of $\mathbf{u}/2$, which is the best that we can do for the computation of $G_{\boldsymbol{\ell}}$ whose indexes are symmetric with respect to $\mathbf{u}/2$.

2.4. Proof of Theorem 1.4. First, we set $\boldsymbol{\ell} = \mathbf{i} + \mathbf{v}$ for $\mathbf{v}$ in $\mathbb{Z}^d \backslash \Gamma$, giving

$$G_{\boldsymbol{\ell}} = G_{\mathbf{i}+\mathbf{v}} = \frac{\mathcal{W}(\mathbf{i}+\mathbf{j}+\mathbf{v})}{\mathcal{W}(-\mathbf{v})} = \frac{\mathcal{W}(\mathbf{u}+\mathbf{v})}{\mathcal{W}(-\mathbf{v})} = -\frac{\mathcal{W}(\mathbf{u}+\mathbf{v})}{\mathcal{W}(\mathbf{v})}.$$

Therefore, from (2.3), we obtain, in the cases where $G_{-\mathbf{1}}$ is well defined,

$$\mathcal{W}(\mathbf{u}+\mathbf{v}) = -G_{\mathbf{i}+\mathbf{v}}\mathcal{W}(\mathbf{v}) = -\Big(\prod_{r=1}^{d} q_r^{i_r+v_r+1}\Big) G_{-\mathbf{1}} \times \mathcal{W}(\mathbf{v}),$$

which holds for $\mathbf{v}$ in $\mathbb{Z}^d$ such that $\mathcal{W}(\mathbf{v}) = 0$. Note that, in this case, since G is geometric in each direction, $G_{-\mathbf{1}} = \prod_{r=1}^d q_r^{-\overline{u_r}} \times G_{\bar{\mathbf{u}}-\mathbf{1}}$; therefore, $G_{-\mathbf{1}}^2 = \prod_{r=1}^d q_r^{-\overline{u_r}}$. This shows that $\prod_{r=1}^d q_r^{u_r}$ is a square.

For all r in $\{1,2,\ldots,d\}$, when $G_{-\mathbf{1}}$ is well defined, we set $\mathcal{A}_r = q_r$ and $C = -(\prod_{r=1}^d q_r^{i_r+1})G_{-\mathbf{1}}$. Thus, we can write $C^2 = \prod_{r=1}^d q_r^{2(i_r+1)} \times G_{-\mathbf{1}}^2 = \prod_{r=1}^d \mathcal{A}_r^{u_r}$ (which is just $\xi(\mathbf{u})^2 = \chi(\mathbf{u},\mathbf{u})$; see (2.5)). Hence, $\mathcal{W}(\mathbf{u}+\mathbf{v}) = C\prod_{r=1}^d \mathcal{A}_r^{v_r} \times \mathcal{W}(\mathbf{v})$ and a simple induction on k give the desired result (1.10). The formulas for $\mathcal{A}$ and C in (1.10) follow immediately from the existence of these quantities.

On the other hand, if we set $\mathbf{u}_1 = (\mathbf{u} - \bar{\mathbf{u}})/2$ and $\mathbf{u}_2 = (\mathbf{u} + \bar{\mathbf{u}})/2$ with possibly $\mathbf{u}_1 = \mathbf{u}_2$, we have $G_{-\mathbf{1}} = \mathcal{W}(\mathbf{u}_1)/\mathcal{W}(\mathbf{u}_2)$. Hence, $G_{-\mathbf{1}}$ is not defined if $\mathbf{u} = \pm\mathbf{1}$ or $\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2$ with $\mathbf{u}_1.\mathbf{P} = 0_E$ and $\mathbf{u}_2.\mathbf{P} = 0_E$. Suppose that $\mathbf{u} \neq \pm\mathbf{1}$. For s in $\{1,2,\ldots,d\}$, we have $G_{-\mathbf{e}_s-\mathbf{1}+\bar{\mathbf{u}}} = 1/G_{-\mathbf{e}_s-\mathbf{1}}$ and thus $q_s^2 \prod_{r=1}^d q_r^{-\bar{\mathbf{u}}_r} = G_{-\mathbf{e}_s-\mathbf{1}}^2$. We still have

$$\mathcal{W}(\mathbf{u}+\mathbf{v}) = -G_{\mathbf{i}+\mathbf{v}}\mathcal{W}(\mathbf{v}) = -\Big(\prod_{r=1}^{d} q_r^{i_r+v_r+1}\Big)\frac{G_{\mathbf{e}_s-\mathbf{1}}}{q_s} \times \mathcal{W}(\mathbf{v}),$$

https://doi.org/10.1017/S0004972724000583 Published online by Cambridge University Press

TABLE 1. Calculations illustrating Theorem 1.4 in characteristic zero.

$\mathbf{v}$	k	$\mathcal{W}(k\mathbf{u}+\mathbf{v})$	$C^{k^2}(\prod_{r=1}^d \mathcal{A}_r^{v_r})^k$	$\mathcal{W}(\mathbf{v})$
$(1,1,1)$	1	$-\frac{2310968614448527454698011812 07}{2074596720994616193681719296}$	$\frac{4643296392301642464733 7991}{433653160743021779615744}$	$-\frac{4977}{4784}$
$(-1,-1,1)$	1	$-\frac{794}{64}$	$\frac{9243}{1472}$	$-\frac{18193}{9243}$
$(1,1,1)$	-1	$-\frac{7}{4}$	$\frac{1196}{711}$	$-\frac{4977}{4784}$
$(1,1,1)$	-2	$-\frac{642961909517339482497}{1212663059537985536}$	$\frac{129186640449535761}{253483081007104}$	$-\frac{4977}{4784}$

and so we set $\mathcal{A}_r = q_r$ and $C = -(\prod_{r=1}^d q_r^{i_r+1} G_{\mathbf{e}_s-\mathbf{1}}/q_s)$. Note that, for $s \neq s'$, $G_{\mathbf{e}_s+\mathbf{e}_{s'}-\mathbf{1}} = G_{\mathbf{e}_s-\mathbf{1}}q_{s'} = G_{\mathbf{e}_{s'}-\mathbf{1}}q_s$. Again, we obtain $C^2 = \prod_{r=1}^d \mathcal{A}_r^{u_r}$.

For $\mathbf{u} = \mathbf{1}$ (the case $\mathbf{u} = -\mathbf{1}$ can be handled in the same manner), we write instead

$$\mathcal{W}(\mathbf{u}+\mathbf{v}) = -\Big(\prod_{r=1}^d q_r^{i_r+v_r}\Big) G_{-\mathbf{e}_s} q_s \times \mathcal{W}(\mathbf{v}) = \Big(\prod_{r=1}^d q_r^{v_r}\Big)(-\mathcal{W}(\mathbf{1}-\mathbf{e}_s)q_s) \times \mathcal{W}(\mathbf{v})$$

and set $\mathcal{A}_r = q_r$ and $C = -\mathcal{W}(\mathbf{1}-\mathbf{e}_s)q_s$ for s in $\{1,2,\dots,d\}$. Note that, since $G_{-\mathbf{e}_s-\mathbf{e}_{s'}} = G_{-\mathbf{e}_{s'}-\mathbf{e}_s}$ for $s \neq s'$, we have $\mathcal{W}(\mathbf{1}-\mathbf{e}_s)q_s = \mathcal{W}(\mathbf{1}-\mathbf{e}_{s'})q_{s'}$. Moreover, $C^2 = q_1q_2\mathcal{W}(\mathbf{1}-\mathbf{e}_1)\mathcal{W}(\mathbf{1}-\mathbf{e}_2)$ but

$$\begin{aligned} q_3 = \frac{G_{-\mathbf{e}_1}}{G_{-\mathbf{e}_1-\mathbf{e}_3}} &= \mathcal{W}(\mathbf{1}-\mathbf{e}_1) \times \frac{\mathcal{W}(\mathbf{1}-\mathbf{e}_2-\mathbf{e}_4-\cdots-\mathbf{e}_d)}{\mathcal{W}(\mathbf{e}_2+\mathbf{e}_4+\cdots+\mathbf{e}_d)} \\ &= \mathcal{W}(\mathbf{1}-\mathbf{e}_1) \times G_{-\mathbf{e}_2-\mathbf{e}_4-\cdots-\mathbf{e}_d} = \mathcal{W}(\mathbf{1}-\mathbf{e}_1) \times (q_4\cdots q_d)^{-1} G_{-\mathbf{e}_2}, \end{aligned}$$

and hence $C^2 = \prod_{r=1}^d q_r$ since $G_{-\mathbf{e}_2} = \mathcal{W}(\mathbf{1}-\mathbf{e}_2)$. This completes the proof of Theorem 1.4.

Moreover, this result includes [2, Theorem 1] for $u > 3$ (see (2.6) for $u = 2$ or 3). If $u = 2m$ then, $\mathcal{A} = q = \psi_{m+1}/\psi_{m-1} = \omega$ and $C = -q^{i+1}G_{-1} = -q^m$, which gives $\psi_{ku+v} = (-1)^k\omega^{k(v+km)}\psi_v$. If $u = 2m+1$, then $\mathcal{A} = q = (\psi_{m+1}/\psi_m)^2 = \omega^2$ and $C = -q^{i+1}G_{-1} = -q^{m+1}/\omega = -\omega^{2m+1}$, which gives $\psi_{ku+v} = (-1)^k\omega^{k(2v+k(2m+1))}\psi_v$.

EXAMPLE 2.4. Over $\mathbb{Q}$, the curve $y^2 = x^3 - 4x + 1$ with

$$P_1 = (0,1), \quad P_2 = (82264/505521, 213664697/359425431), \quad P_3 = (4,7),$$

gives $\mathbf{u} = (3,1,2)$ and

$$C = 255551481441/19041697792, \quad \mathcal{A} = (711/208, 359425431/297526528, 711/368).$$

We give some calculations to illustrate Theorem 1.4 in Table 1.

According to the Lutz–Nagell theorem [3, Ch. 8], the only possible points of $E(\mathbb{Q})_{tors}$ are $(0,1), (2,\pm1)$ and $(-2,\pm1)$, which cannot arise according to Mazur's

TABLE 2. Calculations illustrating Theorem 1.4 in nonzero characteristic.

$\mathbf{v}$	k	$\mathcal{W}(k\mathbf{u}+\mathbf{v})$	$C^{k^2}(\prod_{r=1}^{d}\mathcal{A}_r^{v_r})^k$	$\mathcal{W}(\mathbf{v})$
$(1,1,1,1)$	1	944	2164	7129
$(2,3,1,5)$	2	5742	3270	7078
$(1,7,11,15)$	3	6155	3676	1766
$(2,1,3,5)$	−1	2254	2788	3165
$(3,7,8,10)$	−2	6418	1532	2475
$(7,3,5,10)$	−3	2331	3928	7845

theorem. As a result, none of the sequences $\psi_n(P_1);\psi_n(P_2);\psi_n(P_3)$ have a rank of zero-apparition.

Over $\mathbb{F}_{7919}$, the curve $y^2=x^3+1562x+1805$ with the points $P_1=(4856,5835)$, $P_2=(6128,7637)$, $P_3=(3336,2121)$ and $P_4=(2415,7795)$ gives $\mathbf{u}=(18,17,12,17)$ and $C=3648$, $\mathcal{A}=(2664,4758,5312,531)$. Some calculations are given in Table 2.

2.5. The latest known general result. We now link our results to [1, Theorem 1.13]. With the assumptions and the notation χ and ξ of this theorem, one can write

$$\mathcal{W}(\mathbf{u}+\mathbf{v})=\xi(\mathbf{u})\chi(\mathbf{u},\mathbf{v})\mathcal{W}(\mathbf{v}).$$

More precisely, with $\Lambda=\{\mathbf{v}\in\mathbb{Z}^d \mid W(\mathbf{v})=0\}$, the functions χ and ξ are defined by

$$\begin{aligned}\delta:\Lambda\times(\mathbb{Z}^d\backslash\Lambda) &\to \mathbb{K}^*\\ (\mathbf{u},\mathbf{v}) &\mapsto \frac{\mathcal{W}(\mathbf{u}+\mathbf{v})}{\mathcal{W}(\mathbf{v})}\end{aligned}$$

and the relations

$$\begin{aligned}\chi:\Lambda\times\mathbb{Z}^d &\to \mathbb{K}^*,\\ (\mathbf{u},\mathbf{v}) &\mapsto \frac{\delta(\mathbf{u},\mathbf{v}+\mathbf{v}')}{\delta(\mathbf{u},\mathbf{v}')} \quad \text{where } \mathbf{v}'\in\mathbb{Z}^d \text{ but } \mathbf{v}',\mathbf{v}'+\mathbf{v}\notin\Lambda,\\ \xi:\Lambda &\to \mathbb{K}^*,\\ \mathbf{u} &\mapsto \frac{\delta(\mathbf{u},\mathbf{v})}{\chi(\mathbf{u},\mathbf{v})} \quad \text{for any } \mathbf{v}\in\mathbb{Z}^d\backslash\Lambda.\end{aligned}$$

We now relate the functions δ of (1.8) and χ,ξ of (1.9) to our notation. We have

$$\chi(\mathbf{u},\mathbf{v})=\frac{\mathcal{W}(\mathbf{u}+\mathbf{v}+\mathbf{v}')}{\mathcal{W}(\mathbf{v}+\mathbf{v}')}\frac{\mathcal{W}(\mathbf{v}')}{\mathcal{W}(\mathbf{u}+\mathbf{v}')}=\prod_{r=1}^{d}\mathcal{A}_r^{v_r}.$$

So we deduce, for all k in $\{1,2,\ldots,d\}$, that $\chi(\mathbf{u},\mathbf{e}_k)=\mathcal{A}_k$, and, in the same way,

$$\xi(\mathbf{u})=C \quad\text{and}\quad \delta(\mathbf{u},\mathbf{v})=C\prod_{r=1}^{d}\mathcal{A}_r^{v_r}=\xi(\mathbf{u})\chi(\mathbf{u},\mathbf{v}).$$

https://doi.org/10.1017/S0004972724000583 Published online by Cambridge University Press

Now, we recall the results of [1, Theorem 1.13, Lemma 4.2] to which we can give an immediate proof.

THEOREM 2.5. *The functions ξ and χ have the following properties.*

(1) *χ is bilinear symmetric: that is, for all $\mathbf{u}, \mathbf{u}^{(1)}, \mathbf{u}^{(2)} \in \Lambda$ and $\mathbf{v}, \mathbf{v}^{(1)}, \mathbf{v}^{(2)} \in \mathbb{Z}^d$,*

   (a) $\chi(\mathbf{u}, \mathbf{v}^{(1)} + \mathbf{v}^{(2)}) = \chi(\mathbf{u}, \mathbf{v}^{(1)})\chi(\mathbf{u}, \mathbf{v}^{(2)})$,
   (b) $\chi(\mathbf{u}^{(1)} + \mathbf{u}^{(2)}, \mathbf{v}) = \chi(\mathbf{u}^{(1)}, \mathbf{v})\chi(\mathbf{u}^{(2)}, \mathbf{v})$,
   (c) $\chi(\mathbf{u}^{(1)}, \mathbf{u}^{(2)}) = \chi(\mathbf{u}^{(2)}, \mathbf{u}^{(1)})$,
   (d) $\chi(\mathbf{u}, -\mathbf{v}) = \chi(\mathbf{u}, \mathbf{v})^{-1}$.

(2) $\xi(\mathbf{u}^{(1)} + \mathbf{u}^{(2)}) = \xi(\mathbf{u}^{(1)})\xi(\mathbf{u}^{(2)})\chi(\mathbf{u}^{(1)}, \mathbf{u}^{(2)})$.
(3) $\xi(-\mathbf{u}) = \xi(\mathbf{u})$.
(4) $\xi(\mathbf{u})^2 = \chi(\mathbf{u}, \mathbf{u})$.
(5) $\xi(n\mathbf{u}) = \xi(\mathbf{u})^{n^2}$, *for all $n \in \mathbb{Z}$.*

PROOF.

(1) (a) is obvious; (b) is obtained from (1.4) with $\mathbf{p} = \mathbf{e}_r$, $\mathbf{q} = -\mathbf{u}^{(2)}$, $\mathbf{r} = 2\mathbf{e}_r$ and $\mathbf{s} = \mathbf{u}^{(1)} + \mathbf{u}^{(2)}$; (c) is easily obtained from $\mathcal{W}(\mathbf{u}^{(1)} + (\mathbf{u}^{(2)} + \mathbf{v})) = \mathcal{W}(\mathbf{u}^{(2)} + (\mathbf{u}^{(1)} + \mathbf{v}))$; and (d) is obvious.
(2) This is easily obtained from $\mathcal{W}((\mathbf{u}^{(1)} + \mathbf{u}^{(2)}) + \mathbf{v}) = \mathcal{W}(\mathbf{u}^{(1)} + (\mathbf{u}^{(2)} + \mathbf{v}))$.
(3) From (1.5) with $\mathbf{p} = 2\mathbf{e}_r$, $\mathbf{q} = \mathbf{u}$ and $\mathbf{r} = \mathbf{e}_r$, we deduce that $\chi(-\mathbf{u}, \mathbf{v}) = \chi(\mathbf{u}, \mathbf{v})^{-1}$ so $\chi(-\mathbf{u}, -\mathbf{v}) = \chi(\mathbf{u}, \mathbf{v})$. The result comes from $\mathcal{W}(-\mathbf{u} - \mathbf{v}) = -\mathcal{W}(\mathbf{u} + \mathbf{v})$.
(4) This follows from $1 = \xi(0) = \xi(\mathbf{u} - \mathbf{u}) = \xi(\mathbf{u})\xi(-\mathbf{u})\chi(\mathbf{u}, -\mathbf{u})$.
(5) This result can be deduced from the previous statements. □

EXAMPLE 2.6. Following [6, Section 5.1], we consider $Q = k.P$ on an elliptic curve E with P and Q of order m. The elliptic net associated to P and Q cancels at the points $\mathbf{u} = (-k, 1)$, $\mathbf{s} = (m, 0)$ and $\mathbf{t} = (0, m)$. With obvious notation,

$$\chi((-km, m), \mathbf{e}_r) = \chi(m(-k, 1), \mathbf{e}_r) = \chi^m((-k, 1), \mathbf{e}_r) = (\mathcal{A}_r^{(\mathbf{u})})^m$$

and

$$\chi((-km, m), \mathbf{e}_r) = \chi^{-k}((m, 0), \mathbf{e}_r)\chi((0, m), \mathbf{e}_r) = (\mathcal{A}_r^{(\mathbf{s})})^{-k}\mathcal{A}_r^{(\mathbf{t})}.$$

Thus, we easily obtain $(\mathcal{A}_r^{(\mathbf{u})})^m = (\mathcal{A}_r^{(\mathbf{s})})^{-k}\mathcal{A}_r^{(\mathbf{t})}$, which is [6, Equation (9)].

For the curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_{11}$, with the points $P_1 = (6, 5)$ and $P_2 = (3, 3)$ of order seven, we have the values shown in Table 3.

2.6. Points of order two or three. We return here to special cases related to the degeneracy conditions of $\mathcal{W}$, namely, $\mathcal{W}(2e_i) \neq 0$ for $1 \leq i \leq d$ and $\mathcal{W}(3e_1) \neq 0$ when $d = 1$. This, therefore, concerns cases where there are points of order two, or order three when $d = 1$, on the elliptic curve E. Note that $|\mathbb{Z}^d/\Lambda| = 2$ occurs only in the case $d = 1$ when $\mathbf{P} = P$ is of order two. We have $|\mathbb{Z}^d/\Lambda| = 3$ if either $d = 1$ and $\mathbf{P} = P$ is of order three, or $d = 2$ and $\mathbf{P} = (P_1, P_2)$ are two points of order two and $\mathbf{u} = (2, 2)$.

https://doi.org/10.1017/S0004972724000583 Published online by Cambridge University Press

TABLE 3. Calculations illustrating Theorem 2.5 for various $u \in \Lambda$.

$\mathbf{u}$	$q_r = \mathcal{A}_r = \chi(\mathbf{u}, \mathbf{e}_r)$
$(1, 5)$	$(7, 8)$
$(2, 3)$	$(8, 9)$
$(3, 1)$	$(6, 6)$
$(5, 4)$	$(4, 10)$
$(4, 6)$	$(9, 4)$
$(6, 2)$	$(3, 3)$
$(7, 7)$	$(10, 2)$

For the case $d = 1$ with $\mathbf{P} = P$ of order two on E, we have $u = 2$ so $i = 0$ and $j = 2$, and hence $G_\ell = \psi_{2+\ell}/\psi_\ell$ with ℓ odd. In (1.1) with $m = 2\ell + 1$ and $n = 2$, we obtain $G_{2\ell+1} = -\psi_3 G_{2\ell-1}$. But we can easily show that, when $y = 0$, we have $\psi_3(x, y) = -((2ax + 3b)/x)^2$ if $x \neq 0$ and $\psi_3(x, y) = -a^2$ if $x = 0$. Hence, in every case, we can write $-\psi_3 = q^2$ with q in $\mathbb{K}$. So, we deduce that $G_{2\ell+1} = q^{2\ell+2} G_{-1} = q^{2\ell+2}$, and writing $2\ell + 1 = i + v = v$ for v odd in $\mathbb{Z}$, since $G_{i+v} = \psi_{u+v}/\psi_{-v}$, we have $\psi_{u+v} = -q^{v+1}\psi_v$. Finally, we set $C = -q$ and $\mathcal{A} = q$, to obtain $C^2 = \mathcal{A}^u$ and $\psi_{ku+v} = C^{k^2}\mathcal{A}^{kv}\psi_v$. We also find the result of [2, Theorem 1].

For the case $d = 1$ with $\mathbf{P} = P$ of order three on E, we proceed in the same way. We have $u = 3$ so $i = 1$ and $j = 2$, and hence $G_\ell = \psi_{2+\ell}/\psi_{1-\ell}$ with $\ell \not\equiv 1 \bmod 3$. In (1.1) with $m = \ell + 1$ and $n = 2$, we obtain $G_{\ell+1} = \psi_2^2 G_\ell$ for $\ell \equiv 2 \bmod 3$. The rest follows in the same way as before with $C = -\psi_2^3$ and $\mathcal{A} = \psi_2^2$ ($C^2 = \mathcal{A}^3 = \mathcal{A}^u$) or $w = \psi_2$ to obtain [2, Theorem 1] when $u = 3$.

For the case $d = 2$, with one or two points of order two, as already mentioned, if G_ℓ creates a problem, then the $G_{\ell'}$ are well defined for $\ell' = \ell \pm \mathbf{e}_r$ or $\ell + \mathbf{e}_s$ or $\ell + \mathbf{e}_s \pm \mathbf{e}_r$ with $r \neq s$ in $\{1, 2, \dots d\}$, and we can then 'bypass' the index ℓ by setting $G_\ell = (G_{\ell+\mathbf{e}_s-\mathbf{e}_r}/G_{\ell+\mathbf{e}_s})G_{\ell-\mathbf{e}_r} = q_r G_{\ell-\mathbf{e}_r}$. Furthermore, $G_{\ell+\mathbf{e}_r} = q_s^{-1} G_{\ell+\mathbf{e}_r+\mathbf{e}_s} = q_s^{-1} q_r^2 G_{\ell-\mathbf{e}_r+\mathbf{e}_s} = q_r^2 G_{\ell-\mathbf{e}_r}$, and hence $G_{\ell+\mathbf{e}_r} = q_r G_\ell$.

For the case $d = 3$, we can have three points of order two but, in this case, $\mathbf{u} = \mathbf{1}$, which we have already dealt with. For $d > 3$, we can always make sure that the geometric character of G_ℓ subsists with the same ratio through a problematic index with points of order two by 'bypassing' in another direction.

Acknowledgement

The author would like to thank the anonymous referee for their comments.

References

[1] A. Akbary, J. Bleaney and S. Yazdani, 'On symmetries of elliptic nets and valuations of net polynomials', *J. Number Theory* **158** (2016), 185–216.

[2] L. Dewaghe, 'Périodicité des polynômes de division sur une courbe elliptique', *Math. Res. Lett.* **14**(6) (2007), 887–891.

[3] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 151 (Springer, New York, 1986).
[4] K. E. Stange, *Elliptic Nets and Elliptic Curves*, PhD Thesis (Brown University, 2008).
[5] K. E. Stange, 'Elliptic nets and elliptic curves', *Algebra Number Theory* **5**(2) (2011), 197–229.
[6] K. E. Stange and K. E. Lauter, 'The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences', in: *Selected Areas in Cryptography*, Lecture Notes in Computer Science, 5381 (eds. R. M. Avanzi, L. Keliher and F. Sica) (Springer, Berlin, 2009), 309–327.
[7] M. Ward, 'Memoir on elliptic divisibility sequences', *Amer. J. Math.* **70** (1948), 31–74.
[8] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd edn, Discrete Mathematics and its Applications, 50 (CRC Press, Boca Raton, FL, 2008).

L. DEWAGHE, Institut Polytechnique UniLaSalle,
SYMADE, Campus Amiens, 14 quai de la somme, 80082 Amiens, France
e-mail: laurent.dewaghe@unilasalle.fr