Stange's Elliptic Nets and Coxeter Group F_4

Daniel R. L. Brown*

April 8, 2010

Abstract

Stange, generalizing Ward's elliptic divisibility sequences, introduced elliptic nets, and showed an equivalence between elliptic nets and elliptic curves. This note relates Stange's recursion for elliptic nets and the Coxeter group F_4.

1 Introduction

Stange [Sta06] generalized Ward's elliptic divisibility sequences to elliptic nets. Two main aspects of Stange's generalization are (a) expansion of the domain from integers (sequence) to arbitrary free abelian groups, and (b) expanding the family of recursive equations from three degrees of freedom to four degrees of freedom.

This note observes a relationship between Stange's recursion for elliptic nets and the finite reflection group F_4 (a Coxeter group). This observation is used to reprove some of Stange's result that certain functions, including Jacobi theta functions, are elliptic nets.

Stange's equivalence between elliptic nets and elliptic curves suggests that perhaps properties of F_4 may also useful for reproving classical results about elliptic curves, such as group structure. Indeed, Coxeter group F_4 is closely related to the group of integral quaternions, and quaternions arise the endomorphism groups of supersingular elliptic curves, so perhaps the connection between elliptic curves and F_4 is deeper than just the elliptic net recursion.

It is tempting to generalize from F_4 to other groups, such as as the finite reflection group E_8 (which is associated with the octonions). Perhaps new recursive equations for elliptic division polynomials may be found. Perhaps new larger-valued divisibility sequences may be found.

2 Definitions

This section provides the basic definitions.

2.1 Notational conventions

The following conventions in notations will generally be used.

*Certicom Research

- Let R be a commutative ring with a multiplicative identity 1. Let $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$ be the ring of integers, the fields of rationals, reals, complex numbers, and the finite field of size q for a prime power q. Elements of these rings have their usual notation. We will usually take R to be an integral domain.

- Let X be an abelian group. We will use additive notation for the group operation of X. (More generally, we make take X to be an S-module for some commutative ring S.)

- If R is a ring, we write R^+ for the abelian group obtained from the ring's addition operation. (More generally, R^+ be the R-module.) We sometimes omit the $+$ superscript, if clear, especially in the case of $\mathbb{Z}$ indicates the infinite cyclic group $\mathbb{Z}^+$. In this paper, we are most interested in the case $X = \mathbb{Z}$. Elements of $\mathbb{Z}^+$ will often be indicated by n or x_i.

- Given abelian group X, the direct product of d copies of X is an abelian group denoted X^d. Elements of X^d will be indicated by $x = (x_1, \ldots, x_d)$ with $x_i \in X$. We usually write elements of X^d as row vectors, but we also consider them as column vectors which can be multiplied on the left by $d \times d$ square matrices over $\mathbb{Z}$.

- If $x \in X$ and $z \in \mathbb{Z}$, we write zx for the sum of z copies of x. More generally, if $x \in X$ and $z = (z_1, \ldots, z_d) \in \mathbb{Z}^d$, we may occasionally write $zx \in X^d$ for $(z_1x, \ldots, z_dx)$. When writing such products, we may also take the factors to be sets, implying the result is the corresponding set of products.

- If $z \in \mathbb{Z}^d$ and $x \in X^d$, then we may write $z \cdot x$ for $z_1x_1 + \cdots + z_dx_d$.

- Also, if $y \in X$ and $z \in \mathbb{Z}$, we write $z|y$ if and only if there exists $x \in X$ such that $y = zx$.

- If $r, s \in R$, we write $r|s$ if there exists $t \in R$ such that $s = rt$. If $r|1$, then we say that r is a unit. The units of a ring R form a group R^* under multiplication. Note that $\{1, -1\}$ forms a subgroup of R^*.

2.2 Two Matrices in the Coxeter Group F_4

Definition 2.1. *An abelian group X is 2-torsion-free if for all $x \in X$, $2x = 0$ implies that $x = 0$.*

If X is 2-torsion-free, and $2|x$, then there exists a unique $y \in X$ such that $x = 2y$. Therefore, we can sensibly apply the notation $y = \frac{1}{2}x$. If X is 2-torsion-free, then so is X^d. If R is a field, then $X = R^+$ to be 2-torsion-free if and only if the characteristic of R is not two.

Remark 2.1. If X is not 2-torsion-free, then the notation $y = \frac{1}{2}x$ is ambiguous because there will be more than one such y.

Definition 2.2. *Let* $X_2^4 = \{(x_1, x_2, x_3, x_4) \in X^4 : 2|x_1 + x_2 + x_3 + x_4\}$.

Definition 2.3. *Let*

$$A = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}, \qquad B = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{1}$$

The matrices A and B are symmetric. They have order two $A^2 = B^2 = 1$, so are orthogonal. If $x \in \mathbb{R}^4$, then $-Ax$ is the reflection of the x in the plane orthogonal to $(1,1,1,1)$, and Bx is the reflection of x in the plane orthogonal to $(-1,1,1,1)$. The determinants of A and B are both -1.

Recall that we will consider $x \in X^4$ as column vectors, so it makes sense to multiply them by integer matrices. The factors $\frac{1}{2}$ in A and B can then be considered as halving operators to applied after application of the matrices, which makes sense if X is 2-torsion-free.

Lemma 2.1. *If X is 2-torsion-free, then sets AX_2^4 and BX_2^4 are subsets of X_2^4.*

Proof. Let $x \in X_2^4$. Then there exists a unique $y \in X$ such that $x_1 + x_2 + x_3 + x_4 = 2y$.

From the definition of A, we have $Ax = (y, y, y, y) - x$, which has entries in X whose sum is $4y - 2y = 2y$. Therefore $Ax \in X_2^4$.

From the definition of B, we have $Bx = (y, y - x_3 - x_4, y - x_2 - x_4, y - x_2 - x_3)$, which entries in X whose sum is $4y - 2(x_2 + x_3 + x_4)$, which is divisible by two. Therefore $Bx \in X_2^4$. □

The result above can fail if X is not 2-torsion-free.

Remark 2.2. The symmetry group of $\mathbb{Z}_2^4$, under isometries, is the finite reflection group F_4, as shown by Coxeter. So matrices A and B are members of this group.

Remark 2.3. The group F_4 has order 1152, and is the second in size of the six finite reflection groups $(H_3, F_4, H_4, E_6, E_7, E_8)$ that are exceptional in the sense of not belonging to one of four infinite families of finite reflection groups $(A_n, B_n, D_n, I_2(n))$.

Remark 2.4. The matrices 1, A and B form a set of coset representatives for the subgroup B_4 of signed permutation matrices.

Remark 2.5. The F_4 symmetry group can also be understood via the Hurwitz quaternions. Probably, many of the results in this paper can be re-expressed in terms of quaternions.

Remark 2.6. The endomorphism group of some elliptic curves, specifically supersingular curves, is an order of the ring of the quaternions. Therefore the close connection between the group F_4 and quaternions probably indicates the connection here between F_4 and Stange's elliptic nets is merely a dim reflection on the general action of quaternions as endomorphisms.

2.3 Stange's Elliptic Nets

In this section, we will define a variant of Stange's elliptic nets. In certain cases, these nets are equivalent to Stange's.

Definition 2.4. *For function $f : X \to R$ and positive integer d, let $f^d : X^d \to R$ be defined by*

$$f^d(x_1, \ldots, x_d) = \prod_{i=1}^{d} f(x_i) \tag{2}$$

Lemma 2.1 allows the following definition to be well-formed.

Definition 2.5. *A function $f : X \to R$ is a* net *from X to R, if X is 2-torsion-free abelian group, R is a commutative ring, and for all $x \in X_2^4$,*

$$f^4(x) = f^4(Ax) + f^4(Bx). \tag{3}$$

Remark 2.7. Stange's elliptic nets restrict X to be a free abelian group.

$$f(Mx) + f(RMx) + f^4(R^2Mx) = 0 \tag{4}$$

where R is a matrix in F_4, with $R^3 = I$, and M is a matrix mapping X^4 to X_2^4. If R is an integral domain, then both (3) and (4) can be shown to imply that f is an odd function. It then follows that $f^4(Rx) = -f^4(Ax)$ and $f^4(R^2x) = -f^4(Bx)$. This then gives an equivalence of the recursions.

Remark 2.8. Although Stange's nets require X to be free abelian, Stange's recursion (4) works well even if X is not 2-torsion-free. Perhaps, then, some of the results in this note will generalize to the X being any abelian group, not necessarily 2-torsion-free.

Remark 2.9. Consider the ring $R[X]$ of polynomials with set of variables being the elements of X and the coefficients being elements of R. We may think of a function $p : X \to R$, as a point in a space R^X, and we can think of an element $e \in R[X]$ as polynomial functions $e : R^X \to R$, with the rule that $e(p)$ is obtained by replacing each variable x appearing in e with its value given by $p(x)$. For $x = (x_1, x_2, x_3, x_4) \in X_2^4$, let $m(x) \in R[X]$ be the quartic monomial $x_1x_2x_3x_4$. Let I be the ideal of $R[X]$ generated by $m(x) - m(Ax) - m(Bx)$. The set of nets is the set $V(I)$ of points in R^X (functions from X to R), which vanish everywhere on I.

3 Examples of Nets

This section gives some examples of nets. All of the results are essentially due to Stange (generalizing earlier results of Ward)[1]. These results are reproven here with a focus on the Coxeter group F_4.

3.1 New Nets from Old Ones

New nets can be built from existing nets using the next three lemmas.

Lemma 3.1. *If*

1. *$g : Y \to X$ is a group homomorphism,*
2. *$f : X \to R$ is a net,*
3. *$h : R \to S$ is a ring homomorphism, and*
4. *Y is 2-torsion-free,*

then $h \circ f \circ g : Y \to S$ is a net.

Proof. Let $F = h \circ f \circ g$. Then, $F^4 = h \circ f^4 \circ g^4$. It follows from g being a homomorphism that $g^4(Y_2^4) \subseteq X_2^4$ and, for $y \in Y_2^4$, that $g^4(Ay) = Ag^4(y)$ and $g^4(By) = Bg^4(y)$. Consequently, if $y \in Y_2^4$ then $F^4(y) = F^4(Ay) + F^4(By)$. □

Lemma 3.2. *If f is a net from X to S, and R is a ring containing subring S, then f with range extended (vacuously) to R is a net from R to S. If f is a net from X to R and S is a subring of R and $f(X) \subseteq S$, then the function f with range restricted to S is a net from X to S.*

[1] Mumford [Mum83] describes Riemann's theta relations, which may also be related to Stange's elliptic net equations.

Proof. Equation (3) holds for the restricted f. □

Remark 3.1. For example, if f is a net from $\mathbb{Z}$ to $\mathbb{Q}$, then f is a net from $\mathbb{Z}$ to $\mathbb{C}$. If also $f(\mathbb{Z}) \subseteq \mathbb{Z}$, then f is a net from $\mathbb{Z}$ to $\mathbb{Z}$.

Definition 3.1. *A function $s : X \to R$ is a* scale *from X to R, if X is a 2-torsion-free abelian group, R is a commutative ring, and for all $x \in X_2^4$:*

$$s^4(x) = s^4(Ax) = s^4(Bx) \tag{5}$$

Lemma 3.3. *If f is a net from X to R, and s is a scale from X to R, the function $F : X \to R$ defined by $F(x) = s(x)f(x)$ is a net from X to R*

Proof. We have $F^4(x) = s^4(x)f^4(x)$. Multiply (3) by $s^4(x)$, using (5) to match the arguments of s with those of f to get $F^4(x) = F^4(Ax) + F^4(Bx)$ for all $x \in X_2^4$. □

The next three lemmas show that scales exist.

Lemma 3.4. *If X is a 2-torsion-free group, R is a commutative ring, and $r \in R$, the function $s : X \to R : x \mapsto r$ is a scale.*

Proof. Equation (5) becomes $r = r = r$. □

Lemma 3.5. *If X is a 2-torsion-free abelian group, R is a commutative ring, $s : X \to R^*$ is a group homomorphism such that $s(x)^2 = 1$ for all $x \in X$, then s is a scale from X to R.*

Proof. Because s is group homomorphism, $s^4(x) = s(x_1 + x_2 + x_3 + x_4)$. If $x \in X_2^4$, then $x_1 + x_2 + x_3 + x_4 = 2y$ for some y, and $s^4(x) = s(2y) = s(y)^2 = 1$. Therefore $s(x) = s(Ax) = s(Bx) = 1$ for all $x \in X_2^4$. □

Lemma 3.6. *If*

1. *$X = \mathbb{Z}$, R is a commutative ring, and $q \in R$, or*
2. *$X = \mathbb{R}^+$ and $R = \mathbb{R}$, and $q \in \mathbb{R}$ with $q > 0$, or*
3. *$X = \mathbb{C}^+$ and $R = \mathbb{C}$, and $q = e$,*

then $s : X \to R : x \mapsto q^{x^2}$ is a scale from X to R.

Proof. In each case, $s^4(x) = q^{|x|^2}$. Because A and B are isometries, we have $|x| = |Ax| = |Bx|$. □

Remark 3.2. The constructions above do not give any actual nets, except perhaps the constant net $f : X \to R : x \mapsto 0$, which is easily seen to be a net.

Remark 3.3. Versions of Lemma 3.1 and 3.2 apply to scales. In particular, for any $u \in \mathbb{C}$, the function defined by $s(x) = e^{(ux)^2}$ is a scale from $\mathbb{C}^+$ to $\mathbb{C}$.

3.2 Neat Nets

The next three lemmas show that nets exist.

Lemma 3.7. *Let R be a commutative ring such that R^+ is 2-torsion-free. The function $f(x) = x$ is a net from R^+ to R.*

Proof. Let $g(x) = f^4(Ax)+f^4(Bx)$. Then $g(x) = q(x)$ where q is some polynomial $q(x_1, x_2, x_3, x_4) \in \mathbb{Z}[x_1, x_2, x_3, x_4]$ that is a homogeneous quartic polynomial in the variables x_1, x_2, x_3, x_4. It will suffice to show that $q(x) = x_1x_2x_3x_4$. Let R_i be the 4×4 diagonal matrix whose i^{th} entry on the diagonal is -1, and all other diagonal entries are 1. Then $AR_i = S_iB$ and $BR_i = T_iA$ for

$$S_1 = \begin{pmatrix} 1 & . & . & . \\ . & -1 & . & . \\ . & . & -1 & . \\ . & . & . & -1 \end{pmatrix}, \qquad T_1 = \begin{pmatrix} 1 & . & . & . \\ . & -1 & . & . \\ . & . & -1 & . \\ . & . & . & -1 \end{pmatrix}, \tag{6}$$

$$S_2 = \begin{pmatrix} . & -1 & . & . \\ 1 & . & . & . \\ . & . & . & 1 \\ . & . & 1 & . \end{pmatrix}, \qquad T_2 = \begin{pmatrix} . & 1 & . & . \\ -1 & . & . & . \\ . & . & . & 1 \\ . & . & 1 & . \end{pmatrix}, \tag{7}$$

$$S_3 = \begin{pmatrix} . & . & -1 & . \\ . & . & . & 1 \\ 1 & . & . & . \\ . & 1 & . & . \end{pmatrix}, \qquad T_3 = \begin{pmatrix} . & . & 1 & . \\ . & . & . & 1 \\ -1 & . & . & . \\ . & 1 & . & . \end{pmatrix}, \tag{8}$$

$$S_4 = \begin{pmatrix} . & . & . & -1 \\ . & . & 1 & . \\ . & 1 & . & . \\ 1 & . & . & . \end{pmatrix}, \qquad T_4 = \begin{pmatrix} . & . & . & 1 \\ . & . & 1 & . \\ . & 1 & . & . \\ -1 & . & . & . \end{pmatrix}, \tag{9}$$

where "." indicates 0. These identities imply $f^4(AR_ix) = -f^4(Bx)$ and $f^4(BR_ix) = -f^4(Ax)$, and therefore

$$g(R_ix) = -g(x) \tag{10}$$

In particular, if $x_i = 0$, then $R_ix = x$, so $g(x) = 0$ because R^+ is 2-torsion-free. This means that $x_i|q(x)$ in $\mathbb{Z}[x_1, x_2, x_3, x_4]$. Therefore, q is a scalar multiple of $x_1x_2x_3x_4$. Direct evaluation of $q(1, 1, 1, 1) = f^4(1, 1, 1, 1) - f^4(2, 0, 0, 0) = 1$ determines the scalar multiple, so therefore $q(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 = f^4(x)$. □

In the following lemma, we use the usual notation of e for the base of the natural logarithm. In particular $e^x = \sum_{n \geqslant 0} x^n/n!$.

Lemma 3.8. *If*

1. *$X = \mathbb{Z}$, R is a commutative ring, and $r \in R^*$, or*
2. *$X = \mathbb{R}^+$, $R = \mathbb{R}$, and $r \in \mathbb{R}$ with $r > 0$, or*
3. *$X = \mathbb{C}^+$, $R = \mathbb{C}$, and $r = e$,*

then the function f defined by $f(x) = r^x - r^{-x}$ is a net from X to R.

Proof. Let $g : \mathbb{Z} \to R : z \mapsto z1$.[2] Lemmas 3.1, 3.2 and 3.7 imply that g is a net from $\mathbb{Z}$ to R.

Let U be the set of all vectors in $\mathbb{Z}_2^4$ of norm 4, which consists of all u of the form $(\pm 1, \pm 1, \pm 1, \pm 1)$ or some permutation of $(\pm 2, 0, 0, 0)$. Then

$$f^4(x) = \sum_{u \in U} g^4(u) r^{u \cdot x} \tag{11}$$

because the terms in the sum with u that are permutations of $(\pm 2, 0, 0, 0)$ vanish as $g^4(u) = 0$, while other terms correspond to the expansion by distributivity.

Matrices A and B permute U. Because these matrices are symmetric, we also have $u \cdot Ax = Au \cdot x$ and $u \cdot Bx = Bu \cdot x$. Recall that $A^2 = B^2 = I$, so the indices u and Au can be swapped in a sum, likewise for u and Bu. Applying these observations, the right hand side of (3) under (11), transforms as follows:

$$\begin{aligned} f^4(Ax) + f^4(Bx) &= \sum_{u \in U} g^4(u) r^{u \cdot Ax} + \sum_{u \in U} g^4(u) r^{u \cdot Bx} \\ &= \sum_{u \in U} g^4(u) r^{Au \cdot x} + \sum_{u \in U} g^4(u) r^{Bu \cdot x} \\ &= \sum_{u \in U} g^4(Au) r^{u \cdot x} + \sum_{u \in U} g^4(Bu) r^{u \cdot x} \\ &= \sum_{u \in U} \left(g^4(Au) + g^4(Bu) \right) r^{u \cdot x} \\ &= \sum_{u \in U} g^4(u) r^{u \cdot x} \\ &= f^4(x), \end{aligned} \tag{12}$$

using the fact that g is a net to get $g^4(Au) + g^4(Bu) = g^4(u)$. □

Remark 3.4. More generally, the proof above should also work for the following claim. If X is a 2-torsion-free abelian group, R is a commutative ring, and $e : X \to R^*$ is a group homomorphism, then $f : X \to R$ defined by $f(x) = e(x) - e(-x)$ is a net from X to R.

Remark 3.5. The function $x \mapsto \sinh(x) = (1/2)(e^x - e^{-x})$ is net from $\mathbb{C}^+$ to $\mathbb{C}$, because $(1/2)$ is a scale by Lemma 3.4 and $e^x - e^{-x}$ is a net by Lemma 3.8.

Remark 3.6. The function $x \mapsto \sin(x)$ is a net from $\mathbb{C}^+$ to $\mathbb{C}$, because $\sin(x) = (-i)\sinh(ix)$ and $-i$ is a scale and $x \mapsto ix$ is a group homomorphism from $\mathbb{C}^+$ to $\mathbb{C}^+$.

Remark 3.7. The function $x \mapsto \sin(x)$ is a net from $\mathbb{R}^+$ to $\mathbb{C}$ by Lemma 3.1 with the embedding homomorphism $x \mapsto x$ from $\mathbb{R}^+$ to $\mathbb{C}^+$. The function $x \mapsto \sin(x)$ is a net from $\mathbb{R}^+$ to $\mathbb{R}$ by Lemma 3.2.

Remark 3.8. The constructions above allow us to devise a net f from $\mathbb{Z}$ to $\mathbb{Z}$ such that $|f(n)| = F_{|n|}$ where F_n is the n^{th} Fibonacci number, and to devise a net from $\mathbb{Z}$ to $\mathbb{Z}$ such that $f(n) = \left(\frac{n}{3}\right)$ meaning the Legendre symbol to base 3.

[2] If $z \in \mathbb{Z}$ and $1 \in R$, then $z1 \in R$.

Let $\delta \in \mathbb{C}$ with $0 < |\delta| < 1$. A function $\epsilon_\delta : \mathbb{C} \to \mathbb{C}$ such that

$$\epsilon_\delta(x) = \sum_{n\in\mathbb{Z}} \delta^{n^2} e^{nx} i^n \tag{13}$$

exists because the series converges.

Remark 3.9. This function is essentially a Jacobi theta function.

Remark 3.10. The function ϵ is quasiperiodic in the sense that $\epsilon(x + 2\pi i) = \epsilon(x)$ and, for $m \in \mathbb{Z}$, $\epsilon_\delta(x) = \sum_{n+m} \delta^{(n+m)^2} e^{(n+m)x} = \delta^{m^2} e^{mx} i^m \epsilon_\delta(x + 2m \log \delta)$.

Lemma 3.9. *The function f defined by $f(x) = \epsilon_\delta(x) - \epsilon_\delta(-x)$ is a net from $\mathbb{C}^+$ to $\mathbb{C}$ if $\delta \in \mathbb{C}$ and $|\delta| < 1$.*

Proof. Upon negating the summation index, $\epsilon_\delta(-x) = \sum_{n\in\mathbb{Z}} i^n e^{-nx} \delta^{n^2} = \sum_{n\in\mathbb{Z}} i^{-n} e^{nx} \delta^{n^2}$, so $f(x) = \sum_{n\in\mathbb{Z}} g(n) e^{nx} \delta^{n^2}$, where $g : \mathbb{Z} \to \mathbb{C}$ is defined by $g(n) = i^n - i^{-n}$. Then f^4 expands as

$$f^4(x) = \sum_{v\in\mathbb{Z}^4} g^4(v) e^{v\cdot x} \delta^{v\cdot v}. \tag{14}$$

If $v \in \mathbb{Z}^4$ but $v \notin \mathbb{Z}_2^4$, then the sum of the entries in the vector v is odd, so not all the entries of v can be odd, implying one entry is even with value, say $2m$. Now $g(2m) = i^{2m} - i^{-2m} = (i^{4m} - 1) i^{-2m} = 0$, because i is a fourth root of unity. Therefore, $g^4(v) = 0$ for $v \in \mathbb{Z}^4 \setminus \mathbb{Z}_2^4$, and the sum (14) can be done only over indices $v \in \mathbb{Z}_2^4$, so

$$f^4(x) = \sum_{v\in\mathbb{Z}_2^4} g^4(v) \delta^{v\cdot v} e^{v\cdot x} \tag{15}$$

Arguing similarly to the proof of Lemma 3.8,

$$\begin{aligned}
f^4(Ax) + f^4(Bx) &= \sum_{v\in\mathbb{Z}_2^4} g^4(v) \delta^{v\cdot v} e^{v\cdot Ax} + \sum_{v\in\mathbb{Z}_2^4} g^4(v) \delta^{v\cdot v} e^{v\cdot Bx} \\
&= \sum_{v\in\mathbb{Z}_2^4} g^4(v) \delta^{v\cdot v} e^{Av\cdot x} + \sum_{v\in\mathbb{Z}_2^4} g^4(v) \delta^{v\cdot v} e^{Bv\cdot x} \\
&= \sum_{v\in\mathbb{Z}_2^4} g^4(Av) \delta^{Av\cdot Av} e^{v\cdot x} + \sum_{v\in\mathbb{Z}_2^4} g^4(Bv) \delta^{Bv\cdot Bv} e^{v\cdot x} \\
&= \sum_{v\in\mathbb{Z}_2^4} g^4(Av) \delta^{v\cdot v} e^{v\cdot x} + \sum_{v\in\mathbb{Z}_2^4} g^4(Bv) \delta^{v\cdot v} e^{v\cdot x} \\
&= \sum_{v\in\mathbb{Z}_2^4} \left(g^4(Av) + g^4(Bv) \right) \delta^{v\cdot v} e^{v\cdot x} \\
&= \sum_{v\in\mathbb{Z}_2^4} g^4(v) \delta^{v\cdot v} e^{v\cdot x} \\
&= f^4(x)
\end{aligned} \tag{16}$$

using the fact that g is a net from $\mathbb{Z}$ to $\mathbb{C}$ by Lemma 3.8. □

Remark 3.11. If $\delta \in \mathbb{C}$ with $|\delta| < 1$, then ϵ_δ is a quasiperiodic, as noted above. It follows that $f(x) = \epsilon_\delta(x) - \epsilon_\delta(-x)$ is also quasiperiodic in exactly the same way: $f(x+2\pi i m) = f(x)$ and $f(x+2m\log\delta) = f(x)\delta^{m^2}e^{mx}$. Because $f(0) = 0$ and f is quasiperiodic, it follows that for all $m, n \in \mathbb{Z}$, that $f(2\pi m + 2n\log\delta) = 0$. Therefore, f has zeros on the subgroup of $\mathbb{C}^+$ generated by the elements $2\pi i$ and $2\log\delta$.

Remark 3.12. Taking Jacobi theta function $f(x) = \epsilon_\delta(x) - \epsilon_\delta(-x)$, which is a net from $\mathbb{C}^+$ to $\mathbb{C}$, one can apply the homomorphism $g : \mathbb{Z}^+ \to \mathbb{C}^+ : n \mapsto n$, to get that $f \circ g$, or effectively just f by restriction, is a net from $\mathbb{Z}$ to $\mathbb{C}$. If $f(\mathbb{Z}) \subseteq \mathbb{Z}$ also happens to hold, then f is a net from $\mathbb{Z}$ to $\mathbb{Z}$ by subring restriction. Taking a homomorphism $h : \mathbb{Z} \to \mathbb{Z}/(p)$ for some prime p, then $h \circ f$ is a net from $\mathbb{Z}$ to $\mathbb{Z}/(p)$, which is a function perhaps more applicable to cryptology.

Remark 3.13. Cryptology seldom deals with infinite series. It may be worthwhile to determine whether Lemma 3.9 can be generalized to finite sums that yield interesting nets.

3.3 Not So Nice Nets

Lemma 3.10. *If*

1. *X is 2-torsion-free abelian group,*
2. *$y \in X$,*
3. *R is an integral domain, and*
4. *$f : \mathbb{Z} \to R$ is a function,*
5. *$f(x) = 0$ for all $x \neq \pm y$, and*
6. *$f(-y) = -f(y)$,*

then f is a net from X to R.

Proof. Using the notation of the proof of Lemma 3.8, $f^4(x) = 0$ if $x \notin Uy$. Therefore, (3) holds for $x \notin Uy$, because Uy is closed under the action of A and B.

We note that $f(0) = 0$ because if $y \neq 0$, and, if not, by the property of $f(-y) = -f(y)$ and R being an integral domain. If $x \in Uy$, then $f^4(x) = 0$ unless $x = (\pm y, \pm y, \pm y, \pm y)$, in which case $f^4(x) = y^4 g^4(x)$. In fact, $f^4(x) = y^4 g^4(x)$ for all $x \in Uy$. Therefore (3) holds since it holds for g. □

4 Oddity of Nets

Nets have some simple properties.

Lemma 4.1. *If f is a net from X to R, then $f(0)^4 = 0$.*

Proof. Put $x = (0,0,0,0) \in X_2^4$, in (3). Then $Ax = Bx = x$, so (3) becomes $f^4(x) = 2f^4(x)$. Subtracting $f^4(x)$ implies $f(0)^4 = f^4(x) = 0$. □

Corollary 4.1. *If f is a net from X to R, and R has no nonzero nilpotent elements, then $f(0) = 0$.*

Proof. Lemma 4.1 says that $f(0)$ is nilpotent. Because $f(0)$ has no nonzero nilpotent elements, we must have $f(0) = 0$. □

Remark 4.1. Corollary 4.1 includes the case that R is an integral domain. In cryptology, though, rings R that are not integral domains are sometimes considered, such as $R = \mathbb{Z}/(n)$ for n a composite number.

Remark 4.2. In RSA public key cryptography system, one form a public key from $n = pq$, for distinct primes p and q. The ring $R = \mathbb{Z}/(n)$ has no nonzero nilpotent elements.

Remark 4.3. For certain variants of RSA, one takes $n = p^2q$ for distinct primes p and q. In this case, $R = \mathbb{Z}/(n)$ has nonzero nilpotent elements, such as $r = pq$.

A partial converse to Corollary 4.1 is the following:

Lemma 4.2. *If X is 2-torsion-free abelian group, and R is a commutative ring with a nonzero nilpotent element, then there exists a net f from X to R with $f(0) \neq 0$.*

Proof. By the hypothesis, some $r \in R$ is such that $r \neq 0$ and $r^n = 0$ for some positive intger n. Let m be the smallest positive integer such that $r^m = 0$. Then $m \neq 1$, because $r \neq 0$, so $m \geqslant 2$.

Let $s = r^{m-1}$. Then $s \neq 0$, otherwise m would not have been the smallest integer with the given property. Since $m \geqslant 2$, we have $3m \geqslant 6$. Therefore $3m - 4$ is a postive number. Now $s^4 = 0$, because $s^4 = r^{4m-4} = r^m r^{3m-4}$ and $r^m = 0$, so $s^4 = 0$.

Let $f : X \to R$ be defined by $f(x) = s$ for all x. Then $f^4(x) = s^4 = 0$ for all $x \in X^4$. Therefore (3) holds because $0 = 0 + 0$, and f is net. Also, $f(0) = s \neq 0$. □

Lemma 4.3. *If f is a net from X to R, and R has no nonzero nilpotent elements, then $f(-x) = -f(x)$ for all $x \in X$.*

Proof. Let $y = (2x, 0, 0, 0)$. Then $y \in X_2^4$ because the sum of entries is $2x$. From the definitions of matrices A and B, we have $Ay = (-x, x, x, x)$ and $By = (x, x, x, x)$. By Lemma 4.1, $f(0) = 0$. Therefore, $f^4(y) = f(2x)f(0)^3 = 0$. By f being a net $f(y) = f^4(Ay) + f^4(By)$. By the expansions Ay and By above, $f^4(Ay) + f^4(By) = (f(x) + f(-x))f(x)^3$. Therefore $0 = (f(x) + f(-x))f(x)^3$ for all $x \in X$. Let $t = (f(x) + f(-x))f(x)$. Then $t^3 = 0$, so $t = 0$, by the property of R.

Negating x in t, we have similarly, $s = f(-x)(f(-x) + f(x)) = 0$. Therefore, $0 = s + t = (f(-x) + f(x))^2$. Now $f(-x) + f(x)$ is nilpotent, so $f(-x) + f(x) = 0$, by the property of R, so $f(-x) = -f(x)$. □

Definition 4.1. *A function $f : X \to R$ is odd if $f(-x) = -f(x)$ for all $x \in R$.*

Remark 4.4. Lemma 4.3 says every net to a ring with trivial nilradical is odd. In particular, a net to an integral domain or field is odd.

Remark 4.5. Let N be the nilradical of R, and let $h : R \to R/N$ be the natural homomorphism. Then $h \circ f$ is a net from X to R/N, and $h \circ f$ must be odd.

Remark 4.6. In general, the results above suggest that for an arbitrary ring R, a net f from X to R decomposes as $f = d + n$, where $d : X \to R$ is odd, and the $n : X \to R$ is nilpotent.

Definition 4.2. *If X is a 2-torsion-free abelian group, and R is a commutive ring, a function $f : X \to R$ is a pseudonet from X to R if (3) for all $x \in X_2^4$ such that one of the entries of x is zero.*

Lemma 4.4. *If R^+ is 2-torsion-free and $f : X \to R$ is an odd, then f is a pseudonet from X to R. If R has no nonzero nilpotent elements and f is a pseudonet from X to R, then f is odd.*

Proof. Suppose R has no nonzero nilopotent elements that f is a pseudonet. The proof of Lemmas 4.3 and Lemma 4.1 only uses (3) for x with an entry of zero, so they apply if f is just a pseudonet. Therefore, f is odd.

Suppose that f is odd, that R^+ is 2-torsion-free, and that x has an entry of zero. Now $f(0) = f(-0) = -f(0)$, so $2f(0) = 0$. Since R^+ is 2-torsion-free, we have that $f(0) = 0$. Therefore $f^4(x) = 0$. With the notation of the proof of Lemma 3.7, if $x_i = 0$, then $R_i x = x$. Therefore, $f^4(Ax) + f^(Bx) = f^4(AR_i x) + f^4(BR_i x) = f^4(S_i Bx) + f^4(T_i Ax) = -f^4(Bx) + f^4(Ax)$. Therefore, $2(f^4(Ax) + f^4(Bx) = 0$. Since R^+ is 2-torision-free, we have $f^4(Ax) + f^4(Bx) = 0 = f^4(x)$. □

Remark 4.7. If R is a commutative ring, R has trivial nilradical, and R^+ is 2-torsion-free, and X is a 2-torsion-free abelian group, then $f : X \to R$ is a pseudonet if and only if it is odd.

Remark 4.8. For the rings R above, equations (3) can only imply something more substantial than f being odd, for x with no nonzero entries.

Remark 4.9. The definition of pseudonet can be generalized to the case when any one of x, Ax and Bx has a zero entry. The relevant lemma and remarks above generalize.

5 Groups from Nets

5.1 Quadratic Hypersurfaces

In this section, we try to show that nets sometimes define an algebraic group which is a homomorphic image of X. First we show that a net maps X to an algebraic (quadratic) set in R^5.

Lemma 5.1. *Let f be a net from X to R. Let $o \in X$. Define $g_o : X \to R^5$, by*

$$g_o(n) = (f(n-2o), f(n-o), f(n), f(n+o), f(n+2o)). \tag{17}$$

Then there are four quadratic polynomials Q_o in five variables, such that $Q_o(g_o(x)) = 0$ for all $x \in X$.

Proof. Let $h_j(n) = f(n + jo)$. It suffices to show $g_o(n) = (h_{-2}(n), h_{-1}(n), h_0(n), h_1(n), h_2(n))$ satisfies three quadratic equations.

Let $x = (n, n, o, 3o)$. Then $x \in X_2^4$, because the sum of its entries is $2(n + 2o) \in 2X$. Direct calculation gives $Ax = (2o, 2o, n + o, n - o)$ and $Bx = (n + 2o, n - 2o, -o, o)$. Because f is a net, we have $f^4(x) = f^4(Ax) + f^4(Bx)$, which implies that

$$f(o)f(3o)h_0(n)^2 = f(2o)^2 h_1(n)h_{-1}(n) + f(o)f(-o)h_2(n)h_{-2}(n) \tag{18}$$

Let

$$Q_o : (z_{-2}, z_{-1}, z_0, z_1, z_2) \mapsto f(o)f(3o)z_0^2 - f(2o)^2 z_1 z_{-1} - f(o)f(-o)z_2 z_{-2}, \tag{19}$$

which is quadratic function in five variables, with the property that $Q_o(g_o(n)) = 0$ for all $n \in X$. Shifting the z indices down by one, and up by one and two gives three other quadratic polynomials. □

If R is an integral domain, then we can form its field F of fractions. We can then form usual the projective space $F\mathbb{P}^4$ with element $z = [z_{-2} : z_{-1} : z_0 : z_1 : z_2]$, such that not all the z_i are zero, two such quintuples z and y are considered equal if there exists $r \in F^*$ such that $z_j = ry_j$ for all j.

Definition 5.1. *Let f be a net from X to R. Let $o \in X$. If there exists $n \in X$ such that $g_o(n)$, then we say that f is degenerate at o. Otherwise, we say that f is non-degenerate at o.*

The homogeneous quadratic in five variables Q_o above defines a subset V_o of the $F\mathbb{P}^4$. If f is non-degenerate at o, then we can define $e_o : X \to V_o$ by

$$e_o(n) = [f(n-2o) : f(n-o) : f(n) : f(n+o) : f(n+2o)], \tag{20}$$

which belongs to $F\mathbb{P}^4$ because by non-degeneracy of f at o, at least one of the five entries above is non-zero.

Lemma 5.2. *Let R be an integral domain. Let f be a net from X to R, such that $f(o), f(2o) \in R^*$. There exists an algebraic function $a_o : V_o^2 \to V_o$ such that $e_o(m+n) = a_o(e_o(m), e_o(n))$.*

Proof. Let

$$L = \begin{pmatrix} -2 & -1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 & 1 \end{pmatrix}, \tag{21}$$

then

$$AL = \begin{pmatrix} 2 & 2 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 2 \\ -1 & 0 & 0 & 1 & 1 \\ -1 & -1 & 0 & 0 & 1 \end{pmatrix}, \qquad BL = \begin{pmatrix} 0 & 1 & 1 & 2 & 2 \\ -2 & -2 & -1 & -1 & 0 \\ -1 & -1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 & 1 \end{pmatrix}. \tag{22}$$

Let k be column of L, and let $x = (m+n, m-n, 0, 0) + ok$. One can verify that $x \in X_2^4$. Then $f^4(x) = f(m+n+so)f(m-n)f(o)f(to)$ where $s \in \{-2,-1,0,1,2\}$ and $t \in \{1,2\}$. Because $A(m+n, m-n, 0, 0) = (-n, n, m, m)$ and $B(m+n, m-n, 0, 0) = (m, m, n, n)$ and matrix equations (22) and f is odd, both $f^4(Ax)$ and $f^4(Bx)$ are expressible as quartic polynomials in the ten variables in the entries of the representives of $e_o(m)$ and $e_o(n)$ as given in (20).

Write $r = m + n$ and

$$e_o(m) = [m_{-2} : m_{-1} : m_0 : m_1 : m_2] \tag{23}$$
$$e_o(n) = [n_{-2} : n_{-1} : n_0 : n_1 : n_2] \tag{24}$$
$$e_o(r) = [r_{-2} : r_{-1} : r_0 : r_1 : r_2]. \tag{25}$$

Then the arguments above have established that

$$r_{-2}f(m-n) = (-m_{-1}^2 n_{-2} n_0 + m_0 m_{-2} n_{-1}^2) f(o)^{-2} \tag{26}$$

$$r_{-1}f(m-n) = (-m_{-1} m_0 n_{-2} n_1 + m_1 m_{-2} n_{-1} n_0)(f(o)f(2o))^{-1} \tag{27}$$

$$r_0 f(m-n) = (-m_0^2 n_{-1} n_1 + m_1 m_{-1} n_0^2) f(o)^{-2} \tag{28}$$

$$r_1 f(m-n) = (-m_1 m_0 n_{-1} n_2 + m_2 m_{-1} n_1 n_0)(f(o)f(2o))^{-1} \tag{29}$$

$$r_2 f(m-n) = (-m_1^2 n_0 n_2 + m_2 m_0 n_1^2) f(o)^{-2} \tag{30}$$

Let a_o be defined as follows. For any $[m_j], [n_j] \in V_o$, define $[r_j] = a_o(m, n)$ by taking the right hand sides of the five equations above, unless all five results are zero, in which case a definition below will be given.

If $f(m-n) \neq 0$, then the five equations above imply that $e_o(m+n) = a_o(e_o(m), e_o(n))$. If $f(m-n) = 0$, the five right hand sides above are each zero, so a_0 is not defined above, will instead be defined as follows.

TO BE COMPLETED. □

References

[Mum83] D. Mumford. *Tata Lectures on Theta I.* Birkhäuser, 1983.

[Sta06] K. E. Stange. *The Tate pairing via elliptic nets.* ePrint 2006/392, International Association of Cryptologic Research, 2006.