ELLIPTIC NETS AND POINTS ON ELLIPTIC CURVES

KATHERINE E. STANGE

Elliptic divisibility sequences were first studied by Morgan Ward in 1948 [11]. These are integer sequences $h_0, h_1, \ldots, h_n, \ldots$ satisfying the following two properties:

(1) For all positive integers $m > n$,

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \; . \tag{1}$$

(2) h_n divides h_m whenever n divides m.

They have attracted number theoretical and combinatorial interest as some of the simplest non-linear recurrence sequences (see [3] for references), but for us their interest lives in the underlying geometry: Ward demonstrates that an elliptic divisibility sequence arises from any choice of elliptic curve over $\mathbb{Q}$ and rational point on that curve.

Theorem 1 (M. Ward, 1948, [11])**.** *Suppose E is an elliptic curve defined over $\mathbb{Q}$, $\sigma : \mathbb{C} \to \mathbb{C}$ is its Weierstrass sigma function, and $u \in \mathbb{C}$ corresponds to a rational point on E. Then there exists an integer k such that the sequence*

$$h_n := k^{n^2-1}\frac{\sigma(nu)}{\sigma(u)^{n^2}}$$

forms an elliptic divisibility sequence.

The recurrence sequence reflects the behaviour of a point under multiplication; it provides access to information about $[n]P$ via a recurrence relation instead of direct curve computations. Indeed, Rachel Shipsey used this idea to solve the elliptic curve discrete logarithm problem in certain situations [6], while Mohamad Ayad used it to develop methods of finding integer points on elliptic curves of rank one [1]. To fully exploit this paradigm, then, it is desirable to extend to additions in general. Is there a multidimensional version of the sequences "reflecting" all the possible linear combinations

$$[n_1]P_1 + \ldots + [n_k]P_k \; ?$$

To accomplish this, in place of sequences we will define *elliptic nets.*

Definition 1. *Let A be a finitely generated free abelian group, and R be an integral domain. An* elliptic net *is any map $W : A \to R$ such that the following recurrence holds for all p, q, r, $s \in A$.*

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

We say W is normalised *if $A = \mathbb{Z}^n$ and $W(\mathbf{z}) = 1$ whenever $\mathbf{z} = \mathbf{e}_i$ or $\mathbf{z} = \mathbf{e}_i + \mathbf{e}_j$ with $i \neq j$ (where $\mathbf{e}_i$ are the standard basis vectors).*

Date: April 15, 2007.

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

$\uparrow Q$ $P \rightarrow$

over $\mathbb{Q}$

0	4	4	3	1	2	4
4	4	4	4	1	3	0
4	3	2	0	3	2	1
0	3	1	4	4	4	4
1	3	4	2	4	1	0
1	1	2	0	2	4	1
0	1	1	2	1	3	4

$\uparrow Q$ $P \rightarrow$

over $\mathbb{F}_5$

FIGURE 1. A portion of the elliptic net of $E : y^2 + y = x^3 + x^2 - 2x$, $P = (0, 0)$, $Q = (1, 0)$.

Elliptic nets have the symmetry property that $W(-z) = -W(z)$ for any $z \in A$ (and in particular $W(0) = 0$). When $A = R = \mathbb{Z}$ and $W(1) = 1$, the positive terms of an elliptic net satisfy Ward's equation (1) above. Under the further condition that $W(2)|W(4)$, these terms form an elliptic divisibility sequence.

Christine Swart studied a general class of Somos-4 sequences arising from elliptic curves and including elliptic divisibility sequences [9]. Her work, and related work of van der Poorten [10], provided the clues that the more general theory of nets existed. It has recently come to my attention that the possibility of such a definition was briefly discussed in correspondence by Noam Elkies, James Propp and Michael Somos in 2001 [5].

To extend Ward's Theorem 1 to the elliptic net case (with $R = \mathbb{C}$), we define appropriate multi-elliptic functions and show that they satisfy the recurrence (2).

Definition 2. *Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. For $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$, define a function $\Psi_{\mathbf{v}}$ on $\mathbb{C}^n$ in variables $\mathbf{z} = (z_1, \ldots, z_n)$ as follows:*

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

In particular, we have for each $k \in \mathbb{Z}$, a function Ψ_k on $\mathbb{C}$ in the variable z:

$$\Psi_k(z; \Lambda) = \frac{\sigma(kz; \Lambda)}{\sigma(z; \Lambda)^{k^2}}$$

and for each pair $(k, l) \in \mathbb{Z} \times \mathbb{Z}$, a function $\Psi_{k,l}$ on $\mathbb{C} \times \mathbb{C}$ in variables z and w:

$$\Psi_{k,l}(z, w; \Lambda) = \frac{\sigma(kz + lw; \Lambda)}{\sigma(z; \Lambda)^{k2 - kl} \sigma(z + w; \Lambda)^{kl} \sigma(w; \Lambda)^{l2 - kl}}$$

These functions are elliptic in each variable.

We will now see that the $\Psi_{\mathbf{v}}$ form an elliptic net as a function of $\mathbf{v} \in \mathbb{Z}^n$ when $\mathbf{z} \in \mathbb{C}^n$ and the lattice Λ are fixed. Denote by $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ the complex uniformisation of an elliptic curve. Then for any number field $L \subset \mathbb{C}$, define the free abelian group $\hat{E}_L = \pi^{-1}(E(L))$. As a means of fixing $\mathbf{z}$, we specify a homomorphism $\phi : \mathbb{Z}^n \to \hat{E}_L$.

Definition 3. *Suppose $\phi : \mathbb{Z}^n \to \hat{E}_L$ is a homomorphism such that the images of $\pm\mathbf{e}_i$ under $\pi \circ \phi$ are all distinct. Define $W_\phi : \mathbb{Z}^n \to \mathbb{C}$ by*

$$W_\phi(\mathbf{v}) = \Psi_{\mathbf{v}}(\phi(\mathbf{e}_1), \phi(\mathbf{e}_2), \ldots, \phi(\mathbf{e}_n); \Lambda)$$

Theorem 2. *$W_\phi : \mathbb{Z}^n \to L$ is an elliptic net.*

In this way, we can associate an elliptic net to any choice of n points $P_i \in E(L)$ which, along with their negatives, are all distinct. We call W_ϕ the *elliptic net associated to* $E, P_1, \dots, P_n$. A portion of such an example net is shown in Figure 1.

It can be shown that all normalised elliptic nets with $R = \mathbb{C}$ arise in this manner. In fact, the curve and points concerned can be calculated explicitly.

To extend to curves defined over other fields, it is necessary to remove the dependence on the complex analytic definition. The functions $\Psi_{\mathbf{v}}$ may be written as rational functions in the coordinates $x_i = \wp(P_i), y_i = \wp'(P_i)$. In the case of elliptic divisibility sequences, these are exactly the so-called division polynomials. In the more general case, we have the following theorem:

Theorem 3. *Let $n \geq 1$. Consider an elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{C}$. Let $p_i : E^n \to E$ be projection maps and $s : E^n \to E$ the summation. Let*

$$U = E^n \backslash \left(\bigcup_{k=1}^{n} p_k^*(\mathcal{O}) \bigcup_{1 \leq k < j \leq n} (p_k^* \times p_j^*) s^*(\mathcal{O}) \right) \ .$$

The $\Psi_{\mathbf{v}}$ associated to E are regular on U and are in the subring

$$\mathbb{Z}[A,B][x_i, y_i]_{i=1}^n \left[(x_i - x_j)^{-1} \right]_{1 \leq i < j \leq n} \Big/ \left\langle y_i^2 - x_i^3 - Ax_i - B \right\rangle_{i=1}^n \subset \mathcal{O}_{E^n}(U) \ .$$

The geometric content of the theorem is that there are functions defined on $U_{\mathbb{Z}}$ whose restrictions to U are the $\Psi_{\mathbf{v}}$.

In particular, we may define elliptic nets over finite fields. It remains to examine the relationship between the elliptic net of a curve over a number field and its reduction modulo a prime.

Let E be an elliptic curve over a number field $L \subset \mathbb{C}$ with ring of integers R. Let $\mathfrak{p}$ be a prime of good reduction for an elliptic curve E and let δ denote both the reduction modulo $\mathfrak{p}$ on the curve E and on the ring of integers R.

Theorem 4. *Consider points $P_1, \dots, P_n \in E(L)$ such that the reductions modulo $\mathfrak{p}$ of the $\pm P_i$ are all distinct and nonzero. Then for each $\mathbf{v} \in \mathbb{Z}$ there exists a function $\Omega_{\mathbf{v}}$ such that the following diagram commutes:*

$$\begin{tikzcd}
E_L^n(R) \arrow[r, "\Psi_{\mathbf{v}}"] \arrow[d, "\delta"'] & \mathbb{P}^1(L) \arrow[d, "\delta"] \\
E_{k_{\mathfrak{p}}}^n(k_{\mathfrak{p}}) \arrow[r, "\Omega_{\mathbf{v}}"] & \mathbb{P}^1(k_{\mathfrak{p}})
\end{tikzcd}$$

Furthermore $\operatorname{div}(\Omega_{\mathbf{v}}) = \delta^* \operatorname{div}(\Psi_{\mathbf{v}})$.

Figure 1 illustrates the relationship between an example elliptic net associated to E, P, Q over $\mathbb{Q}$ and the elliptic net associated to their reductions $\tilde{E}, \tilde{P}, \tilde{Q}$ modulo 5. The order of $\tilde{Q}$ in this example is 3, but if we let W be the elliptic divisibility sequence associted to $\tilde{E}, \tilde{Q}$, then $W(4) \not\equiv W(1)$ mod $\mathfrak{p}$. The exact relationship is given by the "periodicity properties" of elliptic nets. For the case of elliptic divisibility sequences it has a particularly simple statement:

Theorem 5 (M. Ward, 1948, [11])**.** *Let W is an elliptic divisibility sequence, and $p \geq 3$ a prime not dividing $W(2)W(3)$. Let r be the least positive integer such that $W(r) = 0$. Then there exist integers a, b such that for all n,*

$$W(kr + n) \equiv W(n) a^{nk} b^{k^2} \mod p \ .$$

In the case of elliptic nets in general, the periodicity properties relate to the Tate pairing. Choose $m \in \mathbb{Z}^+$. Let E be an elliptic curve defined over a field K containing the m-th roots of unity. Suppose $P \in E(K)[m]$ and $Q \in E(K)/mE(K)$. Since P is an m-torsion point, $m(P) - m(\mathcal{O})$ is a principal divisor, say $\operatorname{div}(f_P)$. Choose another divisor D_Q defined over K such that $D_Q \sim (Q) - (\mathcal{O})$ and with support disjoint from $\operatorname{div}(f_P)$. Then, we may define the Tate pairing

$$\tau_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$$

by

$$\tau_m(P, Q) = f_P(D_Q)$$

This pairing is well-defined, bilinear and Galois invariant. The well-known Weil pairing e_m satisfies $e_m(P, Q) = \tau_m(P, Q)/\tau_m(Q, P)$. The Tate pairing is commonly used in implementations of pairing-based elliptic curve cryptography. In this case, it is usually considered over finite fields, where it is non-degenerate. For details, see [2, 4].

The following theorem is example of the computation of the Tate pairing using an elliptic net.

Theorem 6. *Let E be an elliptic curve defined over a finite field K, m a positive integer, $P \in E(K)[m]$ and $Q \in E(K)$. If W is the elliptic net associated to E, P, Q, then we have*

$$\tau_m(P, Q) = \frac{W(m+1, 1)W(1, 0)}{W(m+1, 0)W(1, 1)}$$

There are methods of computing terms of elliptic nets which allow one to compute this value in $\log(m)$ time. This method may also be used to compute the Weil pairing. For further details and more such theorems see [7] and [8].

Other work in progress includes extending the work of Ayad [1] for finding integer points on curves of higher rank.

References

[1] Mohamed Ayad. Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques. *Ann. Inst. Fourier (Grenoble)*, 43(3):585–618, 1993.

[2] Sylvain Duquesne and Gerhard Frey. Background on pairings. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 115–124. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[3] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Elliptic Divisibility Sequences*, pages 163–175. American Mathematical Society, Providence, 2003.

[4] S. Galbraith. Pairings. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 183–213. Cambridge Univ. Press, Cambridge, 2005.

[5] James Propp. Robbins forum. `http://www.math.wisc.edu/~propp/about-robbins`.

[6] Rachel Shipsey. *Elliptic Divibility Sequences.* PhD thesis, Goldsmiths, University of London, 2001.

[7] Katherine E. Stange. The tate pairing via elliptic nets. To appear in PAIRING 2007.

[8] Katherine E. Stange. *Elliptic Nets.* PhD thesis, Brown University, in preparation.

[9] Christine Swart. *Elliptic curves and related sequences.* PhD thesis, Royal Holloway and Bedford New College, University of London, 2003.

[10] Alfred J. van der Poorten. Elliptic curves and continued fractions. *J. Integer Seq.*, 8(2):Article 05.2.5, 19 pp. (electronic), 2005.

[11] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.