Elliptic Nets and Points on Elliptic Curves

Katherine Stange

Department of Mathematics
Brown University
http://www.math.brown.edu/~stange/

Algorithmic Number Theory, Turku, Finland, 2007

Outline

Divisibility in Linear Recurrences

Consider an integer linear recurrence of the form

$$L_0 = 0; \qquad L_1 = 1; \qquad L_n = aL_{n-1} - L_{n-2}$$

Theorem (Divisibility Property)

If $n|m$ then $L_n|L_m$.

Proof.

Let α be a root of $x^2 - ax + 1 = 0$. Then

$$L_n = \Phi_n(\alpha) := \frac{\alpha^n - \alpha^{-n}}{\alpha - \alpha^{-1}} \quad .$$

□

Geometric Viewpoint

The function

$$\boxed{\Phi_n(x) = \frac{x^n - x^{-n}}{x - x^{-1}}}$$

is the function on $\mathbb{G}_m$ with simple zeroes at the $2n$-torsion points besides 1 and -1.

Reducing Modulo a Prime

$$\begin{array}{ccc} \mathfrak{p} & & \mathbb{Q}(\alpha) \\ | & & | \\ p & & \mathbb{Q} \end{array}$$

- Reducing modulo $\mathfrak{p}$, we obtain $\mathbb{G}_m$ over $\mathbb{F}_q$.
- The image $\widetilde{\alpha}^2$ has some finite order n_p.
- For all k, $\Phi_{kn_p}(\alpha) \equiv 0 \mod p$.

Divisibility Restated (Almost)

For each prime p there is a positive integer n_p such that

$$L_n \equiv 0 \mod p \iff n_p | n$$

What Geometry Tells Us

- The geometry gives meaning to the statement that $p|L_n$.
- It also tells us more: e.g. $n_p|q-1$.

Example

The even-index Fibonaccis satisfy $F_n = 3F_{n-1} - F_{n-2}$. They are

$$1, 3, 8, 21, 55, 144, 377, \ldots$$

The prime 7 appears first at index $4|7^2 - 1$. The prime 11 appears first at index $5|11 - 1$.

Elliptic Divisibility Sequences

Definition

A sequence h_n is an *elliptic divisibility sequence* if for all positive integers $m > n$,

$$h_{m+n}h_{m-n}h_1^2 = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 .$$

- Generated by initial conditions $h_0, \ldots, h_4$ via the recurrence.
- Necessarily $h_0 = 0$; by convention $h_1 = 1$.
- If initial terms are integers and $h_2 | h_4$, then the sequence is entirely integer and satisfies the divisibility property.

Defining An Appropriate Function

Definition

Let σ be the Weierstrass sigma function associated to the complex uniformization of an elliptic curve.

$$\Psi_n(z) = \frac{\sigma(nz)}{\sigma(z)^{n^2}}$$

- Elliptic functions.
- Simple zeroes at non-zero n-torsion points.

Elliptic Divisibility Sequences from Elliptic Curves

Theorem (M. Ward, 1948)

Let E be an elliptic curve defined over $\mathbb{Q}$ with lattice $\Lambda \subset \mathbb{C}$, and let $u \in \mathbb{C}$ correspond to a rational point P on E. Then

$$h_n := \Psi_n(u)$$

forms an elliptic divisibility sequence.

- We call this the sequence associated to E, P.

Example: $y^2 + y = x^3 + x^2 - 2x$, $P = (0,0)$

$$\begin{aligned}
P &= (0,0) & h_1 &= 1\\
[2]P &= (3,5) & h_2 &= 1\\
[3]P &= \left(-\frac{11}{9}, \frac{28}{27}\right) & h_3 &= -3\\
[4]P &= \left(\frac{114}{121}, -\frac{267}{1331}\right) & h_4 &= 11\\
[5]P &= \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right) & h_5 &= 38\\
[6]P &= \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right) & h_6 &= 249\\
[7]P &= \left(-\frac{2182983}{5555449}, -\frac{20464084173}{13094193293}\right) & h_7 &= -2357
\end{aligned}$$

The Recurrence Calculates the Group Law

Points on the curve have the form

$$[n]P = \left(\frac{a_n}{h_n^2}, \frac{b_n}{h_n^3} \right)$$

- The sequences a_n and b_n can be calculated from h_n.
- The point $[n]P$ can be recovered from $h_{n-2}, h_{n-1}, h_n, h_{n+1}, h_{n+2}$.

Lesson 1

The recurrence calculates the group law (for multiples of P).

History of Research

- Applications to Elliptic Curve Discrete Logarithm Problem in cryptography (R. Shipsey)
- Finding integral points (M. Ayad)
- Primes in EDS (G. Everest, J. Silverman, T. Ward, ...)
- EDS are a special case of Somos Sequences (A. van der Poorten, J. Propp, M. Somos, C. Swart, ...)
- p-adic and function field cases (J. Silverman)
- Continued fractions and elliptic curve group law (W. Adamas, A. van der Poorten, M. Razar)
- Sigma function perspective (A. Hone, ...)
- Hyper-elliptic curves (A. Hone, A. van der Poorten, ...)
- More...

Can we do more?

The elliptic divisibility sequence is associated to the sequence of points $[n]P$ on the curve.

$$\boxed{[n]P \leftrightarrow h_n}$$

The Mordell-Weil group of an elliptic curve may have rank > 1. We might dream of ...

$$\boxed{[n]P + [m]Q \leftrightarrow h_{n,m}}$$

Elliptic Nets

Definition (KS)

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

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

- The recurrence generates the full array from finitely many initial values.
- The recurrence implies the elliptic divisibility sequence recurrence for $A = \mathbb{Z}$.

Elliptic Nets of Rank 2

Note

We will specialise to

$$\boxed{rank(A) = 2}$$

for the remainder of this talk.

- All results hold for general rank.
- The rank 1 case is the theory of elliptic divisibility sequences.
- Results stated for $\mathbb{Q}$ and $\mathbb{Z}$ hold generally for number fields.
- In fact, with more work, many of the same results hold for any field.

Elliptic Functions $\Psi_{n,m}$

Definition (KS)

Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. For each pair $(n, m) \in \mathbb{Z} \times \mathbb{Z}$, define a function $\Psi_{n,m}$ on $\mathbb{C} \times \mathbb{C}$ in variables z and w:

$$\Psi_{n,m}(z, w) = \frac{\sigma(nz + mw)}{\sigma(z)^{n^2 - nm}\sigma(z + w)^{nm}\sigma(w)^{m^2 - nm}}$$

- These functions are elliptic in each variable.
- The function is zero if $nz + mw = 0$.

Elliptic Nets from Elliptic Curves

Theorem (KS)

Let E be an elliptic curve defined over $\mathbb{Q}$, $\sigma : \mathbb{C} \to \mathbb{C}$ its Weierstrass sigma function, and let $u, v \in \mathbb{C}$ correspond to rational points P, Q on E. Then

$$W(n, m) := \Psi_{n,m}(u, v)$$

forms an elliptic net.

- We call this the elliptic net associated to the curve E and points P, Q.
- We call P, Q the basis of the elliptic net.

Example

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

$\uparrow Q$

$P \rightarrow$

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

Primes in an Elliptic Net

	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
$\uparrow$	1	1	2	-5	7	89	-149
Q	0	1	1	-3	11	38	249
	$P \rightarrow$						

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

Reduction Modulo p

We wish to show that the elliptic net associated to E, P_1, P_2 reduced modulo a prime p will be the elliptic net associated to the mod-p-reduced curve and points $\widetilde{E}, \widetilde{P}_1, \widetilde{P}_2$.

This requires showing the the net functions $\Psi_{\mathbf{v}}$ can be reduced modulo p. We can obtain a nice polynomial form for them.

1-D Case: Division Polynomials

$E : y^2 = x^3 + Ax + B, P = (x, y)$

$$\Psi_1 = 1, \Psi_2 = 2y, \Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \ .$$

Net Functions

Theorem (KS)

The net functions $\Psi_{\mathbf{v}}$ can be expressed as polynomials in the ring

$$\mathbb{Z}[A,B]\left[x_1, y_1, x_2, y_2, \frac{1}{x_1 - x_2}\right] / \left\langle y_i^2 - x_i^3 - Ax_i - B\right\rangle_{i=1}^{2} \quad .$$

Example

$$\Psi_{2,1} = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \quad , \Psi_{-1,1} = x_1 - x_2 \quad ,$$

$$\Psi_{2,-1} = (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \quad .$$

Reduction Modulo p for Elliptic Nets

Theorem (KS)

Consider points $P_1, P_2 \in E(\mathbb{Q})$ such that the reductions modulo p of the $\pm P_i$ are all distinct and nonzero. Then for each $\mathbf{v} \in \mathbb{Z}^2$ there exists a function $\Omega_{\mathbf{v}}$ such that the following diagram commutes:

$$\begin{array}{ccc} E^2(\mathbb{Q}) & \xrightarrow{\Psi_{\mathbf{v}}} & \mathbb{P}^1(\mathbb{Q}) \\ \downarrow \delta & & \downarrow \delta \\ \widetilde{E}^2(\mathbb{F}_p) & \xrightarrow{\Omega_{\mathbf{v}}} & \mathbb{P}^1(\mathbb{F}_p) \end{array}$$

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

Prime Appearance in an Elliptic Net

- As in the motivational example,

$$p | W(m,n) \iff mP + nQ \equiv 0 \mod p$$

- The terms of a net divisible by a given prime p form a sublattice of A.

Lesson 2

Elliptic nets calculate the order of points modulo p.

Periodicity Properties

If P is an n-torsion point, W is the elliptic net associated to E, P, then

$$W(n+k) \text{ is not necessarily equal to } W(k)\ .$$

Example

$E : y^2 + y = x^3 + x^2 - 2x$ over $\mathbb{F}_5$.
$P = (0, 0)$ has order 9.
The associated sequence is
$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

Periodicity for Elliptic Divisibility Sequences

Theorem (M. Ward, 1948)

Let W be 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 $W(r) \equiv 0 \mod p$. Then there exist integers a, b such that for all n,

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

Example ($E : y^2 + y = x^3 + x^2 - 2x$, $P = (0,0)$ over $\mathbb{F}_5$)

$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

$W(9k+n) \equiv W(n)4^{nk}2^{k^2} \mod 5$

$W(10) \equiv 3W(1) \mod 5$

$k = 2 : W(18+n) \equiv W(n)4^{2n}2^4 \equiv W(n) \mod 5$

Example of Reduction Mod 5 of an Elliptic Net

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

$\uparrow Q$ $P \rightarrow$

The appropriate periodicity property should tell how to obtain the green values from the blue values.

Periodicity for Elliptic Nets

Theorem (KS)

Let W be an elliptic net such that $W(2,0)W(0,2) \neq 0$. Suppose $W(r_1, r_2)$ and $W(s_1, s_2)$ are trivial modulo p. Then there exist integers $a_s, b_s, c_s, a_r, b_r, c_r, d$ such that for all $m, n, k, l \in \mathbb{Z}$,

$$W(kr_1 + ls_1 + m, kr_2 + ls_2 + n) \equiv W(m,n) a_r^{km} b_r^{kn} c_r^{k^2} a_s^{lm} b_s^{ln} c_s^{l^2} d^{kl} \mod p$$

Example of Net Periodicity

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

$\uparrow Q$

$P \rightarrow$

$$a_r = 2, b_r = 2, c_r = 1$$

$$W(5,4) \equiv W(1,2)2^1 2^2 1^1$$
$$\equiv 3W(1,2) \mod 5$$

The Basis of an Elliptic Net

- If W_i is the elliptic net associated to E, P_i, Q_i for $i = 1, 2$, and
$$a_1 P_1 + b_1 Q_1 = a_2 P_2 + b_2 Q_2$$
then
$$W_1(a_1, b_1) \text{ is not necessarily equal to } W_2(a_2, b_2) \ .$$
- The net is not a function on points of $E(K)$.
- The net is associated to a *basis*, not a *subgroup*.
- There is a *basis change formula*.

Defining a Net on a Free Abelian Cover

- Let K be a finite or number field. Let $\hat{E}$ be any finite rank free abelian group surjecting onto $E(K)$.

$$\pi : \hat{E} \to E(K)$$

- For a basis P_1, P_2, choose $p_i \in \hat{E}$ such that $\pi(p_i) = P_i$.
- We specify an identification

$$\mathbb{Z}^2 \cong \langle p_1, p_2 \rangle$$

  via $\mathbf{e}_i \mapsto p_i$.
- The elliptic net W associated to E, P_1, P_2 and defined on $\mathbb{Z}^2$ is now identified with an elliptic net W' defined on $\hat{E}$.
- This allows us to compare elliptic nets associated to different bases.

Defining a Special Equivalence Class

Definition

Let W_1, W_2 be elliptic nets. Suppose $\alpha, \beta \in K^*$, and $f : A \to \mathbb{Z}$ is a quadratic form. If

$$W_1(\mathbf{v}) = \alpha\beta^{f(\mathbf{v})} W_2(\mathbf{v})$$

for all $\mathbf{v}$, then we say W_1 *is equivalent to* W_2.

- The basis change formula is an equivalence, when the elliptic nets are viewed as maps on $\hat{E}$ as explained in the previous slide.
- In this way, we can associate an equivalence class to a subgroup of $E(K)$.

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 $\mathrm{div}(f_P)$. Choose another divisor D_Q defined over K such that $D_Q \sim (Q) - (\mathcal{O})$ and with support disjoint from $\mathrm{div}(f_P)$. Then, we may define the Tate pairing

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

by

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

It is well-defined, bilinear and Galois invariant.

Weil Pairing

For $P, Q \in E(\mathbb{Q})[m]$, the more well-known Weil pairing can be computed via two Tate pairings:

$$e_m(P, Q) = \tau_m(P, Q)\tau_m(Q, P)^{-1} \quad .$$

It is bilinear, alternating, and non-degenerate.

Tate Pairing from Elliptic Nets

Theorem (KS - Lesson 3)

Fix a positive $m \in \mathbb{Z}$. Let E be an elliptic curve defined over a finite field K containing the m-th roots of unity. Let P, $Q \in E(K)$, with $[m]P = \mathcal{O}$. Choose $S \in E(K)$ such that $S \notin \{\mathcal{O}, -Q\}$. Choose $p, q, s \in \hat{E}$ such that $\pi(p) = P$, $\pi(q) = Q$ and $\pi(s) = S$. Let W be an elliptic net associated to a subgroup of $E(K)$ containing P, Q, and S. Then the quantity

$$T_m(P, Q) = \frac{W(s + mp + q)W(s)}{W(s + mp)W(s + q)}$$

is the Tate pairing.

Tate Pairing Governs Periodicity Relations

Choosing W to be the net associated to E, P and letting $p = q = s$, the periodicity relations give

$$\tau_m(P,P) = \frac{W(m+2)}{W(2)}\frac{W(1)}{W(m+1)} = (a^2b)(ab)^{-1} = a$$

So the values needed for the periodicity relations are

$$a = \tau_m(P,P), b^2 = a^m$$

A similar statement holds for elliptic nets in general.
The Tate pairing governs the periodicity relations!

Choosing an Elliptic Net

Corollary

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_P is the elliptic net associated to E, P, then

$$\tau_m(P,P) = \frac{W_P(m+2)W_P(1)}{W_P(m+1)W_P(2)} \quad .$$

Further, if $W_{P,Q}$ is the elliptic net associated to E, P, Q, then

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

Computing Terms of an Elliptic Net

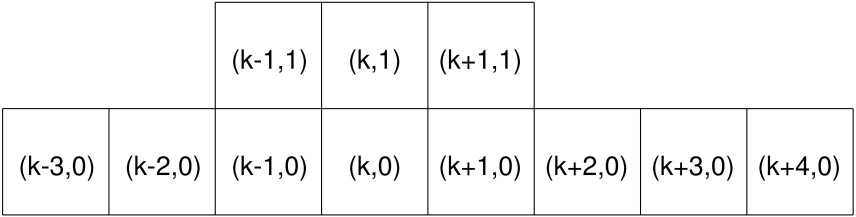

Figure: A block centred at k

Computing Terms of an Elliptic Net

Block centred at k

Block centred at $2k$

Block centred at $2k+1$

Summary

- The arithmetic of elliptic curves is reflected in elliptic divisibility sequences and more generally in elliptic nets.
- Elliptic nets contain information about group law, reduction modulo p and pairings on the curve.
- Group law, reduction and pairing computations can be done via the recurrence.

For Further Reading I

- G. Everest, A. van der Poorten, I. Shparlinsky, T. Ward.
  Recurrence Sequences.
  Mathematical Surveys and Monographs, vol 104.
  American Mathematical Society, 2003.

- M. Ward.
  Memoir on Elliptic Divisibility Sequences.
  American Journal of Mathematics, 70:13–74, 1948.

- K. Stange.
  The Tate Pairing via Elliptic Nets.
  To appear in PAIRING 2007, *Springer Lecture Notes in Computer Science*.

Slides and Preprint at http://www.math.brown.edu/~stange/