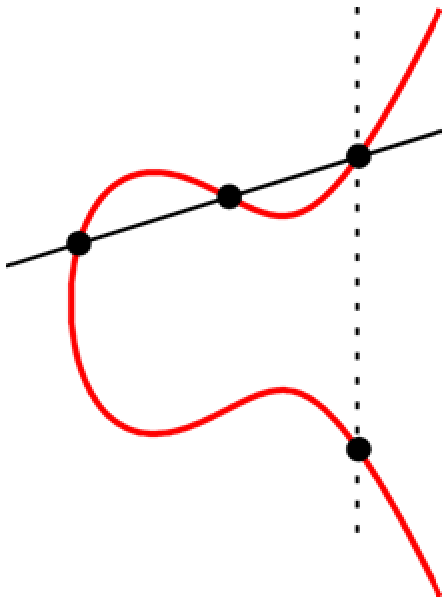
Elliptic Nets

With Applications to Cryptography

Katherine Stange
Brown University

http://www.math.brown.edu/~stange/

Elliptic Divisibility Sequences: Seen In Their Natural Habitat



$$P \in E(\mathbb{Q})$$

$$P = \left(\frac{a_P}{d_P^2}, \frac{b_P}{d_P^3} \right)$$

$$\begin{array}{ccccc} P, & 2P, & 3P, & 4P, & \ldots \quad \in E(\mathbb{Q}) \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ d_P, & d_{2P}, & d_{3P}, & d_{4P}, & \ldots \quad \in \mathbb{Z} \end{array}$$

Example $y^2 + y = x^3 + x^2 - 2x$

$$P = (0, 0)$$

$$P = \left(\frac{0}{1}, \frac{0}{1}\right) \qquad d_P = 1$$

$$2P = \left(\frac{3}{1}, \frac{5}{1}\right) \qquad d_{2P} = 1$$

$$3P = \left(-\frac{11}{9}, \frac{28}{27}\right) \qquad d_{3P} = -3$$

$$4P = \left(\frac{114}{121}, -\frac{267}{1331}\right) \qquad d_{4P} = 11$$

$$5P = \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right) \qquad d_{5P} = 38 = 2 \times 19$$

$$6P = \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right) \qquad d_{6P} = 249 = 3 \times 83$$

$$7P = \left(-\frac{2182983}{5555449}, -\frac{20464084173}{13094193293}\right) \qquad d_{7P} = -2357$$

$$8P = \left(\frac{1169154495}{76860289}, -\frac{41440508823358}{673834153663}\right) \qquad d_{8P} = 8767 = 11 \times 797$$

Elliptic Divisibility Sequences: Two Good Definitions

$$W_n \in \mathbb{Z}, \text{ for all } n \in \mathbb{Z}$$

Definition A

Define elliptic functions

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

Fix elliptic curve $\mathbb{C}/\Lambda$
and rational point $z \in \mathbb{C}/\Lambda$
(z not 2- or 3−torsion,
Λ appropriately normalised)

$$W_n = \Psi_n(z)$$

Elliptic Divisibility Sequences: Two Good Definitions

$$W_n \in \mathbb{Z}, \text{ for all } n \in \mathbb{Z}$$

Definition A

Define elliptic functions

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

Fix elliptic curve $\mathbb{C}/\Lambda$
and rational point $z \in \mathbb{C}/\Lambda$
(z not 2- or 3−torsion,
Λ appropriately normalised)

$$W_n = \Psi_n(z)$$

Definition B

Given initial conditions

$$W_0, W_1, W_2, W_3, W_4 \in \mathbb{Z}$$

$$W_0 = 0,\ W_1 = 1,\ W_2 | W_4,\ W_2 W_3 \neq 0$$

and recurrence for all $m, n \in \mathbb{Z}$

$$W_{m+n} W_{m-n} = W_{m+1} W_{m-1} W_n^2 - W_{n+1} W_{n-1} W_m^2$$

Theorem (M Ward, 1948): A and B are equivalent.

From the initial conditions in Definition B, one can explicitly calculate the curve and point needed for Definition A.

Definition A	Definition B
Define elliptic functions $$\Psi_n(z) = \frac{\sigma(nz)}{\sigma(z)^{n^2}}$$ Fix elliptic curve $\mathbb{C}/\Lambda$ and rational point $z \in \mathbb{C}/\Lambda$ (z not 2- or 3−torsion, Λ appropriately normalised) $$W_n = \Psi_n(z)$$	Given initial conditions $$W_0,\, W_1,\, W_2,\, W_3,\, W_4 \in \mathbb{Z}$$ $$W_0 = 0,\, W_1 = 1,\, W_2 \mid W_4,\, W_2 W_3 \neq 0$$ and recurrence for all $m, n \in \mathbb{Z}$ $$W_{m+n} W_{m-n} = W_{m+1} W_{m-1} W_n^2 - W_{n+1} W_{n-1} W_m^2$$

Reflects the structure of a cyclic subgroup of the Mordell-Weil group

- $P \in E(\mathbb{Q})$ is an n-torsion point iff $W_n = 0$
- $n\tilde{P} = \tilde{0}$ in $\tilde{E}(\mathbb{F}_p)$ iff $W_n \equiv 0 \mod p$

  (Divisibility: If $n|m$, then $W_n|W_m$.)
- Suppose $P \in E(\mathbb{Q})$ is an integral point, and $\gcd(W_2, W_3) = 1$. Then nP is an integral point iff $W_n = \pm 1$

Research (Partial List)

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

From Sequences to Nets

It is natural to look for a generalisation that reflects the structure of the entire Mordell-Weil group:

$$W_P \in \mathbb{Z} \text{ indexed by all } P \in E(\mathbb{Q})??$$

In this talk, we work with a rank 2 example

If P, $Q \in E(\mathbb{Q})$ are independent and non-torsion, then the subgroup of $E(\mathbb{Q})$ they generate can be indexed by $\mathbb{Z} \times \mathbb{Z}$:

$$mP + nQ \rightsquigarrow W_{m,n}$$

Nearly everything can be done for general rank

Elliptic Nets: Rank 2 Case

$$W_{m,n} \in \mathbb{Z}, \text{ for all } m,\ n \in \mathbb{Z}$$

Definition A

Define doubly elliptic functions on $E \times E$

$$\Psi_{m,n}(z,w) = \frac{\sigma(mz+nw)}{\sigma(z)^{m^2-mn}\sigma(z+w)^{mn}\sigma(w)^{n^2-mn}}, \quad m,n \in \mathbb{Z}$$

Fix elliptic curve $\mathbb{C}/\Lambda$ and rational points $z,w \in \mathbb{C}/\Lambda$

$$W_{m,n} = \Psi_{m,n}(z,w)$$

Elliptic Nets: Rank 2 Case

$$W_{m,n} \in \mathbb{Z}, \text{ for all } m,\, n \in \mathbb{Z}$$

Definition B

Give initial conditions

$$W_{0,0},\, W_{1,0},\, W_{0,1},\, W_{1,1},\, W_{1,2},\, W_{1,2},\, W_{0,2},\, W_{0,2}$$

$$W_{0,0} = 0,\, W_{1,0} = W_{0,1} = W_{1,1} = 1$$

and recurrence for all $\mathbf{p}$, $\mathbf{q}$, $\mathbf{r}$, $\mathbf{s} \in \mathbb{Z} \times \mathbb{Z}$

$$W_{\mathbf{p}+\mathbf{q}+\mathbf{s}} W_{\mathbf{p}-\mathbf{q}} W_{\mathbf{r}+\mathbf{s}} W_{\mathbf{r}} + W_{\mathbf{q}+\mathbf{r}+\mathbf{s}} W_{\mathbf{q}-\mathbf{r}} W_{\mathbf{p}+\mathbf{s}} W_{\mathbf{p}} + W_{\mathbf{r}+\mathbf{q}+\mathbf{s}} W_{\mathbf{r}-\mathbf{p}} W_{\mathbf{q}+\mathbf{s}} W_{\mathbf{q}} = 0$$

Example $y^2 + y = x^3 + x^2 - 2x$

$$P = (0,0),\ Q = (1,0)$$

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

↑ Q

P ⟶

Example $y^2 + y = x^3 + x^2 - 2x$

$$P = (0, 0),\ Q = (1, 0)$$

	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
Q	0	1	1	-3	11	38	249

P⟶

Example $y^2 + y = x^3 + x^2 - 2x$

$$P = (0,0),\ Q = (1,0)$$

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

↑ Q

P ⟶

Example $y^2 + y = x^3 + x^2 - 2x$

$$P = (0,0),\ Q = (1,0)$$

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

↑ Q

P ⟶

Example $y^2 + y = x^3 + x^2 - 2x$

$$P = (0,0),\ Q = (1,0)$$

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

↑ Q

P ⟶

Example $y^2 + y = x^3 + x^2 - 2x$

$$P = (0,0),\ Q = (1,0)$$

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

↑ Q

P ⟶

Equivalence of Definitions

The definitions A and B can be generalised to any rank n. Then we have

Theorem (S). *The definitions A and B are equivalent. Furthermore, there is a bijection*

$$(E, P_1, \ldots, P_n) \quad \longleftrightarrow \quad (a_1, \ldots, a_n)$$

curve $+\ n$ points $\qquad\qquad$ $n + 2$ initial values of net

For any given *n*, one can compute the explicit bijection.

Given initial values $W_{1,0} = W_{0,1} = W_{1,1} = 1, W_{1,-1} = a$, $W_{2,1} = b, W_{2,-1} = c$, and $W_{2,0} = d$ the associated curve is $y^2 = 4x^3 - g_2 x - g_3$ where

$$g_2 = \tfrac{1}{48d^4a^4}\big(a^8b^4 - 8a^7b^2d^2 + 4a^6b^3c + 4a^6b^3d^2 + 16a^6d^4 - 16a^5bcd^2 + 8a^5bd^4 + 6a^4b^2c^2 + 4a^4b^2cd^2 + 6a^4b^2d^4 - 8a^3c^2d^2 - 8a^3cd^4 + 16a^3d^6 + 4a^2bc^3 - 4a^2bc^2d^2 - 4a^2bcd^4 + 4a^2bd^6 + c^4 - 4c^3d^2 + 6c^2d^4 - 4cd^6 + d^8\big)$$

$$g_3 = \tfrac{1}{864d^6a^6}\big(-a^{12}b^6 + 12a^{11}b^4d^2 - 6a^{10}b^5c - 6a^{10}b^5d^2 - 48a^{10}b^2d^4 + 48a^9b^3cd^2 + 12a^9b^3d^4 + 64a^9d^6 - 15a^8b^4c^2 - 18a^8b^4cd^2 - 15a^8b^4d^4 - 96a^8bcd^4 + 48a^8bd^6 + 72a^7b^2c^2d^2 + 12a^7b^2cd^4 - 36a^7b^2d^6 - 20a^6b^3c^3 - 12a^6b^3c^2d^2 - 12a^6b^3cd^4 - 20a^6b^3d^6 - 48a^6c^2d^4 - 48a^6cd^6 - 120a^6d^8 + 48a^5bc^3d^2 - 12a^5bc^2d^4 + 24a^5bcd^6 - 60a^5bd^8 - 15a^4b^2c^4 + 12a^4b^2c^3d^2 + 6a^4b^2c^2d^4 + 12a^4b^2cd^6 - 15a^4b^2d^8 + 12a^3c^4d^2 - 12a^3c^3d^4 - 36a^3c^2d^6 + 60a^3cd^8 - 24a^3d^10 - 6a^2bc^5 + 18a^2bc^4d^2 - 12a^2bc^3d^4 - 12a^2bc^2d^6 + 18a^2bcd^8 - 6a^2bd^10 + -c^6 + 6c^5d^2 - 15c^4d^4 + 20c^3d^6 - 15c^2d^8 + 6cd^{10} - d^{12}\big)$$

Proof of Equivalence

- $\Psi_{\mathbf{v}}$ satisfy recurrence (check divisors & value)
- The axes of a net are elliptic divisibility sequences, from which we determine curve and points
- A proof using the recurrence relation shows that the axes determine a net

Nets are Integral

Theorem (S). *Suppose* $1 \leq n \leq 6$. *Given integral initial terms satisfying a certain finite set of divisibility conditions, the values of a net are all integers.*

(e.g. for $n = 1$, the conditions are $W_2 | W_4$.)

Proof of Integrality

- By clever choice of recurrence relations, you can control the divisions necessary to calculate each term
- Very messy & long multivariable induction!

Reduction Mod p

$$1 \le n \le 6$$

$\Psi_{\mathbf{v}}$	with $\mathbf{v} \in \mathbb{Z}^n$
E	an elliptic curve over $\mathbb{Q}$
p	prime of good reduction for E
δ	reduction modulo p

Theorem (S)**.** *There exists a unique* $f_{\mathbf{v}}$ *such that the following diagram commutes and* $div(f_{\mathbf{v}}) = \delta^*(div(\Psi_{\mathbf{v}}))$.

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

Example $y^2 + y = x^3 + x^2 - 2x$

$P = (0,0),\ Q = (1,0)$

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

↑ Q

P ⟶

Example $y^2 + y = x^3 + x^2 - 2x$

$P = (0,0),\ Q = (1,0)$ $\mod 5$

0	4	1	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

Q ↑

P ⟶

Proof of Reduction Theorem

- Relies on integrality
- Requires understanding how nets behave under endomorphisms of E^n, to reduce to the rank 1 case

Divisibility Property

Theorem (S). *Suppose p is a prime of good reduction for E. Then*

$$\{\mathbf{v} \in \mathbb{Z}^n : p \textit{ divides } W_{\mathbf{v}}\}$$

is a sub-lattice of $\mathbb{Z}^n$.

$$n \leq 6$$

Periodicity of Sequences

If $W_r \equiv 0 \mod p$, then there exist a and b such that for all n,

$$W_{n+kr} \equiv W_n a^{nk} b^{k^2} \mod p$$

Here we may take

$$a = \frac{W_{r+2}}{W_{r+1} W_2}, \qquad b = \frac{W_{r+1}^2 W_2}{W_{r+2}}$$

Periodicity of Sequences: Restatement

Let W be an elliptic divisibility sequence, and K a finite field.

If $W_r = 0$, there exists an $\alpha \in \bar{K}$ such that $\alpha^r \in K$ and $\alpha^{n^2} W_n$ has period r.

$(a = \alpha^{2r}$ and $b = \alpha^{r^2})$

Periodicity of Nets

Theorem (S). *Suppose*

$$W(\mathbf{r_1}) = W(\mathbf{r_2}) = 0.$$

Let d be the gcd *of the coordinates of the* $\mathbf{r_i}$. *Then there exists an $\alpha \in \bar{K}$ such that $\alpha^d \in K$ and*

$$\alpha^{m^2+n^2-mn} W(m,n)$$

is periodic with respect to the lattice generated by $\mathbf{r_1}, \mathbf{r_2}$.

$$n \leq 6$$

Proof of Periodicity

- The vanishing condition gives a relation on the points generating the net
- Prove identity on elliptic functions
- By reduction theorem, this applies mod p

There are a great many more periodicity results!

The Tate Pairing

m	$\in \mathbb{Z}^+$
E	an elliptic curve over field $K \supset \mu_m$
P	$\in E(K)[m]$
Q	$\in E(K)/mE(K)$
f_P	such that $\operatorname{div}(f_P) = m(P) - m(\mathcal{O})$
D_Q	$\sim (Q) - (\mathcal{O})$ with disjoint support from $\operatorname{div}(f_P)$

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

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

Tate Pairing from Elliptic Nets

m	$\in \mathbb{Z}^+$
E	elliptic curve $/K$
P	$\in E(K)[m]$
Q	$\in E(K)/mE(K)$
S	$\in E(K) \setminus \{\mathcal{O}, -Q\}$

W an elliptic net such that

$$W(\mathbf{s}) \longleftrightarrow S$$
$$W(\mathbf{p}) \longleftrightarrow P$$
$$W(\mathbf{q}) \longleftrightarrow Q$$

Theorem (S). *The Tate pairing may be calculated by*

$$\tau_m(P,Q) = \frac{W(\mathbf{s}+m\mathbf{p}+\mathbf{q})W(\mathbf{s})}{W(\mathbf{s}+m\mathbf{p})W(\mathbf{s}+\mathbf{q})}$$

Proof of Tate Pairing Relation

- Show that the formula is independent of "equivalence"
- Choose an appropriate equivalent net so that the quotient of functions is exactly $f_P(D_Q)$.

Choosing a Nice Net

If W is the elliptic net associated to E, P, then

$$\tau_m(P,P) = \frac{W(m+2)W(1)}{W(m+1)W(2)}$$

If W is the elliptic net associated to E, P, Q, then

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

Calculating the Net (Rank 2)

Based on an algorithm by Rachel Shipsey

A block centred on k:

		(k-1,1)	(k,1)	(k+1,1)			
(k-3,0)	(k-2,0)	(k-1,0)	(k,0)	(k+1,0)	(k+2,0)	(k+3,0)	(k+4,0)

block centred on k → **Double** → block centred on $2k$

block centred on k → **DoubleAdd** → block centred on $2k+1$

Calculating the Tate Pairing

- Find the initial values of the net associated to *E*, *P*, *Q* (there are simple formulae)
- Use a Double & Add algorithm to calculate the block centred on *m*
- Use the terms in this block to calculate

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

Embedding Degree *k*

$$m|(q^k - 1)$$

$$\mathbb{F}_{q^k}$$

$$\Big|$$

$$\mathbb{F}_q$$

$$\begin{aligned} P &\in E(\mathbb{F}_q)[m] \\ Q &\in E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k}) \end{aligned}$$

Efficiency

S	squaring in $\mathbb{F}_q$
M	multiplication in $\mathbb{F}_q$
S_k	squaring in $\mathbb{F}_{q^k}$
M_k	multiplication in $\mathbb{F}_{q^k}$

Algorithm	Double	DoubleAdd
Miller's	$4S + (k+7)M + S_k + M_k$	$7S + (2k+19)M + S_k + 2M_k$
Net	$6S + (6k+26)M + S_k + \frac{3}{2}M_k$	$6S + (6k+26)M + S_k + 2M_k$

Comparison of Operations for Double and DoubleAdd steps

Embedding degree	2	4	6	8	10	12
Optimised Miller's	18-38	31-58	46-82	64-109	84-140	106-174
Elliptic Net	51-52	76-80	104-112	136-147	171-186	207-228

Approximate $\mathbb{F}_q$ Multiplications per Step

Possible Research Directions

- Extend this to Jacobians of higher genus curves?
- Use periodicity relations to find integer points? (M. Ayad does this for sequences)
- Other computational applications: counting points on elliptic curves over finite fields?
- Other cryptographic applications of Tate pairing relationship?

References

- Morgan Ward. "Memoir on Elliptic Divisibility Sequences". American Journal of Mathematics, 70:13-74, 1948.
- Christine S. Swart. *Elliptic Curves and Related Sequences.* PhD thesis, Royal Holloway and Bedford New College, University of London, 2003.
- Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence Sequences.* Mathematical Surveys and Monographs, vol 104. American Mathematical Society, 2003.
- Elliptic net algorithm for Tate pairing implemented in the PBC Library, http://crypto.stanford.edu/pbc/

Slides, preprint, scripts at

http://www.math.brown.edu/~stange/