Elliptic nets

Katherine Stange, Harvard University

MIT Combinatorics Seminar, Sept 26, 2008

Elliptic divisibility sequences

Definition

An integer sequence W is an *elliptic divisibility sequence* if for all positive integers $m > n$,

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 .$$

Elliptic divisibility sequences

Definition

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

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 .$$

Elliptic divisibility sequences

Definition

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

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 .$$

- Generated by $W_1, \ldots, W_4$ via the recurrence.

Elliptic divisibility sequences

Definition

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

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 .$$

- Generated by $W_1, \ldots, W_4$ via the recurrence.
- Example: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$

Elliptic divisibility sequences

Definition

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

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 .$$

- Generated by $W_1, \ldots, W_4$ via the recurrence.
- Example: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$
- Example: $1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, \ldots$

Elliptic divisibility sequences

Definition

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

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 .$$

- Generated by $W_1, \ldots, W_4$ via the recurrence.
- Example: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$
- Example: $1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, \ldots$
- Example: $1, 1, -3, 11, 38, 249, -2357, 8767, 496036, -3769372, -299154043, -12064147359, \ldots$

Divisibility and Integrality

If $W_1, \ldots, W_4$ are integer with $W_1 = 1$, $W_2 W_3 \neq 0$, and $W_2 | W_4$, then the sequence ...

Divisibility and Integrality

If $W_1, \ldots, W_4$ are integer with $W_1 = 1$, $W_2 W_3 \neq 0$, and $W_2 | W_4$, then the sequence ...

1. is entirely integer;

Divisibility and Integrality

If $W_1, \ldots, W_4$ are integer with $W_1 = 1$, $W_2 W_3 \neq 0$, and $W_2 | W_4$, then the sequence ...

1. is entirely integer;
2. satisfies the **Divisibility Property**

$$m|n \implies W_m | W_n \ ; \text{ and}$$

Divisibility and Integrality

If $W_1, \ldots, W_4$ are integer with $W_1 = 1$, $W_2 W_3 \neq 0$, and $W_2 | W_4$, then the sequence ...

1. is entirely integer;
2. satisfies the **Divisibility Property**

$$m|n \implies W_m|W_n \ ; \text{ and}$$

3. if $gcd(W_3, W_4) = 1$, it satisfies the **Strong Divisibility Property**

$$W_{gcd(m,n)} = gcd(W_m, W_n) \ .$$

Somos sequences

A Somos-k sequence is a sequence satisfying the recurrence

$$C_n C_{n+k} = \sum_{j=1}^{[k/2]} C_{n-j} C_{n-(k-j)}.$$

But in this talk, we will mean more generally with coefficients allowed, so

$$C_n C_{n+k} = \sum_{j=1}^{[k/2]} a_j C_{n-j} C_{n-(k-j)}.$$

- EDS are Somos-4, Somos-5, Somos-6, etc. (van der Poorten, Swart, 2004)

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

$P = (0, 0)$

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

$$\begin{aligned} P &= (0,0) \\ [2]P &= (3,5) \end{aligned}$$

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

$$\begin{aligned} P &= (0,0) \\ [2]P &= (3,5) \\ [3]P &= \left(-\frac{11}{9}, \frac{28}{27}\right) \end{aligned}$$

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

$$\begin{aligned} P &= (0,0) \\ [2]P &= (3,5) \\ [3]P &= \left(-\frac{11}{9}, \frac{28}{27}\right) \\ [4]P &= \left(\frac{114}{121}, -\frac{267}{1331}\right) \end{aligned}$$

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

$$\begin{aligned}
P &= (0,0) \\
[2]P &= (3,5) \\
[3]P &= \left(-\frac{11}{9}, \frac{28}{27}\right) \\
[4]P &= \left(\frac{114}{121}, -\frac{267}{1331}\right) \\
[5]P &= \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right)
\end{aligned}$$

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

$$
\begin{aligned}
P &= (0,0) \\
[2]P &= (3,5) \\
[3]P &= \left(-\frac{11}{9}, \frac{28}{27}\right) \\
[4]P &= \left(\frac{114}{121}, -\frac{267}{1331}\right) \\
[5]P &= \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right) \\
[6]P &= \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right)
\end{aligned}
$$

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

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

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

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

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

$$\begin{aligned}
P &= (0,0)\\
[2]P &= (3,5)\\
[3]P &= \left(-\frac{11}{3^2}, \frac{28}{3^3}\right)\\
[4]P &= \left(\frac{114}{11^2}, -\frac{267}{11^3}\right)\\
[5]P &= \left(-\frac{2739}{38^2}, -\frac{77033}{38^3}\right)\\
[6]P &= \left(\frac{89566}{249^2}, -\frac{31944320}{249^3}\right)\\
[7]P &= \left(-\frac{2182983}{2357^2}, -\frac{20464084173}{2357^3}\right)
\end{aligned}$$

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

$$
\begin{array}{rll}
P = & (0,0) & 1 \\
[2]P = & (3,5) & 1 \\
[3]P = & \left(-\frac{11}{3^2}, \frac{28}{3^3}\right) & 3 \\
[4]P = & \left(\frac{114}{11^2}, -\frac{267}{11^3}\right) & 11 \\
[5]P = & \left(-\frac{2739}{38^2}, -\frac{77033}{38^3}\right) & 38 \\
[6]P = & \left(\frac{89566}{249^2}, -\frac{31944320}{249^3}\right) & 249 \\
[7]P = & \left(-\frac{2182983}{2357^2}, -\frac{20464084173}{2357^3}\right) & 2357
\end{array}
$$

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

$$
\begin{aligned}
P &= (0,0) & +1 \\
[2]P &= (3,5) & +1 \\
[3]P &= \left(-\frac{11}{3^2}, \frac{28}{3^3}\right) & -3 \\
[4]P &= \left(\frac{114}{11^2}, -\frac{267}{11^3}\right) & +11 \\
[5]P &= \left(-\frac{2739}{38^2}, -\frac{77033}{38^3}\right) & +38 \\
[6]P &= \left(\frac{89566}{249^2}, -\frac{31944320}{249^3}\right) & +249 \\
[7]P &= \left(-\frac{2182983}{2357^2}, -\frac{20464084173}{2357^3}\right) & -2357
\end{aligned}
$$

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

$$
\begin{aligned}
P &= (0,0) & W_1 &= +1\\
[2]P &= (3,5) & W_2 &= +1\\
[3]P &= \left(-\frac{11}{3^2}, \frac{28}{3^3}\right) & W_3 &= -3\\
[4]P &= \left(\frac{114}{11^2}, -\frac{267}{11^3}\right) & W_4 &= +11\\
[5]P &= \left(-\frac{2739}{38^2}, -\frac{77033}{38^3}\right) & W_5 &= +38\\
[6]P &= \left(\frac{89566}{249^2}, -\frac{31944320}{249^3}\right) & W_6 &= +249\\
[7]P &= \left(-\frac{2182983}{2357^2}, -\frac{20464084173}{2357^3}\right) & W_7 &= -2357
\end{aligned}
$$

Sequences from division polynomials

Consider a point $P = (x, y)$ and its multiples on an elliptic curve $E : y^2 = x^3 + Ax + B$:

$$P, [2]P, [3]P, [4]P, \ldots$$

Sequences from division polynomials

Consider a point $P = (x, y)$ and its multiples on an elliptic curve $E : y^2 = x^3 + Ax + B$. Then

$$[n]P = \left(\frac{\phi_n(P)}{\Psi_n(P)^2}, \frac{\omega_n(P)}{\Psi_n(P)^3} \right)$$

Sequences from division polynomials

Consider a point $P = (x, y)$ and its multiples on an elliptic curve $E : y^2 = x^3 + Ax + B$. Then

$$[n]P = \left(\frac{\phi_n(P)}{\Psi_n(P)^2}, \frac{\omega_n(P)}{\Psi_n(P)^3} \right)$$

where

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

Sequences from division polynomials

Consider a point $P = (x, y)$ and its multiples on an elliptic curve $E : y^2 = x^3 + Ax + B$. Then

$$[n]P = \left(\frac{\phi_n(P)}{\Psi_n(P)^2}, \frac{\omega_n(P)}{\Psi_n(P)^3} \right)$$

where

$$\Psi_1 = 1, \qquad \Psi_2 = 2y,$$
$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$
$$\Psi_{m+n}\Psi_{m-n}\Psi_1^2 = \Psi_{m+1}\Psi_{m-1}\Psi_n^2 - \Psi_{n+1}\Psi_{n-1}\Psi_m^2 .$$

Sequences from division polynomials

Consider a point $P = (x, y)$ and its multiples on an elliptic curve $E : y^2 = x^3 + Ax + B$. Then

$$[n]P = \left(\frac{\phi_n(P)}{\Psi_n(P)^2}, \frac{\omega_n(P)}{\Psi_n(P)^3} \right)$$

where

$$\Psi_1 = 1, \qquad \Psi_2 = 2y,$$
$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$
$$\Psi_{m+n}\Psi_{m-n}\Psi_1^2 = \Psi_{m+1}\Psi_{m-1}\Psi_n^2 - \Psi_{n+1}\Psi_{n-1}\Psi_m^2 .$$

It gives an elliptic divisibility sequence of *division polynomials*.

Sequences from division polynomials

Consider a point $P = (x, y)$ and its multiples on an elliptic curve $E : y^2 = x^3 + Ax + B$. Then

$$[n]P = \left(\frac{\phi_n(P)}{\Psi_n(P)^2}, \frac{\omega_n(P)}{\Psi_n(P)^3} \right)$$

where

$$\Psi_1 = 1, \qquad \Psi_2 = 2y,$$
$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$
$$\Psi_{m+n}\Psi_{m-n}\Psi_1^2 = \Psi_{m+1}\Psi_{m-1}\Psi_n^2 - \Psi_{n+1}\Psi_{n-1}\Psi_m^2 .$$

It gives an elliptic divisibility sequence of *division polynomials*.
If we evaluate at P, we get the *elliptic divisibility sequence* associated to E and P.

Division polynomials as complex elliptic functions

The n-th division polynomial has divisor

$$\sum_{P \in E[n]} (P) - n^2(\mathcal{O}).$$

Division polynomials as complex elliptic functions

The n-th division polynomial has divisor

$$\sum_{P \in E[n]} (P) - n^2(\mathcal{O}).$$

In complex case, fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. For each $n \in \mathbb{Z}$, define a function Ω_n on $\mathbb{C}$ in the variable z:

$$\Omega_n(z;\Lambda) = \frac{\sigma(nz;\Lambda)}{\sigma(z;\Lambda)^{n^2}}$$

Division polynomials and sequences over finite fields

Division polynomials and sequences over finite fields

- Using the formulae, we can consider divison polynomials over any field.

Division polynomials and sequences over finite fields

- Using the formulae, we can consider divison polynomials over any field.
- Over a finite field, the point P will always have finite order, say n. The associated sequence will have $W_n = 0$.

Division polynomials and sequences over finite fields

- Using the formulae, we can consider divison polynomials over any field.
- Over a finite field, the point P will always have finite order, say n. The associated sequence will have $W_n = 0$.

Example

$E : y^2 + y = x^3 + x^2 - 2x$ over $\mathbb{F}_5$.
$P = (0, 0)$ has order 9.

Division polynomials and sequences over finite fields

- Using the formulae, we can consider divison polynomials over any field.
- Over a finite field, the point P will always have finite order, say n. The associated sequence will have $W_n = 0$.

Example

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

Division polynomials and sequences over finite fields

- Using the formulae, we can consider divison polynomials over any field.
- Over a finite field, the point P will always have finite order, say n. The associated sequence will have $W_n = 0$.

Example

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

Division polynomials and sequences over finite fields

- Using the formulae, we can consider divison polynomials over any field.
- Over a finite field, the point P will always have finite order, say n. The associated sequence will have $W_n = 0$.

Example

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

Division polynomials and sequences over finite fields

- Using the formulae, we can consider divison polynomials over any field.
- Over a finite field, the point P will always have finite order, say n. The associated sequence will have $W_n = 0$.

Example

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

The question - upping the dimension

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

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

The question - upping the dimension

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

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

We might dream of . . .

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

The question - upping the dimension

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

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

We might dream of ...

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

Or even ...

$$\boxed{[n]P + [m]Q + [t]R \leftrightarrow W_{n,m,t}}$$

etc.

History of this question

- Robbins forum discussions of ’denominators’ (c. 2001): Noam Elkies, Michael Somos, James Propp.
- Graham Everest, Peter Rogers, Thomas Ward, Nelson Stephens considered when these denominators may be prime (2002).

Definition of an elliptic net

Definition (S)

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 $p, q, r, s \in A$.

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

Definition of an elliptic net

Definition (S)

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 $p, q, r, s \in A$.

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

- Elliptic divisibility sequences are a special case ($A = \mathbb{Z}$)

Definition of an elliptic net

Definition (S)

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 $p, q, r, s \in A$.

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

- Elliptic divisibility sequences are a special case ($A = \mathbb{Z}$)
- In this talk, we will mostly discuss rank 2: $A = \mathbb{Z}^2$.

The octahedron recurrence

In the case of $p = (l, m-1, n)$, $q = (1, 1, 0)$, $r = (0, 1, 1)$, $s = (0, -2, 0)$ for example, we obtain a recurrence of the form

$$\begin{aligned} aW(l+1, m, n)W(l-1, m, n) \\ + bW(l, m+1, n)W(l, m-1, n) \\ + cW(l, m, n+1)W(l, m, n-1) = 0 \end{aligned}$$

called the Octahedron Recurrence or Hirota Bilinear Equation. (Hirota (1981), subsequently many people, including David Speyer.)

Laurentness

Theorem (S)

The terms of an elliptic net are generated by the recurrence relation from a finite set of initial terms. Furthermore, the terms are Laurent polynomials in a set of initial terms of size 4 *for rank one, and size no larger than* $3^n - 1$ *for rank* $n > 1$.

Laurentness

Theorem (S)

The terms of an elliptic net are generated by the recurrence relation from a finite set of initial terms. Furthermore, the terms are Laurent polynomials in a set of initial terms of size 4 for rank one, and size no larger than $3^n - 1$ for rank $n > 1$.

Proof.

A lot of induction. $\square$

Laurentness in rank one

In rank one, the terms are polynomials in initial conditions, with $W(2)$ and $W(1)$ possibly appearing to negative powers:
If $a = W_1, b = W_2, c = W_3, d = W_4$, then

$$W_5 = \frac{db^3 - ac^3}{a^3}, \qquad W_6 = \frac{-a^4cd^2 - c^4b^2a + dcb^5}{ba^5}, etc.$$

Laurentness in rank two

Theorem (S.)

Let $W : \mathbb{Z}^2 \to R$ be an elliptic net. All terms are polys with $\mathbb{Z}$-coeffs in variables
$W(1,1), W(1,0), W(0,1)$, $W(1,1)^{-1}, W(1,0)^{-1}, W(0,1)^{-1}$,
$W(2,1)$, $W(1,2)$, $W(2,0)$, $W(0,2)$,

$$\frac{W(0,2)W(2,1)W(1,0) - W(0,1)W(2,0)W(1,2)}{W(0,1)^3 W(2,1) - W(1,0)^3 W(1,2)}.$$

Integer terms

In particular, if

- $W(1,0) = W(0,1) = W(1,1) = 1$,
- the terms $W(2,0)$, $W(0,2)$, $W(1,2)$, $W(2,1)$ are integers and
- $W(2,1) - W(1,2)$ divides $W(0,2)W(2,1) - W(2,0)W(1,2)$,

then all terms of the elliptic net are integers.
e.g.

$$W(2,3) = W(0,2)\left(\frac{W(0,2)W(2,1) - W(2,0)W(1,2)}{W(2,1) - W(1,2)}\right) - W(1,2)^2 W(2,1).$$

Laurentness in higher rank

Theorem

$$S_n = \{\mathbf{v} \in \mathbb{Z}^n : \max_{i=1,\ldots,n} |v_i| = 1\},$$

$$S_n' = S_n \cap \{\mathbf{v} \in \mathbb{Z}^n : v_i = 0 \textit{ for at least one } i\}.$$

The terms of an elliptic net of rank n are Laurent polynomials in the following variables and coefficients:

1. *For $n = 3$:*

$$\textit{Variables: } \{W(\mathbf{v}) : \mathbf{v} \in S_3\}; \quad \textit{Coefficients: } \mathbb{Z}$$

2. *For $n \geq 4$:*

$$\textit{Variables: } \{W(\mathbf{v}) : \mathbf{v} \in S_n'\}; \quad \textit{Coefficients: } \mathbb{Z}[W(\mathbf{v}) : \mathbf{v} \in S_n \backslash S_n']$$

Elliptic nets in their natural habitat

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

∘ $[3]Q$	∘ $[1]P + [3]Q$	∘ $[2]P + [3]Q$
∘ $[2]Q$	∘ $[1]P + [2]Q$	∘ $[2]P + [2]Q$
∘ $[1]Q$	∘ $[1]P + [1]Q$	∘ $[2]P + [1]Q$
∘ ∞	∘ $[1]P$	∘ $[2]P$

Elliptic nets in their natural habitat

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

$\circ\ \left(\frac{56}{25}, \frac{371}{125}\right)$	$\circ\ \left(-\frac{95}{64}, \frac{495}{512}\right)$	$\circ\ \left(\frac{328}{361}, -\frac{2800}{6859}\right)$
$\circ\ \left(\frac{6}{1}, -\frac{16}{1}\right)$	$\circ\ \left(\frac{1}{9}, -\frac{19}{27}\right)$	$\circ\ \left(\frac{39}{1}, \frac{246}{1}\right)$
$\circ\ \left(\frac{1}{1}, \frac{0}{1}\right)$	$\circ\ \left(-\frac{2}{1}, -\frac{1}{1}\right)$	$\circ\ \left(\frac{5}{4}, -\frac{13}{8}\right)$
$\circ\ \infty$	$\circ\ \left(\frac{0}{1}, \frac{0}{1}\right)$	$\circ\ \left(\frac{3}{1}, \frac{5}{1}\right)$

Elliptic nets in their natural habitat

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

$\left(\frac{56}{5^2}, \frac{371}{5^3}\right)$	$\left(-\frac{95}{8^2}, \frac{495}{8^3}\right)$	$\left(\frac{328}{19^2}, -\frac{2800}{19^3}\right)$
$\left(\frac{6}{1^2}, -\frac{16}{1^3}\right)$	$\left(\frac{1}{3^2}, -\frac{19}{3^3}\right)$	$\left(\frac{39}{1^2}, \frac{246}{1^3}\right)$
$\left(\frac{1}{1^2}, \frac{0}{1^3}\right)$	$\left(-\frac{2}{1^2}, -\frac{1}{1^3}\right)$	$\left(\frac{5}{2^2}, -\frac{13}{2^3}\right)$
∞	$\left(\frac{0}{1^2}, \frac{0}{1^3}\right)$	$\left(\frac{3}{1^2}, \frac{5}{1^3}\right)$

Elliptic nets in their natural habitat

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

5	8	19
1	3	1
1	1	2
0	1	1

Elliptic nets in their natural habitat

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

-5	$+8$	-19
$+1$	$+3$	-1
$+1$	$+1$	$+2$
$+0$	$+1$	$+1$

Elliptic nets in their natural habitat

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

-5	$+8$	-19
$+1$	$+3$	-1
$+1$	$+1$	$+2$
$+0$	$+1$	$+1$

An elliptic net!

Curve + points give net

Let E be an elliptic curve defined over a field K. For all $\mathbf{v} \in \mathbb{Z}^n$, we define rational functions $\Psi_{\mathbf{v}}$ on E^n which:

Curve + points give net

Let E be an elliptic curve defined over a field K. For all $\mathbf{v} \in \mathbb{Z}^n$, we define rational functions $\Psi_{\mathbf{v}}$ on E^n which:

- form an elliptic net (in $\mathbf{v}$)

Curve + points give net

Let E be an elliptic curve defined over a field K. For all $\mathbf{v} \in \mathbb{Z}^n$, we define rational functions $\Psi_{\mathbf{v}}$ on E^n which:

- form an elliptic net (in $\mathbf{v}$)
- generalise division polynomials

Curve + points give net

Let E be an elliptic curve defined over a field K. For all $\mathbf{v} \in \mathbb{Z}^n$, we define rational functions $\Psi_{\mathbf{v}}$ on E^n which:

- form an elliptic net (in $\mathbf{v}$)
- generalise division polynomials
- vanish at $\mathbf{P}$ such that $\mathbf{v} \cdot \mathbf{P} = 0$

Curve + points give net

Let E be an elliptic curve defined over a field K. For all $\mathbf{v} \in \mathbb{Z}^n$, we define rational functions $\Psi_{\mathbf{v}}$ on E^n which:

- form an elliptic net (in $\mathbf{v}$)
- generalise division polynomials
- vanish at $\mathbf{P}$ such that $\mathbf{v} \cdot \mathbf{P} = 0$
- have poles only on $P_i + P_j = 0$ and $P_i = 0$

Curve + points give net

Let E be an elliptic curve defined over a field K. For all $\mathbf{v} \in \mathbb{Z}^n$, we define rational functions $\Psi_{\mathbf{v}}$ on E^n which:

- form an elliptic net (in $\mathbf{v}$)
- generalise division polynomials
- vanish at $\mathbf{P}$ such that $\mathbf{v} \cdot \mathbf{P} = 0$
- have poles only on $P_i + P_j = 0$ and $P_i = 0$
- $\Psi_{\mathbf{v}} = 1$ whenever $\mathbf{v}$ is $\mathbf{e}_i$ or $\mathbf{e}_i + \mathbf{e}_j$ for some standard basis vectors $\mathbf{e}_i \neq \mathbf{e}_j$.

Curve + points give net

Let E be an elliptic curve defined over a field K. For all $\mathbf{v} \in \mathbb{Z}^n$, we define rational functions $\Psi_{\mathbf{v}}$ on E^n which:

- form an elliptic net (in $\mathbf{v}$)
- generalise division polynomials
- vanish at $\mathbf{P}$ such that $\mathbf{v} \cdot \mathbf{P} = 0$
- have poles only on $P_i + P_j = 0$ and $P_i = 0$
- $\Psi_{\mathbf{v}} = 1$ whenever $\mathbf{v}$ is $\mathbf{e}_i$ or $\mathbf{e}_i + \mathbf{e}_j$ for some standard basis vectors $\mathbf{e}_i \neq \mathbf{e}_j$.

Then for any fixed $\mathbf{P} \in E(K)^n$, the function $W : \mathbb{Z}^n \to K$ defined by

$$W(\mathbf{v}) = \Psi_{\mathbf{v}}(\mathbf{P})$$

is an elliptic net.

Make functions

We know the divisor we want:

$$\begin{aligned}([v_1]P_1 + [v_2]P_2 = \mathcal{O}) &- (v_1 v_2)(P_1 + P_2 = \mathcal{O}) \\ &- (v_1^2 - v_1 v_2)(P_1 = \mathcal{O}) - (v_2^2 - v_1 v_2)(P_2 = \mathcal{O})\end{aligned}$$

Make functions

We know the divisor we want:

$$([v_1]P_1 + [v_2]P_2 = \mathcal{O}) - (v_1 v_2)(P_1 + P_2 = \mathcal{O})$$
$$- (v_1^2 - v_1 v_2)(P_1 = \mathcal{O}) - (v_2^2 - v_1 v_2)(P_2 = \mathcal{O})$$

As before, over complexes this allows us to define polynomials:

$$\Omega_{u,v}(z, w; \Lambda) = \frac{\sigma(uz + vw; \Lambda)}{\sigma(z; \Lambda)^{u^2-uv}\sigma(z + w; \Lambda)^{uv}\sigma(w; \Lambda)^{v^2-uv}}.$$

Net polynomial examples

$$\Psi_{-1,1} = x_1 - x_2 \quad ,$$

Net polynomial examples

$$\Psi_{-1,1} = x_1 - x_2 \ ,$$

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

Net polynomial examples

$$\Psi_{-1,1} = x_1 - x_2 \ ,$$

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

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

Net polynomial examples

$$\Psi_{-1,1} = x_1 - x_2 \ ,$$

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

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

$$\Psi_{1,1,1} = \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \ ,$$

Net polynomial examples

$$\Psi_{-1,1} = x_1 - x_2 \quad ,$$

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

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

$$\Psi_{1,1,1} = \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \quad ,$$

Can calculate more via the recurrence...

Net polynomial examples

$$\Psi_{-1,1} = x_1 - x_2 \ ,$$

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

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

$$\Psi_{1,1,1} = \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \ ,$$

Can calculate more via the recurrence...

$$\begin{aligned}\Psi_{3,1} = {} & (x_2 - x_1)^{-3}(4x_1^6 - 12x_2x_1^5 + 9x_2^2x_1^4 + 4x_2^3x_1^3 \\ & - 4y_2^2x_1^3 + 8y_1^2x_1^3 - 6x_2^4x_1^2 + 6y_2^2x_2x_1^2 - 18y_1^2x_2x_1^2 \\ & + 12y_1^2x_2^2x_1 + x_2^6 - 2y_2^2x_2^3 - 2y_1^2x_2^3 + y_2^4 - 6y_1^2y_2^2 \\ & + 8y_1^3y_2 - 3y_1^4) \ .\end{aligned}$$

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{ \begin{array}{c} \textit{elliptic net} \\ W : \mathbb{Z}^n \to K \\ \textit{modulo scale} \\ \textit{equivalence} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{cubic Weierstrass curve } C \textit{ over } K \\ \textit{together with } m \textit{ points in } C(K) \\ \textit{modulo change of variables} \\ x' = x + r, y' = y + sx + t \end{array} \right\}$$

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{ \begin{array}{c} \textit{elliptic net} \\ W : \mathbb{Z}^n \to K \\ \textit{modulo scale} \\ \textit{equivalence} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{cubic Weierstrass curve } C \textit{ over } K \\ \textit{together with } m \textit{ points in } C(K) \\ \textit{modulo change of variables} \\ x' = x + r, y' = y + sx + t \end{array} \right\}$$

- $n = m$ and $W(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \ldots, P_m, C)$

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{ \begin{array}{c} \textit{elliptic net} \\ W : \mathbb{Z}^n \to K \\ \textit{modulo scale} \\ \textit{equivalence} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{cubic Weierstrass curve } C \textit{ over } K \\ \textit{together with } m \textit{ points in } C(K) \\ \textit{modulo change of variables} \\ x' = x + r, y' = y + sx + t \end{array} \right\}$$

- $n = m$ and $W(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \ldots, P_m, C)$
- explicit equations to go back and forth!

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{ \begin{array}{c} \textit{elliptic net} \\ W : \mathbb{Z}^n \to K \\ \textit{modulo scale} \\ \textit{equivalence} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{cubic Weierstrass curve } C \textit{ over } K \\ \textit{together with } m \textit{ points in } C(K) \\ \textit{modulo change of variables} \\ x' = x + r, y' = y + sx + t \end{array} \right\}$$

- $n = m$ and $W(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \ldots, P_m, C)$
- explicit equations to go back and forth!
- singular cubics correspond to Lucas sequences or integers

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{ \begin{array}{c} \textit{elliptic net} \\ W : \mathbb{Z}^n \to K \\ \textit{modulo scale} \\ \textit{equivalence} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{cubic Weierstrass curve } C \textit{ over } K \\ \textit{together with } m \textit{ points in } C(K) \\ \textit{modulo change of variables} \\ x' = x + r, y' = y + sx + t \end{array} \right\}$$

- $n = m$ and $W(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \ldots, P_m, C)$
- explicit equations to go back and forth!
- singular cubics correspond to Lucas sequences or integers
- scale equivalence: $W \sim W' \iff W(\mathbf{v}) = f(\mathbf{v})W'(\mathbf{v})$ for $f : \mathbb{Z}^n \to K^*$ quadratic
- on left, remove nets with zeroes too close to the origin
- on right, remove cases with small torsion points or pairs which are equal or inverses

Example over $\mathbb{Q}$

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

-5	8	-19			
1	3	-1			
1	1	2			
0	1	1			

$\uparrow Q$

$P \rightarrow$

Example over $\mathbb{Q}$

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

	4335	5959	12016	−55287	23921	1587077
	94	479	919	−2591	13751	68428
	−31	53	−33	−350	493	6627
	−5	8	−19	−41	−151	989
	1	3	−1	−13	−36	181
$\uparrow$	1	1	2	−5	7	89
Q	0	1	1	−3	11	38
	$P \rightarrow$					

Example over $\mathbb{Q}$

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

	4335	5959	12016	−55287	23921	1587077
	94	479	919	− 2591	13751	68428
	− 31	53	−33	−350	493	6627
	−5	8	−19	− 41	− 151	989
	1	3	−1	− 13	−36	181
$\uparrow$	1	1	2	−5	7	89
Q	0	1	1	−3	11	38
	$P \rightarrow$					

Example over $\mathbb{Q}$

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

	4335	5959	12016	−55287	23921	1587077
	94	479	919	− 2591	13751	68428
	− 31	53	−33	−350	493	6627
	−5	8	−19	− 41	− 151	989
	1	3	−1	− 13	−36	181
$\uparrow$	1	1	2	−5	7	89
Q	0	1	1	−3	11	38
	$P \rightarrow$					

Example over $\mathbb{Q}$

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

	4335	5959	12016	-55287	23921	1587077
	94	479	919	-2591	13751	68428
	-31	53	-33	-350	493	6627
	-5	8	-19	-41	-151	989
	1	3	-1	-13	-36	181
$\uparrow$	1	1	2	-5	7	89
Q	0	1	1	-3	11	38
	$P \rightarrow$					

Example over $\mathbb{Q}$

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

	4335	5959	12016	−55287	23921	1587077
	94	479	919	−2591	13751	68428
	−31	53	−33	−350	493	6627
	−5	8	−19	−41	−151	989
	1	3	−1	−13	−36	181
$\uparrow$	1	1	2	−5	7	89
Q	0	1	1	−3	11	38
	$P \rightarrow$					

Fibonacci numbers

Consider the sequence of even-indexed Fibonacci numbers,

$$1,\ 3,\ 8,\ 21,\ 55,\ 144,\ 377,\ 987,\ 2584,\ 6765,\ 17711, \ldots$$

satisfying $W(n+2) = 3W(n+1) - W(n)$. Associated to: $y^2 + 3xy + 3y = x^3 + 2x^2 + x$, $P = (0,0)$ (nodal).

Fibonacci numbers

Consider the sequence of even-indexed Fibonacci numbers,

$$1,\ 3,\ 8,\ 21,\ 55,\ 144,\ 377,\ 987,\ 2584,\ 6765,\ 17711, \ldots$$

satisfying $W(n+2) = 3W(n+1) - W(n)$. Associated to: $y^2 + 3xy + 3y = x^3 + 2x^2 + x$, $P = (0,0)$ (nodal). Non-singular points of the curve isomorphic with $\bar{\mathbb{Q}}^*$:

$$(x, y) \mapsto \frac{2y + (3+\sqrt{5})(x+1)}{2y + (3-\sqrt{5})(x+1)}.$$

That is to say, C_{ns} is a twisted form of $\mathbb{G}_m$.

Fibonacci numbers

Consider the sequence of even-indexed Fibonacci numbers,

$$1,\ 3,\ 8,\ 21,\ 55,\ 144,\ 377,\ 987,\ 2584,\ 6765,\ 17711,\ldots$$

satisfying $W(n+2) = 3W(n+1) - W(n)$. Associated to: $y^2 + 3xy + 3y = x^3 + 2x^2 + x$, $P = (0,0)$ (nodal). Non-singular points of the curve isomorphic with $\bar{\mathbb{Q}}^*$:

$$(x,y) \mapsto \frac{2y + (3+\sqrt{5})(x+1)}{2y + (3-\sqrt{5})(x+1)}.$$

That is to say, C_{ns} is a twisted form of $\mathbb{G}_m$. The point $P = (0,0)$ is associated to the unit $\left(\frac{3+\sqrt{5}}{3-\sqrt{5}}\right)$.

Fibonacci numbers

Consider the sequence of even-indexed Fibonacci numbers,

$$1,\ 3,\ 8,\ 21,\ 55,\ 144,\ 377,\ 987,\ 2584,\ 6765,\ 17711, \dots$$

satisfying $W(n+2) = 3W(n+1) - W(n)$. Associated to: $y^2 + 3xy + 3y = x^3 + 2x^2 + x$, $P = (0,0)$ (nodal). Non-singular points of the curve isomorphic with $\bar{\mathbb{Q}}^*$:

$$(x,y) \mapsto \frac{2y + (3+\sqrt{5})(x+1)}{2y + (3-\sqrt{5})(x+1)}.$$

That is to say, C_{ns} is a twisted form of $\mathbb{G}_m$. The point $P = (0,0)$ is associated to the unit $\left(\frac{3+\sqrt{5}}{3-\sqrt{5}}\right)$.
Unit group in $\mathbb{Q}(\sqrt{5})$ is rank 1, so there's no interesting *rational* rank two Fibonacci numbers.

Rank two Fibonacci numbers

Take another point $Q = (1, \sqrt{13} - 3)$ on this curve. The elliptic divisibility sequence associated to C and Q begins

$$1,\ 2\sqrt{13},\ 88,\ 576\sqrt{13},\ 97280,\ 2523136\sqrt{13},\ 1700790272,\ \ldots$$

Rank two Fibonacci numbers

Take another point $Q = (1, \sqrt{13} - 3)$ on this curve. The elliptic divisibility sequence associated to C and Q begins

$$1,\ 2\sqrt{13},\ 88,\ 576\sqrt{13},\ 97280,\ 2523136\sqrt{13},\ 1700790272,\ \ldots$$

It's equivalent to the sequence sequence $A_n = \sqrt{2}^{n^2-1} W_{E,P}(n)$ beginning

$$1,\ \frac{\sqrt{13}}{\sqrt{2}},\ \frac{11}{2},\ \frac{9\sqrt{13}}{2\sqrt{2}},\ \frac{95}{4},\ \frac{77\sqrt{13}}{4\sqrt{2}},\ \frac{811}{8},\ \frac{657\sqrt{13}}{8\sqrt{2}},\ \frac{6919}{16},\ \ldots$$

satisfying $A_{n+2} = \left(\frac{\sqrt{13}}{\sqrt{2}}\right) A_{n+1} - A_n$.

Rank two Fibonacci numbers

$$y^2 + 3xy + 3y = x^3 + 2x^2 + x,\ P = (0,0),\ Q = (1, \sqrt{13} - 3)$$

$$
\begin{array}{ccccc}
\begin{pmatrix} 2523136 \\ 0 \end{pmatrix} & \begin{pmatrix} 624869376 \\ -2252980224 \end{pmatrix} & \begin{pmatrix} 307737706496 \\ -1109564080128 \end{pmatrix} & \begin{pmatrix} 145553031069696 \\ -524798916820992 \end{pmatrix} & \begin{pmatrix} 48306063204990976 \\ -174169987801399296 \end{pmatrix} \\
\begin{pmatrix} 0 \\ 97280 \end{pmatrix} & \begin{pmatrix} 2016768 \\ -7270912 \end{pmatrix} & \begin{pmatrix} -294087168 \\ 1060346368 \end{pmatrix} & \begin{pmatrix} 35253070848 \\ -127106754560 \end{pmatrix} & \begin{pmatrix} 3858417639936 \\ -13911722642944 \end{pmatrix} \\
\begin{pmatrix} 576 \\ 0 \end{pmatrix} & \begin{pmatrix} 12864 \\ -46336 \end{pmatrix} & \begin{pmatrix} 512064 \\ -1846272 \end{pmatrix} & \begin{pmatrix} 742464 \\ -2676992 \end{pmatrix} & \begin{pmatrix} -6985271232 \\ 25185753600 \end{pmatrix} \\
\begin{pmatrix} 0 \\ 88 \end{pmatrix} & \begin{pmatrix} 156 \\ -556 \end{pmatrix} & \begin{pmatrix} -924 \\ 3332 \end{pmatrix} & \begin{pmatrix} -101448 \\ 365776 \end{pmatrix} & \begin{pmatrix} 12164268 \\ -43858892 \end{pmatrix} \\
\begin{pmatrix} 2 \\ 0 \end{pmatrix} & \begin{pmatrix} 3 \\ -9 \end{pmatrix} & \begin{pmatrix} -29 \\ 105 \end{pmatrix} & \begin{pmatrix} -1278 \\ 4608 \end{pmatrix} & \begin{pmatrix} -38365 \\ 138327 \end{pmatrix} \\
\begin{pmatrix} 0 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \end{pmatrix} & \begin{pmatrix} 3 \\ -10 \end{pmatrix} & \begin{pmatrix} -27 \\ 98 \end{pmatrix} & \begin{pmatrix} 237 \\ -854 \end{pmatrix} \\
\begin{pmatrix} 0 \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 3 \end{pmatrix} & \begin{pmatrix} 0 \\ 8 \end{pmatrix} & \begin{pmatrix} 0 \\ 21 \end{pmatrix} \\
\begin{pmatrix} 0 \\ -1 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \end{pmatrix} & \begin{pmatrix} 3 \\ 10 \end{pmatrix} & \begin{pmatrix} 27 \\ 98 \end{pmatrix} & \begin{pmatrix} 237 \\ 854 \end{pmatrix} \\
\begin{pmatrix} -2 \\ 0 \end{pmatrix} & \begin{pmatrix} -3 \\ -9 \end{pmatrix} & \begin{pmatrix} 29 \\ 105 \end{pmatrix} & \begin{pmatrix} 1278 \\ 4608 \end{pmatrix} & \begin{pmatrix} 38365 \\ 138327 \end{pmatrix} \\
\begin{pmatrix} 0 \\ -88 \end{pmatrix} & \begin{pmatrix} -156 \\ -556 \end{pmatrix} & \begin{pmatrix} -924 \\ -3332 \end{pmatrix} & \begin{pmatrix} 101448 \\ 365776 \end{pmatrix} & \begin{pmatrix} 12164268 \\ 43858892 \end{pmatrix}
\end{array}
$$

Where $\begin{pmatrix} a \\ b \end{pmatrix}$ means $a\sqrt{13} + b$.

Example over $\mathbb{F}_5$

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

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

$P \rightarrow$

Example over $\mathbb{F}_5$

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

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
$P \longrightarrow$

- The polynomial $\Psi_{\mathbf{v}}(\mathbf{P}) = 0$ if and only if $\mathbf{v} \cdot \mathbf{P} = 0$.

Example over $\mathbb{F}_5$

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

$$
\begin{array}{r|c|c|c|c|c|c|c|}
\hline
 & 0 & 4 & 4 & 3 & 1 & 2 & 4 \\
\hline
 & 4 & 4 & 4 & 4 & 1 & 3 & 0 \\
\hline
 & 4 & 3 & 2 & 0 & 3 & 2 & 1 \\
\hline
 & 0 & 3 & 1 & 4 & 4 & 4 & 4 \\
\hline
 & 1 & 3 & 4 & 2 & 4 & 1 & 0 \\
\hline
\uparrow & 1 & 1 & 2 & 0 & 2 & 4 & 1 \\
\hline
Q & 0 & 1 & 1 & 2 & 1 & 3 & 4 \\
\hline
\multicolumn{8}{l}{\quad P \rightarrow}
\end{array}
$$

- The polynomial $\Psi_{\mathbf{v}}(\mathbf{P}) = 0$ if and only if $\mathbf{v} \cdot \mathbf{P} = 0$.
- These zeroes lie in a lattice: the *lattice of apparition* associated to prime (here, 5).

Periodicity property with respect to lattice of apparition

	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
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \rightarrow$						

Periodicity property with respect to lattice of apparition

	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
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \longrightarrow$						

Periodicity property with respect to lattice of apparition

	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
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \longrightarrow$						

Periodicity property with respect to lattice of apparition

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 elliptic net is not periodic modulo the lattice of apparition.

Periodicity property with respect to lattice of apparition

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 elliptic net is not periodic modulo the lattice of apparition.
- The appropriate translation property should tell how to obtain the green values from the blue values.

Periodicity property with respect to lattice of apparition

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 elliptic net is not periodic modulo the lattice of apparition.
- The appropriate translation property should tell how to obtain the green values from the blue values.

- There are such translation properties.

Translation properties

Let Γ be the lattice of apparition for an elliptic net W. Define $g : \Gamma \times \mathbb{Z}^n \to K^*$ by

$$g(\mathbf{r}, \mathbf{m}) = \frac{W(\mathbf{m} + \mathbf{r})}{W(\mathbf{m})}.$$

Translation properties

Let Γ be the lattice of apparition for an elliptic net W. Define $g : \Gamma \times \mathbb{Z}^n \to K^*$ by

$$g(\mathbf{r}, \mathbf{m}) = \frac{W(\mathbf{m} + \mathbf{r})}{W(\mathbf{m})}.$$

Theorem (Ward $n = 1$; S., $n > 1$)

The function g is quadratic and affine linear in 2nd variable.

Translation properties

Let Γ be the lattice of apparition for an elliptic net W. Define $g : \Gamma \times \mathbb{Z}^n \to K^*$ by

$$g(\mathbf{r}, \mathbf{m}) = \frac{W(\mathbf{m} + \mathbf{r})}{W(\mathbf{m})}.$$

Theorem (Ward $n = 1$; S., $n > 1$)

The function g is quadratic and affine linear in 2nd variable.

Example

If $n = 1$, $W(r) = 0$, then

$$g(kr, m) = a^{mk} b^{k^2},$$

for all $k \in \mathbb{Z}$.

Elliptic curves and pairings

For any divisor $(Q+S)-(S) \in \mathrm{Pic}^0(E)$, we obtain an extension

$$0 \to \mathbb{G}_m \to J_{Q,S} \to E \to 0$$

called a Generalised Jacobian.

Elliptic curves and pairings

For any divisor $(Q+S)-(S) \in \mathrm{Pic}^0(E)$, we obtain an extension

$$0 \to \mathbb{G}_m \to J_{Q,S} \to E \to 0$$

called a Generalised Jacobian. Suppose $[m]P = \mathcal{O}$. If $\sigma : E \to J_{Q,S}$ is a section, then

$$\tau_m(P, Q) = m\sigma(P) - \sigma(\mathcal{O}) \in \mathbb{G}_m$$

Elliptic curves and pairings

For any divisor $(Q+S)-(S) \in \mathrm{Pic}^0(E)$, we obtain an extension

$$0 \to \mathbb{G}_m \to J_{Q,S} \to E \to 0$$

called a Generalised Jacobian. Suppose $[m]P = \mathcal{O}$. If $\sigma : E \to J_{Q,S}$ is a section, then

$$\tau_m(P,Q) = m\sigma(P) - \sigma(\mathcal{O}) \in \mathbb{G}_m$$

is a bilinear map (Tate-Lichtenbaum pairing)

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

Elliptic curves and pairings

For any divisor $(Q+S)-(S) \in \mathrm{Pic}^0(E)$, we obtain an extension

$$0 \to \mathbb{G}_m \to J_{Q,S} \to E \to 0$$

called a Generalised Jacobian. Suppose $[m]P = \mathcal{O}$. If $\sigma : E \to J_{Q,S}$ is a section, then

$$\tau_m(P,Q) = m\sigma(P) - \sigma(\mathcal{O}) \in \mathbb{G}_m$$

is a bilinear map (Tate-Lichtenbaum pairing)

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

and $e_m : E[m] \times E[m] \to \mu_m$ defined by

$$e_m(P,Q) = \tau_m(P,Q)/\tau_m(Q,P)$$

is the Weil pairing (intersection pairing on homology of elliptic curve).

Elliptic nets and pairings

Theorem

Let Q_1, Q_2, Q_3 be points on an elliptic curve E and let W be any elliptic net associated to E and points $\mathbf{T} = (P_1, \ldots, P_n)$ such that we can find $\mathbf{q}_i \in \mathbb{Z}^n$ for which $\mathbf{q}_i \cdot \mathbf{T} = Q_i$ on the curve. The Tate-Lichtenbaum pairing of $Q_1 \in E[m]$ and $Q_2 \in E$ is given by

$$\tau_m(Q_1, Q_2) = \frac{W(m\mathbf{q}_1 + \mathbf{q}_2 + \mathbf{q}_3)W(\mathbf{q}_3)}{W(m\mathbf{q}_1 + \mathbf{q}_3)W(\mathbf{q}_2 + \mathbf{q}_3)}$$

and the Weil pairing of $Q_1, Q_2 \in E[m]$ is given by

$$e_m(Q_1, Q_2) = \frac{W(m\mathbf{q}_1 + \mathbf{q}_2 + \mathbf{q}_3)W(\mathbf{q}_1 + \mathbf{q}_3)W(m\mathbf{q}_2 + \mathbf{q}_3)}{W(m\mathbf{q}_1 + \mathbf{q}_3)W(\mathbf{q}_2 + \mathbf{q}_3)W(\mathbf{q}_1 + m\mathbf{q}_2 + \mathbf{q}_3)}.$$

(These formulæ are independent of $\mathbf{q}_3$ and the choice of $\mathbf{T}$.)

Periodicity and pairings

Reminder:

$$g(\mathbf{r}, \mathbf{m}) = \frac{W(\mathbf{m} + \mathbf{r})}{W(\mathbf{m})}.$$

Periodicity and pairings

Reminder:

$$g(\mathbf{r}, \mathbf{m}) = \frac{W(\mathbf{m} + \mathbf{r})}{W(\mathbf{m})}.$$

Combining our results, we have

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

and

$$e_m(P, Q) = \frac{g(m\mathbf{p}, \mathbf{q} + \mathbf{s})g(m\mathbf{q}, \mathbf{s})}{g(m\mathbf{p}, \mathbf{s})g(m\mathbf{q}, \mathbf{p} + \mathbf{s})}.$$

Primitive Divisors in Elliptic Divisibility Sequences

We may define a **Primitive Divisor** of a term W_n to be a prime p such that $p | W_n$ and $p \nmid W_m$ for any $0 < m < n$. We then have

Primitive Divisors in Elliptic Divisibility Sequences

We may define a **Primitive Divisor** of a term W_n to be a prime p such that $p|W_n$ and $p \not| W_m$ for any $0 < m < n$. We then have

Theorem (Silverman's Elliptic Zsigmondy Theorem)

For every elliptic divisibility sequence there is a finite bound N such that for any $n > N$, W_n has a primitive divisor.

Primitive Divisors in Elliptic Divisibility Sequences

We may define a **Primitive Divisor** of a term W_n to be a prime p such that $p|W_n$ and $p \not| W_m$ for any $0 < m < n$. We then have

Theorem (Silverman's Elliptic Zsigmondy Theorem)

For every elliptic divisibility sequence there is a finite bound N such that for any $n > N$, W_n has a primitive divisor.

There have since been many other results...

Lattices of Apparition and Primitive Divisors

Lattices of Apparition and Primitive Divisors

Question 1

What lattices of apparition arise in an elliptic net?

Lattices of Apparition and Primitive Divisors

Question 1

What lattices of apparition arise in an elliptic net?

Rank 1: all but finitely many lattices of apparition arise in an elliptic net.

Lattices of Apparition and Primitive Divisors

Question 1

What lattices of apparition arise in an elliptic net?

Rank 1: all but finitely many lattices of apparition arise in an elliptic net.

Geometrically, this asks: What groups appear as kernels of reduction mod p of a subgroup $\Gamma \subset E(K)$ as p ranges over primes?

Lattices of Apparition and Primitive Divisors

Question 1

What lattices of apparition arise in an elliptic net?

Rank 1: all but finitely many lattices of apparition arise in an elliptic net.

Geometrically, this asks: What groups appear as kernels of reduction mod p of a subgroup $\Gamma \subset E(K)$ as p ranges over primes?

Question 2

What indices of lattices of apparition arise in an elliptic net?

Lattices of Apparition and Primitive Divisors

Question 1

What lattices of apparition arise in an elliptic net?

Rank 1: all but finitely many lattices of apparition arise in an elliptic net.

Geometrically, this asks: What groups appear as kernels of reduction mod p of a subgroup $\Gamma \subset E(K)$ as p ranges over primes?

Question 2

What indices of lattices of apparition arise in an elliptic net?

Rank 1: all but finitely many integers arise as indices (ranks of apparition) for an elliptic net.

Lattices of Apparition and Primitive Divisors

Question 1

What lattices of apparition arise in an elliptic net?

Rank 1: all but finitely many lattices of apparition arise in an elliptic net.

Geometrically, this asks: What groups appear as kernels of reduction mod p of a subgroup $\Gamma \subset E(K)$ as p ranges over primes?

Question 2

What indices of lattices of apparition arise in an elliptic net?

Rank 1: all but finitely many integers arise as indices (ranks of apparition) for an elliptic net.

Geometrically, this asks: What group orders can be obtained as images of reduction mod p of a subgroup $\Gamma \subset E(K)$ as p ranges over primes?

Applications to Cryptography: Pairing computation

- Can calculate the terms of the sequence with a double-and-add algorithm.
- Thank you to Michael Scott, Augusto Jun Devigili and Ben Lynn for implementing the algorithm.

Applications to Cryptography: Pairing computation

- Can calculate the terms of the sequence with a double-and-add algorithm.
- Thank you to Michael Scott, Augusto Jun Devigili and Ben Lynn for implementing the algorithm.

- **type a**: 512 bit base-field, embedding degree 2, 1024 bits security, $y^2 = x^3 + x$, group order is a Solinas prime.
- **type f**: 160 bit base-field, embedding degree 12, 1920 bits security, Barreto-Naehrig curves [*Pairing Friendly Elliptic Curves of Prime Order*, SAC 2005]

Applications to Cryptography: Pairing computation

- Can calculate the terms of the sequence with a double-and-add algorithm.
- Thank you to Michael Scott, Augusto Jun Devigili and Ben Lynn for implementing the algorithm.

- **type a**: 512 bit base-field, embedding degree 2, 1024 bits security, $y^2 = x^3 + x$, group order is a Solinas prime.
- **type f**: 160 bit base-field, embedding degree 12, 1920 bits security, Barreto-Naehrig curves [*Pairing Friendly Elliptic Curves of Prime Order*, SAC 2005]

Algorithm:	Miller's	Elliptic Net
type a	19.8439 ms	40.6252 ms
type f	238.4378 ms	239.5314 ms

average time of a test suite of 100 randomly generated pairings in each of the two cases

Applications to Cryptography: ECDLP

Problem

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$. Determine k such that $Q = [k]P$.

Applications to Cryptography: ECDLP

Problem

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$. Determine k such that $Q = [k]P$.

Joint work with Kristin Lauter and performed at Microsoft Research.

EDS Discrete Log

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W and terms $W(k)$, $W(k+1), \ldots, W(k+s-1)$, determine k.

EDS Discrete Log

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W and terms $W(k)$, $W(k+1), \ldots, W(k+s-1)$, determine k.

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, and $\mathrm{ord}(P) \geq 4$.

EDS Discrete Log

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W and terms $W(k)$, $W(k+1), \ldots, W(k+s-1)$, determine k.

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, and $\operatorname{ord}(P) \geq 4$.

Problem (EDS Association)

Determine $W_{E,P}(k)$ for the value of $0 < k < \operatorname{ord}(P)$ such that $Q = [k]P$.

EDS Discrete Log

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W and terms $W(k)$, $W(k+1), \ldots, W(k+s-1)$, determine k.

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, and $\mathrm{ord}(P) \geq 4$.

Problem (EDS Association)

Determine $W_{E,P}(k)$ for the value of $0 < k < \mathrm{ord}(P)$ such that $Q = [k]P$.

Problem (EDS Residue)

Determine the quadratic residuosity of $W_{E,P}(k)$ for the value of $0 < k < \mathrm{ord}(P)$ such that $Q = [k]P$.

Equivalence of problems

Theorem (S,L)

Let E be an elliptic curve over a finite field $K =_q$ of characteristic $\neq 2$. If any one of the following problems is solvable in probabilistic sub-exponential time, then all of them are:

1. *ECDLP*
2. *EDS Association for non-perfectly periodic sequences*
3. *Width 3 EDS Discrete Log for perfectly periodic sequences*

In addition, the previous problems are equivalent to the following one in the case that $E(\mathbb{F}_q)$ is of odd order.

4. *EDS Residue for non-perfectly periodic sequences*

(perfectly periodic: period equal to order of point aka rank of apparition)

Is this talk about combinatorics?

- combinatorial interpretations?

Is this talk about combinatorics?

- combinatorial interpretations?
- Laurentness and positivity?

Is this talk about combinatorics?

- combinatorial interpretations?
- Laurentness and positivity?
- You tell me.