Elliptic Nets

Katherine Stange

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

Number Theory and Computability,
Edinburgh, Scotland, 2007

Outline

Elliptic Divisibility Sequences
  Definitions
  Curve-Net Correspondence

Elliptic Nets
  Motivation
  Definitions
  Curve-Net Correspondence

Periodicity
  Elliptic Divisibility Sequences
  Elliptic Nets

Primitive Divisors
  Elliptic Divisibility Sequences
  Elliptic Nets
  Primes

Outline

Elliptic Divisibility Sequences
  - Definitions
  - Curve-Net Correspondence

Elliptic Nets
  - Motivation
  - Definitions
  - Curve-Net Correspondence

Periodicity
  - Elliptic Divisibility Sequences
  - Elliptic Nets

Primitive Divisors
  - Elliptic Divisibility Sequences
  - Elliptic Nets
  - Primes

Definition and Examples

Definition

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

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

Definition and Examples

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.

Definition and Examples

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.
- By convention $W_1 = 1$ and $W_2 W_3 \neq 0$.

Definition and Examples

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.
- By convention $W_1 = 1$ and $W_2W_3 \neq 0$.
- Example: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$

Definition and Examples

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.
- By convention $W_1 = 1$ and $W_2W_3 \neq 0$.
- Example: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$
- Example: $1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, \ldots$

Definition and Examples

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.
- By convention $W_1 = 1$ and $W_2W_3 \neq 0$.
- 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**

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

Outline

- Elliptic Divisibility Sequences
  - Definitions
  - Curve-Net Correspondence
- Elliptic Nets
  - Motivation
  - Definitions
  - Curve-Net Correspondence
- Periodicity
  - Elliptic Divisibility Sequences
  - Elliptic Nets
- Primitive Divisors
  - Elliptic Divisibility Sequences
  - Elliptic Nets
  - Primes

Ψ Functions

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

Definition

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

Ψ Functions

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

Definition

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

- Elliptic functions.

Ψ Functions

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

Definition

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

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

Ψ Functions

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

Definition

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

- Elliptic functions.
- Simple zeroes at non-zero n-torsion points.
- Divisor is $\sum_{P \in E[n]} (P) - n^2(0)$.

Curve-Sequence Correspondence

Theorem (M. Ward, 1948)

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

$$W_n := \Psi_n(z)$$

forms an elliptic divisibility sequence.

Curve-Sequence Correspondence

Theorem (M. Ward, 1948)

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

$$W_n := \Psi_n(z)$$

forms an elliptic divisibility sequence.
Furthermore, every elliptic divisibility sequence satisfying $W_1 = 1$, $W_2 W_3 \neq 0$ arises in this way.

Curve-Sequence Correspondence

Theorem (M. Ward, 1948)

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

$$W_n := \Psi_n(z)$$

forms an elliptic divisibility sequence.
Furthermore, every elliptic divisibility sequence satisfying $W_1 = 1$, $W_2 W_3 \neq 0$ arises in this way.

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

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

$$W_1 = 1$$
$$W_2 = 1$$
$$W_3 = -3$$
$$W_4 = 11$$
$$W_5 = 38$$
$$W_6 = 249$$
$$W_7 = -2357$$

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

$$\begin{aligned}
W_1 &= 1 & P &= (0,0)\\
W_2 &= 1 & [2]P &= (3,5)\\
W_3 &= -3 & [3]P &= \left(-\frac{11}{9}, \frac{28}{27}\right)\\
W_4 &= 11 & [4]P &= \left(\frac{114}{121}, -\frac{267}{1331}\right)\\
W_5 &= 38 & [5]P &= \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right)\\
W_6 &= 249 & [6]P &= \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right)\\
W_7 &= -2357 & [7]P &= \left(-\frac{2182983}{5555449}, -\frac{20464084173}{13094193293}\right)
\end{aligned}$$

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

$$
\begin{aligned}
W_1 &= 1 & P &= (0,0) \\
W_2 &= 1 & [2]P &= (3,5) \\
W_3 &= -3 & [3]P &= \left(-\frac{11}{9}, \frac{28}{27}\right) \\
W_4 &= 11 & [4]P &= \left(\frac{114}{121}, -\frac{267}{1331}\right) \\
W_5 &= 38 & [5]P &= \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right) \\
W_6 &= 249 & [6]P &= \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right) \\
W_7 &= -2357 & [7]P &= \left(-\frac{2182983}{5555449}, -\frac{20464084173}{13094193293}\right)
\end{aligned}
$$

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

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

Division Polynomials

Any elliptic curve E has a Weierstrass equation. Suppose

$$E : y^2 = x^3 + Ax + B \ .$$

The elliptic functions $\Psi_n(z; \Lambda)$ can be written as **Division Polynomials** in terms of x, y, A, B:

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

Coordinates of $[n]P$

Suppose we have

$$E : y^2 = x^3 + Ax + B \ .$$

Define

$$\phi_n = x\Psi_n^2 - \Psi_{n+1}\Psi_{n-1} \ ,$$

$$4y\omega_n = \Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2 \ .$$

Then we have

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

Divisibility as a Curve Property I

1. We have the **Identity Property**:

$$W_n = 0 \iff [n]P = 0 \ .$$

Divisibility as a Curve Property I

1. We have the **Identity Property**:

$$W_n = 0 \iff [n]P = 0 \ .$$

2. An elliptic curve with rational coefficients can be reduced modulo a prime p by reducing coefficients and coordinates. The resulting map is a homomorphism of groups. The associated elliptic divisibility sequence also reduces modulo p.

Divisibility as a Curve Property I

1. We have the **Identity Property**:

$$W_n = 0 \iff [n]P = 0 \ .$$

2. An elliptic curve with rational coefficients can be reduced modulo a prime p by reducing coefficients and coordinates. The resulting map is a homomorphism of groups. The associated elliptic divisibility sequence also reduces modulo p.
3. The Identity Property holds on this new curve over $\mathbb{F}_p$. Therefore there is some **Rank of Apparition** r of p in the sequence W_n such that

$$W_n \equiv 0 \mod p \iff n \equiv 0 \mod r \ .$$

Divisibility as a Curve Property I

1. We have the **Identity Property**:

$$W_n = 0 \iff [n]P = 0 \ .$$

2. An elliptic curve with rational coefficients can be reduced modulo a prime p by reducing coefficients and coordinates. The resulting map is a homomorphism of groups. The associated elliptic divisibility sequence also reduces modulo p.
3. The Identity Property holds on this new curve over $\mathbb{F}_p$. Therefore there is some **Rank of Apparition** r of p in the sequence W_n such that

$$W_n \equiv 0 \mod p \iff n \equiv 0 \mod r \ .$$

4. This implies the divisibility property for squarefree numbers.

Divisibility as a Curve Property II

5. From the theory of formal groups, we also have the property that for r the rank of apparition of p:

$$v_p(W_{kr}) = v_p(W_r) + v_p(k)$$

Divisibility as a Curve Property II

5. From the theory of formal groups, we also have the property that for r the rank of apparition of p:

$$v_p(W_{kr}) = v_p(W_r) + v_p(k)$$

6. Together with the last slide, this implies the **divisibility** of the elliptic divisibility sequence.

Singular Cases

In the case that one has a singular cubic curve

$$C : y^2 = x^3 + Ax + B$$

over $\mathbb{Q}$ and point $P \in C(\mathbb{Q})$, one can still consider the sequence of division polynomials $\Psi_n(P)$.

Singular Cases

In the case that one has a singular cubic curve

$$C : y^2 = x^3 + Ax + B$$

over $\mathbb{Q}$ and point $P \in C(\mathbb{Q})$, one can still consider the sequence of division polynomials $\Psi_n(P)$.

Example (Singular Elliptic Divisibility Sequences)

$$C : y^2 = x^3, P = (1, 1)$$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

Singular Cases

In the case that one has a singular cubic curve

$$C : y^2 = x^3 + Ax + B$$

over $\mathbb{Q}$ and point $P \in C(\mathbb{Q})$, one can still consider the sequence of division polynomials $\Psi_n(P)$.

Example (Singular Elliptic Divisibility Sequences)

$$C : y^2 = x^3, P = (1, 1)$$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

$$C : y^2 = x^3 - \frac{25}{48}x + \frac{125}{864}, P = \left(\frac{17}{12}, \frac{3}{2}\right)$$

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

Outline

Elliptic Divisibility Sequences
  Definitions
  Curve-Net Correspondence

Elliptic Nets
  Motivation
  Definitions
  Curve-Net Correspondence

Periodicity
  Elliptic Divisibility Sequences
  Elliptic Nets

Primitive Divisors
  Elliptic Divisibility Sequences
  Elliptic Nets
  Primes

Can we do more?

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

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

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

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

Outline

- Elliptic Divisibility Sequences
  - Definitions
  - Curve-Net Correspondence
- Elliptic Nets
  - Motivation
  - Definitions
  - Curve-Net Correspondence
- Periodicity
  - Elliptic Divisibility Sequences
  - Elliptic Nets
- Primitive Divisors
  - Elliptic Divisibility Sequences
  - Elliptic Nets
  - Primes

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

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

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

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

- The recurrence generates the net from finitely many initial values.

Elliptic Nets

Definition (KS)

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

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

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

Example

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

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

$\uparrow$ Q

$P \rightarrow$

Example

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

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

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

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

$\uparrow$
Q

$P \rightarrow$

Example

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

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

$P \rightarrow$

Example

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

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

$\uparrow$ Q

$P \rightarrow$

Example

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

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

$\uparrow$ Q

$P \rightarrow$

Prime Divisors in an Elliptic Net

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

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

$\uparrow$
Q

$P \rightarrow$

Prime Divisors in an Elliptic Net

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

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

$\uparrow$ Q

$P \longrightarrow$

Prime Divisors in an Elliptic Net

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

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

$\uparrow$ Q

$P \longrightarrow$

Prime Divisors in an Elliptic Net

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

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

$\uparrow$ Q

$P \rightarrow$

Lattice Property

For an integer elliptic net, for each prime p, there exists a **Lattice of Apparition** $L \subset A$ such that

$$W(\mathbf{v}) \equiv 0 \mod p \iff \mathbf{v} \in L$$

The proof will wait until the curve-relationship is developed.

Scale Equivalence

- Let B, C be abelian groups. A quadratic function $f : B \to C$ is a function such that for all $x, y, z \in B$,

$$f(x+y+z)-f(x+y)-f(y+z)-f(x+z)+f(x)+f(y)+f(z)=0 \quad .$$

Scale Equivalence

- Let B, C be abelian groups. A quadratic function $f : B \to C$ is a function such that for all $x, y, z \in B$,

  $$f(x+y+z)-f(x+y)-f(y+z)-f(x+z)+f(x)+f(y)+f(z)=0 \ .$$

- For any elliptic net $W : A \to K$, and quadratic $f : A \to K^*$, define $W^f : A \to K$ by

  $$W^f(\mathbf{v}) = f(\mathbf{v})W(\mathbf{v}) \ .$$

  This function is an elliptic net.

Scale Equivalence

- Let B, C be abelian groups. A quadratic function $f : B \to C$ is a function such that for all $x, y, z \in B$,

$$f(x+y+z)-f(x+y)-f(y+z)-f(x+z)+f(x)+f(y)+f(z)=0 \quad .$$

- For any elliptic net $W : A \to K$, and quadratic $f : A \to K^*$, define $W^f : A \to K$ by

$$W^f(\mathbf{v}) = f(\mathbf{v})W(\mathbf{v}) \quad .$$

  This function is an elliptic net.
- If two elliptic nets are related in the manner of W and W^f for some quadratic f, then we call them **Scale Equivalent.** This is clearly an equivalence relation.

Outline

- Elliptic Divisibility Sequences
  - Definitions
  - Curve-Net Correspondence
- Elliptic Nets
  - Motivation
  - Definitions
  - Curve-Net Correspondence
- Periodicity
  - Elliptic Divisibility Sequences
  - Elliptic Nets
- Primitive Divisors
  - Elliptic Divisibility Sequences
  - Elliptic Nets
  - Primes

Elliptic Functions Ψ_n

Definition (M. Ward - Rank 1)

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

- Elliptic functions.
- The function is zero if $nz = 0$.

Elliptic Functions $\Psi_{m,n}$

Definition (Rank 2)

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

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

Elliptic Functions $\Psi_{\mathbf{v}}$

Definition (Rank k)

$$\Psi_{\mathbf{v}}(\mathbf{z};\Lambda) = \frac{\sigma(v_1 z_1 + \ldots + v_k z_k;\Lambda)}{\prod_{1 \leq i \leq k} \sigma(z_i;\Lambda)^{2v_i^2 - \sum_{j=1}^{k} v_i v_j} \prod_{\substack{1 \leq i,j \leq k \\ i \neq j}} \sigma(z_i + z_j;\Lambda)^{v_i v_j}}$$

- Elliptic functions in each variable.
- The function is zero if $v_1 z_1 + \ldots + v_k z_k = 0$.

Elliptic Nets from Elliptic Curves

Theorem (KS)

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $\mathbf{u} \in \mathbb{C}^k$ correspond to a vector of rational points $\mathbf{P} = (P_1, \ldots, P_k)$ on E. Then

$$W(\mathbf{v}) := \Psi_{\mathbf{v}}(\mathbf{u})$$

forms an elliptic net.

Elliptic Nets from Elliptic Curves

Theorem (KS)

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $\mathbf{u} \in \mathbb{C}^k$ correspond to a vector of rational points $\mathbf{P} = (P_1, \ldots, P_k)$ on E. Then

$$W(\mathbf{v}) := \Psi_{\mathbf{v}}(\mathbf{u})$$

forms an elliptic net.

- We call this the elliptic net associated to the curve E and points $P_1, \ldots, P_k$.

Elliptic Nets from Elliptic Curves

Theorem (KS)

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $\mathbf{u} \in \mathbb{C}^k$ correspond to a vector of rational points $\mathbf{P} = (P_1, \ldots, P_k)$ on E. Then

$$W(\mathbf{v}) := \Psi_{\mathbf{v}}(\mathbf{u})$$

forms an elliptic net.

- We call this the elliptic net associated to the curve E and points $P_1, \ldots, P_k$.
- We call $P_1, \ldots, P_k$ the basis of the elliptic net.

Matrix and Homothety Actions on Elliptic Nets

Matrix Action:

- A $k \times l$ integer-coefficient matrix M acts on an elliptic net $W : \mathbb{Z}^k \to K$ by
$$W^M(\mathbf{v}) = W(M(\mathbf{v})) \ .$$

Matrix and Homothety Actions on Elliptic Nets

Matrix Action:

- A $k \times l$ integer-coefficient matrix M acts on an elliptic net $W : \mathbb{Z}^k \to K$ by
$$W^M(\mathbf{v}) = W(M(\mathbf{v})) \ .$$

Homothety Action:

- An element λ of K^* acts on an elliptic net $W : \mathbb{Z}^k \to K$ by
$$W^\lambda(\mathbf{v}) = \lambda W(\mathbf{v}) \ .$$

Matrix and Homothety Actions on Elliptic Curves

Matrix Action:

- A $k \times l$ integer-coefficient matrix M takes E^k to E^l (integer-scalar multiplication and addition are defined via the curve group law).

Matrix and Homothety Actions on Elliptic Curves

Matrix Action:

- A $k \times l$ integer-coefficient matrix M takes E^k to E^l (integer-scalar multiplication and addition are defined via the curve group law).

Homothety Action:

- An element λ of K^* acts on an elliptic curve in Weierstrass form by the change of coordinates

$$(x, y) \mapsto (\lambda^2 x, \lambda^3 y) \ .$$

Singularity

One can define polynomials Δ and j in the values of an elliptic net. For elliptic divisibility sequences, these polynomials are

$$\begin{aligned}\Delta = (W_2^8 W_3^3)^{-1}(&-W_4^4 - 3W_2^5W_4^3 - 3W_2^{10}W_4^2 \\ &- 8W_2^2W_3^3W_4^2 - W_2^{15}W_4 + 20W_2^7W_3^3W_4 \\ &+ W_2^{12}W_3^3 - 16W_2^4W_3^6)\\ j = 64\Delta^{-1}(&W_2^{20} + 4W_4W_2^{15} - 16W_3^3W_2^{12} \\ &+ 6W_4^2W_2^{10} - 8W_4W_3^3W_2^7 + 4W_4^3W_2^5 + 16W_3^6W_2^4 \\ &+ 8W_4^2W_3^3W_2^2 + W_4^4)^3(W_3^4W_2^8)^{-3}\end{aligned}$$

Singularity

One can define polynomials Δ and j in the values of an elliptic net. For elliptic divisibility sequences, these polynomials are

$$\begin{aligned}\Delta = (W_2^8 W_3^3)^{-1}(-W_4^4 - 3W_2^5 W_4^3 - 3W_2^{10} W_4^2 \\ - 8W_2^2 W_3^3 W_4^2 - W_2^{15} W_4 + 20W_2^7 W_3^3 W_4 \\ + W_2^{12} W_3^3 - 16W_2^4 W_3^6)\end{aligned}$$

$$\begin{aligned}j = 64\Delta^{-1}(W_2^{20} + 4W_4 W_2^{15} - 16W_3^3 W_2^{12} \\ + 6W_4^2 W_2^{10} - 8W_4 W_3^3 W_2^7 + 4W_4^3 W_2^5 + 16W_3^6 W_2^4 \\ + 8W_4^2 W_3^3 W_2^2 + W_4^4)^3(W_3^4 W_2^8)^{-3}\end{aligned}$$

An elliptic net is called singular if $\Delta = 0$.

Curve-Net Correspondence

Theorem (KS)

Fix a field K. We have an explicit isomorphism of partially ordered sets

$$\left\{ \begin{array}{l} \textit{scale equivalence classes of non-singular elliptic nets} \\ W : \mathbb{Z}^k \to K \textit{ with } W(\mathbf{v}) \neq 0 \textit{ for } \mathbf{v} = \mathbf{e}_i, 2\mathbf{e}_i, 3\mathbf{e}_i \textit{ or } \mathbf{e}_i \pm \mathbf{e}_j \end{array} \right\}$$

$$\updownarrow$$

$$\left\{ \begin{array}{l} \textit{tuples } (E, \Omega, P_1, \ldots, P_k), \textit{ where } E \textit{ is an elliptic curve} \\ \textit{over } K, \Omega \textit{ is a holomorphic 1-form on } E \textit{ over } K, \\ P_i \in E(K) \backslash (E(K)[2] \cup E(K)[3]), \textit{ and } P_i \neq \pm P_j \textit{ for } i \neq j \end{array} \right\}$$

Furthermore, the matrix and homothety actions on the sets preserve the order and respect the isomorphism.

Lattice Property as a Curve Property

The elliptic net analogue of the Identity Property:

$$W(\mathbf{v}) \equiv 0 \mod p$$

$$\Longleftrightarrow$$

$$[v_1]P_1 + [v_2]P_2 + \cdots + [v_k]P_k = 0 \text{ on } E(\mathbb{F}_p)$$

This implies the Lattice Property.

Net Polynomials

Theorem (KS)

Suppose

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

gives an elliptic curve $E : f(x,y) = 0$*. The net functions* $\Psi_{\mathbf{v}}$ *on* E *can be expressed as polynomials in the ring*

$$\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x_i, y_i]_{i=1}^{k} \left[\frac{1}{x_i - x_j}\right]_{1\leq i<j\leq k} \Bigg/ \langle f(x_i, y_i)\rangle_{i=1}^{k} \quad .$$

Net Polynomial Examples

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

Net Polynomial Examples

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

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

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

$$\begin{aligned}
\Psi_{-1,1} &= x_1 - x_2 \ , \\
\Psi_{2,1} &= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \ , \\
\Psi_{2,-1} &= (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \ , \\
\Psi_{1,1,1} &= \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \ ,
\end{aligned}$$

Net Polynomial Examples

$$
\begin{aligned}
\Psi_{-1,1} &= x_1 - x_2 \ , \\
\Psi_{2,1} &= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 \ , \\
\Psi_{2,-1} &= (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \ , \\
\Psi_{1,1,1} &= \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \ , \\
\Psi_{3,1} &= (4x_1^6 - 12x_2x_1^5 + 9x_2^2x_1^4 + 4x_2^3x_1^3 - 4y_2^2x_1^3 + 8y_1^2x_1^3 - 6x_2^4x_1^2 \\
&\quad + 6y_2^2x_2x_1^2 - 18y_1^2x_2x_1^2 + 12y_1^2x_2^2x_1 + x_2^6 - 2y_2^2x_2^3 - 2y_1^2x_2^3 \\
&\quad + y_2^4 - 6y_1^2y_2^2 + 8y_1^3y_2 - 3y_1^4)(x_2 - x_1)^{-3} \ .
\end{aligned}
$$

A Note About the Proofs I

1. **Curves give Nets over** $\mathbb{C}$: Check the recurrence – classical complex elliptic function theory.

A Note About the Proofs I

1. **Curves give Nets over** $\mathbb{C}$: Check the recurrence – classical complex elliptic function theory.
2. **Find a sufficiently simple baseset for nets under the recurrence**: Complicated nested inductions.

A Note About the Proofs I

1. **Curves give Nets over** $\mathbb{C}$: Check the recurrence – classical complex elliptic function theory.
2. **Find a sufficiently simple baseset for nets under the recurrence**: Complicated nested inductions.
3. **Show the** Ψ **are polynomial of a nice form on the baseset**: Classical complex elliptic function theory.

A Note About the Proofs I

1. **Curves give Nets over** $\mathbb{C}$: Check the recurrence – classical complex elliptic function theory.
2. **Find a sufficiently simple baseset for nets under the recurrence**: Complicated nested inductions.
3. **Show the** Ψ **are polynomial of a nice form on the baseset**: Classical complex elliptic function theory.
4. **Extend these net polynomials of the baseset to any field**: Choose an appropriate fibration of E^n over an appropriate ring. Extend the divisors of the Ψ functions from the fibre over $\mathbb{Q}$ and check that there are no vertical components.

A Note About the Proofs II

5. **Show the Ψ are polynomial of a nice form in general**: Use the inductive function theory of Step 2 to show that this type of extension can be done in general.

A Note About the Proofs II

5. **Show the Ψ are polynomial of a nice form in general**: Use the inductive function theory of Step 2 to show that this type of extension can be done in general.
6. **Curves give Nets over any field**: Pullback from the fibration above via inclusion and base extension.

A Note About the Proofs II

5. **Show the Ψ are polynomial of a nice form in general**: Use the inductive function theory of Step 2 to show that this type of extension can be done in general.
6. **Curves give Nets over any field**: Pullback from the fibration above via inclusion and base extension.
7. **Nets give Curves in Rank 1 and 2**: Explicitly calculate the relevant curve and check agreement on the baseset, which implies agreement everywhere.

A Note About the Proofs II

5. **Show the Ψ are polynomial of a nice form in general**: Use the inductive function theory of Step 2 to show that this type of extension can be done in general.
6. **Curves give Nets over any field**: Pullback from the fibration above via inclusion and base extension.
7. **Nets give Curves in Rank 1 and 2**: Explicitly calculate the relevant curve and check agreement on the baseset, which implies agreement everywhere.
8. **Nets give Curves in All Ranks**: Induction from the base case of ranks 1 and 2 by considering subnets.

Outline

- Elliptic Divisibility Sequences
  - Definitions
  - Curve-Net Correspondence
- Elliptic Nets
  - Motivation
  - Definitions
  - Curve-Net Correspondence
- Periodicity
  - Elliptic Divisibility Sequences
  - Elliptic Nets
- Primitive Divisors
  - Elliptic Divisibility Sequences
  - Elliptic Nets
  - Primes

Ward's Periodicity Property

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

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

Example

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

Ward's Periodicity Property

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

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

Example

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

Ward's Periodicity Property

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

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

Example

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

Ward's Periodicity Property

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

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

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*,*

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

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 $\mathbb{F}_5$)

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

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

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 $\mathbb{F}_5$)

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

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

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

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 $\mathbb{F}_5$)

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

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

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

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

Outline

Elliptic Divisibility Sequences
    Definitions
    Curve-Net Correspondence

Elliptic Nets
    Motivation
    Definitions
    Curve-Net Correspondence

Periodicity
    Elliptic Divisibility Sequences
    Elliptic Nets

Primitive Divisors
    Elliptic Divisibility Sequences
    Elliptic Nets
    Primes

Reducing a Net Modulo p

Corollary (KS - Corollory to Curve-Net Theorem)

Let E be an elliptic curve over K and let $P_1, \ldots, P_k$ be K-points of E. Let $\widetilde{E}$ and $\widetilde{P}_1, \ldots, \widetilde{P}_k$ be their reductions modulo a prime p. Then the elliptic net associated to $\widetilde{E}, \widetilde{P}_1, \ldots, \widetilde{P}_k$ is the reduction modulo p of the elliptic net associated to $E, P_1, \ldots, P_k$.

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

$P \longrightarrow$

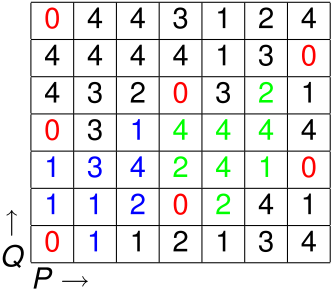
Example of Reduction Mod 5 of an Elliptic Net

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

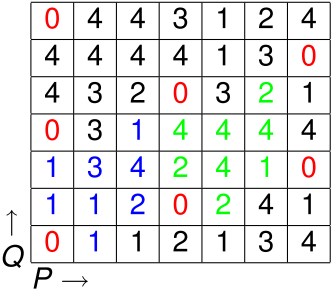
$P \longrightarrow$

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

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

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

Periodicity for Elliptic Nets

Theorem (KS)

Let $W : \mathbb{Z}^2 \to K$ *be an elliptic net such that* $W(2,0)W(0,2) \neq 0$*.*
Suppose $W(r_1, r_2) = W(s_1, s_2) = 0$*. Then there exist*
$a_s, b_s, c_s, a_r, b_r, c_r, d \in K$ *such that for all* $m, n, k, l \in \mathbb{Z}$*,*

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

In particular, if K is a finite field such as $\mathbb{F}_p$, we obtain a statement about reduction modulo p (i.e. for an integer elliptic net, if $W(r_1, r_2)$ and $W(s_1, s_2)$ are trivial mod p, then the equation holds 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

↑ Q

P →

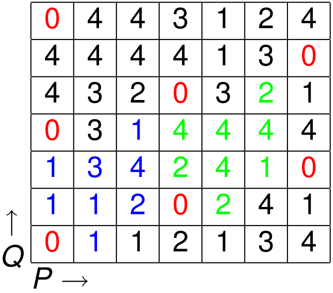
Example of Net Periodicity

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

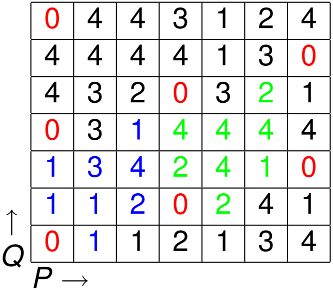
$P \rightarrow$

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

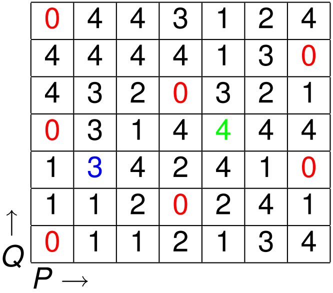
Example of Net Periodicity



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

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

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

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

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

Periodicity from Pairings

For those that know the Tate and Weil pairings, the periodicity contains the values of these pairings. In the previous theorems,

- $a = T_r(P, P)$
- a_r, a_s, b_r, b_s are appropriate Tate pairings of multiples of P and Q

The Tate and Weil pairings can therefore be calculated from elliptic nets efficiently. This is of interest to pairing-based elliptic-curve cryptographers.

Outline

Elliptic Divisibility Sequences
- Definitions
- Curve-Net Correspondence

Elliptic Nets
- Motivation
- Definitions
- Curve-Net Correspondence

Periodicity
- Elliptic Divisibility Sequences
- Elliptic Nets

Primitive Divisors
- Elliptic Divisibility Sequences
- Elliptic Nets
- Primes

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

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...

Outline

Elliptic Divisibility Sequences
  - Definitions
  - Curve-Net Correspondence

Elliptic Nets
  - Motivation
  - Definitions
  - Curve-Net Correspondence

Periodicity
  - Elliptic Divisibility Sequences
  - Elliptic Nets

Primitive Divisors
  - Elliptic Divisibility Sequences
  - Elliptic Nets
  - Primes

The Canonical Height

Recall that a point $[n]P \in E(K)$ has coordinates

$$[n]P = \left(\frac{A_n}{D_n^2}, \frac{B_n}{D_n^3} \right) \quad .$$

The Canonical Height

Recall that a point $[n]P \in E(K)$ has coordinates

$$[n]P = \left(\frac{A_n}{D_n^2}, \frac{B_n}{D_n^3} \right) \quad .$$

So we define the **Canonical Height** to be

$$\hat{h}(P) = \lim_{N \to \infty} 4^{-N} log(D_{2^N}) \quad .$$

The Canonical Height

Recall that a point $[n]P \in E(K)$ has coordinates

$$[n]P = \left(\frac{A_n}{D_n^2}, \frac{B_n}{D_n^3}\right) \quad .$$

So we define the **Canonical Height** to be

$$\hat{h}(P) = \lim_{N\to\infty} 4^{-N} log(D_{2^N}) \quad .$$

This is a quadratic form with an associated bilinear form $\langle \cdot, \cdot \rangle$.

The Canonical Height

Recall that a point $[n]P \in E(K)$ has coordinates

$$[n]P = \left(\frac{A_n}{D_n^2}, \frac{B_n}{D_n^3} \right) \quad .$$

So we define the **Canonical Height** to be

$$\hat{h}(P) = \lim_{N \to \infty} 4^{-N} log(D_{2^N}) \quad .$$

This is a quadratic form with an associated bilinear form $\langle \cdot, \cdot \rangle$. For us, what's relevant is that

$$\log |D_n| \sim \hat{h}(P) n^2 \quad ,$$

and in fact for elliptic nets

$$\log |W_{\mathbf{v}}| \sim \hat{h}(\mathbf{v} \cdot \mathbf{P}) = \sum_{i,j=1}^{k} v_i v_j \left\langle P_i, P_j \right\rangle \quad .$$

Primitive Divisors for Elliptic Nets

Possible Definition

Let p be a primitive divisor for a term $W_{\mathbf{v}}$ if

$$\hat{h}(\mathbf{v}\cdot\mathbf{P}) = \min\left\{\hat{h}(\mathbf{u}\cdot\mathbf{P}) \text{ such that } p|W_{\mathbf{u}}, \mathbf{u}\neq 0\right\} \quad .$$

This agrees with the previous definition in the sequence case.

Primitive Divisors for Elliptic Nets

Possible Definition

Let p be a primitive divisor for a term $W_{\mathbf{v}}$ if

$$\hat{h}(\mathbf{v} \cdot \mathbf{P}) = \min \left\{ \hat{h}(\mathbf{u} \cdot \mathbf{P}) \text{ such that } p | W_{\mathbf{u}}, \mathbf{u} \neq 0 \right\} \quad .$$

This agrees with the previous definition in the sequence case.

Question 1

Does there exist a bound N such that for all $\mathbf{v}$ of height exceeding N, $W_{\mathbf{v}}$ has a primitive divisor?

Primitive Divisors for Elliptic Nets

Possible Definition

Let p be a primitive divisor for a term $W_{\mathbf{v}}$ if

$$\hat{h}(\mathbf{v} \cdot \mathbf{P}) = \min \left\{ \hat{h}(\mathbf{u} \cdot \mathbf{P}) \text{ such that } p | W_{\mathbf{u}}, \mathbf{u} \neq 0 \right\} \quad .$$

This agrees with the previous definition in the sequence case.

Question 1

Does there exist a bound N such that for all $\mathbf{v}$ of height exceeding N, $W_{\mathbf{v}}$ has a primitive divisor?

Geometrically, "for all points P of sufficient height, is it true that P is the point of least height in some kernel of reduction?"

Lattices of Apparition and Primitive Divisors

Taking a different approach...

Lattices of Apparition and Primitive Divisors

Taking a different approach...

Question 2

What lattices of apparition arise in an elliptic net?

Lattices of Apparition and Primitive Divisors

Taking a different approach...

Question 2

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

Taking a different approach...

Question 2

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

Taking a different approach...

Question 2

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 3

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

Lattices of Apparition and Primitive Divisors

Taking a different approach...

Question 2

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 3

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

Taking a different approach...

Question 2

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 3

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?

Outline

- Elliptic Divisibility Sequences
  - Definitions
  - Curve-Net Correspondence
- Elliptic Nets
  - Motivation
  - Definitions
  - Curve-Net Correspondence
- Periodicity
  - Elliptic Divisibility Sequences
  - Elliptic Nets
- Primitive Divisors
  - Elliptic Divisibility Sequences
  - Elliptic Nets
  - Primes

Primes in Elliptic Nets

- When are terms of an elliptic net actually prime?

Primes in Elliptic Nets

- When are terms of an elliptic net actually prime?
- Heuristically, there are finitely many primes in an elliptic divisibility sequence. This can be shown when the point is the image of an appropriate isogeny.

Primes in Elliptic Nets

- When are terms of an elliptic net actually prime?
- Heuristically, there are finitely many primes in an elliptic divisibility sequence. This can be shown when the point is the image of an appropriate isogeny.
- For elliptic nets in general? By a heuristic counting argument, there should be infinitely many prime terms (except when the points of the net are in the image of an appropriate isogeny).

Primes in Elliptic Nets

- When are terms of an elliptic net actually prime?
- Heuristically, there are finitely many primes in an elliptic divisibility sequence. This can be shown when the point is the image of an appropriate isogeny.
- For elliptic nets in general? By a heuristic counting argument, there should be infinitely many prime terms (except when the points of the net are in the image of an appropriate isogeny).
- Proofs??

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/