Elliptic Divisibility Sequences in Computation

Katherine E. Stange

Department of Mathematics, Simon Fraser University, and
Pacific Institute of the Mathematical Sciences, University of British Columbia

CMS Winter Meeting 2010,
Computational Number Theory Session,
Vancouver, December 4, 2010

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

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

Anything satisfying this recurrence relation I'll call an *elliptic divisibility sequence*. In particular, if we evaluate at P, we get the *elliptic divisibility sequence* associated to E and P.

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

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

Note: W_n is a function of n and P, not just $[n]P$!

Elliptic Nets

On an elliptic curve $E : y^2 = x^3 + Ax + B$, with points P and Q,

$$[n]P + [m]Q = \left(\frac{\phi_{n,m}(P,Q)}{\Psi_{n,m}(P,Q)^2}, \frac{\omega_{n,m}(P,Q)}{\Psi_{n,m}(P,Q)^3} \right).$$

Consider the array of $\Psi_{n,m}(P,Q)$.

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

	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 $\mathbb{F}_5$

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

$W_P(n) : 0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 1, 2, 1, 3, 4, \ldots$

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

$P \rightarrow$

- $\Psi_n(P) = 0 \iff [n]P = \mathcal{O}$
- $\Psi_{\mathbf{v}}(\mathbf{P}) = 0 \iff \mathbf{v} \cdot \mathbf{P} = 0.$
- Zeroes lie in *lattice of apparition* associated to prime (here, 5).

Definition of an elliptic net

Definition (S)

Let K be a field. An *elliptic net* is a map $W : A \to K$ such that the following recurrence holds for all $p, q, r, s \in \mathbb{Z}^n$.

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

- Elliptic divisibility sequences are a special case ($n = 1$)
- The recurrence generates the net from finitely many initial values.

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

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

- $W(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \ldots, P_n, C)$
- 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
- consider only nets with $W(\mathbf{v}) = 1$ for $\mathbf{v} = \mathbf{e}_i$ or $\mathbf{v} = \mathbf{e}_i + \mathbf{e}_j$

Group Law

Computing terms of W_n (Rachel Shipsey):

- Work with blocks of terms of length 7.
- Double-and-add (block near index n gives block near index $2n$ or $2n+1$ in a fixed finite number of multiplications.
- Compute W_n in $O(\log n)$.

Recover $[n]P$ from W_n:

$$x(P) - x([k]P) = \frac{W_{k+1}W_{k-1}}{W_k^2}$$

For higher rank elliptic nets, it is possible to create similar algorithms. (Implemented in Pari/Sage for rank 2.)

Canonical Height

Let W_n be the elliptic divisibility sequence associated to E and integral P. Then the canonical height and its local parts are given by (Everest, Ward):

$$\hat{h}(P) = \lim_{N\to\infty} \frac{1}{N^2} \log \left(|W_N|_\infty \prod_{p|\Delta} |W_N|_p \right)$$

$$\hat{h}_\infty(P) = \lim_{N\to\infty} \frac{1}{N^2} \log |W_N|_\infty - \frac{1}{12} \log |\Delta|_\infty$$

p of good reduction:

$$\hat{h}_p(P) = 0$$

p of bad reduction:

$$\hat{h}_p(P) = \lim_{N\to\infty} \frac{1}{N^2} \log |W_N|_p - \frac{1}{12} \log |\Delta|_p$$

Reduction modulo primes

Possibly change W_n to $\lambda^{n^2-1}W_n$ for some $\lambda \in \mathbb{Z}$. Then ($p \neq 2$),

1. For primes of good reduction, $p \mid W_n \iff [n]P = \mathcal{O} \mod p$. Let r be the least positive integer such that $\nu_p(W_r) > 0$. Then

$$\nu_p(W_{mr}) = \nu_p(m) + \nu_p(W_r).$$

2. For primes not having potential good reduction, (S)

$$\nu_p(W_n) = \frac{\ell}{2}\left(B_2\left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor\right) - n^2 B_2\left(\frac{a}{\ell} - \left\lfloor \frac{a}{\ell} \right\rfloor\right) + \frac{(n^2-1)}{6}\right).$$

where $B_2(t) = t^2 - t + \frac{1}{6}$, where $\ell = \nu_p(\Delta)$ and P extends to component a of the singular fibre of the Néron model.

Integral points

Theorem (Mohamed Ayad): Let S be the set of primes at which P becomes singular under reduction. If P is integral, then $[n]P$ is integral exactly when

$$\nu_p(W_n) \neq 0 \iff p \in S.$$

Patrick Ingram uses elliptic divisibility sequences to give bounds on the size of n such that $[n]P$ is integral.

Pairing from Elliptic Nets

$m \geq 1$	$P \in E(K)[m]$
E/K an elliptic curve	$Q \in E(K)/mE(K)$

Theorem (S)

Choose $S \in E(K)$ such that $S \notin \{\mathcal{O}, -Q\}$. Let W be an elliptic net with basis $\mathbf{T}$ such that $p \cdot \mathbf{T} = P$, $q \cdot \mathbf{T} = Q$ and $s \cdot \mathbf{T} = S$. Then the quantity

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

is the Tate pairing.

For $P, Q \in E(K)[m]$, the more well-known Weil pairing:

$$e_m(P, Q) = \frac{\tau_m(P, Q)}{\tau_m(Q, P)} \quad .$$

Discrete Log (joint with Kristin Lauter)

Problem (Elliptic Curve Discrete Logarithm 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 $Q = [k]P$.

Problem (Width s EDS Discrete Log)

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

First posed by Rachel Shipsey:

- Reduced it to $\mathbb{F}_q^*$ discrete logarithm problem.
- Used the solution to give an attack on ECDLP in case $\mathrm{ord}(P) = q - 1$.

Perfect periodicity

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

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

The sequence $\phi([n]P) = 3^{n^2} W_{E,P}(n)$ is

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

There is always some λ for which $\lambda^{n^2} W_{E,P}(n)$ has period equal to the order of P. We call this new sequence the *perfectly periodic* sequence. (Lauter, S.)

Hard problems for EDS

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* $Q = [k]P$*.*

- The smallest positive value of k such that $[k]P = Q$ will be called the *minimal multiplier*.

Relating hard problems

perfectly periodic

not perfectly periodic

$$\begin{tikzcd}[column sep=small]
& {[k]P} \arrow[dl, shift right, "(\log q)^3"'] \arrow[dr, dashed, "\begin{array}{c}EDS\\ Association\end{array}"] \arrow[dd, dashed, "ECDLP"] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right, "(\log q)^2"'] \arrow[dr, dashed, "\begin{array}{c}Width\ 3\\ EDS\ Discrete\ Log\end{array}"'] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, shift left, "\mathbb{F}_q^* DLP"] \\
& k \arrow[ur, shift left, "(\log q)^3"] &
\end{tikzcd}$$

Equivalence of problems

Theorem (Lauter, S.)

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. If any one of the following problems is solvable in 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*

If $|E(\mathbb{F}_q)|$ is odd and $\operatorname{char}(\mathbb{F}_q) \neq 2$, we can also include

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

Bibliography

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

K. Stange.
Elliptic Nets and Elliptic Curves.
To appear, ANT.

K. Stange.
The Tate Pairing via Elliptic Nets.
Pairing 2007.

K. Lauter, K. Stange.
The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences.
SAC 2008.

Slides, Articles and Preprints at http://www.sfu.ca/~kestange/