Elliptic Divisibility Nets

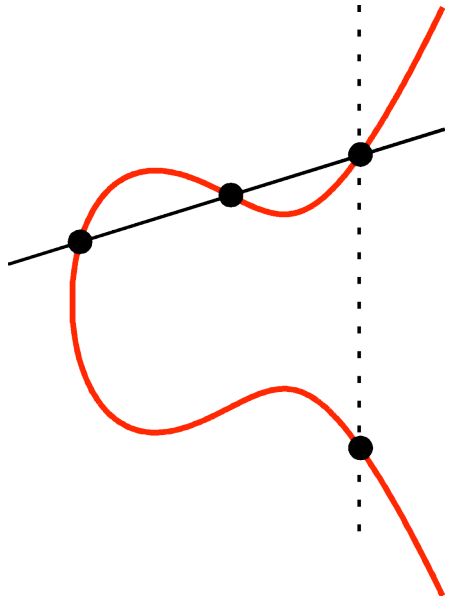
Katherine Stange

Brown University

CNTA IX, Vancouver, July 13, 2006

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

Elliptic Divisibility Sequences: Seen In Their Natural Habitat



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

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

$$P,\ 2P,\ 3P,\ 4P,\ \ldots \quad \in E(\mathbb{Q})$$

$$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$$

$$d_P,\ d_{2P},\ d_{3P},\ d_{4P},\ \ldots \quad \in \mathbb{Z}$$

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

$$P = (0, 0)$$

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

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

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

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

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

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

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

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

Elliptic Divisibility Sequences: Two Good Definitions

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

Definition A

Define elliptic functions

$$\Psi_n(z) = \frac{\sigma(nz)}{\sigma(z)^{n^2}}, \quad n > 0$$

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

$$W_n = \begin{cases} \Psi_n(z) & n > 0 \\ 0 & n = 0 \\ -\Psi_{-n}(z) & n < 0 \end{cases}$$

Definition B

Given initial conditions

$$W_0,\, W_1,\, W_2,\, W_3,\, W_4$$

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

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

$$W_{m+n} W_{m-n} =$$

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

- **Morgan Ward, 1948:** Definitions A and B are equivalent. (From the initial conditions in Definition B, one can explicitly calculate the curve and point needed for Definition A.)

- An EDS has the divisibility property:

$$\text{If } n|m, \text{ then } W_n|W_m.$$

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

- $P \in E(\mathbb{Q})$ is an n-torsion point iff $W_n = 0$
- $n\tilde{P} = \tilde{0}$ in $\tilde{E}(\mathbb{F}_p)$ iff $W_n \equiv 0 \mod p$
- Suppose $P \in E(\mathbb{Q})$ is an integral point, and $\gcd(W_2, W_3) = 1$. Then nP is an integral point iff $W_n = \pm 1$

Research (Partial List)

- Applications to Elliptic Curve Discrete Logarithm Problem in cryptography (R. Shipsey)
- Finding integral points (M. Ayad)
- Study of nonlinear recurrence sequences (Fibonacci numbers, Lucas numbers, and integers are special cases of EDS)
- Appearance of primes (G. Everest, J. Silverman, T. Ward, …) -- Friday, 10:35, Patrick Ingram
- EDS are a special case of Somos Sequences (A. van der Poorten, J. Propp, M. Somos, C. Swart, …)
- p-adic & function field cases (J. Silverman)
- Continued fractions & elliptic curve group law (W. Adams, A. van der Poorten, M. Razar)
- Sigma function perspective (A. Hone, …)
- Hyper-elliptic curves (A. Hone, A. van der Poorten, …)
- More…

From Sequences to Nets

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

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

If $P, Q \in E$, then the subgroup of $E(\mathbb{Q})$ they generate can be indexed over $\mathbb{Z} \times \mathbb{Z}$:

$$W_{m,n} = W_{mP+nQ}$$

Elliptic Divisibility Nets: Rank 2 Case

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

Definition A

Define doubly elliptic functions on $E \times E$

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

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

$$W_{m,n} = \begin{cases} \Psi_{m,n}(z,w) & (m,n) \neq (0,0) \\ 0 & (m,n) = (0,0) \end{cases}$$

Elliptic Divisibility Nets: Rank 2 Case

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

Definition B

Give initial conditions

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

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

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

$$\begin{aligned} &W_{\vec{p}+\vec{q}+\vec{s}} W_{\vec{p}-\vec{q}} W_{\vec{r}+\vec{s}} W_{\vec{r}} \\ &\quad + W_{\vec{q}+\vec{r}+\vec{s}} W_{\vec{q}-\vec{r}} W_{\vec{p}+\vec{s}} W_{\vec{p}} \\ &\quad + W_{\vec{r}+\vec{q}+\vec{s}} W_{\vec{r}-\vec{p}} W_{\vec{q}+\vec{s}} W_{\vec{q}} = 0 \end{aligned}$$

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

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

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

↑ Q

P⟶

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

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

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

↑ Q

P ⟶

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

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

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

↑ Q

P⟶

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

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

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

↑ Q

P⟶

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

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

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

↑ Q

P⟶

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

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

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

↑ Q

P⟶

Theorem (KS):

(Under some extra technical conditions)

1. **Definitions A and B are equivalent**
2. **Definitions give a coherent net of integers** (i.e. all instances of recurrence are consistent and give integers)

- The equivalence is explicit, as in rank 1
- Can be generalised to arbitrary rank
- Proof involves intricate calculations

- **Corollary (Divisibility condition)**

  Let p be a prime of good reduction for E. Then $\{\vec{v} \in \mathbb{Z} \times \mathbb{Z} : p | W_{\vec{v}}\}$ is a sublattice of $\mathbb{Z} \times \mathbb{Z}$.

- **Corollary (Independence in Mordell-Weil)**

  Let $P, Q \in E(\mathbb{Q})$. Then P and Q are independent if and only if $W_{m,n} \neq 0$ for all $(m, n) \neq (0, 0)$ in the associated elliptic divisibility net.

References

- Morgan Ward. “Memoir on Elliptic Divisibility Sequences”. American Journal of Mathematics, 70:13-74, 1948.
- Christine S. Swart. *Elliptic Curves and Related Sequences.* PhD thesis, Royal Holloway and Bedford New College, University of London, 2003.
- Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence Sequences.* Mathematical Surveys and Monographs, vol 104. American Mathematical Society, 2003.

Slides and more references available on my website at
http://www.math.brown.edu/~stange/