Elliptic Nets
(BU Algebra Seminar,
UCSD Number Theory Seminar)

Katherine E. Stange

Updated November 28, 2007

Definition 0.1. *An elliptic divisibility sequences is a sequence satisfying the recurrence*

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

Example 0.2.

$$1, 1, -3, 11, 38, 249, -2357, \dots$$

Definition 0.3. *The n-th* division polynomial *of an elliptic curve $E : f(x, y) = 0$ in Weierstrass form is the element*

$$\Psi_n \in \bar{K}[x, y]/(f(x, y) = 0)$$

such that

$$\mathrm{div}(\Psi_n) = \sum_{P \in E[n]} (P) - n^2(\mathcal{O})$$

and chosen so that, written as a rational function of $x, y \in \bar{K}(E)$, it is of the form

$$\Psi_n = \begin{cases} nx^{\frac{n^2-1}{2}} + (\textit{lower powers of } x) & n \textit{ odd}, \\ y\left(nx^{\frac{n^2}{2}} + (\textit{lower powers of } x)\right) & n \textit{ even}. \end{cases}$$

(Writing Ψ_n in this form is always possible.)

Example 0.4. *For $y^2 = x^3 + Ax + B$,*

$$\Psi_1 = 1, \Psi_2 = 2y, \Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

Theorem 0.5 (M. Ward, 1948)**.** *Fix a curve E defined over $\mathbb{Q}$ and point $P \in E(\mathbb{Q})$ satisfying $P, [2]P, [3]P \neq 0$. The sequence*

$$W_n = \Psi_n(P)$$

is an elliptic divisibility sequence.

Furthermore, every elliptic divisibility sequence with $W_1 = 1$ and $W_2 W_3 \neq 0$ arises from an elliptic curve in this way.

This is called the *elliptic divisibility sequence associated to E,P.*

Observe that $[n]P = \mathcal{O}$ if and only if $\Psi_n(P) = 0$. We may begin a dictionary between sequences and curves...

$$\begin{array}{ccc} \left(\begin{array}{l} \text{elliptic curve } E \\ \text{and point } P \text{ such that} \\ P, [2]P, [3]P \neq \mathcal{O} \end{array} \right) & \leftrightarrow & \left(\begin{array}{l} \text{ellipic divisibility sequence} \\ \text{with } W_1 = 1, W_2 W_3 \neq 0 \end{array} \right) \\ [n]P = \mathcal{O} & \leftrightarrow & W_{nk} = 0 \quad \forall k \in \mathbb{Z} \end{array}$$

Consider the multiples of P.

(Example on overhead slides.)

Usually there are some small cancellations of numerator and denominator, but modulo a few primes we can "see" the elliptic divisibility sequence in $x(P)$.

Therefore we may add to the dictionary...

$$[n]P = \left(\tfrac{a}{d^2}, \tfrac{b}{d^3}\right) \quad \underset{\text{up to } \not\infty \text{ primes}}{\overset{\text{over } \mathbb{Q}}{\longleftrightarrow}} \quad |W_n| = d$$

Proposition 0.6. *Let E be a curve in Weierstrass form over $\mathbb{Q}$. Let $\tilde{E}$ be its reduction modulo a prime p. If W is an integer valued elliptic divisibility sequence associated to E, P, then W* mod p *is the elliptic divisibility sequence associated to $\tilde{E}, \tilde{P}$.*

Proof sketch: The Ψ_n are always $\mathbb{Z}$-coefficient polynomials in x, y and the coefficients the Weierstrass equation. So we happily just take everything mod p.

Now we may add...

$$[n]\tilde{P} = \tilde{\mathcal{O}} \qquad \overset{W \in \mathbb{Z}}{\underset{\text{up to } \not\infty \text{ primes}}{\longleftrightarrow}} \qquad p|W_{nk} \quad \forall k \in \mathbb{Z}$$

In fact we have the slightly stronger criterion that

$$n|m \implies W_n|W_m.$$

Question (mused by Elkies in 2001, and myself in 2004): Can you generalise division polynomials to higher dimensions?

That is, we can collect our properties for elliptic divisibility sequences and make a wish list for dimension 2 (or higher dimensions)...

Are there functions $\Psi_{m,n} \in \bar{K}(E^2)$ such that ...

1. $\Psi_{m,n}(P, Q) = 0$ exactly when $[m]P + [n]Q = \mathcal{O}$, i.e. $\operatorname{div}(\Psi_{m,n})$ has positive part
$$([n]P + [m]Q = \mathcal{O})$$
2. $\Psi_{m,n}$ are generated from finitely many terms by a recurrence relation

3. $|\Psi_{m,n}(P,Q)| = \text{denominator}(x([n]P + [m]Q))$ up to finitely many primes
4. These are also defined over finite fields, so that the bi-sequence $\Psi_{m,n}(P,Q)$ associated to E, P, Q reduces modulo a prime p to that associated to $\tilde{E}, \tilde{P}, \tilde{Q}$.

. . . ?

Theorem 0.7 (KS)**.** *"Yes." There are functions satisfying the above and the divisors of $\Psi_{n,m}$ are of a special form. In two dimensions it is*

$$\begin{aligned}([n]P + [m]Q = \mathcal{O}) &- (n^2 - nm)(\{\mathcal{O}\} \times E) \\ &- (m^2 - nm)(E \times \{\mathcal{O}\}) - nm(P + Q = \mathcal{O})\end{aligned}$$

Furthermore, the $\Psi_{m,n}$ satisfy the recurrence

$$\begin{aligned}W(p+q+s)W(p-q)W(r+s)W(s) \\ + W(q+r+s)W(q-r)W(p+s)W(p) \\ + W(r+p+s)W(r-p)W(q+s)W(q) = 0. \quad (1)\end{aligned}$$

The dictionary of relationships can be adjusted to the two-dimensional case:

$$\begin{pmatrix} \text{elliptic curve } E \\ \text{and point } P \text{ such that} \\ P, Q, P \pm Q \neq \mathcal{O} \end{pmatrix} \quad \leftrightarrow \quad \begin{pmatrix} \text{ellipic nets with} \\ W_{1,0} = W_{0,1} \\ = W_{1,1} = 1, \\ W_{1,-1} \neq 0 \end{pmatrix}$$

$$[n]P + [m]Q = \mathcal{O} \quad \leftrightarrow \quad W_{n,m} = 0$$

$$[n]P + [m]Q = \left(\tfrac{a}{d^2}, \tfrac{b}{d^3}\right) \quad \overset{\text{over } \mathbb{Q}}{\longleftrightarrow} \quad |W_{n,m}| = d$$

$$[n]\tilde{P} + [m]\tilde{Q} = \tilde{\mathcal{O}} \quad \overset{W \in \mathbb{Z}}{\longleftrightarrow} \quad p | W_{n,m}$$

(The latter two up to finitely many primes.)

These are in fact defined over any field.

(Example on slides.)

Show patterns:

- Elliptic divisibility sequences show up as subsequences.
- Translated elliptic divisibility sequences are lines not through origin.
- The 'divisibility property' is now a lattice property for primes.
- The net may not be periodic with respect to this lattice (it is *not* a function of the point $[n]P + [m]Q$).

- Example of reduction modulo a prime, where net must be periodic modulo some sublattice of this lattice.

We now look at the explanation for this 'failure' of periodicity.

Definition 0.8. *A* generalised Jacobian X *is an extension of an abelian variety* A *by an algebraic group* B*:*

$$1 \to B \to X \to A \to 1$$

For each pair $R, S \in E$, there exists a generalised Jacobian $X_{R,S}$ defined as follows:

$$1 \to \mathbb{G}_m \to X_D \to E \to 1.$$

$X_{R,S} = \mathbb{G}_m \times E$ as a set, with operation

$$(a, P) + (b, Q) = (abf_{P,Q}(R)f_{P,Q}(S)^{-1}, P + Q)$$

where

$$\operatorname{div}(f_{P,Q}) = (P) + (Q) - (P + Q) - (\mathcal{O})$$

Note that $f_{P,Q}$ depends only on P, Q, and the constant factor doesn't matter.

Theorem 0.9. *Let* $\mathbf{T}$ *be any collection of* n *non-zero points in* E *(such that no two are equal or inverses) which generate a subgroup containing* P, Q, R*. Let* $\mathbf{p}, \mathbf{q}, \mathbf{r}$ *be such that* $\mathbf{p} \cdot \mathbf{T} = P$*,* $\mathbf{q} \cdot \mathbf{T} = Q$*, and* $\mathbf{r} \cdot \mathbf{T} = R$*.*

Then,

$$f_{P,Q}(R) = c\frac{W_{\mathbf{T}}(\mathbf{r} + \mathbf{p} + \mathbf{q})W_{\mathbf{T}}(\mathbf{r})}{W_{\mathbf{T}}(\mathbf{r} + \mathbf{p})W_{\mathbf{T}}(\mathbf{r} + \mathbf{q})}$$

where c *is a constant that does not depend on* R*.*

Let $\alpha_{n,m}(R,S)$ be such that

$$m(1,P)+n(1,Q)=(\alpha_{n,m}(R,S),\mathcal{O})$$

on $X_{R,S}$.

Theorem 0.10. *Let $\mathbf{r}=(r_1,r_2)$ be such that $[r_1]P+[r_2]Q=\mathcal{O}$. Then*

$$\frac{W(\mathbf{r}+\mathbf{s})}{W(\mathbf{s})}=a_{\mathbf{r}}^{s_1}a_{\mathbf{r}}^{s_2}c_{\mathbf{r}}$$

where

$$\begin{aligned} a_{\mathbf{r}} &= \alpha_{\mathbf{r}}(([2]P)-(P))\left(\tfrac{W(3,0)}{W(2,0)}\right)^{r_1}\left(\tfrac{W(2,1)}{W(2,0)}\right)^{r_2} \\ b_{\mathbf{r}} &= \alpha_{\mathbf{r}}(([2]Q)-(Q))\left(\tfrac{W(0,3)}{W(0,2)}\right)^{r_1}\left(\tfrac{W(1,2)}{W(0,2)}\right)^{r_2} \\ c_{\mathbf{r}} &= \alpha_{\mathbf{r}}((P+Q)-(\mathcal{O}))W(2,1)^{r_1}W(1,2)^{r_2} \end{aligned}$$

(Illustration in overhead slides.)

So this can be viewed in two interesting ways: first, the generalised Jacobians explain the 'extra information' in the nets; second, the nets give a way to calculate the group law on the generalised Jacobian *using addition in the field.*