I was messing with elliptic divisibility sequences and Sage didn't do what I wanted

Katherine E. Stange
Stanford University

Sage Days, September 20th, 2011

Elliptic divisibility sequences

$E : y^2 = x^3 + Ax + B$ an elliptic curve, $\quad P$ a point on E.

Ψ_n – n-th *division polynomial*, vanishes at non-zero n-torsion

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

Ψ_n encode multiplication-by-n:

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

The sequence $\Psi_n(P)$ is an *elliptic divisibility sequence*.

Ward (1948): Anything satisfying (1) is $\Psi_n(P)$ for some (E, P).
(Possibly singular.)

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

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

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

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

Primes appearing in elliptic divisibility sequences

For primes of good reduction,

$$p \mid \Psi_n(P) \iff [n]P \equiv \mathcal{O} \pmod{p}$$

Example

n	1	2	3	4	5	6	7	8
Ψ_n	1	1	2	3	-5	$-2^2 \cdot 7$	-67	$-3 \cdot 137$

n	9	10	11	12
Ψ_n	$-2 \cdot 11 \cdot 23$	$5 \cdot 13 \cdot 167$	74231	$2^3 \cdot 3^2 \cdot 7 \cdot 1319$

Primes appearing in elliptic divisibility sequences

Let $p > 2$ be a prime of *good reduction* for E.
Let v_p be a discrete valuation associated to p.
Let N be the order of P modulo p.

$$v_p(\Psi_n(P)) = \begin{cases} v_p(\Psi_N(P)) + v_p(n/N) & N \mid n \\ 0 & N \nmid n \end{cases}$$

Example

$v_3(\Psi_n)$ for sequence $1, 1, 2, 3, \ldots$

$$\begin{array}{l} 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, \\ 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 3, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, \\ 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 3, \\ 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, \\ 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 4, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, \ldots \end{array}$$

The underlying reason is the formal group of E.

Let $E_0(\mathbb{Q}_p)$ be the points of non-singular reduction modulo p.

There's a filtration of subgroups of $E_0(\mathbb{Q}_p)$:

$$E_0(\mathbb{Q}_p) \supset E_1(\mathbb{Q}_p) \supset E_2(\mathbb{Q}_p) \supset \dots$$

where

$$E_k(\mathbb{Q}_p) = \{P \in E_0(\mathbb{Q}_p) : P \equiv \mathcal{O} \pmod{p^k}\}.$$

The theory of formal groups says that for $k \geq 1$,

$$\frac{E_k(\mathbb{Q}_p)}{E_{k+1}(\mathbb{Q}_p)} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

I wanted to know about bad primes

Example

$$1, 3, 2 \cdot 3, 3^2, 3^3, 2^2 \cdot 3^4, 3^6 \cdot 5, 3^7 \cdot 13, 2 \cdot 3^{10}, \dots$$

has $v_3(\Psi_n)$:

$$0, 1, 1, 2, 3, 4, 6, 7, 10, 11, 14, 16, 19, 22, 25, 29, 32, 38, 40, 45, 49,$$
$$54, 59, 64, 70, 75, 82, 87, 94, 100, 107, 114, 121, 129, 136, 146,$$
$$152, 161, 169, 178, 187, 196, 206, 215, 226, 235, 246, 256, 267, \dots$$

The associated curve E has split multiplicative reduction at 3.
The associated point P reduces to the node.

P has singular reduction

Theorem (S.)

Let $p \neq 2$. Consider an elliptic curve $E/\mathbb{Q}_p$ and $P \in E(\mathbb{Q}_p)$ a non-torsion point. Then there are integers

$$a, \ell, c_1, c_2, c_3, c_4, c_5$$

such that

$$v_p(\Psi_n(P)) = \frac{1}{c_1}\left(R_n(a,\ell) + c_2 n^2 + c_3 + \begin{cases} c_4 + v_p(n) & c_5 \mid n \\ 0 & c_5 \nmid n \end{cases}\right).$$

where

$$R_n(a,\ell) = \left\lfloor \frac{n^2\widehat{a}(\ell - \widehat{a})}{2\ell} \right\rfloor - \left\lfloor \frac{\widehat{na}(\ell - \widehat{na})}{2\ell} \right\rfloor.$$

where $\widehat{x}$ denotes the least non-negative residue of x modulo ℓ.

The bad primes example

Example

$$1, 3, 2 \cdot 3, 3^2, 3^3, 2^2 \cdot 3^4, 3^6 \cdot 5, 3^7 \cdot 13, 2 \cdot 3^{10}, \ldots$$

has $v_3(\Psi_n)$:

$$0, 1, 1, 2, 3, 4, 6, 7, 10, 11, 14, 16, 19, 22, 25, 29, 32, 38, 40, 45, 49,$$
$$54, 59, 64, 70, 75, 82, 87, 94, 100, 107, 114, 121, 129, 136, 146,$$
$$152, 161, 169, 178, 187, 196, 206, 215, 226, 235, 246, 256, 267, \ldots$$

The associated curve E has split multiplicative reduction at 3.
The associated point P reduces to the node.

$$c_1 = 1,\ c_2 = -1,\ c_3 = 1,\ c_4 = -1,\ c_5 = 18,\ a = 4,\ \ell = 9.$$

Everything has a meaning pertaining to reduction modulo 3:
e.g. $\ell = v_3(\Delta_E)$, $[c_5]P \equiv \mathcal{O} \pmod 3$.

Integral points on elliptic curves

Theorem (Siegel)

Any elliptic curve $E/\mathbb{Q}$ has only finitely many integral points.

How many?

Silverman and Hindry: A uniform bound assuming Lang's conjecture, or for curves with integral j-invariant.

How big?

e.g. Fix P; how big can n be such that $[n]P$ is integral?

Theorem (S.)

There is a uniform constant C such that for all elliptic curves $E/\mathbb{Q}$ in minimal Weierstrass form, and non-torsion points $P \in E(\mathbb{Q})$, there is at most one value of

$$n > C\frac{h(E)}{\widehat{h}(P)}$$

such that $[n]P$ is integral.

$$h(p/q) = \log\max\{|p|, |q|\}$$

$$h(E) = \max\{h(j_E), \log\max\{4|A|, 4|B|\}\}$$

$$\widehat{h}(P) = \frac{1}{2}\lim_{n\to\infty}\frac{h(x([2^n]P))}{4^n}$$

Theorem (S.)

There is a uniform constant C such that for all elliptic curves $E/\mathbb{Q}$ in minimal Weierstrass form, and non-torsion points $P \in E(\mathbb{Q})$, there is at most one value of

$$n > C\frac{h(E)}{\widehat{h}(P)}$$

such that $[n]P$ is integral.

Conjecture (Lang)

There is a constant C_L such that for any elliptic curve $E/\mathbb{Q}$ in minimal Weierstrass form, and non-torsion point $P \in E(\mathbb{Q})$,

$$\widehat{h}(P) \geq C_L h(E).$$

Recall that

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

The gcd

$$gcd(\Psi_n(P), \phi_n(P))$$

is supported on the bad primes.

Lemma (S.)

Let $D_n \in \mathbb{Z}$ be the denominator of $[n]P \in E(\mathbb{Q})$. Then I show

$$\log D_n \leq \log |\Psi_n(P)| \leq \log D_n + \frac{n^2+1}{3} \log |\Delta_E|.$$

Proof of theorem Method of Patrick Ingram (linear forms in elliptic logarithms), with this estimate plugged in.