p-adic Properites of Elliptic Divisibility Sequences

Joseph H. Silverman

Brown University

ICMS Workshop on
Number Theory and Computability
Edinburgh, Scotland

Wednesday, June 27, 2007

Elliptic Divisibility Sequences As Recursions

An **Elliptic Divisibility Sequence** (EDS) is a sequence $\mathcal{W} = (W_n)$ defined by a recursion of the form

$$W_0 = 0, \quad W_1 = 1, \quad W_2 W_3 \neq 0, \quad W_2 \mid W_4,$$
$$W_{m+n} W_{m-n} = W_{m+1} W_{m-1} W_n^2 - W_{n+1} W_{n-1} W_m^2$$

If $W_1, \ldots, W_4 \in \mathbb{Z}$, then:

- $W_n \in \mathbb{Z}$ for all $n \geq 0$.
- If $m \mid n$, then $W_m \mid W_n$. Thus $\mathcal{W}$ is a **divisibility sequence**.
- In fact, it is a **strong divisibility sequence**:

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

Aritmetic properties of EDS were first studied by Morgan Ward in the 1940's.

EDS and Elliptic Curves

Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and let $P \in E(\mathbb{Q})$ be a nontorsion point.

We write the multiples of P as

$$nP = \left(\frac{A_{nP}}{D_{nP}^2}, \frac{B_{nP}}{D_{nP}^3} \right).$$

Then the sequence $\mathcal{D} = (D_n)$ is a (strong) divisibility sequence.

Further, if P is nonsingular modulo p for all primes and if we assign signs properly to the D_n, then $\mathcal{D}$ satisfies the EDS recursion.

The Growth Rate of Elliptic Divisibility Sequences

Here is the elliptic divisibility sequence starting $1, 1, 1, -1$.

$$1,\ 1,\ 1,\ -1,\ -2,\ -3,\ -1,\ 7,\ 11,\ 20,\ -19,\ -87,\ -191,\ \ldots$$

It is associated to the point $P = (0, 0)$ on the curve $y^2 + y = x^3 + x^2$.

Don't be fooled by this example into thinking that EDS grow slowly.

Theorem. (Siegel + Néron-Tate) Let (W_n) be an EDS associated to a point $P \in E(\mathbb{Q})$. Then

$$\log |W_n| \sim \hat{h}(P) n^2 \qquad \text{as } n \to \infty.$$

For the EDS starting $1, 1, 1, -1$, we have

$$|W_n| \approx 1.0319^{n^2},$$

so for example W_{100} has about 136 digits.

Variation of the Sign

The sign of an EDS varies rather irregularly. It is not hard to describe the variation, but there are several cases. Here is a representative example.

Theorem. (Stephens-JS) Assume that P is in the identity component of $E(\mathbb{R})$. Then there is a $\beta \in \mathbb{R} \smallsetminus \mathbb{Q}$ and a $\nu \in \{0,1\}$ so that

$$\operatorname{Sign}(W_n) = (-1)^{[n\beta]+\nu} \qquad \text{for all } n \geq 1.$$

Example. Continuing with the EDS that starts $1, 1, 1, -1$,

$$\operatorname{Sign}(W_n) = (-1)^{[n\beta]} \text{ with } \beta = \frac{1}{2}\log_{|q|}(u) = 0.280058\ldots.$$

Here q and u are from the Jacobi parametrization

$$E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}} \quad \text{and} \quad P \leftrightarrow u.$$

Division Polynomials

Ward noted that the division polynomials of an elliptic curve satisfy the EDS recursion. This insight allows one to study EDS using the theory of elliptic functions.

Definition. Let E be an elliptic curve. The n^{th} **division polynomial** F_n is the (suitably normalized) rational function on E whose zeros and poles are

$$\operatorname{div}(F_n) = \sum_{T \in E[n]} (T) - n^2(\mathcal{O}).$$

Theorem. (Ward) Let (W_n) be a nondegenerate elliptic divisibility sequence. Then there exists an elliptic curve $E/\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$ so that

$$W_n = F_n(P) \qquad \text{for all } n \geq 1.$$

N.B. May need a nonminimal Weierstrass equation.

The Classical Theory of Elliptic Functions

An elliptic curve E over $\mathbb{C}$ has a complex uniformization

$$\mathbb{C}/L \xrightarrow{\sim} E(\mathbb{C}).$$

Here L is a lattice in $\mathbb{C}$ and the map is given by the classical Weierstrass $\wp$ function and its derivative.

Integrating $-\wp$ twice and exponentiating gives the **Weierstrass σ function**:

$$\sigma(z;L) = z \prod_{\substack{\omega \in L \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right) e^{(z/\omega)+\frac{1}{2}(z/\omega)^2}.$$

The σ function is not itself an elliptic function, i.e., it is not periodic for L. However, it has a simple transformation formula and can be used to build elliptic functions.

Building the Division Polynomials from the σ Function

Proposition. Let $P \in E$ correspond to $z \in \mathbb{C}/L$. Then the (normalized) division polynomial is given by

$$F_n(P) = \frac{\sigma(nz; L)}{\sigma(z; L)^{n^2}}$$

This formula for F_n, Ward's theorem expressing EDS in terms of F_n, and a product formula for σ are the ingredients that go into determining $\mathrm{Sign}(W_n)$.

Why Study Elliptic Divisibility Sequences?

Here are some possible answers to this question.

(1) They are the "simplest" nontrivial nonlinear recursions.

(2) Ward's theorem $W_n = F_n(P)$ allows us to study nontorsion points in $E(\mathbb{Q})$ via the EDS recursion.

(3) All EDS are defined by a single universal relation; only the three initial values change.

(4) EDS grow extremely rapidly, but in a manner that can be precisely characterized.

Don Zagier (1996) suggested that one might try to develop the entire theory of elliptic curves, and possibly even the theory of modular functions, starting with just the EDS recursion formula.

Elliptic Divisibility Sequences Modulo p

It is natural to study the behavior of EDS modulo p, or more generally modulo p^e.

Definition. Let $p \geq 3$ and assume that $p \nmid W_2 W_3$. The **rank of apparition of p in (W_n)** is the smallest value of n such that $p \mid W_n$.

In other words, W_{r_p} is the first term in the sequence divisible by p.

Recall that p is a **primitive divisor of W_n** if $p \mid W_n$ and $p \nmid W_i$ for $i < n$. Then the basic theorem on primitive divisors discussed by Everest on Monday says:

Theorem. Let (W_n) be an EDS. Then

$$\{r_p : p \text{ prime}\}$$

contains all but finitely many natural numbers.

Periodicity Properties of Elliptic Divisibility Sequences

It is not clear that $r_p < \infty$, i.e., that every prime p divides some term in the sequence, but this is true. More generally:

Theorem. (a) (Ward 1948) $W_n \bmod p$ is purely periodic with period rt, where

$$r = r_p \le 2p+1 \qquad \text{and} \qquad t \mid p-1.$$

(b) (Shipsey 2001) $r_p \le p + 1 + 2\sqrt{p}$.

(c) (Ayad 1993) $W_n \bmod p^e$ is purely periodic with period

$$p^{\max\{e-e_0,0\}} rt, \quad \text{where} \quad e_0 = \operatorname{ord}_p(W_r).$$

Proof. (a,b) Elliptic functions.
(c) The EDS recursion and explicit addition formulas.

An Explicit Periodicity Formula

Under some mild assumptions, Ayad more-or-less proves the following result.

Theorem. (Ayad) For all $e \ge 1$ there are constants A_e and B_e so that for all $k, n \in \mathbb{Z}$,

$$W_{kp^{e-1}r+n} \equiv A_e^{kn} \cdot B_e^{k^2} \cdot W_n \pmod{p^e}.$$

(This was originally proved by Ward for $e = 1$, and Shipsey and Swart studied some higher congruences in their theses.)

Ayad's mild assumptions are

$$p \ge 3, \quad r = r_p \ge 3, \quad \text{and} \quad \tilde{P} \text{ is nonsingular in } E(\mathbb{F}_p).$$

For the remainder of this talk, I will assume that these conditions are satisfied.

p-adic Convergence of Elliptic Divisibility Sequences

Theorem 1. Given an elliptic divisibility sequence (W_n) and a prime p, there exists a power $q = p^N$ so that for all $m \ge 1$, the limit

$$\widehat{W}_{m,q} \stackrel{\text{def}}{=} \lim_{k\to\infty} W_{mq^k} \quad \text{converges in } \mathbb{Z}_p.$$

Proof. Use Ayad's formula to show that the sequence is $\mathbb{Z}_p$-Cauchy.

Remark. $\widehat{W}_{m,q}$ only depends on m modulo q.

Theorem 2. Assume in addition that the underlying elliptic curve is ordinary at p. (This means that $\tilde{E}(\bar{\mathbb{F}}_p)[p] \ne 0$.) Then

$$\widehat{W}_{m,q} \text{ is algebraic over } \mathbb{Q}.$$

Proof Sketch of Theorem 2

The proof of Theorem 2 uses tools that may be useful for further investigations of p-adic properties of EDS.

Tools used in proof.

- Transformation formulas for division polynomials F_n.
- The Mazur-Tate p-adic σ-function, which we denote by σ_p.
- The Teichmüller character on $\mathbb{Z}_p^*$ and on $E(\mathbb{Q}_p)$.
- An elementary lemma on n^{th}-roots of p-adic convergent sequences.
- A case-by-case analysis depending, for example on whether

$$mP \equiv \mathcal{O} \pmod{p} \qquad \text{and/or} \qquad \#\tilde{E}(\mathbb{F}_p) = p.$$

Proof Sketch of Theorem 2 (continued)

Properties of the Mazur-Tate p-adic σ-function.

- σ_p only exists if E is ordinary at p.
- Let $E_1(\mathbb{Q}_p)$ be the formal group of E, i.e., the kernel of reduction,

$$E_1(\mathbb{Q}_p) = \mathrm{Ker}\big(E(\mathbb{Q}_p) \longrightarrow \tilde{E}(\mathbb{F}_p)\big).$$

  The p-adic σ-function is defined on the formal group,

$$\sigma_p : E_1(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p.$$

- For points $Q \in E_1(\mathbb{Q}_p)$, the classical σ-function/division polynomial formula is valid:

$$F_n(Q) = \frac{\sigma_p(nQ)}{\sigma_p(Q)^{n^2}}.$$

Unfortunately, we need to evaluate F_n at $P \notin E_1(\mathbb{Q}_p)$.

Proof Sketch of Theorem 2 (continued)

Let $r = r_p$ be the order of P in $E(\mathbb{F}_p)$ and assume that

$$p \nmid rm \qquad \text{and} \qquad r \nmid m.$$

(This is one of the many cases that must be considered.)
We use the division polynomial transformation formula

$$F_{ab}(Q) = F_a(bQ)F_b(Q)^{a^2} \qquad (*)$$

and the Mazur-Tate formula

$$F_n(Q) = \frac{\sigma_p(nQ)}{\sigma_p(Q)^{n^2}}, \quad \text{valid for } Q \in E_1(\mathbb{Q}_p). \qquad (**)$$

Applying $(*)$ twice and then applying $(**)$ to $Q = rP \in E_1(\mathbb{Q}_p)$ yields

$$W_n^{r^2} = F_n(P)^{r^2} = \frac{\sigma_p(rnP)}{F_r(nP)} \left(\frac{F_r(P)}{\sigma_p(rP)} \right)^{n^2}. \qquad (***)$$

Proof Sketch of Theorem 2 (continued)

Now write

$$P = P' + T \quad \text{with} \quad P' \in E_1(\mathbb{Q}_p) \quad \text{and} \quad T \in E[r].$$

A careful analysis of

$$W_n^{r^2} = F_n(P)^{r^2} = \frac{\sigma_p(rnP')}{F_r(nP)} \left(\frac{F_r(P)}{\sigma_p(rP')} \right)^{n^2} \qquad (***)$$

shows that each of the two factors on the right-hand side has a p-adic limit if we take $n = mq^k$ and let $k \to \infty$. Roughly speaking:

$$\text{First Factor} \longrightarrow \text{“derivative of } F_r \text{ at } mT\text{”},$$
$$\text{Second Factor} \longrightarrow \text{root of unity} = \text{Teich}\big(F_r'(T)\big).$$

Finally, an elementary lemma shows that we can take a unique r^2-root to get the limit of W_n.

EDS Questions and Open Problems

(1) Is the limit in Theorem 2 algebraic in the supersingular case?

(2) Can one use EDS and/or Ayad's arguments to define the p-adic σ-function in the supersingular case. (This is very speculative.)

(3) Are the EDS limits in Theorems 1 and 2 related to values of p-adic height functions and/or to special values of p-adic L-functions?

(4) Graham already mentioned the question of whether there are only finitely many primes in an EDS, or more generally, only finitely many terms with a bounded number of prime factors.

(5) For higher rank elliptic nets (to be discussed by Stange on Thursday), are there infinitely many primes?

EDS Questions and Open Problems (continued)

(6) Let W_n and W'_n be independent EDS. Is it true that for every $\epsilon > 0$ we have

$$\gcd(W_n, W'_m) \le C(\epsilon) \max\bigl\{|W_n|, |W'_m|\bigr\}^{\epsilon} \ ?$$

This would follow from Vojta's conjecture. It is an elliptic analog of a theorem of Corvaja and Zannier concerning the growth rate of $\gcd(a^n - 1, b^n - 1)$.

(7) Let W_n and W'_n be independent EDS. Is

$$\gcd(W_n, W'_n) = 1 \quad \text{for infinitely many } n?$$

This is an elliptic analog of a conjecture of Ailon and Rudnick. To illustrate our present state of knowledge, it is currently not known whether

$$\gcd(2^n - 1, 3^n - 1) = 1$$

for infinitely many n.

Rapidly Growing Sequences and Primitive Divisors in Arithmetic Dynamics

Rapidly Growing Sequences in Arithmetic Dynamics

Let

$$\phi(z) \in \mathbb{Q}(z)$$

be a rational function of degree $d \geq 2$ and let $\alpha \in \mathbb{Q}$ be an initial point. For each $n \geq 0$, write

$$\phi^n(\alpha) = (\phi \circ \phi \circ \cdots \circ \phi)(\alpha) = \frac{A_n}{B_n} \in \mathbb{Q}$$

as a fraction in lowest terms. We assume that α is not **preperiodic**, i.e.,

$$\phi^n(\alpha) \neq \phi^m(\alpha) \quad \text{for all } n \neq m.$$

Theorem. (JS) If $\phi^2(z) \notin \mathbb{Q}[1/z]$, then

$$\lim_{n\to\infty} \frac{\log|A_n|}{d^n} = \hat{h}_\phi(\alpha) > 0.$$

Primitive Divisors in Dynamical Sequences

The theorem says that the sequence (A_n) grows extremely rapidly:

$$|A_n| \approx C^{d^n} \quad \text{for some } C = C(\phi, \alpha) > 1.$$

It is natural to ask for the existence of primitive divisors in the sequence (A_n). Here is a sample result.

Theorem. (JS) Assume that

$$\phi(0) = 0 \quad \text{and} \quad \phi'(0) \in \mathbb{Z}.$$

Then all but finitely many terms in the sequence (A_n) have a primitive prime divisor.

Remarks

(1) A similar statement is true over number fields.

(2) It suffices to assume that 0 is a periodic point with integral multiplier.

Some Open Problems About Dynamical Sequences

(1) What happens if we do not require $\phi'(0) \in \mathbb{Z}$? This leads to p-adic chaotic behavior for primes p dividing the denominator of $\phi'(0)$.

(2) What happens if 0 has an infinite orbit?

(3) There are dynamial analogs of division polynomials. The **n'th dynatomic polynomial for ϕ** is a polynomial $\Phi_{\phi,n}$ whose roots are the points of period n for ϕ. What can one say about the arithmetic properties of the (numerators of the) sequence

$$\big(\Phi_{\phi,n}(\alpha)\big)_{n\ge 1}?$$

p-adic Properites of Elliptic Divisibility Sequences

Joseph H. Silverman

Brown University

ICMS Workshop on
Number Theory and Computability
Edinburgh, Scotland

Wednesday, June 27, 2007