A dynamical system for elliptic divisibility sequences

Katherine E. Stange
Stanford University

in joint work with
Joseph H. Silverman
Brown University

Joint Math Meetings, Dynamical systems in algebraic and arithmetic geometry, January 4th, 2012

A Question

For any integer sequence $(D_n)_{n\geq 1}$ we define the *index divisibility set* of D to be

$$\mathcal{S}(D) = \{n \geq 1 : n \mid D_n\}.$$

Ex: $\mathcal{S}(D)$ for $D_n = b^n - b$ are pseudoprimes to the base b.

Strong divisibility sequences

Definition

An integer sequence $D_n, n \geq 1$ is a *divisibility sequence* if

$$n \mid m \implies D_n \mid D_m.$$

The sequence is a *strong divisibility sequence* if in addition

$$\gcd(D_n, D_m) \mid D_{\gcd(n,m)}.$$

Example (Fibonacci numbers)

n	1	2	3	4	5	6	7	8	9	10	11	12	13
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233

Example (An elliptic divisibility sequence)

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
F_n	1	1	1	1	2	1	3	5	7	4	23	29	59	129

Rank of apparition

Definition

The *rank of apparition* of an integer $n \geq 1$ is

$$r_n = \min_{k>0}\{D_k \equiv 0 \pmod{n}\}$$

- The sequence r_n itself is a divisibility sequence: $n \mid m \implies r_n \mid r_m$.

Example (Fibonacci numbers)

n	1	2	3	4	5	6	7	8	9	10	11	12	13
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233

Ranks of apparition:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
r_n	1	3	4	6	5	12	8	6	12	15	10	12	7

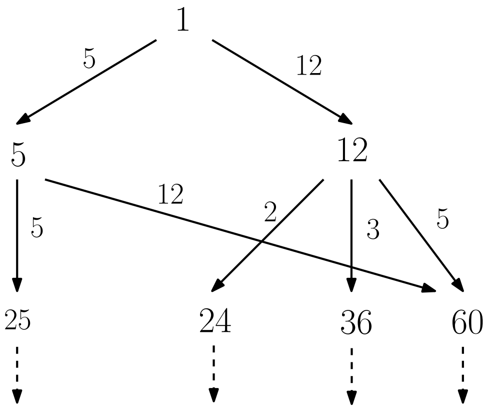
Index divisibility

Suppose $n \in \mathcal{S}(D)$, and p coprime to n satisfies $r_p = p$. Then $np \mid D_{np}$.

So if $n \in \mathcal{S}(D)$, then $np \in \mathcal{S}(D)$.

Make $\mathcal{S}(D)$ a directed graph with arrows $Arrow(D)$.

Index divisibility graph for Fibonacci numbers



n	1	2	3	4	5	6	7	8	9	10	11	12	13
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233

A Theorem of Smyth

Theorem (Smyth)

Let $a, b \in \mathbb{Z}$, and let $L = (L_n)_{n \geq 1}$ be the associated Lucas sequence of the first kind, i.e.,

$$L_{n+2} = aL_{n+1} - bL_n, \qquad L_0 = 0, \quad L_1 = 1.$$

Let $\delta = a^2 - 4b$ and let $n \in \mathcal{S}(L)$ be a vertex. Then the arrows originating at n are

$$\{n \to np : p \text{ is prime and } p \mid L_n\delta\} \cup \mathcal{B}_{a,b,n},$$

where

$$\mathcal{B}_{a,b,n} = \begin{cases} \{n \to 6n\} & \text{if } (a,b) \equiv (3, \pm 1) \pmod 6, (6, L_n) = 1, \\ \{n \to 12n\} & \text{if } (a,b) \equiv (\pm 1, -1) \pmod 6, (6, L_n) = 1, \\ \emptyset & \text{otherwise.} \end{cases}$$

A dynamical system

Let D_n be a divisibility sequence. Define $\phi_D : \mathbb{Z}^{>0} \to \mathbb{Z}^{>0}$ be defined by

$$\phi_D(n) = r_n.$$

Example

Let F_n be the Fibonacci numbers. Then $\phi_F(5) = 5$ is the unique fixed point of ϕ_F.

Fibonacci numbers: Are there any 2-cycles consisting of prime numbers?

For the Fibonacci numbers F_n, and any prime number p, we have

$$r_p \mid p^2 - 1.$$

Suppose $\phi_F(p) = q$ and $\phi_F(q) = p$, for p, q odd primes. Then

$$q \mid (p+1)(p-1) \implies q \leq \frac{p+1}{2}$$

and similarly for p. So

$$q \leq \frac{p+1}{2}, \quad p \leq \frac{q+1}{2}.$$

So the answer is NO.

Elliptic divisibility sequences

Definition

Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$ be a non-torsion point. The *elliptic divisibility sequence* (EDS) associated to the pair (E, P) is the sequence of positive integers D_n for $n \geq 1$ determined by

$$x\big([n]P\big) = \frac{A_n}{D_n^2} \in \mathbb{Q}$$

as a fraction in lowest terms.

Index divisibility in an EDS

Example

$$D_n : 1, 1, 1, 1, 2, 1, 3, 5, 7, 4, 23, 29, 59, 129,$$
$$314, 65, 1529, 3689, 8209, 16264, 83313, \ldots$$

$$E : y^2 + y = x^3 - x, \qquad P = (0, 0).$$

$$\mathcal{S}(D) = \{1, 40, 53, 63, 80, 127, 160, 189, 200, 320, 400, 441, 443, \ldots\}.$$

$$D_{40} = 40 \cdot 13526278251270010,$$
$$D_{53} = 53 \cdot 2997411336915768774003707557471.$$

Index divisibility for EDS

Theorem

Let D be a minimal regular EDS associated to the elliptic curve $E/\mathbb{Q}$ and point $P \in E(\mathbb{Q})$.

1. *If $n \in \mathcal{S}(D)$ and p is prime and $p \mid D_n$, then $(n \to np) \in \mathrm{Arrow}(D)$.*
2. *If $n \in \mathcal{S}(D)$ and d is an aliquot number for D and $\gcd(n, d) = 1$, then $(n \to nd) \in \mathrm{Arrow}(D)$.*
3. *If $p \geq 7$ is a prime of good reduction for E and if $(n \to np) \in \mathrm{Arrow}(D)$, then either $p \mid D_n$ or p is an aliquot number for D.*
4. *If $\gcd(n, d) = 1$ and if $(n \to nd) \in \mathrm{Arrow}(D)$ and if $d = p_1 p_2 \cdots p_\ell$ is a product of $\ell \geq 2$ distinct primes of good reduction for E satisfying $\min p_i > (2^{-1/2\ell} - 1)^{-2}$, then d is an aliquot number for D.*

Aliquot Number

Definition

Let D_n be an EDS, and let $p_1, \ldots, p_\ell$ be an ℓ-cycle for ϕ_D. That is,

$$p_{i+1} = r_{p_i} \qquad \text{for all } 1 \leq i \leq \ell,$$

(define $p_{\ell+1} = p_1$). Then $p_1 \cdots p_\ell$ is an *aliquot number*.

Fact

$p \mid D_n$ if and only if $[n]P = \mathcal{O} \pmod{p}$.

- So, if $\#E(\mathbb{F}_{p_i}) = p_{i+1}$ for each i, then the definition is satisfied.
- An anomalous prime ($\#E(\mathbb{F}_p) = p$) is an aliquot number.

Amicable Pairs

Definition

Let E be an elliptic curve defined over $\mathbb{Q}$. A pair (p, q) of primes is called an ***amicable pair*** for E if

$$\#E(\mathbb{F}_p) = q, \qquad \text{and} \qquad \#E(\mathbb{F}_q) = p.$$

Example

$y^2 + y = x^3 - x$ has one amicable pair with $p, q < 10^7$:

$$(1622311, 1622471)$$

$y^2 + y = x^3 + x^2$ has four amicable pairs with $p, q < 10^7$:

$$(853, 883), \quad (77761, 77999),$$
$$(1147339, 1148359), \quad (1447429, 1447561).$$

Aliquot cycles

Definition

An *aliquot cycle of length* ℓ for $E/\mathbb{Q}$ is a sequence of distinct primes $(p_1, p_2, \ldots, p_\ell)$ such that

$$\#E(\mathbb{F}_{p_1}) = p_2, \quad \#E(\mathbb{F}_{p_2}) = p_3, \quad \ldots \\ \#E(\mathbb{F}_{p_{\ell-1}}) = p_\ell, \quad \#E(\mathbb{F}_{p_\ell}) = p_1.$$

Example

$$y^2 = x^3 - 25x - 8 : (83, 79, 73)$$

$$E : y^2 = x^3 + 176209333661915432764478x + \\ 60625229794681596832262 :$$

$$(23, 31, 41, 47, 59, 67, 73, 79, 71, 61, 53, 43, 37, 29)$$

Constructing aliquot cycles with CRT

Let $p_1, p_2, \ldots, p_\ell$ be a sequence of primes such that

$$|p_i + 1 - p_{i+1}| \le 2\sqrt{p_i} \quad \text{for all } 1 \le i \le \ell,$$

(where $p_{\ell+1} = p_1$). For each p_i find (by Deuring) an elliptic curve $E_i/\mathbb{F}_{p_i}$ satisfying

$$\#E_i(\mathbb{F}_{p_i}) = p_{i+1}.$$

By the Chinese remainder theorem, find $E/\mathbb{Q}$ such that

$$E \bmod p_i \cong E_i \quad \text{for all } 1 \le i \le \ell.$$

Then $(p_1, \ldots, p_\ell)$ is an aliquot cycle of length ℓ for $E/\mathbb{Q}$.

A growth rate question

Question

Let

$$\mathcal{Q}_E(X) = \#\{\text{amicable pairs } (p, q) \text{ such that } p, q < X\}$$

How does $\mathcal{Q}_E(X)$ grow with X?

Heuristic

$$\begin{aligned}&\mathrm{Prob}(p \text{ is part of an amicable pair})\\ &\quad = \mathrm{Prob}(q \overset{\text{def}}{=} \#E(\mathbb{F}_p) \text{ is prime})\,\mathrm{Prob}(\#E(\mathbb{F}_q) = p).\end{aligned}$$

Conjecture of Koblitz:

$$\mathrm{Prob}(\#E(\mathbb{F}_p) \text{ is prime}) \asymp \frac{1}{\log p},$$

Conjecture of Sato–Tate:

$$\mathrm{Prob}(\#E(\mathbb{F}_q) = p) \asymp \frac{1}{\sqrt{q}} \sim \frac{1}{\sqrt{p}}.$$

Together:

$$\mathrm{Prob}(p \text{ is part of an amicable pair}) \asymp \frac{1}{\sqrt{p}(\log p)}.$$

$$\mathcal{Q}_E(X) \asymp \frac{\sqrt{X}}{(\log X)^2}$$

Conjectures

$$\mathcal{Q}_E(X) = \#\{\text{amicable pairs } (p,q) \text{ such that } p,q < X\}$$

Conjecture (Version 1)

Assume infinitely many primes p such that $\#E(\mathbb{F}_p)$ is prime.

Then

$$\mathcal{Q}_E(X) \asymp \frac{\sqrt{X}}{(\log X)^2} \quad \text{as } X \to \infty,$$

where the implied constants depend on E.

Unfortunately, Andrew Sutherland has only been able to find 117 amicable pairsless than 10^{12} on $y^2 + y = x^3 + x^2$.

Another example

$y^2 + y = x^3 - x$ has one amicable pair with $p, q < 10^7$:

$$(1622311, 1622471)$$

$y^2 + y = x^3 + x^2$ has four amicable pairs with $p, q < 10^7$:

$$(853, 883), \quad (77761, 77999),$$
$$(1147339, 1148359), \quad (1447429, 1447561).$$

$y^2 = x^3 + 2$ has 5578 amicable pairs with $p, q < 10^7$:

$$(13, 19), (139, 163), (541, 571), (613, 661), (757, 787), \ldots.$$

CM case: Twist Theorem

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve ($j \neq 0$) with complex multiplication. Suppose that p and q are primes of good reduction for E with $p \geq 5$ and $q = \#E(\mathbb{F}_p)$.

Then either

$$\#E(\mathbb{F}_q) = p \qquad \text{or} \qquad \#E(\mathbb{F}_q) = 2q + 2 - p.$$

Remark: In the latter case, $\#\tilde{E}(\mathbb{F}_q) = p$ for the non-trivial quadratic twist $\tilde{E}$ of E over $\mathbb{F}_q$.

Pairs on CM curves

(D, f)	(3,3)	(11,1)	(19,1)	(43,1)	(67,1)	(163,1)
$X = 10^4$	18	8	17	42	48	66
$X = 10^5$	124	48	103	205	245	395
$X = 10^6$	804	303	709	1330	1671	2709
$X = 10^7$	5581	2267	5026	9353	12190	19691

Table: $\mathcal{Q}_E(X)$ for elliptic curves with CM

(D, f)	(3,3)	(11,1)	(19,1)	(43,1)	(67,1)	(163,1)
$X = 10^4$	0.217	0.250	0.233	0.300	0.247	0.237
$X = 10^5$	0.251	0.238	0.248	0.260	0.238	0.246
$X = 10^6$	0.250	0.247	0.253	0.255	0.245	0.247
$X = 10^7$	0.249	0.251	0.250	0.251	0.250	0.252

Table: $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ for elliptic curves with CM

Conjectures

$$\mathcal{Q}_E(X) = \#\{\text{amicable pairs } (p,q) \text{ such that } p,q < X\}$$

Conjecture (Version 2)

Assume infinitely many primes p such that $\#E(\mathbb{F}_p)$ is prime.

(a) If E does not have CM, then

$$\mathcal{Q}_E(X) \asymp \frac{\sqrt{X}}{(\log X)^2} \quad \text{as } X \to \infty,$$

where the implied constants depend on E.

(b) If E has CM, then there is a constant $A_E > 0$ such that

$$\mathcal{Q}_E(X) \sim A_E \frac{X}{(\log X)^2}.$$