Elliptic divisibility sequences

Katherine E. Stange
Stanford University

Berkeley Algebraic Dynamics, May 13th, 2012

Happy Mother's Day, Mom!

An integer sequence

$$W_{n+m}W_{n-m}W_1^2 = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2 \qquad (*)$$

$$\textit{e.g.}, 1, 1, 1, -1, -2, -3, -1, 7, 11, 20, -19, -87, -191,$$
$$-197, 1018, 2681, 8191, -5841, -81289, -261080\ldots$$

If $W_1 = 1$, $W_2, W_3, W_4/W_2 \in \mathbb{Z} \setminus \{0\}$, then W_n is entirely integer. Why?

An integer sequence

$$W_{n+m}W_{n-m}W_1^2 = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2 \qquad (*)$$

$$e.g., 1, 1, 1, -1, -2, -3, -1, 7, 11, 20, -19, -87, -191,$$
$$-197, 1018, 2681, 8191, -5841, -81289, -261080\ldots$$

If $W_1 = 1$, $W_2, W_3, W_4/W_2 \in \mathbb{Z} \setminus \{0\}$, then W_n is entirely integer. Why?

1. Induction.

An integer sequence

$$W_{n+m}W_{n-m}W_1^2 = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2 \qquad (*)$$

e.g., $1, 1, 1, -1, -2, -3, -1, 7, 11, 20, -19, -87, -191,$
$-197, 1018, 2681, 8191, -5841, -81289, -261080\ldots$

If $W_1 = 1$, $W_2, W_3, W_4/W_2 \in \mathbb{Z} \setminus \{0\}$, then W_n is entirely integer. Why?

1. Induction.
2. $|W_n|$ counts perfect matchings on certain graphs (Bousquet-Mélu–West, REACH, Speyer)

An integer sequence

$$W_{n+m}W_{n-m}W_1^2 = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2 \qquad (*)$$

$e.g.$, $1, 1, 1, -1, -2, -3, -1, 7, 11, 20, -19, -87, -191,$
$-197, 1018, 2681, 8191, -5841, -81289, -261080\dots$

If $W_1 = 1$, W_2, W_3, $W_4/W_2 \in \mathbb{Z} \setminus \{0\}$, then W_n is entirely integer. Why?

1. Induction.
2. $|W_n|$ counts perfect matchings on certain graphs (Bousquet-Mélu–West, REACH, Speyer)
3. Laurentness of W_n in terms of W_1, W_2, W_3, W_4 (Fomin–Zelevinsky: cluster algebras)

An integer sequence

$$W_{n+m}W_{n-m}W_1^2 = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2 \qquad (*)$$

$$e.g., 1, 1, 1, -1, -2, -3, -1, 7, 11, 20, -19, -87, -191,$$
$$-197, 1018, 2681, 8191, -5841, -81289, -261080 \ldots$$

If $W_1 = 1$, $W_2, W_3, W_4/W_2 \in \mathbb{Z} \setminus \{0\}$, then W_n is entirely integer. Why?

1. Induction.
2. $|W_n|$ counts perfect matchings on certain graphs (Bousquet-Mélu–West, REACH, Speyer)
3. Laurentness of W_n in terms of W_1, W_2, W_3, W_4 (Fomin–Zelevinsky: cluster algebras)
4. W_n is the denominator of a point on an elliptic curve.

An integer sequence

$$W_{n+m}W_{n-m}W_1^2 = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2 \qquad (*)$$

e.g., $1, 1, 1, -1, -2, -3, -1, 7, 11, 20, -19, -87, -191,$
$-197, 1018, 2681, 8191, -5841, -81289, -261080 \ldots$

If $W_1 = 1$, $W_2, W_3, W_4/W_2 \in \mathbb{Z} \setminus \{0\}$, then W_n is entirely integer. Why?

1. Induction.
2. $|W_n|$ counts perfect matchings on certain graphs (Bousquet-Mélu–West, REACH, Speyer)
3. Laurentness of W_n in terms of W_1, W_2, W_3, W_4 (Fomin–Zelevinsky: cluster algebras)
4. W_n is the denominator of a point on an elliptic curve.

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

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

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

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

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

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

Division Polynomials

One defines elliptic functions Ψ_n on $E : y^2 = x^3 + Ax + B$ with

$$\begin{cases} \text{zeroes at the } n\text{-torsion points of } E, \\ \text{pole supported on } \mathcal{O}. \end{cases}$$

Then

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

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

$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \ldots$$

$$\Psi_n, \phi_n, \omega_n \in \mathbb{Z}[A, B, x, y]$$

Division Polynomials

One defines elliptic functions Ψ_n on $E : y^2 = x^3 + Ax + B$ with

$$\begin{cases} \text{zeroes at the } n\text{-torsion points of } E, \\ \text{pole supported on } \mathcal{O}. \end{cases}$$

Then

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

$$\Psi_1 = 1, \qquad \Psi_2 = 2y, \qquad \Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \ldots$$

$$\Psi_n, \phi_n, \omega_n \in \mathbb{Z}[A, B, x, y]$$

Ψ_n satisfy $(*)$

The recurrence relation encodes the group law.

Division Polynomials

One defines elliptic functions Ψ_n on $E : y^2 = x^3 + Ax + B$ with

$$\begin{cases} \text{zeroes at the } n\text{-torsion points of } E, \\ \text{pole supported on } \mathcal{O}. \end{cases}$$

Then

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

$$\Psi_1 = 1, \qquad \Psi_2 = 2y, \qquad \Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \ldots$$

$$\Psi_n, \phi_n, \omega_n \in \mathbb{Z}[A, B, x, y]$$

Ψ_n satisfy $(*)$

Note: $\gcd(\phi_n, \Psi_n) = 1$ in $\mathbb{Z}[A, B, x, y]$
$\gcd(\phi_n(P), \Psi_n(P))$ is supported on $p \mid \Delta_E$ for $P \in E(\mathbb{Q})$.

Thus $\Psi_n(P)$ is almost the denominator of $[n]P$ as a rational.

Elliptic divisibility sequences

Theorem (Ward, 1948)

If $W_n : \mathbb{Z} \to \mathbb{Q}$ *satisfies* $(*)$ *and* $W_1 = 1$*, then for some*

$$E : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q}, \quad P \in E(\mathbb{Q})$$

we obtain

$$W_n = \Psi_n(E, P).$$

Somos, Zagier: alternative foundation for elliptic/theta functions?

Ward's Correspondence

$$\left\{ \begin{array}{l} \text{elliptic divisibility} \\ \text{sequences} \\ W_n : \mathbb{Z} \to \mathbb{Q} \\ W_1 = 1, W_2 W_3 \neq 0 \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{curve-point pairs } (E, P) \\ E : y^2 = x^3 + Ax + B, \\ A, B \in \mathbb{Q}, P \in E(\mathbb{Q}) \\ P \notin E[2] \cup E[3] \end{array} \right\}$$

Elliptic, Multiplicative, Dynamical

Elliptic	Multiplicative	Dynamical
$\Psi_n(z)$	$x^n - 1$	
n-torsion	n-th roots of 1	
degree $\frac{n^2-1}{2}$	degree n	

The multiplicative sequence of polynomials is closely related to Lucas sequences, such as Fibonacci numbers (depth-two linear recurrences).

Elliptic, Multiplicative, Dynamical

Elliptic	Multiplicative	Dynamical
$\Psi_n(z)$	$x^n - 1$	$\phi^n(z) - z$
n-torsion	n-th roots of 1	period n
degree $\frac{n^2-1}{2}$	degree n	degree d^n

The multiplicative sequence of polynomials is closely related to Lucas sequences, such as Fibonacci numbers (depth-two linear recurrences).

EDS modulo p

Main Observation

If $p \nmid \Delta_E$, then

$$W_n \equiv 0 \pmod{p} \iff [n]P = \mathcal{O} \pmod{p} \text{ on } E$$

Definition

The rank of apparition r_p is

$$r_p = \min\{r \geq 1 : W_r \equiv 0 \pmod{p}\}$$

Note

If $p \nmid \Delta_E$, then r_p is the order of P modulo p.
By the Hasse bound, $r_p < p + 1 + 2\sqrt{p}$.

Primitive Divisors

Theorem (Silverman 1988)

For all sufficiently large n, W_n has a primitive divisor, i.e. a prime p such that $r_p = n$.

Divisibility

$$n \mid m \implies W_n \mid W_m$$

In fact, $\quad W_{\gcd(n,m)} = \gcd(W_n, W_m)$

Primes appearing in elliptic divisibility sequences

$p > 2$, good reduction
v_p the discrete valuation

$$v_p(W_n) = \begin{cases} v_p(W_{r_p}) + v_p(n/r_p) & r_p \mid n \\ 0 & r_p \nmid n \end{cases}$$

Example

$$W_n : \quad 1, 1, 2, 3, \ldots$$

$$v_3(W_n) :$$

$$0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2,$$
$$0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 3, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2,$$
$$0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 3, \ldots$$

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 $k \geq 1$,

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

Growth rate

1,
1,
3,
11,
38,
249,
2357,
8767,
496035,
3769372,
299154043,
12064147359,
632926474117,
65604679199921,
6662962874355342,
720710377683595651,
285131375126739646739,
52061747034847247 19135,
3604215776624692378883 7209,
14146372186375322613610002376,
1392607142093325246643577493 9177,
18907140173988982482283529896228001,
235633460974235657040938747031546 29107,
5261384319610660513180051011111076793 7939,
1910424746438412543757552724201369014393 12318,
20114356286861041671776028186810557052010 1027137,
509582199125499055223626535390012994946103658 2268645,
1619616042354576251961847118847539207230645302109465 2577,
390721759789017211388827166946590849427517620851066278956107,
59862800550349625879021174118566267998002605647683803723116 18644,
108902005168517871203290899980149905032338645609229377887214046958803,
40105964555339722329839406179275418892906132034496414296072201258599 83231,
15250620746565227776253146214239379101285644244123584071443010376281973 6595413,
528649172822313462640043111723426214253020950871850484923488956968408312589 2420201,
835397059891704991632636814121353141297683871830623235928141040342038068512341019315446,
10861789122218115292139551508417628820932571356531654998704845795890033629344542872385904645,
1335187608764981748605073273611954101623580211116392574773217113192642141130643615832345105750 8131,
2042977307842020707295863142858393936350596442010700266977612272386600979584155605002856821221263113151,
666758599738582427580962194986025574476589178060749335314959464037321543378395210027048006648288905711378993,
33316708658847856167209825975212203644033544158093267723708612909985155910861815688221530712645593855290823 1344016,
1508667302911383743310250456590052444494586956505489305431742613742983874555901417002336021629647219442014422744468 53073,
1137600657772348828650069406546548957188965200420250483064935150521493631662714106669634948134138364954378034196219820274 12929,
159253169967307321375677555136314569434529937177007635953107117202675658212866813320738037987472039386883798439657624623140677934307,
444163101673188802564614281909651939798541498443205797140275002837542739529893800448085178516630798250976861723342317516378378376732 62107, ...

Growth rate

1,
1,
3,
11,
38,
249,
2357,
8767,
496035,
3769372,
299154043,
12064147359,
632926474117,
65604679199921,
6662962874355342,
720710377683595651,
285131375126739646739,
5206174703484724719135,
36042157766246923788837209,
14146372186375322613610002376,
13926071420933252466435774939177,
18907140173988982482283529896228001,
23563346097423565704093874703154629107,
52613843196106605131800510111110767937939,
191042474643841254375755272420136901439312318,
201143562868610416717760281868105570520101027137,
5095821991254990552236265353900129949461036582268645,
16196160423545762519618471188475392072306453021094652577,
390721759789017211388827166946590849427517620851066278956107,
5986280055034962587902117411856626799800260564768380372311618644,
108902005168517871203290899980149905032338645609229377887214046958803,
4010596455533972232983940617927541889290613203449641429607220125859983231,
152506207465652277762531462142393791012856442441235840714430103762819736595413,
5286491728223134626400431117234262142530209508718504849234889569684083125892420201,
835397059891704991632636814121353141297683871830623235928141040342038068512341019315446,
10861789122218115292139551508417628820932571356531654998704845795890033629344542872385904645,
13351876087649817486050732736119541016235802111163925747732171131926421411306436158323451057508131,
2042977307842020707295863142858393936350596442010700266977612272386600979584155605002856821221263113151,
666758599738582427580962194986025574476589178060749335314959464037321543378395210027048006648288905711378993,
3331670865884785616720982597521220364403354415809326772370861290999851559108618156882215307126455938552908231344016,
1508667302911383743310250456590052444494586956505489305431742613742983874555901417002336021629647219442014422744446853073,
113760065777234882865006940654654895718896520042025048306493515052149363166271410666963494813413836495437803419621982027412929,
159253169967307321375677555136314569434529937177007635953107117202675658212866813320738037987472039386883798439657624623140677934307,
44416310167318880256461428190965193979854149844320579714027500283754273952989380044808517851663079825097686172334231751637837837673262107, ...

$$C^{n^2}$$

Primitive Divisors

Theorem (Silverman 1988)

For all sufficiently large n, W_n has a primitive divisor, i.e. a prime p such that $r_p = n$.

Proof:

- Sequence grows quickly.
- Contribution from earlier primes is bounded.

Hilbert's Tenth Problem

$H10(R)$: decideability of $\exists X_1, \ldots, X_n : f(X_1, \ldots, X_n) = 0$ in R.
$R = \mathbb{Z}$: undecideable (Davis–Matiyasevich–Putnam–Robinson)
$R = \mathbb{Q}$: not known

A conjecture of Cornelissen and Zahidi similar to Silverman's Theorem implies the undecidability of $\forall\exists f(X)$ in $\mathbb{Q}$.

Idea: EDS give description of $\mathbb{Z}$ in $\mathbb{Q}$.

Undecideability of $\forall\exists f(X)$ proven by Poonen in 2008.

Primitive Divisors

Let $\phi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \geq 2$, and let $\alpha \in \mathbb{Q}$ be a ϕ-wandering point.

Theorem (Ingram, Silverman)

Suppose $\phi(0) = 0$ but ϕ does not vanish to order d at $z = 0$. Write in lowest terms

$$\phi^n(\alpha) = \frac{A_n}{B_n}.$$

For sufficiently large n, A_n has a primitive divisor.

Conjecture (Ingram, Silverman)

Write in lowest terms

$$\phi^n(\alpha) - \alpha = \frac{A_n}{B_n}.$$

For sufficiently large n, A_n has a primitive divisor.

Index divisibility

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.

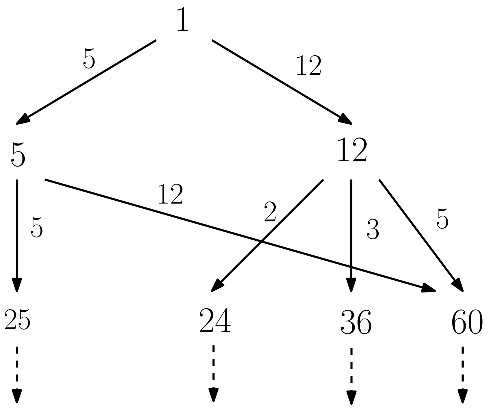
Index divisibility

Assume a divisibility sequence.
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 $a, b \in \mathbb{Z}$. *Define* $L = (L_n)_{n \geq 1}$ *by*

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

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 prime 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 $p \neq 5$, 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.

Index divisibility in an EDS

Warning: use denominator definition.

Example

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

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

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

$$D_{40} = 40 \cdot 13526278251270010,$$
$$D_{53} = 53 \cdot 29974113369157687740037075747 1.$$

Index divisibility for EDS

Theorem (Silverman, S.)

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 $(n \to nd) \in \mathrm{Arrow}(D)$.*

Index divisibility for EDS

Theorem (Silverman, S.)

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*.

Elliptic nets

If an elliptic divisibility sequence reflects a cyclic subgroup of $E(\mathbb{Q})$, can we do the same for any subgroup?

Elliptic nets

On an elliptic curve $E : y^2 = x^3 + Ax + B$, with points P and Q,

$$[n]P + [m]Q = \left(\frac{\phi_{n,m}(P,Q)}{\Psi_{n,m}(P,Q)^2}, \frac{\omega_{n,m}(P,Q)}{\Psi_{n,m}(P,Q)^3} \right).$$

Consider the array of $\Psi_{n,m}(P,Q)$.

Example: $E : y^2 + y = x^3 + x^2 - 2x$; $P = (0,0)$, $Q = (1,0)$

	4335	5959	12016	-55287	23921	1587077
	94	479	919	-2591	13751	68428
	-31	53	-33	-350	493	6627
	-5	8	-19	-41	-151	989
	1	3	-1	-13	-36	181
$\uparrow$	1	1	2	-5	7	89
Q	0	1	1	-3	11	38
	$P \rightarrow$					

Definition of an elliptic net

Definition (S)

Let K be a field. An *elliptic net* is a map $W : \mathbb{Z}^n \to K$ such that the following recurrence holds for all $p, q, r, s \in \mathbb{Z}^n$.

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\quad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\quad + W(r+p+s)W(r-p)W(q+s)W(q) = 0 \qquad (**) \end{aligned}$$

Note

- Elliptic divisibility sequences are a special case ($n = 1$)
- The recurrence generates the net from finitely many initial values.

Curve-net bijection

Theorem (S.)

For each r, there is a bijection:

$$\left\{ \begin{array}{l} \textit{elliptic nets} \\ W_{\mathbf{v}} : \mathbb{Z}^r \to \mathbb{Q} \\ W_{\mathbf{e}_i} = W_{\mathbf{e}_i + \mathbf{e}_j} = 1, \\ W_{\mathbf{e}_i - \mathbf{e}_j} \neq 0 \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \textit{curve-point-tuple pairs} \\ (E, P_1, \ldots, P_r) \\ E : y^2 = x^3 + Ax + B, \\ A, B \in \mathbb{Q}, P_i \in E(\mathbb{Q}) \\ P_i \pm P_j \neq \mathcal{O} \end{array} \right\}$$

Note:

- $W_{\mathbf{v}} = \Psi_{\mathbf{v}}(P_1, \ldots, P_n, E)$
- explicit equations to go back and forth