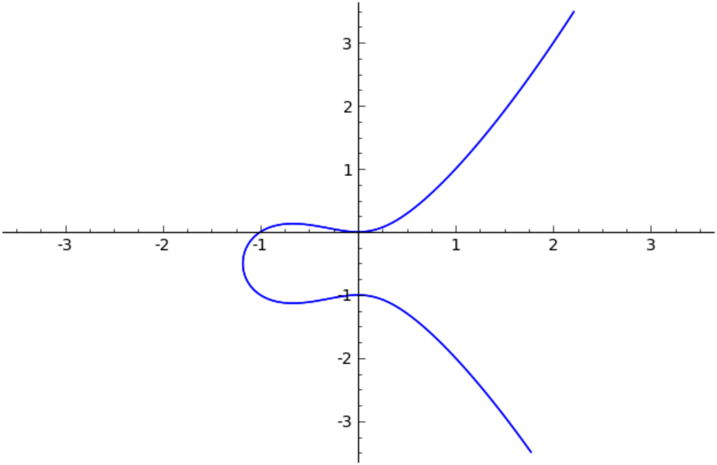
Elliptic Curves over Finite Fields

Katherine E. Stange
Stanford University

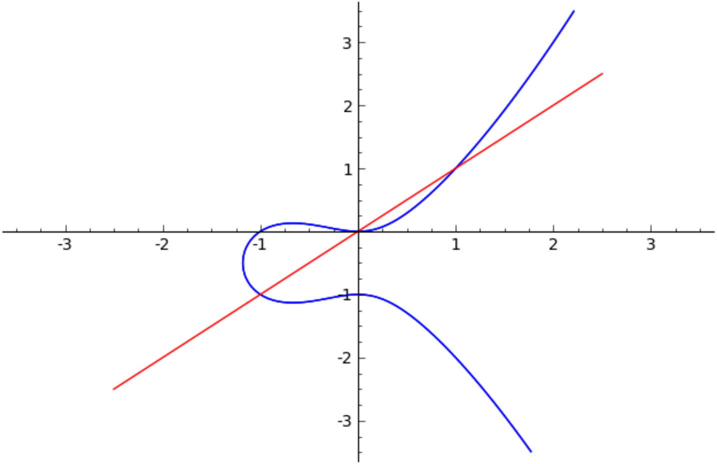
Boise REU, June 14th, 2011

Consider a cubic curve of the form

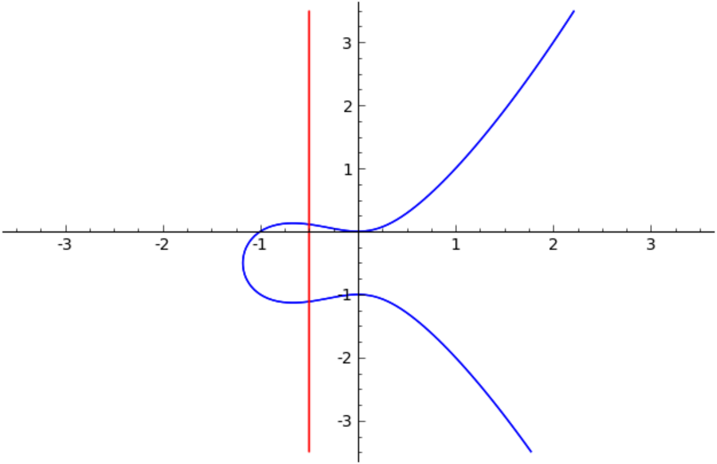
$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$



If you intersect with any line, there are exactly 3 solutions:

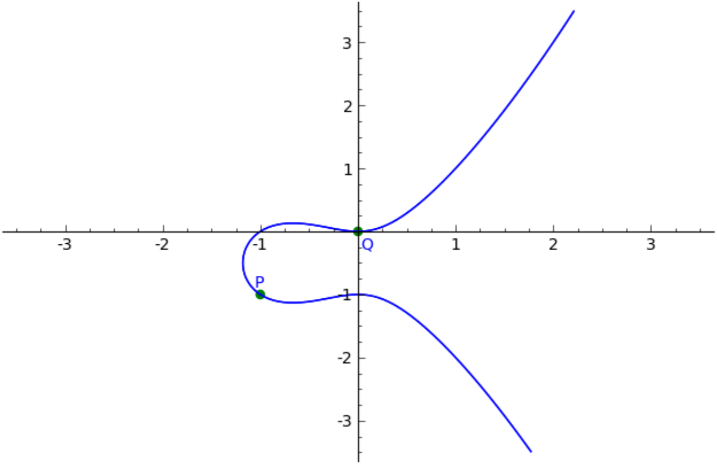


Actually, sometimes it looks like 2 solutions.

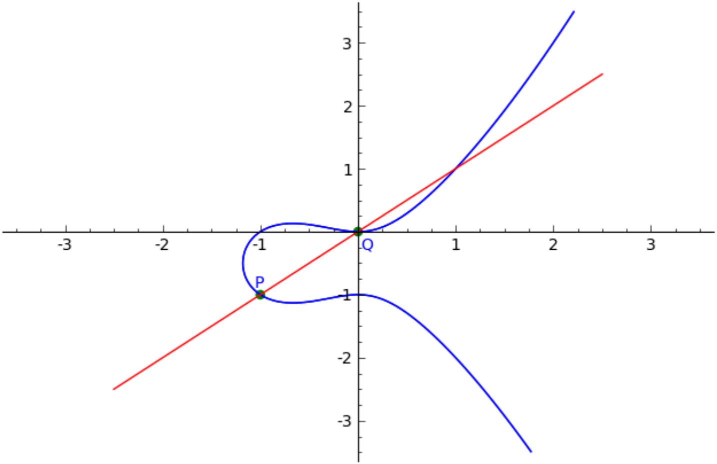


But in this case we imagine an extra "point at infinity", ∞, that the line goes through.

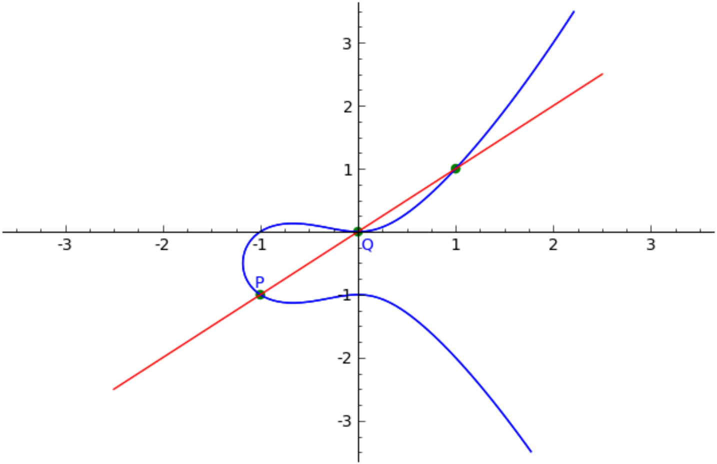
So if we start with two points on the curve. . .



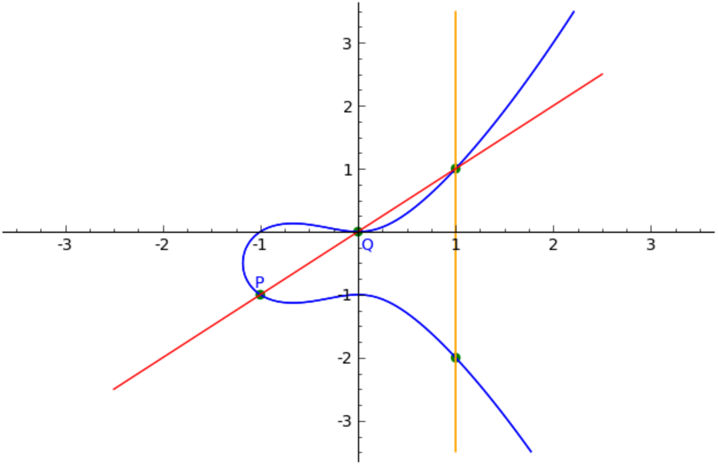
So if we start with two points on the curve, and draw a line through them. . .



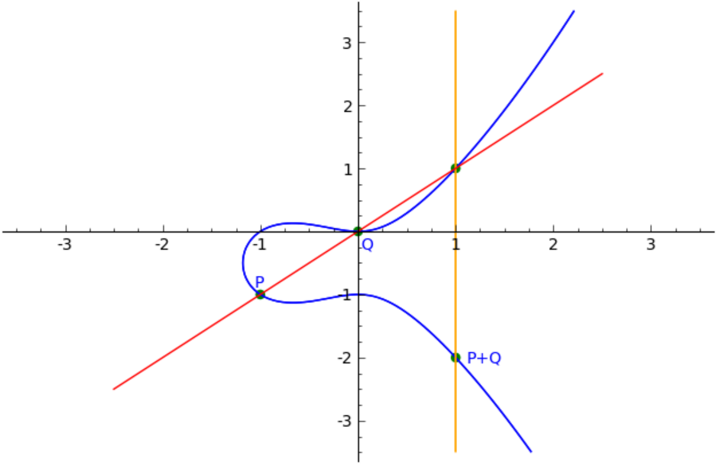
So if we start with two points on the curve, and draw a line through them to get another point. . .



This is almost a group law. To make it work (all the axioms) we actually have to add a reflection at the end:



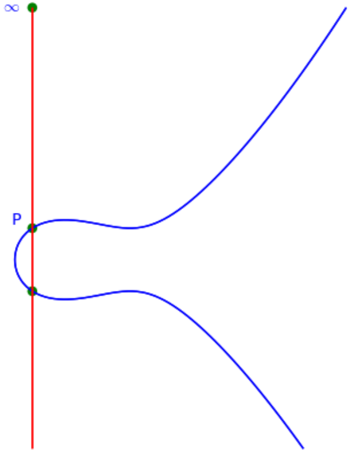
Group Law



And that's how we get $P + Q$.

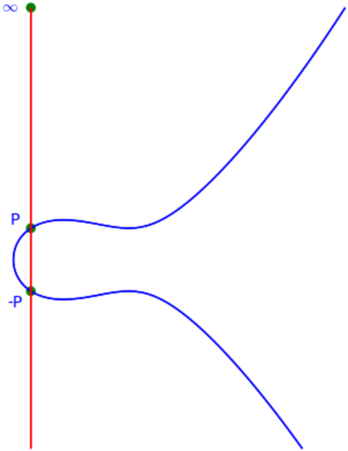
Identity

Identity: ∞

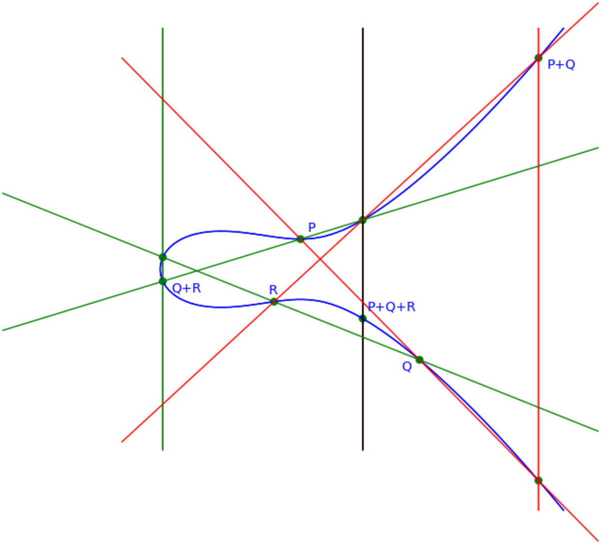


Inverses

Inverses: Two points on a line with ∞.

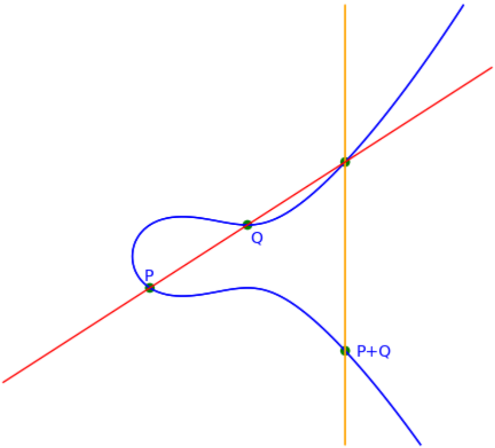


Associativity



Hard to check, but true!

The points of the elliptic curve form a group!



$\mathbb{Z}/p\mathbb{Z}$, the integers modulo p

…has addition

$$(3 \bmod 7) + (6 \bmod 7) = 2 \bmod 7$$

…has subtraction

$$(3 \bmod 7) - (6 \bmod 7) = 4 \bmod 7$$

…has multiplication

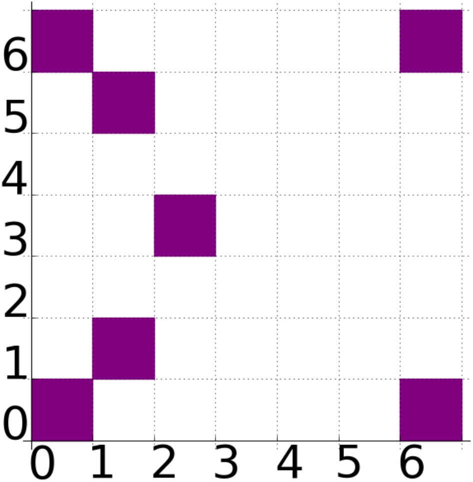
$$(2 \bmod 7) \times (4 \bmod 7) = 1 \bmod 7$$

…has division

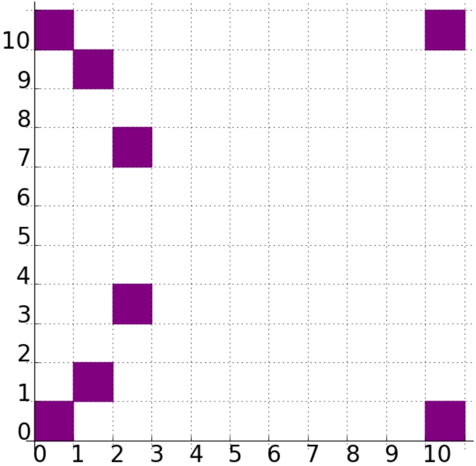
$$(1 \bmod 7) \div (2 \bmod 7) = 1/2 \bmod 7 = 4 \bmod 7$$

In fact, it's a field. We call it $\mathbb{F}_p$, the finite field of p elements.

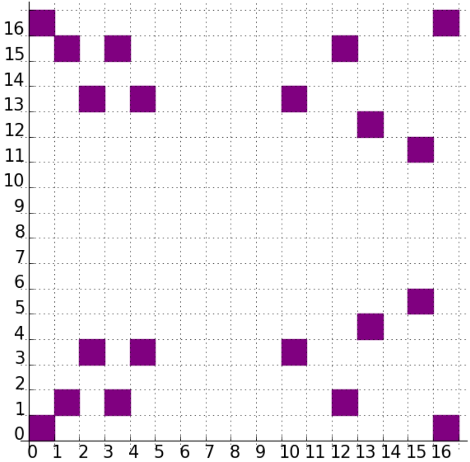
$$y^2 + y = x^3 + x^2 \quad \text{over } \mathbb{F}_7$$



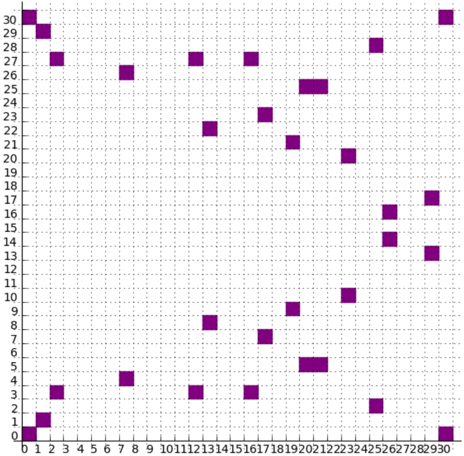
$$y^2 + y = x^3 + x^2 \quad \text{over } \mathbb{F}_{11}$$



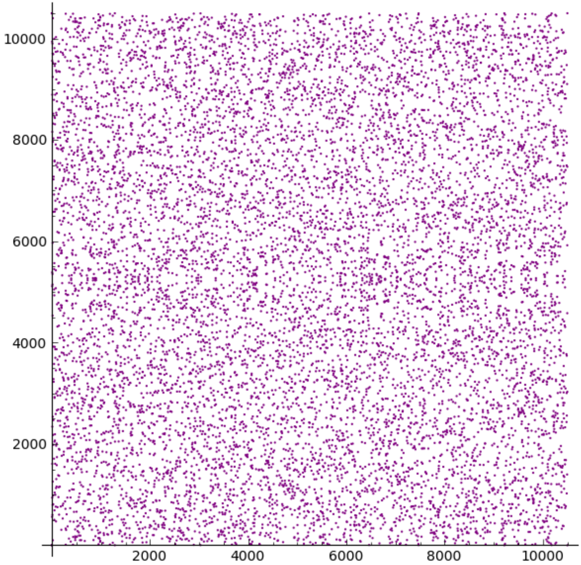
$$y^2 + y = x^3 + x^2 \quad \text{over } \mathbb{F}_{17}$$



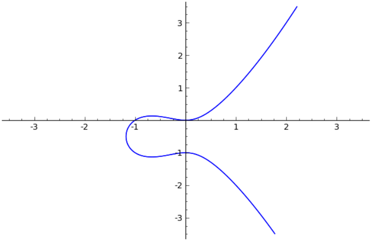
$$y^2 + y = x^3 + x^2 \quad \text{over } \mathbb{F}_{31}$$



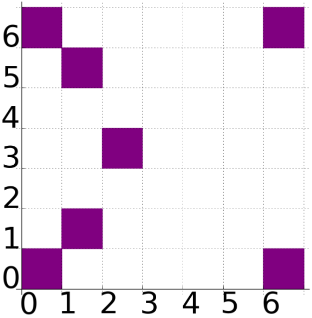
$$y^2 + y = x^3 + x^2 \quad \text{over } \mathbb{F}_{10501}$$



An elliptic curve $E/\mathbb{Q}$ gives rise to an elliptic curve $E/\mathbb{F}_p$ for each p:



$\rightarrow$



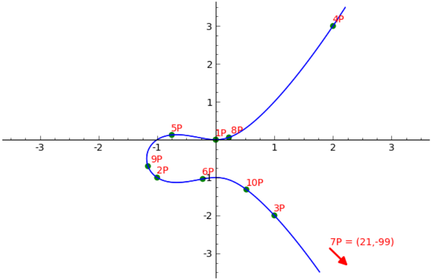
$y^2 + y = x^3 + x^2$

Also, given $P \in E(\mathbb{Q})$, we get a list of orders modulo p:

prime	2	3	5	7	11	13	17	19	23	29	31
order of P	5	6	10	8	9	19	21	11	25	12	33

(This point P has infinite order in $E(\mathbb{Q})$.)

Elliptic Divisibility Sequences



$$
\begin{aligned}
P &= (0,0) & 1\\
2P &= (-1,-1) & 1\\
3P &= (1,-2) & 1\\
4P &= (2,3) & -1\\
5P &= \left(-\frac{3}{2^2},\frac{1}{2^3}\right) & -2\\
6p &= \left(-\frac{2}{3^2},-\frac{28}{3^3}\right) & -3\\
7P &= (21,-99) & -1\\
8P &= \left(\frac{11}{7^2},\frac{20}{7^3}\right) & 7\\
9P &= \left(-\frac{140}{11^2},-\frac{931}{11^3}\right) & 11\\
10P &= \left(\frac{209}{20^2},-\frac{10527}{20^3}\right) & 20
\end{aligned}
$$

Definition

An *elliptic divisibility sequence* (EDS) is an integer sequence W_n satisfying

$$W_{n+m}W_{n-m}W_r^2 + W_{m+r}W_{m-r}W_n^2 + W_{r+n}W_{r-n}W_m^2 = 0.$$

On any elliptic curve, we can define A_n, B_n, W_n recursively so that

$$nP = \left(\frac{A_n}{W_n^2}, \frac{B_n}{W_n^3}\right),$$

and W_n is an EDS.

$$W_n = 0 \iff nP = \infty$$

Reducing an EDS modulo p

EDS from $P = (0,0)$ on $y^2 + y = x^3 + x^2$

$$1, 1, 1, -1, -2, -3, -1, 7, 11, 20, -19, -87, -191, -197, 1018$$

EDS from $P = (0,0)$ on $y^2 + y = x^3 + x^2$ modulo 7:

$$1, 1, 1, 6, 5, 4, 6, 0, 4, 6, 2, 4, 5, 6, 3$$

Let's put together some of the data:

prime	2	3	5	7	11	13	17	19	23	29	31
order of P	5	6	10	8	9	19	21	11	25	12	33
W_0	0	0	0	0	0	0	0	0	0	0	0
W_1	1	1	1	1	1	1	1	1	1	1	1
W_2	1	1	1	1	1	1	1	1	1	1	1
W_3	1	1	1	1	1	1	1	1	1	1	1
W_4	1	2	4	6	10	12	16	18	22	28	30
W_5	0	1	3	5	9	11	15	17	21	27	29
W_6	1	0	2	4	8	10	14	16	20	26	28
W_7	1	2	4	6	10	12	16	18	22	28	30
W_8	1	1	2	0	7	7	7	7	7	7	7
W_9	1	2	1	4	0	11	11	11	11	11	11
W_{10}	0	2	0	6	9	7	3	1	20	20	20
W_{11}	1	2	1	2	3	7	15	0	4	10	12
W_{12}	1	0	3	4	1	4	15	8	5	0	6
W_{13}	1	1	4	5	7	4	13	18	16	12	26
W_{14}	1	1	3	6	1	11	7	12	10	6	20
W_{15}	0	1	3	3	6	4	15	11	6	3	26
W_{16}	1	2	1	0	8	3	12	2	13	13	15
W_{17}	1	1	1	1	7	1	14	2	3	13	7
W_{18}	1	0	4	4	0	9	7	11	1	17	18
W_{19}	1	2	1	2	1	0	5	12	16	27	24
W_{20}	0	1	0	6	5	12	6	18	16	7	2
W_{21}	1	2	4	6	3	4	0	8	12	20	7
W_{22}	1	2	1	1	7	10	7	0	5	5	16
W_{23}	1	2	4	6	4	1	5	1	19	23	29
W_{24}	1	0	4	0	8	5	6	11	17	0	20
W_{25}	0	1	2	1	6	9	3	7	0	4	23
W_{26}	1	1	2	6	10	1	14	18	2	1	7
W_{27}	1	1	1	1	0	2	15	16	3	22	24
W_{28}	1	2	2	1	4	6	6	17	16	9	5
W_{29}	1	1	4	5	3	6	4	18	22	19	25

When we reduce mod 7, where does

$$8P = \left(\frac{11}{49}, \frac{20}{343}\right)$$

go?

To ∞! The identity.

So $8\widetilde{P} = \infty$ modulo 7.

In the associated EDS, $7 \mid W_8$.

The primes appear in the EDS at the multiples of the order of P.

n	W_n	factorisation
1	1	1
2	1	1
3	1	1
4	-1	-1
5	-2	$-1 \cdot 2$
6	-3	$-1 \cdot 3$
7	-1	-1
8	7	7
9	11	11
10	20	$2^2 \cdot 5$
11	-19	$-1 \cdot 19$
12	-87	$-1 \cdot 3 \cdot 29$
13	-191	$-1 \cdot 191$
14	-197	$-1 \cdot 197$
15	1018	$2 \cdot 509$
16	2681	$7 \cdot 383$
17	8191	8191
18	-5841	$-1 \cdot 3^2 \cdot 11 \cdot 59$
19	-81289	$-1 \cdot 13^3 \cdot 37$

n	W_n	factorisation
20	-261080	$-1 \cdot 2^3 \cdot 5 \cdot 61 \cdot 107$
21	-620551	$-1 \cdot 17 \cdot 173 \cdot 211$
22	3033521	$19 \cdot 43 \cdot 47 \cdot 79$
23	14480129	$1447 \cdot 10007$
24	69664119	$3 \cdot 7 \cdot 29 \cdot 73 \cdot 1567$
25	-2664458	$-1 \cdot 2 \cdot 23 \cdot 57923$
26	-1612539083	$-1 \cdot 191 \cdot 1439 \cdot 5867$
27	-7758440129	$-1 \cdot 11 \cdot 827 \cdot 852857$
28	-37029252553	$-1 \cdot 197 \cdot 187965749$
29	181003520899	$3323 \cdot 6521 \cdot 8353$
30	1721180313660	$2^2 \cdot 3 \cdot 5 \cdot 509 \cdot 647 \cdot 87107$
31	12437589708389	12437589708389
32	19206818781913	$7 \cdot 383 \cdot 7164050273$
33	-672004824959359	$-1 \cdot 19 \cdot 31 \cdot 1699 \cdot 671527369$
34	-5070370671429517	$-1 \cdot 8191 \cdot 619017295987$
35	-44138469613743118	$-1 \cdot 2 \cdot 71 \cdot 32401 \cdot 39563 \cdot 242483$
36	205791799565838321	$3^2 \cdot 11 \cdot 29 \cdot 59 \cdot 1214906514389$
37	4451821019236847359	$41 \cdot 1237 \cdot 29443 \cdot 2981275289$
38	47106384726033313759	$13^3 \cdot 37 \cdot 233 \cdot 354643 \cdot 7012949$

$$\text{If } p \mid W_n \text{ and } n \mid m, \text{ then } p \mid W_m.$$

n	L_n	factorisation
1	1	1
2	3	3
3	8	2^3
4	21	$3 \cdot 7$
5	55	$5 \cdot 11$
6	144	$2^4 \cdot 3^2$
7	377	$13 \cdot 29$
8	987	$3 \cdot 7 \cdot 47$
9	2584	$2^3 \cdot 17 \cdot 19$
10	6765	$3 \cdot 5 \cdot 11 \cdot 41$
11	17711	$89 \cdot 199$
12	46368	$2^5 \cdot 3^2 \cdot 7 \cdot 23$
13	121393	$233 \cdot 521$
14	317811	$3 \cdot 13 \cdot 29 \cdot 281$
15	832040	$2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$
16	2178309	$3 \cdot 7 \cdot 47 \cdot 2207$
17	5702887	$1597 \cdot 3571$
18	14930352	$2^4 \cdot 3^3 \cdot 17 \cdot 19 \cdot 107$
19	39088169	$37 \cdot 113 \cdot 9349$
20	102334155	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 41 \cdot 2161$

n	L_n	factorisation
21	267914296	$2^3 \cdot 13 \cdot 29 \cdot 211 \cdot 421$
22	701408733	$3 \cdot 43 \cdot 89 \cdot 199 \cdot 307$
23	1836311903	$139 \cdot 461 \cdot 28657$
24	4807526976	$2^6 \cdot 3^2 \cdot 7 \cdot 23 \cdot 47 \cdot 1103$
25	12586269025	$5^2 \cdot 11 \cdot 101 \cdot 151 \cdot 3001$
26	32951280099	$3 \cdot 233 \cdot 521 \cdot 90481$
27	86267571272	$2^3 \cdot 17 \cdot 19 \cdot 53 \cdot 109 \cdot 5779$
28	225851433717	$3 \cdot 7^2 \cdot 13 \cdot 29 \cdot 281 \cdot 14503$
29	591286729879	$59 \cdot 19489 \cdot 514229$
30	1548008755920	$2^4 \cdot 3^2 \cdot 5 \cdot 11 \cdot 31 \cdot 41 \cdot 61 \cdot 2521$
31	4052739537881	$557 \cdot 2417 \cdot 3010349$
32	10610209857723	$3 \cdot 7 \cdot 47 \cdot 1087 \cdot 2207 \cdot 4481$
33	27777890035288	$2^3 \cdot 89 \cdot 199 \cdot 9901 \cdot 19801$
34	72723460248141	$3 \cdot 67 \cdot 1597 \cdot 3571 \cdot 63443$
35	190392490709135	$5 \cdot 11 \cdot 13 \cdot 29 \cdot 71 \cdot 911 \cdot 141961$
36	498454011879264	$2^5 \cdot 3^3 \cdot 7 \cdot 17 \cdot 19 \cdot 23 \cdot 107 \cdot 103681$
37	1304969544928657	$73 \cdot 149 \cdot 2221 \cdot 54018521$
38	3416454622906707	$3 \cdot 37 \cdot 113 \cdot 9349 \cdot 29134601$
39	8944394323791464	$2^3 \cdot 79 \cdot 233 \cdot 521 \cdot 859 \cdot 135721$

If $p \mid L_n$ and $n \mid m$, then $p \mid L_m$.

$E(\mathbb{F}_p)$ - group of points over $\mathbb{F}_p$

For each $x_0 \in \mathbb{F}_p$ (there are p of them), the quadratic equation in y

$$y^2 + a_1 x_0 y + a_3 y = x_0^3 + a_2 x_0^2 + a_4 x_0 + a_6$$

has either 0 or 2 solutions. So either

no points or 2 points: (x_0, y_1) and (x_0, y_2).

So, if we assume that half the time it has solutions, then we get about p points.

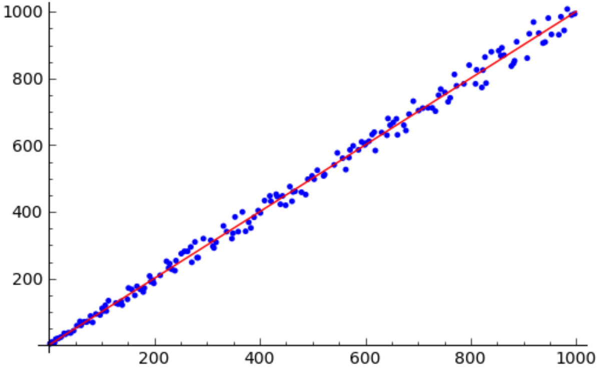
Oh, and there's the point ∞. So that makes about

$$p + 1 \text{ points}$$

Given $E/\mathbb{Q}$, we get a list of group-orders $\#E(\mathbb{F}_p)$:

$$y^2 + y = x^3 + x^2$$

p	2	3	5	7	11	13	17	19	23	29	31	37
$\#E(\mathbb{F}_p)$	5	6	10	8	9	19	21	22	25	36	33	38



Theorem (Hasse (1933))

$$|\#E(\mathbb{F}_p) - p - 1| < 2\sqrt{p}$$

We write $a_p = p + 1 - \#E(\mathbb{F}_p)$.

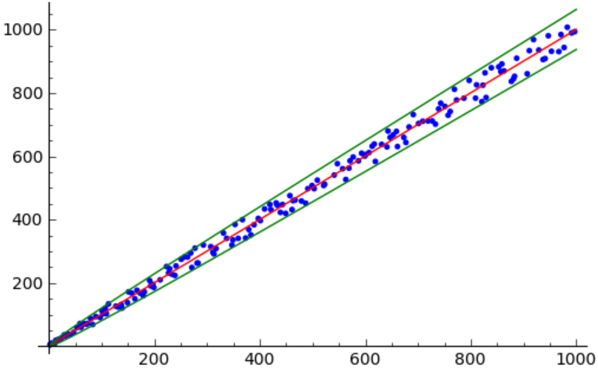
p	$\#E(\mathbb{F}_p)$	a_p	$\lfloor 2\sqrt{p} \rfloor$
2	5	-2	2
3	6	-2	3
5	10	-4	4
7	8	0	5
11	9	3	6
13	19	-5	7
17	21	-3	8
19	22	-2	8
23	25	-1	9
29	36	-6	10
31	33	-1	11
37	38	0	12

p	$\#E(\mathbb{F}_p)$	a_p	$\lfloor 2\sqrt{p} \rfloor$
41	37	5	12
47	44	4	13
53	59	-5	14
59	72	-12	15
61	60	2	15
67	71	-3	16
71	70	2	16
73	72	2	17
79	88	-8	17
83	69	15	18
89	94	-4	18
97	91	7	19

Theorem (Hasse (1933))

$$|\#E(\mathbb{F}_p) - p - 1| < 2\sqrt{p}$$

We write $a_p = p + 1 - \#E(\mathbb{F}_p)$.



Theorem (Deuring, 1941)

For any n such that $|n - p - 1| < 2\sqrt{p}$, there exists some elliptic curve E over $\mathbb{F}_p$ such that

$$\#E(\mathbb{F}_p) = n$$

Theorem (Cassells, 1966)

The group $E(\mathbb{F}_p)$ is of the form

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

where $m_1 \mid m_2$ and $m_1 \mid p-1$.

Index divisibility

Joseph H. Silverman and I saw a paper of Chris Smyth, in which he asked, for Lucas sequences L_n:

$$\text{When does } n \mid L_n?$$

So we wondered the same thing for W_n an elliptic divisibility sequence:

$$\text{When does } n \mid W_n?$$

When does $n \mid W_n$?

Does it happen for $n = p$?

If P has order p modulo p, then $p \mid W_p$.

This can happen if $\#E(\mathbb{F}_p) = p$. Such a curve is called anomalous and is unsafe for cryptography because it has special structure.

Can we generalise this? What about if $n = pq$?

If $p \mid W_q$ and $q \mid W_p$, then $p \mid W_{pq}$ and $q \mid W_{pq}$. So $pq \mid W_{pq}$.

This happens if P has order p modulo q and order q modulo p.

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

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

Question

(How often) does this happen?

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

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

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 $p, q < 10^7$:

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

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

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

Heuristic

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

A conjecture of Koblitz says that

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

Heuristic

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

A conjecture of Koblitz says that

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

A conjecture of Sato and Tate says that

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

Heuristic

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

A conjecture of Koblitz says that

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

A conjecture of Sato and Tate says that

$$\text{Prob}(\#E(\mathbb{F}_q) = p) \approx \frac{1}{\sqrt{q}} \approx \frac{1}{\sqrt{p}}.$$

Together:

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

Heuristic

$$\mathcal{Q}_E(X) \approx \sum_{p \le X} \text{Prob}(p \text{ is the smaller prime in an amicable pair }) \approx \sum_{p \le X} \frac{1}{\sqrt{p}(\log p)}.$$

Use the rough approximation

$$\sum_{p \le X} f(X) \approx \sum_{n \le X/\log X} f(n \log n) \approx \int^{X/\log X} f(t \log t)\, dt \approx \int^{X} f(u) \frac{du}{\log u}$$

to obtain

$$\mathcal{Q}_E(X) \approx \int^{X} \frac{1}{\sqrt{u}\log u} \cdot \frac{du}{\log u} \approx \frac{\sqrt{X}}{(\log X)^2}.$$

Conjecture (Version 1)

Let $E/\mathbb{Q}$ be an elliptic curve, let

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

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

Conjecture (Version 1)

Let $E/\mathbb{Q}$ be an elliptic curve, let

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

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

Then

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

Data agreement...?

X	$\mathcal{Q}(X)$	$\mathcal{Q}(X) / \frac{\sqrt{X}}{(\log X)^2}$	$\frac{\log \mathcal{Q}(X)}{\log X}$
10^6	2	0.382	0.050
10^7	4	0.329	0.086
10^8	5	0.170	0.087
10^9	10	0.136	0.111
10^{10}	21	0.111	0.132
10^{11}	59	0.120	0.161
10^{12}	117	0.089	0.172

Table: Counting amicable pairs for $y^2 + y = x^3 + x^2$ (thanks to Andrew Sutherland with smalljac)

Aliquot cycles

Definition

Let E be an elliptic curve. An aliquot cycle of length ℓ for E is a sequence of distinct primes $(p_1, p_2, \ldots, p_\ell)$ such that

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

Aliquot cycles

Definition

Let E be an elliptic curve. An aliquot cycle of length ℓ for E is a sequence of distinct primes $(p_1, p_2, \ldots, p_\ell)$ such that

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

Example

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

Aliquot cycles

Definition

Let E be an elliptic curve. An aliquot cycle of length ℓ for E 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

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

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

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

Chinese Remainder Theorem

If you have a bunch of congruence conditions for distinct primes:

$$\begin{aligned} x &\equiv b_1 \mod p_1 \\ x &\equiv b_2 \mod p_2 \\ &\vdots \\ x &\equiv b_n \mod p_n \end{aligned}$$

Then there is a solution $x \in \mathbb{Z}$.

Constructing aliquot cycles with CRT

Fix ℓ and let $p_1, p_2, \ldots, p_\ell$ be a sequence of primes such that

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

where by convention we set $p_{\ell+1} = p_1$.

Constructing aliquot cycles with CRT

Fix ℓ and let $p_1, p_2, \ldots, p_\ell$ be a sequence of primes such that

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

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

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

Constructing aliquot cycles with CRT

Fix ℓ and let $p_1, p_2, \dots, p_\ell$ 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 by convention we set $p_{\ell+1} = p_1$. For each p_i find (by Deuring) an elliptic curve E_i over $\mathbb{F}_{p_i}$ satisfying

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

Use the Chinese remainder theorem on the coefficients of the Weierstrass equations for $E_1, \dots, E_\ell$ to find an elliptic curve E over $\mathbb{Q}$ satisfying

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

Constructing aliquot cycles with CRT

Fix ℓ and let $p_1, p_2, \ldots, p_\ell$ be a sequence of primes such that

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

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

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

Use the Chinese remainder theorem on the coefficients of the Weierstrass equations for $E_1, \ldots, E_\ell$ to find an elliptic curve E over $\mathbb{Q}$ satisfying

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

Then by construction, the sequence $(p_1, \ldots, p_\ell)$ is an aliquot cycle of length ℓ for E.

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 $p, q < 10^7$:

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

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

Theorem

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

CM case

Theorem

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

Then either

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

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

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

Conjecture (Version 2)

Let $E/\mathbb{Q}$ be an elliptic curve, let

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

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

Conjecture (Version 2)

Let $E/\mathbb{Q}$ be an elliptic curve, let

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

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

(a) If E does not have complex multiplication, then

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

Conjecture (Version 2)

Let $E/\mathbb{Q}$ be an elliptic curve, let

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

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

(a) If E does not have complex multiplication, then

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

(b) If E has complex multiplication, then

$$\mathcal{Q}_E(X) \approx \frac{X}{(\log X)^2} \quad \text{as } X \to \infty.$$

No longer aliquot cycles in CM case

Theorem

A CM elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0$ has no aliquot cycles of length $\ell \geq 3$ consisting of primes $p \geq 5$.

No longer aliquot cycles – proof

Let $(p_1, p_2, \ldots, p_\ell)$ be an aliquot cycle of length $\ell \geq 3$, with $p_i \geq 3$. We must have

$$p_i = 2p_{i-1} + 2 - p_{i-2} \quad \text{for } 3 \leq i \leq \ell,$$

$$p_1 = 2p_\ell + 2 - p_{\ell-1}.$$

No longer aliquot cycles – proof

Let $(p_1, p_2, \ldots, p_\ell)$ be an aliquot cycle of length $\ell \geq 3$, with $p_i \geq 3$. We must have

$$p_i = 2p_{i-1} + 2 - p_{i-2} \quad \text{for } 3 \leq i \leq \ell,$$

$$p_1 = 2p_\ell + 2 - p_{\ell-1}.$$

Determining the general term for the recursion, we get

$$p_{\ell+1} = \ell p_2 - (\ell - 1)p_1 + \ell(\ell - 1).$$

$$p_1 = p_{\ell+1} \implies p_1 = p_2 + \ell - 1.$$

No longer aliquot cycles – proof

Let $(p_1, p_2, \ldots, p_\ell)$ be an aliquot cycle of length $\ell \geq 3$, with $p_i \geq 3$. We must have

$$p_i = 2p_{i-1} + 2 - p_{i-2} \quad \text{for } 3 \leq i \leq \ell,$$

$$p_1 = 2p_\ell + 2 - p_{\ell-1}.$$

Determining the general term for the recursion, we get

$$p_{\ell+1} = \ell p_2 - (\ell - 1)p_1 + \ell(\ell - 1).$$

$$p_1 = p_{\ell+1} \implies p_1 = p_2 + \ell - 1.$$

Cyclically permuting the cycle gives

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

where we set $p_{\ell+1} = p_1$.

No longer aliquot cycles – proof

Let $(p_1, p_2, \ldots, p_\ell)$ be an aliquot cycle of length $\ell \geq 3$, with $p_i \geq 3$. We must have

$$p_i = 2p_{i-1} + 2 - p_{i-2} \quad \text{for } 3 \leq i \leq \ell,$$

$$p_1 = 2p_\ell + 2 - p_{\ell-1}.$$

Determining the general term for the recursion, we get

$$p_{\ell+1} = \ell p_2 - (\ell - 1)p_1 + \ell(\ell - 1).$$

$$p_1 = p_{\ell+1} \implies p_1 = p_2 + \ell - 1.$$

Cyclically permuting the cycle gives

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

where we set $p_{\ell+1} = p_1$. So $p_i > p_{i+1}$ for all $1 \leq i \leq \ell$ and $p_\ell > p_1$. Contradiction!