Amicable pairs for elliptic curves

Katherine E. Stange
SFU / PIMS-UBC
.
joint work with
.
Joseph H. Silverman
Brown University / Microsoft Research

Sage Days 26
December 7th, 2010

A Question

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

$$\mathcal{S}(A) = \{n \geq 1 : n \mid A_n\}.$$

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

Make it a directed graph: $\mathcal{S}(A)$ are vertices and $n \to m$ if and only if

1. $n \mid m$ with $n < m$.
2. If $k \in \mathcal{S}(A)$ satisfies $n \mid k \mid m$, then $k = n$ or $k = m$.

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

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

Elliptic divisibility sequences

Definition

Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$ be a nontorsion point.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad P = (x, y)$$

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 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 associated to the elliptic curve E. If the list $p_1, \ldots, p_\ell$ of distinct primes of good reduction for E satisfies

$$p_{i+1} = \min\{r \geq 1 : p_i \mid D_r\} \qquad \text{for all } 1 \leq i \leq \ell,$$

(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 $p, q < 10^7$:

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

Hasse Interval

Theorem (Hasse)

Let $E/\mathbb{F}_p$ be an elliptic curve defined over a finite field. Define the trace of Frobenius to be

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

Then

$$|a_p| \leq 2\sqrt{p}$$

- A theorem of Deuring says every value in this *Hasse interval* is attained as a_p for some E.
- The Sato-Tate conjecture governs the distribution of a_p within the Hasse interval.

Questions

Question (1)

Let

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

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

Question (2)

Let

$$\mathcal{N}_E(X) = \#\{\textit{primes } p \leq X \textit{ such that } \#E(\mathbb{F}_p) \textit{ is prime}\}$$

What about $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$*?*

$\mathcal{N}_E(X)$

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

$$\mathcal{N}_E(X) = \#\{\text{primes } p \leq X \text{ such that } \#E(\mathbb{F}_p) \text{ is prime}\}.$$

Conjecture (Koblitz, Zywina)

There is a constant $C_{E/\mathbb{Q}}$ such that

$$\mathcal{N}_E(X) \sim C_{E/\mathbb{Q}} \frac{X}{(\log X)^2}.$$

Further, $C_{E/\mathbb{Q}} > 0$ if and only if there are infinitely many primes p such that $\#E_p(\mathbb{F}_p)$ is prime.

$C_{E/\mathbb{Q}}$ can be zero (e.g. if $E/\mathbb{Q}$ has rational torsion).

Heuristic

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

Conjecture of Koblitz and Zywina says that

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

Rough estimate using Sato–Tate conjecture (for non-CM):

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

Together:

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

Growth of $\mathcal{Q}_E(X)$

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

$$\gg\ll \sum_{p \le X} \frac{1}{\sqrt{p}(\log p)}.$$

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

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

Conjectures

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

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

where the implied constants depend on E.

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)

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 $p, q < 10^7$:

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

Complex Multiplication

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

The endomorphism ring $\mathrm{End}(E)$ is usually isomorphic to $\mathbb{Z}$ (consisting of multiplication-by-m for all m).

Otherwise, $\mathrm{End}(E) \cong \mathcal{O}$ where $\mathcal{O}$ is an order of class number 1 in a quadratic imaginary number field.

CM case: Twist Theorem

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$, 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

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

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

CM case: Twist Theorem proof

1. Eliminating curves with 2-torsion leaves $D \equiv 3 \mod 4$.
2. p splits as $p = \mathfrak{p}\overline{\mathfrak{p}}$ (if it were inert, we would have supersingular reduction, $\#E(\mathbb{F}_p) = p + 1$)
3. $\#E(\mathbb{F}_\mathfrak{p}) = N(\Psi(\mathfrak{p})) + 1 - Tr(\Psi(\mathfrak{p}))$ where Ψ is the Grössencharacter of E.
4. $N(1 - \Psi(\mathfrak{p})) = \#E(\mathbb{F}_\mathfrak{p}) = \#E(\mathbb{F}_p) = q$ so q splits as $q = \mathfrak{q}\overline{\mathfrak{q}}$.
5. $N(\Psi(\mathfrak{q})) = q$.
6. So $1 - \Psi(\mathfrak{p}) = u\Psi(\mathfrak{q})$ for some unit $u \in \{\pm 1\}$.
7. $Tr(\Psi(\mathfrak{q})) = \pm Tr(1 - \Psi(\mathfrak{p})) = \pm(2 - Tr(\Psi(\mathfrak{p}))) = \pm(q + 1 - p)$. So...

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

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

(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

Conjecture (Version 2)

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.

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

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

where the implied constants depend on E.

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

$$\mathcal{Q}_E(X) \sim \frac{1}{4}\mathcal{N}_E(X) \sim A_E \frac{X}{(\log X)^2}.$$

Aliquot cycles

Definition

Let $E/\mathbb{Q}$ be an elliptic curve. 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 has good reduction at every p_i and 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

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

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

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

Constructing aliquot cycles with CRT

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 $E_i/\mathbb{F}_{p_i}$ 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 $E/\mathbb{Q}$ 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 $E/\mathbb{Q}$.

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

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

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

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!

A little review of $K = \mathbb{Q}(\sqrt{-3})$.

$$K = \mathbb{Q}(\sqrt{-3}), \quad \omega = \frac{1+\sqrt{-3}}{2}.$$

Ring of integers: $\mathcal{O}_K = \mathbb{Z}[\omega]$.

Units: $\mathcal{O}_K^* = \mu_6 = \{1, \omega, \omega^2, \ldots, \omega^5\}$ ($\omega^6 = 1$)

The map

$$\mathcal{O}_K^* \to (\mathcal{O}_K/3\mathcal{O}_K)^*$$

is an isomorphism.

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ relatively prime to 3. For $\alpha \in \mathcal{O}_K \setminus \mathfrak{p}$, the sextic residue symbol is defined by

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_6 \in \mu_6, \quad \left(\frac{\alpha}{\mathfrak{p}}\right)_6 \equiv \alpha^{\frac{1}{6}(N_{K/\mathbb{Q}}(\mathfrak{p})-1)} \mod \mathfrak{p}.$$

CM $j = 0$ case: Twist Theorem

Theorem

Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + k$, and suppose that p and q are primes of good reduction for E with $p \geq 5$ and $q = \#E(\mathbb{F}_p)$. Then p splits in K, and we write $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. Define $\mathfrak{q} = \big(1 - \Psi(\mathfrak{p})\big)\mathcal{O}_K$. Then we have $q\mathcal{O}_K = \mathfrak{q}\overline{\mathfrak{q}}$.

The values of the Grössencharacter at $\mathfrak{p}$ and $\mathfrak{q}$ are related by

$$1 - \Psi(\mathfrak{p}) = \left(\frac{4k}{\mathfrak{p}}\right)_6 \left(\frac{4k}{\mathfrak{q}}\right)_6 \Psi(\mathfrak{q}).$$

Finally, $\#E(\mathbb{F}_q) = p$ if and only if $\left(\frac{4k}{\mathfrak{p}}\right)_6 \left(\frac{4k}{\mathfrak{q}}\right)_6 = 1$.

Remarks on Twist Theorem

The values of the Grössencharacter at $\mathfrak{p}$ and $\mathfrak{q}$ are related by

$$1 - \Psi(\mathfrak{p}) = \left(\frac{4k}{\mathfrak{p}}\right)_6 \left(\frac{4k}{\mathfrak{q}}\right)_6 \Psi(\mathfrak{q}).$$

Remark 1: Each value of $\left(\frac{4k}{\mathfrak{p}}\right)_6 \left(\frac{4k}{\mathfrak{q}}\right)_6 \in \mu_6$ corresponds to an isomorphism class of sextic twists E' of E over $\mathbb{F}_q$ for which $\#E'(\mathbb{F}_q) = p$. There are six possible values of $\#E(\mathbb{F}_q)$.

Remark 2: Proof much as before, using the fact that

$$\Psi(\mathfrak{p}) \equiv \left(\frac{4k}{\mathfrak{p}}\right)_6^{-1} \mod 3\mathcal{O}_K$$

Data on twist frequencies

k	2	3	5	6	7	10
$X = 10^4$	0.217	0.141	0.097	0.085	0.165	0.118
$X = 10^5$	0.251	0.122	0.081	0.134	0.139	0.125
$X = 10^6$	0.250	0.139	0.083	0.142	0.133	0.107
$X = 10^7$	0.249	0.139	0.082	0.139	0.129	0.107

Table: $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ for elliptic curves $y^2 = x^3 + k$

$$1/12 = 0.08333\ldots$$

Data on twist frequencies

k	$\mathcal{N}_p(X)$	I (1)	II (-1)	III	IV	V	VI
2	22314	0.5001	0.4999	0.0000	0.0000	0.0000	0.0000
3	22630	0.2795	0.2766	0.1144	0.1093	0.1103	0.1099
5	23463	0.1644	0.1679	0.1663	0.1690	0.1660	0.1663
7	22364	0.2584	0.2602	0.1192	0.1214	0.1206	0.1202
11	22390	0.1988	0.1952	0.1499	0.1530	0.1538	0.1492
13	22242	0.1629	0.1655	0.1646	0.1677	0.1668	0.1724
17	22289	0.1909	0.1876	0.1571	0.1556	0.1545	0.1543
19	22207	0.1931	0.1853	0.1553	0.1565	0.1517	0.1581
23	22251	0.1751	0.1828	0.1631	0.1600	0.1596	0.1594
29	22478	0.1627	0.1684	0.1679	0.1668	0.1669	0.1672

Table: Distribution of primes $p \leq 10^7$ of Types I–VI for $y^2 = x^3 + k$

Cubic reciprocity in $K = \mathbb{Q}(\sqrt{-3})$.

$$K = \mathbb{Q}(\sqrt{-3}), \quad \omega = \frac{1+\sqrt{-3}}{2}, \quad \mathcal{O}_K = \mathbb{Z}[\omega],$$
$$\mathcal{O}_K^* = \{1, \omega, \omega^2, \dots, \omega^5\}.$$

Cubic Reciprocity in $\mathcal{O}_K$:
For $\alpha, \beta \in \mathcal{O}_K$ *primary primes*, i.e. $\alpha, \beta \equiv 1, 2 \mod 3\mathcal{O}_K$,

$$\left(\frac{\alpha}{\beta}\right)_3 \left(\frac{\beta}{\alpha}\right)_3 = 1$$

Quadratic Reciprocity in $\mathbb{Z}$:
For $p, q \in \mathbb{Z}$ *primary primes*, i.e. $p, q \equiv 1 \mod 4$, i.e. $(-3, 5, -7, -11, 13, \dots)$,

$$\left(\frac{p}{q}\right)_2 \left(\frac{q}{p}\right)_2 = 1$$

Applying Cubic Reciprocity

Let E be the curve $y^2 = x^3 + k$ and suppose $\#\tilde{E}_p(\mathbb{F}_p)$ is prime.

$$\begin{aligned}&\left(\frac{4k}{\Psi_E(\mathfrak{p})}\right)_6 \left(\frac{4k}{1 - \Psi_E(\mathfrak{p})}\right)_6 \\ &= \cdots \\ &= \pm \left(\frac{\Psi_E(\mathfrak{p})(1 - \Psi_E(\mathfrak{p}))}{k}\right)_3^{-1}.\end{aligned}$$

Let M_k be the set of elements m in $\mathcal{O}_K/k\mathcal{O}_K$ for which $m(1 - m)$ is invertible.
Let M_k^* be the set of those also satisfying $\left(\frac{m(1-m)}{k}\right)_3 = 1$.
Then we may expect

$$\mathcal{Q}_E(X)/\mathcal{N}_E(X) \to \#M_k^*/4\#M_k.$$

The symbol $\left(\frac{m(1-m)}{k}\right)_3$ when $k \equiv 2 \mod 3$ is prime

The curve $E : y(1-y) = x^3$ has $j = 0$.

Then E is supersingular modulo k and has $(k+1)^2$ points over $\mathbb{F}_{k\mathcal{O}_K} = \mathbb{F}_{k^2}$.

Removing 3 points (∞, $(0,0)$ and $(0,1)$), the remaining points have $y \neq 0, 1$ and $\left(\frac{y(1-y)}{k}\right)_3 = 1$.

Therefore, $((k+1)^2 - 3)/3$ is the number of residues $m \neq 0, 1$ modulo $k\mathcal{O}_K$ having $\left(\frac{m(1-m)}{k}\right)_3 = 1$.

Therefore, $M_k = k - 1$ and $M_k^* = ((k+1)^2 - 3)/3$.

Sadly...

It's much more complicated than that...

Sometimes $\Psi(\mathfrak{p})$ avoids quadratic or cubic residues.

We have to break up cases according $k \pmod{36}$. (In the case of $k \equiv 11, 23 \mod 36$, the previous analysis works.)

We have to move to point counting on Jacobians of curves

$$\gamma z^n(1 - \gamma z^n) = \delta x^3$$

for $n = 1, 2, 3, 6$.

And when k splits it's (complicated)^2.

And if k isn't prime ...

Conjecture for $j = 0$

Let $k \in \mathbb{Z}$ satisfy $\gcd(6, k) = 1$.

$$S_k = \left\{ m \in \frac{\mathcal{O}_K}{k\mathcal{O}_K} : \gcd\big(m(1-m), k\mathcal{O}_K\big) = 1 \right\}.$$

$\boxed{\text{(a) } k \equiv 1 \pmod 4 \text{ and } k \overset{pr}{\equiv} \pm 1 \pmod 9}$

$$M_k = \left\{ m \in S_k : \left(\frac{m}{k}\right)_2 = -1 \text{ and } \left(\frac{m}{k}\right)_3 \neq 1 \right\}.$$

$\boxed{\text{(b) } k \equiv 1 \pmod 4 \text{ and } k \overset{pr}{\not\equiv} \pm 1 \pmod 9}$

$$M_k = \left\{ m \in S_k : \left(\frac{m}{k}\right)_2 = -1 \right\}.$$

Conjecture for $j = 0$

$$\boxed{\text{(c) } k \equiv 3 \pmod 4 \text{ and } k \overset{pr}{\equiv} \pm 1 \pmod 9}$$

$$M_k = \left\{ m \in S_k : \left(\frac{m}{k}\right)_3 \neq 1 \right\}.$$

$$\boxed{\text{(d) } k \equiv 3 \pmod 4 \text{ and } k \overset{pr}{\not\equiv} \pm 1 \pmod 9}$$

$$M_k = S_k.$$

Further, for every k we define a subset of M_k by

$$M_k^* = \left\{ m \in M_k : \left(\frac{m(1-m)}{k}\right)_3 = 1 \right\}.$$

Conjecture for $j = 0$

Conjecture

Let $k \in$ be an integer satisfying $\gcd(6, k) = 1$*. Then*

$$\lim_{X \to \infty} \frac{\mathcal{Q}_k(X)}{\mathcal{N}_k(X)} = \frac{\#M_k^*}{4\#M_k}. \tag{1}$$

Conjecture for $j = 0$ with k prime

$$\lim_{X \to \infty} \frac{\mathcal{Q}_k(X)}{\mathcal{N}_k(X)} = \frac{1}{6} + \frac{1}{2} R(k),$$

where $R(k)$ depends on $k \pmod{36}$ and is given by:

k mod 36	$R(k)$
$1, 19$	$\frac{2}{3(k-3)}$
$13, 25$	0
$7, 31$	$\frac{2k}{3(k-2)^2}$

k mod 36	$R(k)$
$17, 35$	$\frac{2}{3(k-1)}$
$5, 29$	0
$11, 23$	$\frac{2k}{3(k^2-2)}$

Data for $j = 0$ as k varies

					Density of Type I/II	
k	$\mathcal{Q}_k(X)$	$\mathcal{N}_k^{(1)}(X)$	$\mathcal{N}_k(X)$	$\mathcal{Q}/\mathcal{N}^{(1)}$	exper't	conjecture
5 (b.2)	29340	58594	175703	0.251	0.3335	$\frac{1}{3} = 0.3333$
7 (d.1)	43992	87825	168743	0.251	0.5205	$\frac{13}{25} = 0.5200$
11 (d.2)	33721	66698	169062	0.253	0.3945	$\frac{47}{119} = 0.3950$
13 (b.1)	28036	55766	167333	0.252	0.3333	$\frac{1}{3} = 0.3333$
17 (a.2)	32008	63810	169226	0.251	0.3771	$\frac{3}{8} = 0.3750$
19 (c.1)	31729	63066	168196	0.252	0.3750	$\frac{3}{8} = 0.3750$
23 (d.2)	30480	61210	168512	0.249	0.3632	$\frac{191}{527} = 0.3624$
29 (b.2)	28085	56286	168642	0.249	0.3338	$\frac{1}{3} = 0.3333$
31 (d.1)	30301	60349	168344	0.251	0.3585	$\frac{301}{841} = 0.3579$
37 (a.1)	29728	59430	168471	0.250	0.3528	$\frac{6}{17} = 0.3529$
41 (b.2)	28050	56381	168567	0.249	0.3345	$\frac{1}{3} = 0.3333$
43 (d.1)	29619	58807	168410	0.252	0.3492	$\frac{589}{1681} = 0.3504$
47 (d.2)	29220	58400	168365	0.250	0.3469	$\frac{767}{2207} = 0.3475$
53 (a.2)	29278	58257	168353	0.252	0.3460	$\frac{9}{26} = 0.3462$
59 (d.2)	29378	58422	168783	0.252	0.3461	$\frac{1199}{3479} = 0.3446$
61 (b.1)	28027	55816	168197	0.251	0.3318	$\frac{1}{3} = 0.3333$
67 (d.1)	29242	57944	168239	0.253	0.3444	$\frac{1453}{4225} = 0.3439$
71 (c.2)	28789	57661	168508	0.249	0.3422	$\frac{12}{35} = 0.3429$

Table: Density of Amicable and Type I/II primes with $p \leq X = 10^8$ for the curve $y^2 = x^3 + k$, prime k.

Final Remarks / Further Ideas

1. The predictions, even for the very complicated cases, are coming out to quadratic polynomials in k. In other words, *all the point counting and traces of Frobenius cancel!* We don't have a simple explanation for this. **Questions:** Can Sage do these computations? Can doing these computations in Sage provide any insight? Are there other approaches to counting residues m modulo k satisfying $\left(\frac{f(m)}{k}\right)_6 = 1$ for a fixed polynomial f?

2. One might look at this as a dynamical system: iterating $f(p) = \#E(\mathbb{F}_p)$. Only what if $f(p)$ is composite? One idea: defining a_n as in the L-series $L(E/\mathbb{Q}, s) = \sum_{n \geq 1} a_n/n^s$, and set $f(n) = n + 1 - a_n$ (H. Sahinoglu). **Other ideas?**

3. If p is anomalous for E, then $E(\mathbb{F}_p)$ has special properties (anomalous ECDLP attack). What if (p, q) is an amicable pair?

4. Are there fast ways to search for or construct amicable pairs or aliquot cycles?

Appendix: CM curves used in data

$$(D,f)=(3,3) \qquad y^2 = x^3 - 120x + 506,$$
$$(D,f)=(11,1) \qquad y^2 + y = x^3 - x^2 - 7x + 10,$$
$$(D,f)=(19,1) \qquad y^2 + y = x^3 - 38x + 90,$$
$$(D,f)=(43,1) \qquad y^2 + y = x^3 - 860x + 9707,$$
$$(D,f)=(67,1) \qquad y^2 + y = x^3 - 7370x + 243528,$$
$$(D,f)=(163,1) \qquad y^2 + y = x^3 - 2174420x + 1234136692.$$

A lemma

Lemma

Let k, E, p, q, $\mathfrak{p}$, and $\mathfrak{q}$ be as above. Then

$$\left(\frac{4}{\Psi(\mathfrak{p})}\right)_6 \left(\frac{4}{1-\Psi(\mathfrak{p})}\right)_6 = 1.$$

Proof of lemma

Proof.

Check that $w(1-w) \equiv 1 \mod 3\mathcal{O}_K$ whenever $w, 1-w \in (\mathcal{O}_K/3\mathcal{O}_K)^*$. Choose $u \in \mu_6$ such that $2, u\Psi(\mathfrak{p}), u^{-1}(1-\Psi(\mathfrak{p}))$ are primary.

$$\begin{aligned}
\left(\frac{2}{\psi_E(\mathfrak{p})}\right)_3 \left(\frac{2}{1-\psi_E(\mathfrak{p})}\right)_3 &= \left(\frac{2}{u\psi_E(\mathfrak{p})}\right)_3 \left(\frac{2}{u^{-1}(1-\psi_E(\mathfrak{p}))}\right)_3 \\
&= \left(\frac{u\psi_E(\mathfrak{p})}{2}\right)_3 \left(\frac{u^{-1}(1-\psi_E(\mathfrak{p}))}{2}\right)_3 \\
&= \left(\frac{\psi_E(\mathfrak{p})(1-\Psi(\mathfrak{p}))}{2}\right)_3 .
\end{aligned}$$

And $w(1-w) \equiv 1 \mod 2\mathcal{O}_K$ whenever $w, 1-w \in (\mathcal{O}_K/2\mathcal{O}_K)^*$. $\square$

Applying Cubic Reciprocity

Let E be the curve $y^2 = x^3 + k$ and suppose $\#\tilde{E}_p(\mathbb{F}_p)$ is prime.

$$\begin{aligned}
&\left(\frac{4k}{\Psi_E(\mathfrak{p})}\right)_6 \left(\frac{4k}{1-\Psi_E(\mathfrak{p})}\right)_6 \\
&= \left(\frac{4}{\Psi_E(\mathfrak{p})}\right)_6 \left(\frac{4}{1-\Psi_E(\mathfrak{p})}\right)_6 \left(\frac{k}{\Psi_E(\mathfrak{p})}\right)_6 \left(\frac{k}{1-\Psi_E(\mathfrak{p})}\right)_6 \\
&= \left(\frac{k}{\Psi_E(\mathfrak{p})}\right)_6 \left(\frac{k}{1-\Psi_E(\mathfrak{p})}\right)_6 \\
&= \left(\frac{k}{\Psi_E(\mathfrak{p})}\right)_2 \left(\frac{k}{1-\Psi_E(\mathfrak{p})}\right)_2 \left(\frac{k}{\Psi_E(\mathfrak{p})}\right)_3^{-1} \left(\frac{k}{1-\Psi_E(\mathfrak{p})}\right)_3^{-1} \\
&= \pm \left(\frac{k}{\Psi_E(\mathfrak{p})}\right)_3^{-1} \left(\frac{k}{1-\Psi_E(\mathfrak{p})}\right)_3^{-1} \\
&= \pm \left(\frac{\Psi_E(\mathfrak{p})(1-\Psi_E(\mathfrak{p}))}{k}\right)_3^{-1}.
\end{aligned}$$