Amicable pairs for elliptic curves

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

CMS Winter Meeting - Number Theory Session
December 6, 2009

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 $p, q < 10^7$:

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

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?

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

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

Heuristic

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

Conjecture of Koblitz and Zywina:

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

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 and Zywina:

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

Rough estimate using Sato–Tate conjecture:

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

Heuristic

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

Conjecture of Koblitz and Zywina:

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

Rough estimate using Sato–Tate conjecture:

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

Together:

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

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

$$
\begin{aligned}
\mathcal{Q}_E(X) &\approx \sum_{p \leq X} \text{Prob}(p \text{ is part of an amicable pair }) \\
&\gg\ll \sum_{p \leq X} \frac{1}{\sqrt{p}(\log p)} \\
&\gg\ll \frac{\sqrt{X}}{(\log X)^2}.
\end{aligned}
$$

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.

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.

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: 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 $q = \#E(\mathbb{F}_p)$.

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

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

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

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

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

CM case: Twist Theorem proof

Eliminating curves with 2-torsion leaves $D \equiv 3 \mod 4$.

CM case: Twist Theorem proof

Eliminating curves with 2-torsion leaves $D \equiv 3 \mod 4$.

p splits as $p = \mathfrak{p}\overline{\mathfrak{p}}$ (if it were inert, we would have supersingular reduction, $\#E(\mathbb{F}_p) = p + 1$).

CM case: Twist Theorem proof

Eliminating curves with 2-torsion leaves $D \equiv 3 \mod 4$.

p splits as $p = \mathfrak{p}\overline{\mathfrak{p}}$ (if it were inert, we would have supersingular reduction, $\#E(\mathbb{F}_p) = p + 1$).

$\#E(\mathbb{F}_p) = N(\Psi(\mathfrak{p})) + 1 - Tr(\Psi(\mathfrak{p}))$ where Ψ is the Grössencharacter of E.

CM case: Twist Theorem proof

Eliminating curves with 2-torsion leaves $D \equiv 3 \mod 4$.

p splits as $p = \mathfrak{p}\overline{\mathfrak{p}}$ (if it were inert, we would have supersingular reduction, $\#E(\mathbb{F}_p) = p + 1$).

$\#E(\mathbb{F}_p) = N(\Psi(\mathfrak{p})) + 1 - Tr(\Psi(\mathfrak{p}))$ where Ψ is the Grössencharacter of E.

$N(1 - \Psi(\mathfrak{p})) = \#E(\mathbb{F}_\mathfrak{p}) = \#E(\mathbb{F}_p) = q$ so q splits as $q = \mathfrak{q}\overline{\mathfrak{q}}$.

CM case: Twist Theorem proof

Eliminating curves with 2-torsion leaves $D \equiv 3 \mod 4$.

p splits as $p = \mathfrak{p}\overline{\mathfrak{p}}$ (if it were inert, we would have supersingular reduction, $\#E(\mathbb{F}_p) = p + 1$).

$\#E(\mathbb{F}_p) = N(\Psi(\mathfrak{p})) + 1 - Tr(\Psi(\mathfrak{p}))$ where Ψ is the Grössencharacter of E.

$N(1 - \Psi(\mathfrak{p})) = \#E(\mathbb{F}_\mathfrak{p}) = \#E(\mathbb{F}_p) = q$ so q splits as $q = \mathfrak{q}\overline{\mathfrak{q}}$.

$N(\Psi(\mathfrak{q})) = q$.

CM case: Twist Theorem proof

Eliminating curves with 2-torsion leaves $D \equiv 3 \mod 4$.

p splits as $p = \mathfrak{p}\bar{\mathfrak{p}}$ (if it were inert, we would have supersingular reduction, $\#E(\mathbb{F}_p) = p + 1$).

$\#E(\mathbb{F}_p) = N(\Psi(\mathfrak{p})) + 1 - Tr(\Psi(\mathfrak{p}))$ where Ψ is the Grössencharacter of E.

$N(1 - \Psi(\mathfrak{p})) = \#E(\mathbb{F}_\mathfrak{p}) = \#E(\mathbb{F}_p) = q$ so q splits as $q = \mathfrak{q}\bar{\mathfrak{q}}$.

$N(\Psi(\mathfrak{q})) = q$.

So $1 - \Psi(\mathfrak{p}) = u\Psi(\mathfrak{q})$ for some unit $u \in \{\pm 1\}$.

CM case: Twist Theorem proof

Eliminating curves with 2-torsion leaves $D \equiv 3 \mod 4$.

p splits as $p = \mathfrak{p}\bar{\mathfrak{p}}$ (if it were inert, we would have supersingular reduction, $\#E(\mathbb{F}_p) = p + 1$).

$\#E(\mathbb{F}_p) = N(\Psi(\mathfrak{p})) + 1 - Tr(\Psi(\mathfrak{p}))$ where Ψ is the Grössencharacter of E.

$N(1 - \Psi(\mathfrak{p})) = \#E(\mathbb{F}_\mathfrak{p}) = \#E(\mathbb{F}_p) = q$ so q splits as $q = \mathfrak{q}\bar{\mathfrak{q}}$.

$N(\Psi(\mathfrak{q})) = q$.

So $1 - \Psi(\mathfrak{p}) = u\Psi(\mathfrak{q})$ for some unit $u \in \{\pm 1\}$.

$Tr(\Psi(\mathfrak{q})) = \pm Tr(1 - \Psi(\mathfrak{p})) = \pm(2 - Tr(\Psi(\mathfrak{p}))) = \pm(q + 1 - p)$.

CM case: Twist Theorem proof

Eliminating curves with 2-torsion leaves $D \equiv 3 \mod 4$.

p splits as $p = \mathfrak{p}\overline{\mathfrak{p}}$ (if it were inert, we would have supersingular reduction, $\#E(\mathbb{F}_p) = p + 1$).

$\#E(\mathbb{F}_p) = N(\Psi(\mathfrak{p})) + 1 - Tr(\Psi(\mathfrak{p}))$ where Ψ is the Grössencharacter of E.

$N(1 - \Psi(\mathfrak{p})) = \#E(\mathbb{F}_\mathfrak{p}) = \#E(\mathbb{F}_p) = q$ so q splits as $q = \mathfrak{q}\overline{\mathfrak{q}}$.

$N(\Psi(\mathfrak{q})) = q$.

So $1 - \Psi(\mathfrak{p}) = u\Psi(\mathfrak{q})$ for some unit $u \in \{\pm 1\}$.

$Tr(\Psi(\mathfrak{q})) = \pm Tr(1 - \Psi(\mathfrak{p})) = \pm(2 - Tr(\Psi(\mathfrak{p}))) = \pm(q + 1 - p)$.

So...

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

Twist frequencies for CM case

(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 by $\mathbb{Q}(\sqrt{-D})$

Twist frequencies for CM case

(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 by $\mathbb{Q}(\sqrt{-D})$

(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 by $\mathbb{Q}(\sqrt{-D})$

Conjectures

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.

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.

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

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

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

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

Example

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

Aliquot cycles

Definition

Let $E/\mathbb{Q}$ 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

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

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

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

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 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 $p \geq 5$.

Proof (sketch).

Postulate a cycle $p_1, \ldots, p_\ell$ (for a contradiction). Use CM theorem on pairs to write a linear recurrence relation for p_ℓ. See that it is strictly monotonic. $\square$

CM $j = 0$ case: Twist Theorem

$$K = \mathbb{Q}(\sqrt{-3}), \qquad \mu_6 \subset \mathcal{O}_K = \mathbb{Z}[\omega]$$

CM $j = 0$ case: Twist Theorem

$$K = \mathbb{Q}(\sqrt{-3}), \qquad \mu_6 \subset \mathcal{O}_K = \mathbb{Z}[\omega]$$

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 $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Define $\mathfrak{q} = \big(1 - \Psi(\mathfrak{p})\big)\mathcal{O}_K$. Then we have $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$.

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

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 $y^2 = x^3 + k$

$$1/12 = 0.08333\ldots$$

Applying Cubic Reciprocity

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

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

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

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

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

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

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

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

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

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

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 $\left(\frac{y(1-y)}{k}\right)_3 = 1$.

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

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 $\left(\frac{m(1-m)}{k}\right)_3 = 1$.

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:

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

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

Data for $j = 0$ as k varies

k	$\mathcal{Q}_k(X)$	$\mathcal{N}_k^{(1)}(X)$	$\mathcal{N}_k(X)$	$\mathcal{Q}/\mathcal{N}^{(1)}$	Density of Type I/II	
					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

1. The predictions, even for the very complicated cases, are coming out to simple rational functions of k (all the point counting cancels). We don't have a simple explanation for this.

Final Remarks

1. The predictions, even for the very complicated cases, are coming out to simple rational functions of k (all the point counting cancels). We don't have a simple explanation for this.

2. One might look at this as a dynamical system: define a_n as in the L-series $L(E/\mathbb{Q}, s) = \sum_{n \geq 1} a_n/n^s$, and iterate the function $f(n) = n + 1 - a_n$ (future work).

Final Remarks

1. The predictions, even for the very complicated cases, are coming out to simple rational functions of k (all the point counting cancels). We don't have a simple explanation for this.

2. One might look at this as a dynamical system: define a_n as in the L-series $L(E/\mathbb{Q}, s) = \sum_{n \geq 1} a_n/n^s$, and iterate the function $f(n) = n + 1 - a_n$ (future work).

3. This question arises naturally from a question about when $n | W_n$ for an elliptic divisibility sequence (also work-in-progress). Smyth recently studied this for Lucas sequences.

Final Remarks

1. The predictions, even for the very complicated cases, are coming out to simple rational functions of k (all the point counting cancels). We don't have a simple explanation for this.

2. One might look at this as a dynamical system: define a_n as in the L-series $L(E/\mathbb{Q}, s) = \sum_{n \geq 1} a_n/n^s$, and iterate the function $f(n) = n + 1 - a_n$ (future work).

3. This question arises naturally from a question about when $n | W_n$ for an elliptic divisibility sequence (also work-in-progress). Smyth recently studied this for Lucas sequences.

4. We're currently running large searches to test the non-CM conjecture.