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

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

and

$$\#E(\mathbb{F}_q) = p.$$
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

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

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

$$\quad (1622311, 1622471)$$

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

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

Question (1)

Let

\[ Q_E(X) = \#\{ \text{amicable pairs } (p, q) \text{ such that } p, q < X \} \]

How does \( Q_E(X) \) grow with \( X \)?
Questions

Question (1)

Let

\[ Q_E(X) = \# \{ \text{amicable pairs } (p, q) \text{ such that } p, q < X \} \]

How does \( Q_E(X) \) grow with \( X \)?

Question (2)

Let

\[ N_E(X) = \# \{ \text{primes } p \leq X \text{ such that } \#E(F_p) \text{ is prime} \} \]

What about \( Q_E(X)/N_E(X) \)?
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

\[ \text{Prob}(p \text{ is part of an amicable pair}) \]
\[ = \text{Prob}(q \overset{\text{def}}{=} \#E(\mathbb{F}_p) \text{ is prime}) \cdot \text{Prob}(\#E(\mathbb{F}_q) = p). \]
Heuristic

\[ \text{Prob}(p \text{ is part of an amicable pair}) \]
\[ = \text{Prob}(q \overset{\text{def}}{=} \#E(\mathbb{F}_p) \text{ is prime}) \text{Prob}(\#E(\mathbb{F}_q) = p). \]

Conjecture of Koblitz and Zywina:

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

\[ \text{Prob}(\rho \text{ is part of an amicable pair}) = \text{Prob}(q \overset{\text{def}}{=} \#E(\mathbb{F}_p) \text{ is prime}) \cdot \text{Prob}(\#E(\mathbb{F}_q) = p). \]

Conjecture of Koblitz and Zywina:

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

Rough estimate using Sato–Tate conjecture:

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

Prob($p$ is part of an amicable pair) 

\[ = \text{Prob}(q \overset{\text{def}}{=} \#E(\mathbb{F}_p) \text{ is prime}) \text{Prob}(\#E(\mathbb{F}_q) = p). \]

Conjecture of Koblitz and Zywina:

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

Rough estimate using Sato–Tate conjecture:

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

Together:

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

$$Q_E(X) \approx \sum_{p \leq X} \text{Prob}(p \text{ is part of an amicable pair })$$

$$\gg \ll \sum_{p \leq X} \frac{1}{\sqrt{p} \log p}$$

$$\gg \ll \frac{\sqrt{X}}{(\log X)^2}.$$
Conjecture (Version 1)

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

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

Assume infinitely many primes $p$ such that $\#E(\mathbb{F}_p)$ is prime.
Conjecture (Version 1)

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

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

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

Then

$$Q_E(X) \ll \frac{\sqrt{X}}{(\log X)^2} \quad \text{as } X \to \infty,$$

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 \( p, q < 10^7 \):

\[
(853, 883), \ (77761, 77999), \\
(1147339, 1148359), \ (1447429, 1447561).
\]

\( y^2 = x^3 + 2 \) 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 $q = \#E(\mathbb{F}_p)$. 

Then either

\[\#E(\mathbb{F}_q) = p\] or

\[\#E(\mathbb{F}_q) = 2q + 2 - p\]

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

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

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

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

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 $D \equiv 3 \pmod{4}$.

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

$\#E(\mathbb{F}_p) = N(\psi(p)) + 1 - Tr(\psi(p))$ where $\psi$ is the Grössencharacter of $E$. 
CM case: Twist Theorem proof

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

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

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

$N(1 - \psi(p)) = \#E(\mathbb{F}_p) = \#E(\mathbb{F}_p) = q$ so $q$ splits as $q = q\overline{q}$.
CM case: Twist Theorem proof

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

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

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

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

$N(\psi(q)) = q$. 

D ≡ 3 mod 4.
CM case: Twist Theorem proof

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

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

$\#E(F_p) = N(\psi(p)) + 1 - Tr(\psi(p))$ where $\psi$ is the Grössencharacter of $E$.

$N(1 - \psi(p)) = \#E(F_p) = \#E(F_p) = q$ so $q$ splits as $q = q\overline{q}$.

$N(\psi(q)) = q$.

So $1 - \psi(p) = u\psi(q)$ 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 $p = p\overline{p}$ (if it were inert, we would have supersingular reduction, $\#E(\mathbb{F}_p) = p + 1$).

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

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

$N(\psi(q)) = q$.

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

$Tr(\psi(q)) = \pm Tr(1 - \psi(p)) = \pm(2 - Tr(\psi(p))) = \pm(q + 1 - p)$. 
CM case: Twist Theorem proof

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

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

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

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

$N(\psi(q)) = q$.

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

$Tr(\psi(q)) = \pm Tr(1 - \psi(p)) = \pm (2 - Tr(\psi(p))) = \pm (q + 1 - p)$.

So...

$\# E(\mathbb{F}_q) = p$ or $\# E(\mathbb{F}_q) = 2q + 2 - p$. 
## Twist frequencies for CM case

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

**Table:** $Q_E(X)$ for elliptic curves with CM by $\mathbb{Q}(\sqrt{-D})$
### Twist frequencies for CM case

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

**Table:** $Q_E(X)$ for elliptic curves with CM by $\mathbb{Q}(\sqrt{-D})$

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

**Table:** $Q_E(X)/N_E(X)$ for elliptic curves with CM by $\mathbb{Q}(\sqrt{-D})$
Conjectures

Conjecture (Version 2)

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

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

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

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

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

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

$$Q_E(X) \gg \ll \frac{\sqrt{X}}{(\log X)^2} \quad \text{as } X \to \infty,$$

where the implied constants depend on $E$. 
Conjecture (Version 2)

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

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

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

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

$$Q_E(X) \gg \ll \frac{\sqrt{X}}{(\log X)^2} \quad \text{as } X \to \infty,$$

where the implied constants depend on $E$.

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

$$Q_E(X) \sim \frac{1}{4}N_E(X) \sim A_E \frac{X}{(\log X)^2}.$$
Aliquot cycles

**Definition**

Let $E/\mathbb{Q}$ be an elliptic curve. An *aliquot cycle of length* $\ell$ 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

\begin{align*}
y^2 &= x^3 - 25x - 8: \quad (83, 79, 73) \\
y^2 &= x^3 + 176209333661915432764478x + 60625229794681596832262: \quad (23, 31, 41, 47, 59, 67, 73, 79, 71, 61, 53, 43, 37, 29)
\end{align*}
Aliquot cycles

Definition
Let $E / \mathbb{Q}$ be an elliptic curve. An *aliquote cycle of length* $\ell$ 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

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

Definition
Let $E/\mathbb{Q}$ be an elliptic curve. An *aliquot cycle of length* $\ell$ 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

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

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

$$(23, 31, 41, 47, 59, 67, 73, 79, 71, 61, 53, 43, 37, 29)$$
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 $p_\ell$. See that it is strictly monotonic.
CM $j = 0$ case: Twist Theorem

\[ K = \mathbb{Q}(\sqrt{-3}), \quad \mu_6 \subset \mathcal{O}_K = \mathbb{Z}[\omega] \]
CM $j=0$ case: Twist Theorem

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

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 $p\mathcal{O}_K = p\overline{p}$. Define $q = (1 - \psi(p))\mathcal{O}_K$. Then we have $q\mathcal{O}_K = q\overline{q}$.

The values of the Grössencharacter at $p$ and $q$ are related by

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

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

<table>
<thead>
<tr>
<th>$k$</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X = 10^4$</td>
<td>0.217</td>
<td>0.141</td>
<td>0.097</td>
<td>0.085</td>
<td>0.165</td>
<td>0.118</td>
</tr>
<tr>
<td>$X = 10^5$</td>
<td>0.251</td>
<td>0.122</td>
<td>0.081</td>
<td>0.134</td>
<td>0.139</td>
<td>0.125</td>
</tr>
<tr>
<td>$X = 10^6$</td>
<td>0.250</td>
<td>0.139</td>
<td>0.083</td>
<td>0.142</td>
<td>0.133</td>
<td>0.107</td>
</tr>
<tr>
<td>$X = 10^7$</td>
<td>0.249</td>
<td>0.139</td>
<td>0.082</td>
<td>0.139</td>
<td>0.129</td>
<td>0.107</td>
</tr>
</tbody>
</table>

Table: $Q_E(X)/N_E(X)$ 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.

\[
\left(\frac{4k}{\psi_E(p)}\right)_6 \left(\frac{4k}{1 - \psi_E(p)}\right)_6 = \cdots \\
= \pm \left(\frac{\psi_E(p)(1 - \psi_E(p))}{k}\right)^{-1}.
\]
Applying Cubic Reciprocity

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

\[
\left(\frac{4k}{\psi_E(p)}\right)_6 \left(\frac{4k}{1 - \psi_E(p)}\right)_6 = \ldots \\
= \pm \left(\frac{\psi_E(p)(1 - \psi_E(p))}{k}\right)_3^{-1}.
\]

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

\[
\mathcal{O}_E(X)/\mathcal{N}_E(X) \to M^*(k)/4M(k).
\]
The symbol \( \left( \frac{m(1-m)}{k} \right)_3 \) when \( k \equiv 2 \text{ mod } 3 \)

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 \((\infty, (0, 0)\) 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 \((\infty, (0, 0)\) 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

\[
\lim_{X \to \infty} \frac{Q_k(X)}{N_k(X)} = \frac{1}{6} + \frac{1}{2} R(k),
\]

where \( R(k) \) depends on \( k \) (mod 36) and is given by:

<table>
<thead>
<tr>
<th>( k ) mod 36</th>
<th>( R(k) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 19</td>
<td>( \frac{2}{3(k - 3)} )</td>
</tr>
<tr>
<td>13, 25</td>
<td>0</td>
</tr>
<tr>
<td>7, 31</td>
<td>( \frac{2k}{3(k - 2)^2} )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( k ) mod 36</th>
<th>( R(k) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>17, 35</td>
<td>( \frac{2}{3(k - 1)} )</td>
</tr>
<tr>
<td>5, 29</td>
<td>0</td>
</tr>
<tr>
<td>11, 23</td>
<td>( \frac{2k}{3(k^2 - 2)} )</td>
</tr>
</tbody>
</table>
### Data for $j = 0$ as $k$ varies

<table>
<thead>
<tr>
<th>$k$</th>
<th>$\mathcal{Q}_k(X)$</th>
<th>$\mathcal{N}_k^{(1)}(X)$</th>
<th>$\mathcal{N}_k(X)$</th>
<th>$\mathcal{Q}/\mathcal{N}^{(1)}$</th>
<th>exper’t</th>
<th>conjecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 (b.2)</td>
<td>29340</td>
<td>58594</td>
<td>175703</td>
<td>0.251</td>
<td>0.3335</td>
<td>$\frac{1}{3} = 0.3333$</td>
</tr>
<tr>
<td>7 (d.1)</td>
<td>43992</td>
<td>87825</td>
<td>168743</td>
<td>0.251</td>
<td>0.5205</td>
<td>$\frac{13}{25} = 0.5200$</td>
</tr>
<tr>
<td>11 (d.2)</td>
<td>33721</td>
<td>66698</td>
<td>169062</td>
<td>0.253</td>
<td>0.3945</td>
<td>$\frac{119}{25} = 0.3950$</td>
</tr>
<tr>
<td>13 (b.1)</td>
<td>28036</td>
<td>55766</td>
<td>167333</td>
<td>0.252</td>
<td>0.3333</td>
<td>$\frac{1}{3} = 0.3333$</td>
</tr>
<tr>
<td>17 (a.2)</td>
<td>32008</td>
<td>63810</td>
<td>169226</td>
<td>0.251</td>
<td>0.3771</td>
<td>$\frac{13}{3} = 0.3750$</td>
</tr>
<tr>
<td>19 (c.1)</td>
<td>31729</td>
<td>63066</td>
<td>168196</td>
<td>0.252</td>
<td>0.3750</td>
<td>$\frac{191}{527} = 0.3624$</td>
</tr>
<tr>
<td>23 (d.2)</td>
<td>30480</td>
<td>61210</td>
<td>168512</td>
<td>0.249</td>
<td>0.3632</td>
<td>$\frac{1}{3} = 0.3333$</td>
</tr>
<tr>
<td>29 (b.2)</td>
<td>28085</td>
<td>56286</td>
<td>168642</td>
<td>0.249</td>
<td>0.3338</td>
<td>$\frac{1}{3} = 0.3333$</td>
</tr>
<tr>
<td>31 (d.1)</td>
<td>30301</td>
<td>60349</td>
<td>168344</td>
<td>0.251</td>
<td>0.3585</td>
<td>$\frac{301}{841} = 0.3579$</td>
</tr>
<tr>
<td>37 (a.1)</td>
<td>29728</td>
<td>59430</td>
<td>168471</td>
<td>0.250</td>
<td>0.3528</td>
<td>$\frac{3}{17} = 0.3529$</td>
</tr>
<tr>
<td>41 (b.2)</td>
<td>28050</td>
<td>56381</td>
<td>168567</td>
<td>0.249</td>
<td>0.3345</td>
<td>$\frac{1}{3} = 0.3333$</td>
</tr>
<tr>
<td>43 (d.1)</td>
<td>29619</td>
<td>58807</td>
<td>168410</td>
<td>0.252</td>
<td>0.3492</td>
<td>$\frac{589}{1681} = 0.3504$</td>
</tr>
<tr>
<td>47 (d.2)</td>
<td>29220</td>
<td>58400</td>
<td>168365</td>
<td>0.250</td>
<td>0.3469</td>
<td>$\frac{767}{2207} = 0.3475$</td>
</tr>
<tr>
<td>53 (a.2)</td>
<td>29278</td>
<td>58257</td>
<td>168353</td>
<td>0.252</td>
<td>0.3460</td>
<td>$\frac{9}{25} = 0.3642$</td>
</tr>
<tr>
<td>59 (d.2)</td>
<td>29378</td>
<td>58422</td>
<td>168783</td>
<td>0.252</td>
<td>0.3461</td>
<td>$\frac{1199}{3479} = 0.3446$</td>
</tr>
<tr>
<td>61 (b.1)</td>
<td>28027</td>
<td>55816</td>
<td>168197</td>
<td>0.251</td>
<td>0.3318</td>
<td>$\frac{1}{3} = 0.3333$</td>
</tr>
<tr>
<td>67 (d.1)</td>
<td>29242</td>
<td>57944</td>
<td>168239</td>
<td>0.253</td>
<td>0.3444</td>
<td>$\frac{1453}{4225} = 0.3439$</td>
</tr>
<tr>
<td>71 (c.2)</td>
<td>28789</td>
<td>57661</td>
<td>168508</td>
<td>0.249</td>
<td>0.3422</td>
<td>$\frac{12}{35} = 0.3429$</td>
</tr>
</tbody>
</table>

**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.