Amicable Pairs
for
Elliptic Curves

Joseph H. Silverman
(joint work with Katherine Stange)

Brown University

Palmetto Number Theory Series (PANTS XII)
Clemson University

February 20–21, 2010

Perfect Numbers and Amicable Pairs

A **Perfect Number** is an integer n that equals the sum of its proper divisors

$$n = s(n) = \sum_{\substack{d \mid n \\ d < n}} d.$$

For example,

$$6 = 1 + 2 + 3 \quad \text{and} \quad 28 = 1 + 2 + 4 + 7 + 14.$$

Perfect Numbers and Amicable Pairs

A **Perfect Number** is an integer n that equals the sum of its proper divisors

$$n = s(n) = \sum_{\substack{d|n \\ d<n}} d.$$

For example,

$$6 = 1 + 2 + 3 \quad \text{and} \quad 28 = 1 + 2 + 4 + 7 + 14.$$

An **Amicable Pair** is a pair of distinct integers (m, n) satisfying

$$n = s(m) \quad \text{and} \quad m = s(n).$$

The smallest amicable pair is $(220, 284)$,

$$\begin{aligned} 220 &= 1 + 2 + 4 + 71 + 142, \\ 284 &= 1 + 2 + 4 + 5 + 10 + 11 + 20 \\ &\qquad + 22 + 44 + 55 + 110. \end{aligned}$$

Perfect Numbers, Amicable Pairs, and Aliquot Cycles

The study of perfect numbers and amicable pairs dates back to the Pythagoreans.

Perfect Numbers, Amicable Pairs, and Aliquot Cycles

The study of perfect numbers and amicable pairs dates back to the Pythagoreans.

More generally, an **Aliquot Cycle** is a sequence

$$(n_1, n_2, \ldots, n_\ell)$$

satisfying

$$s(n_1) = n_2, \quad s(n_2) = n_3, \ldots, s(n_\ell) = n_1.$$

Perfect Numbers, Amicable Pairs, and Aliquot Cycles

The study of perfect numbers and amicable pairs dates back to the Pythagoreans.

More generally, an **Aliquot Cycle** is a sequence

$$(n_1, n_2, \ldots, n_\ell)$$

satisfying

$$s(n_1) = n_2, \quad s(n_2) = n_3, \ldots, s(n_\ell) = n_1.$$

For example,

$$1264460, 1547860, 1727636, 1305184$$

is an aliquot cycle of length 4. The longest known aliquot cycle has length 28.

Perfect Numbers, Amicable Pairs, and Aliquot Cycles

The study of perfect numbers and amicable pairs dates back to the Pythagoreans.

More generally, an **Aliquot Cycle** is a sequence

$$(n_1, n_2, \ldots, n_\ell)$$

satisfying

$$s(n_1) = n_2, \quad s(n_2) = n_3, \ldots, s(n_\ell) = n_1.$$

For example,

$$1264460, 1547860, 1727636, 1305184$$

is an aliquot cycle of length 4. The longest known aliquot cycle has length 28.

In this talk, which is joint work with **Kate Stange**, I will discuss elliptic curve analogues of these ideas.

Elliptic Curves

Recall that an elliptic curve is the set of solutions to an equation of the form

$$E : y^2 = x^3 + Ax + B, \qquad \text{with } \Delta = -16(4A^3 + 27B^2) \neq 0.$$

The set of rational points $E(\mathbb{Q})$ forms a group in the usual way using secant and tangent lines to define the group law.

Elliptic Curves

Recall that an elliptic curve is the set of solutions to an equation of the form

$$E : y^2 = x^3 + Ax + B, \qquad \text{with } \Delta = -16(4A^3 + 27B^2) \neq 0.$$

The set of rational points $E(\mathbb{Q})$ forms a group in the usual way using secant and tangent lines to define the group law.

Making a change of variables, we will assume that $A, B \in \mathbb{Z}$, so we can reduce the equation modulo p to get a curve $\tilde{E}/\mathbb{F}_p$. We say that E has **good reduction** if $p \nmid \Delta$, in which case $\tilde{E}(\mathbb{F}_p)$ is also a group.

Elliptic Curves

Recall that an elliptic curve is the set of solutions to an equation of the form

$$E : y^2 = x^3 + Ax + B, \qquad \text{with } \Delta = -16(4A^3 + 27B^2) \neq 0.$$

The set of rational points $E(\mathbb{Q})$ forms a group in the usual way using secant and tangent lines to define the group law.

Making a change of variables, we will assume that $A, B \in \mathbb{Z}$, so we can reduce the equation modulo p to get a curve $\tilde{E}/\mathbb{F}_p$. We say that E has **good reduction** if $p \nmid \Delta$, in which case $\tilde{E}(\mathbb{F}_p)$ is also a group.

Theorem. (Hasse)

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 - a_p \qquad \text{with } |a_p| \leq 2\sqrt{p}.$$

Perfect Primes for Elliptic Curves

By analogy with the classical situation, we might say that a prime p is **perfect** for E if

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

Elliptic perfect primes arise as exceptional cases in many settings, ranging from the abstract (ℓ-adic represnta- tions) to the practical (cryptography).

Perfect Primes for Elliptic Curves

By analogy with the classical situation, we might say that a prime p is **perfect** for E if

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

Elliptic perfect primes arise as exceptional cases in many settings, ranging from the abstract (ℓ-adic represntations) to the practical (cryptography).

The cryptographic application is related to the elliptic curve discrete logarithm problem (ECDLP), which underlies many practical cryptographic constructions. In general, the ECDLP is very (exponentially) hard to solve; but for perfect primes, it's trivial (linear time).

Perfect Primes for Elliptic Curves

By analogy with the classical situation, we might say that a prime p is **perfect** for E if

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

Elliptic perfect primes arise as exceptional cases in many settings, ranging from the abstract (ℓ-adic represnta-tions) to the practical (cryptography).

The cryptographic application is related to the elliptic curve discrete logarithm problem (ECDLP), which underlies many practical cryptographic constructions. In general, the ECDLP is very (exponentially) hard to solve; but for perfect primes, it's trivial (linear time).

Side Note: Our use of the word "perfect" in this context is non-standard. In the literature, our elliptic perfect primes are called **anomalous primes**.

Amicable Pairs for Elliptic Curves

An **Amicable Pair** for the elliptic curve E is a pair of distinct good reduction primes (p, q) satisfying

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

Amicable Pairs for Elliptic Curves

An **Amicable Pair** for the elliptic curve E is a pair of distinct good reduction primes (p, q) satisfying

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

Example. The smallest amicable pair on the elliptic curve

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

is $(1622311, 1622471)$ and there are no other amicable pairs smaller than 10^7.

Aliquot Cycles for Elliptic Curves

More generally, an **Aliquot Cycle** for E is a list of distinct good reduction primes $(p_1, \ldots, p_\ell)$ satisfying

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

Aliquot Cycles for Elliptic Curves

More generally, an **Aliquot Cycle** for E is a list of distinct good reduction primes $(p_1, \ldots, p_\ell)$ satisfying

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

Example The elliptic curve

$$\begin{aligned} y^2 = x^3 &+ 4545482133607498579268567738514832922289740324532x \\ &+ 5958672654621121182914302458943794649678857947 13. \end{aligned}$$

has an aliquot cycle of length 25, starting with the prime $p = 41$.

Aliquot Cycles for Elliptic Curves

More generally, an **Aliquot Cycle** for E is a list of distinct good reduction primes $(p_1, \ldots, p_\ell)$ satisfying

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

Example The elliptic curve

$$\begin{aligned} y^2 = x^3 &+ 4545482133607498579268567738514832922289740324532x \\ &+ 5958672654621121182914302458943794649678857947 13. \end{aligned}$$

has an aliquot cycle of length 25, starting with the prime $p = 41$.

Elliptic amicable pairs and longer aliquot cycles seem not to have been studied before. They arise naturally when studying index divisibility of elliptic divisibility sequences, but seem quite interesting in their own right. This talk will explore some of their properties.

Creating Curves with Long Aliquot Cycles

Theorem. For every $\ell \geq 1$ there exists an elliptic curve $E/\mathbb{Q}$ with an aliquot cycle of length ℓ.

The proof is three easy steps:

Creating Curves with Long Aliquot Cycles

Theorem. For every $\ell \geq 1$ there exists an elliptic curve $E/\mathbb{Q}$ with an aliquot cycle of length ℓ.

The proof is three easy steps:

- Choose primes $(p_1, \ldots, p_\ell)$ with $p_{i+1} < p_i + 2\sqrt{p_i} + 1$. (The prime number theorem lets us take consecutive primes if p_1 is large enough.)

Creating Curves with Long Aliquot Cycles

Theorem. For every $\ell \geq 1$ there exists an elliptic curve $E/\mathbb{Q}$ with an aliquot cycle of length ℓ.

The proof is three easy steps:

- Choose primes $(p_1, \ldots, p_\ell)$ with $p_{i+1} < p_i + 2\sqrt{p_i} + 1$. (The prime number theorem lets us take consecutive primes if p_1 is large enough.)
- For each p_i, choose an elliptic curve $\tilde{E}_i/\mathbb{F}_{p_i}$ satisfying $\#\tilde{E}_i(\mathbb{F}_{p_i}) = p_{i+1}$. (A result of Deuring says that such curves exist.)

Creating Curves with Long Aliquot Cycles

Theorem. For every $\ell \geq 1$ there exists an elliptic curve $E/\mathbb{Q}$ with an aliquot cycle of length ℓ.

The proof is three easy steps:

- Choose primes $(p_1, \ldots, p_\ell)$ with $p_{i+1} < p_i + 2\sqrt{p_i} + 1$. (The prime number theorem lets us take consecutive primes if p_1 is large enough.)
- For each p_i, choose an elliptic curve $\tilde{E}_i/\mathbb{F}_{p_i}$ satisfying $\#\tilde{E}_i(\mathbb{F}_{p_i}) = p_{i+1}$. (A result of Deuring says that such curves exist.)
- Use the Chinese remainder theorem applied to the coefficients of equations for $\tilde{E}_1, \ldots, \tilde{E}_\ell$ to find a curve $E/\mathbb{Q}$ with $E \bmod p_i = \tilde{E}_i$.

Elliptic Groups of Prime Order

For some elliptic curves, $\#E(\mathbb{F}_p)$ is never prime. This happens if $E(\mathbb{Q})$ has points of finite order, because (more-or-less)

$$\boxed{E(\mathbb{Q})_{\text{tors}} \hookrightarrow \tilde{E}(\mathbb{F}_p).}$$

So we restrict attention to curves with $E(\mathbb{Q})_{\text{tors}} = 0$.

Elliptic Groups of Prime Order

For some elliptic curves, $\#E(\mathbb{F}_p)$ is never prime. This happens if $E(\mathbb{Q})$ has points of finite order, because (more-or-less)

$$E(\mathbb{Q})_{\text{tors}} \hookrightarrow \tilde{E}(\mathbb{F}_p).$$

So we restrict attention to curves with $E(\mathbb{Q})_{\text{tors}} = 0$. Koblitz and Zywina give a precise conjecture concerning the density of primes such that $\#\tilde{E}(\mathbb{F}_p)$ is prime.

Conjecture. (Koblitz, Zywina) The is a constant C_E such that

$$\#\{p < X : \#\tilde{E}(\mathbb{F}_p) \text{ is prime}\} \sim C_E \frac{X}{(\log X)^2}.$$

They give an explicit formula for C_E in terms of the Galois representation attached to E.

Counting Amicable Pairs and Aliquot Cycles

For simplicity, I'll restrict to amicable pairs. Let

$$\mathcal{A}_E(X) = \#\left\{ p < X : \begin{array}{l} p \text{ is part of an} \\ \text{amicable pair } (p,q) \end{array} \right\}.$$

Counting Amicable Pairs and Aliquot Cycles

For simplicity, I'll restrict to amicable pairs. Let

$$\mathcal{A}_E(X) = \#\left\{ p < X : \begin{array}{l} p \text{ is part of an} \\ \text{amicable pair } (p,q) \end{array} \right\}.$$

Conjecture. Either $\mathcal{A}_E(X)$ is bounded, or else

$$\mathcal{A}_E(X) \gg\ll \frac{\sqrt{X}}{(\log X)^2} \qquad \text{as } X \to \infty.$$

Counting Amicable Pairs and Aliquot Cycles

For simplicity, I'll restrict to amicable pairs. Let

$$\mathcal{A}_E(X) = \#\left\{ p < X : \begin{array}{l} p \text{ is part of an} \\ \text{amicable pair } (p, q) \end{array} \right\}.$$

Conjecture. Either $\mathcal{A}_E(X)$ is bounded, or else

$$\mathcal{A}_E(X) \gg\ll \frac{\sqrt{X}}{(\log X)^2} \qquad \text{as } X \to \infty.$$

[I've omitted one condition]

Counting Amicable Pairs and Aliquot Cycles

For simplicity, I'll restrict to amicable pairs. Let

$$\mathcal{A}_E(X) = \#\left\{ p < X : \begin{array}{l} p \text{ is part of an} \\ \text{amicable pair } (p,q) \end{array} \right\}.$$

Conjecture. Either $\mathcal{A}_E(X)$ is bounded, or else

$$\mathcal{A}_E(X) \gg\ll \frac{\sqrt{X}}{(\log X)^2} \qquad \text{as } X \to \infty.$$

[I've omitted one condition]

Justification: Let $N_p = \#\tilde{E}(\mathbb{F}_p)$ and $N_q = \#\tilde{E}(\mathbb{F}_q)$.

$$\begin{aligned} &\text{Prob}(p \text{ is part of an amicable pair}) \\ &\qquad = \text{Prob}(q = N_p \text{ is prime and } N_q = p) \\ &\qquad = \text{Prob}(q = N_p \text{ is prime}) \\ &\qquad\qquad\qquad \cdot \text{Prob}(N_q = p \mid q = N_p \text{ is prime}) \\ &\qquad \gg\ll \frac{1}{\log p} \cdot \frac{1}{\sqrt{p}}. \end{aligned}$$

Counting Amicable Pairs

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

Counting Amicable Pairs

$$\mathcal{A}_E(X) \approx \sum_{p<X} \mathrm{Prob}(p \text{ is part of amicable pair})$$

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

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

Example The curve $y^2 + y = x^3 + x^2$ has 55 amicable pairs with $p < q < 10^{11}$.

$$(853, 883),\ (77761,77999), \ldots,$$
$$(94248260597, 94248586591).$$

Counting Amicable Pairs

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

Example The curve $y^2 + y = x^3 + x^2$ has 55 amicable pairs with $p < q < 10^{11}$.

$$
\begin{aligned}
&(853, 883),\ (77761{,}77999), \ldots, \\
&\qquad\qquad\qquad (94248260597, 94248586591).
\end{aligned}
$$

This supports the conclusion that amicable pairs exist, but are rare. But even up to 10^{11}, it is difficult to distinguish a growth rate of $\sqrt{X}/(\log X)^2$ from alternatives.

A Surprise

At this point, Kate and I had discovered the material described on the preceding slides. To finish up our work, we decided to compile data on the number of amicable pairs for the classical family of curves

$$E_k : y^2 = x^3 + k.$$

A Surprise

At this point, Kate and I had discovered the material described on the preceding slides. To finish up our work, we decided to compile data on the number of amicable pairs for the classical family of curves

$$E_k : y^2 = x^3 + k.$$

E_1 has no amicable pairs, which is not surprising, since $E_1(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/6\mathbb{Z}$.

A Surprise

At this point, Kate and I had discovered the material described on the preceding slides. To finish up our work, we decided to compile data on the number of amicable pairs for the classical family of curves

$$E_k : y^2 = x^3 + k.$$

E_1 has no amicable pairs, which is not surprising, since $E_1(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/6\mathbb{Z}$.
Moving on to $k = 2$, we have $E_2(\mathbb{Q})_{\text{tors}} = 0$, so there should(?) be some amicable pairs.

A Surprise

At this point, Kate and I had discovered the material described on the preceding slides. To finish up our work, we decided to compile data on the number of amicable pairs for the classical family of curves

$$E_k : y^2 = x^3 + k.$$

E_1 has no amicable pairs, which is not surprising, since $E_1(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/6\mathbb{Z}$.
Moving on to $k = 2$, we have $E_2(\mathbb{Q})_{\text{tors}} = 0$, so there should(?) be some amicable pairs.
What we found:

E_2 has 800 amicable pairs with $p < q < 10^6$!!!!!

A Surprise

At this point, Kate and I had discovered the material described on the preceding slides. To finish up our work, we decided to compile data on the number of amicable pairs for the classical family of curves

$$E_k : y^2 = x^3 + k.$$

E_1 has no amicable pairs, which is not surprising, since $E_1(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/6\mathbb{Z}$.
Moving on to $k = 2$, we have $E_2(\mathbb{Q})_{\text{tors}} = 0$, so there should(?) be some amicable pairs.
What we found:

E_2 has 800 amicable pairs with $p < q < 10^6$!!!!!

Compare this with the previous example, which had only 55 amicable pairs up to 10^{11}. This is an unexpected development. The game is afoot!

Complex Multiplication

The E_k curves have complex multiplication, so it is natural to guess that this is the source of the phenomenon.

Complex Multiplication

The E_k curves have complex multiplication, so it is natural to guess that this is the source of the phenomenon.

Recall that an elliptic curve is said to have **complex multiplication** (CM for short) if its ring of endomorphisms

$$\mathrm{End}(E) = \{\text{homomorphisms } \phi : E \to E\}$$

is strictly larger than $\mathbb{Z}$.

Complex Multiplication

The E_k curves have complex multiplication, so it is natural to guess that this is the source of the phenomenon.

Recall that an elliptic curve is said to have **complex multiplication** (CM for short) if its ring of endomorphisms

$$\mathrm{End}(E) = \{\text{homomorphisms } \phi : E \to E\}$$

is strictly larger than $\mathbb{Z}$.

Example. The curve

$$E : y^2 = x^3 + k$$

has CM, because if we let $\rho = e^{2\pi i/3}$ be a primitive cube root of unity, then the homomorphism

$$E \longrightarrow E, \qquad (x, y) \longmapsto (\rho x, y),$$

is not in $\mathbb{Z}$.

Amicable Pairs and Complex Multiplication

There are only a handful of CM curves defined over $\mathbb{Q}$ and having $E(\mathbb{Q})_{\mathrm{tors}} = 0$. We checked all of them, and they do indeed have a large number of amicable pairs.

Amicable Pairs and Complex Multiplication

There are only a handful of CM curves defined over $\mathbb{Q}$ and having $E(\mathbb{Q})_{\text{tors}} = 0$. We checked all of them, and they do indeed have a large number of amicable pairs.

Further experiments revealed the step in our heuristic argument that is flawed for CM curves. Recall we said

$$\operatorname{Prob}(N_q = p \mid q = N_p \text{ is prime}) \gg\ll \frac{1}{\sqrt{p}},$$

because $p \approx q$ and N_q lies in an interval of length $4\sqrt{q}$, so the chance of N_q hitting any particular value is about $1/4\sqrt{p}$.

Amicable Pairs and Complex Multiplication

There are only a handful of CM curves defined over $\mathbb{Q}$ and having $E(\mathbb{Q})_{\text{tors}} = 0$. We checked all of them, and they do indeed have a large number of amicable pairs.

Further experiments revealed the step in our heuristic argument that is flawed for CM curves. Recall we said

$$\operatorname{Prob}(N_q = p \mid q = N_p \text{ is prime}) \gg\ll \frac{1}{\sqrt{p}},$$

because $p \approx q$ and N_q lies in an interval of length $4\sqrt{q}$, so the chance of N_q hitting any particular value is about $1/4\sqrt{p}$.

This appears to be true for non-CM curves, but for CM curves (other than the E_k curves) we found that

$$\operatorname{Prob}(N_q = p \mid q = N_p \text{ is prime}) \approx \frac{1}{2}.$$

CM Curves of Prime Order

This led us to conjecture, and then prove,

Theorem. Let $E/\mathbb{Q}$ be a CM curve with $j(E) \neq 0$, and suppose that p is a prime such that $q = \#\tilde{E}(\mathbb{F}_p)$ is also prime. Then either

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

CM Curves of Prime Order

This led us to conjecture, and then prove,

Theorem. Let $E/\mathbb{Q}$ be a CM curve with $j(E) \neq 0$, and suppose that p is a prime such that $q = \#\tilde{E}(\mathbb{F}_p)$ is also prime. Then either

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

Assuming the theorem, which justifies

$$\operatorname{Prob}(N_q = p \mid q = N_p \text{ is prime}) \approx \frac{1}{2},$$

our earlier calculation yields

Conjecture. Let $E/\mathbb{Q}$ be a CM curve with $j(E) \neq 0$. Then either $\mathcal{A}_E(X)$ is bounded, or

$$\mathcal{A}_E(X) \sim c_E \frac{X}{(\log X)^2} \quad \text{for some } c_E > 0.$$

CM Curves of Prime Order — Sketch of Proof

Can check that

$$\operatorname{End}(E) = \mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right] = \mathcal{O}.$$

Let

$$\psi_E : (\text{primes of } \mathcal{O}) \longrightarrow \mathcal{O}$$

be the Grössencharacter associated to E. For a prime ideal $\mathfrak{p} \subset \mathcal{O}$, it satisfies $\mathfrak{p} = \psi_E(\mathfrak{p})\mathcal{O}$ and

$$\#\tilde{E}(\mathbb{F}_{\mathfrak{p}}) = \mathsf{N}\,\psi_E(\mathfrak{p}) - \mathsf{Tr}\,\psi_E(\mathfrak{p}) + 1.$$

CM Curves of Prime Order — Sketch of Proof

Can check that

$$\mathrm{End}(E) = \mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right] = \mathcal{O}.$$

Let

$$\psi_E : (\text{primes of } \mathcal{O}) \longrightarrow \mathcal{O}$$

be the Grössencharacter associated to E. For a prime ideal $\mathfrak{p} \subset \mathcal{O}$, it satisfies $\mathfrak{p} = \psi_E(\mathfrak{p})\mathcal{O}$ and

$$\#\tilde{E}(\mathbb{F}_\mathfrak{p}) = \mathsf{N}\,\psi_E(\mathfrak{p}) - \mathsf{Tr}\,\psi_E(\mathfrak{p}) + 1.$$

Factor $p\mathcal{O} = \mathfrak{p}\bar{\mathfrak{p}}$ and $q\mathcal{O} = \mathfrak{q}\bar{\mathfrak{q}}$. (They always split.) Then

$$\mathsf{N}\,\psi_E(\mathfrak{q}) = q = \#\tilde{E}(\mathbb{F}_\mathfrak{p}) = \mathsf{N}\big(1 - \psi_E(\mathfrak{p})\big).$$

CM Curves of Prime Order — Sketch of Proof

Hence

$$\psi_E(\mathfrak{q}) = u\big(1 - \psi_E(\mathfrak{p})\big) \text{ or } u\big(\overline{1 - \psi_E(\mathfrak{p})}\big)$$

for some unit $u \in \mathcal{O}^* = \{\pm 1\}$. (Here's why we want $j(E) \neq 1$, since otherwise $\#\mathcal{O}^* = 6$.)

CM Curves of Prime Order — Sketch of Proof

Hence

$$\psi_E(\mathfrak{q}) = u\bigl(1 - \psi_E(\mathfrak{p})\bigr) \text{ or } u\bigl(\overline{1 - \psi_E(\mathfrak{p})}\bigr)$$

for some unit $u \in \mathcal{O}^* = \{\pm 1\}$. (Here's why we want $j(E) \neq 1$, since otherwise $\#\mathcal{O}^* = 6$.)
Ths allows us to compute

$$\begin{aligned}
\mathsf{Tr}\,\psi_E(\mathfrak{q}) &= u\,\mathsf{Tr}\bigl(1 - \psi_E(\mathfrak{p})\bigr) \\
&= \pm\bigl(2 - \mathsf{Tr}\,\psi_E(\mathfrak{p})\bigr) \\
&= \pm\Bigl(2 - \bigl(p + 1 - \#\tilde{E}(\mathbb{F}_{\mathfrak{p}})\bigr)\Bigr) \\
&= \pm\bigl(2 - \bigl(p + 1 - q\bigr)\bigr) \\
&= \pm(q + 1 - p).
\end{aligned}$$

This gives the two stated values for

$$\#\tilde{E}(\mathbb{F}_{\mathfrak{q}}) = q + 1 - \mathsf{Tr}\,\psi_E(\mathfrak{q}).$$

Aliquot Cycles on CM Curves

As an easy corollary of the theorem, we get:

Corollary. Let $E/\mathbb{Q}$ be a CM curve with $j(E) \neq 0$. Then E has no aliquot cycles of length $\ell \geq 3$.

Aliquot Cycles on CM Curves

As an easy corollary of the theorem, we get:

Corollary. Let $E/\mathbb{Q}$ be a CM curve with $j(E) \neq 0$. Then E has no aliquot cycles of length $\ell \geq 3$.

Proof (for $\ell = 3$) Suppose (p, q, r) is an aliquot triple. WLOG, by a cyclic permuation, we may assume that $p < q$. The theorem gives

$$p \longrightarrow q \longrightarrow r = 2q + 2 - p \longrightarrow p = 2r + 2 - q.$$

Solving yields $p = q + 2$, contradicting $p < q$.

Amicable Pairs on $j = 0$ Curves

The curves

$$E_k : y^2 = x^3 + k$$

were excluded from our theorem, because they have $\mathcal{O}^* \cong \boldsymbol{\mu}_6$. This should lead to six possibilities for $\#\tilde{E}_k(\mathbb{F}_q)$, so we might expect that

$$\operatorname{Prob}(N_q = p \mid q = N_p \text{ is prime}) \approx \frac{1}{6}.$$

Amicable Pairs on $j = 0$ Curves

The curves

$$E_k : y^2 = x^3 + k$$

were excluded from our theorem, because they have $\mathcal{O}^* \cong \boldsymbol{\mu}_6$. This should lead to six possibilities for $\#\tilde{E}_k(\mathbb{F}_q)$, so we might expect that

$$\operatorname{Prob}(N_q = p \mid q = N_p \text{ is prime}) \approx \frac{1}{6}.$$

It is true that $\#\tilde{E}_k(\mathbb{F}_q)$ takes on one of six values, but experiments show that they do *not* appear with equal probabilities!

Amicable Pairs on $j = 0$ Curves

The curves

$$E_k : y^2 = x^3 + k$$

were excluded from our theorem, because they have $\mathcal{O}^* \cong \boldsymbol{\mu}_6$. This should lead to six possibilities for $\#\tilde{E}_k(\mathbb{F}_q)$, so we might expect that

$$\operatorname{Prob}(N_q = p \mid q = N_p \text{ is prime}) \approx \frac{1}{6}.$$

It is true that $\#\tilde{E}_k(\mathbb{F}_q)$ takes on one of six values, but experiments show that they do *not* appear with equal probabilities!

Two of those possibilities are

$$\psi_E(\mathfrak{q}) = \pm(q + 1 - p), \qquad (*)$$

one of which leads to an amicable pair. We will call the primes satisfying $(*)$ *primes of Type* 1.

Counting Type 1 Primes

Experimentally, we find that about half the Type 1 primes give an amicable pair. It remains to count the Type 1 primes, so we let

$$\mathcal{T}_k(X) = \frac{\#\{p < X : p \text{ is a Type 1 prime for } E_k\}}{\#\{p < X : \#E_k(\mathbb{F}_p) \text{ is prime}\}}.$$

Counting Type 1 Primes

Experimentally, we find that about half the Type 1 primes give an amicable pair. It remains to count the Type 1 primes, so we let

$$\mathcal{T}_k(X) = \frac{\#\{p < X : p \text{ is a Type 1 prime for } E_k\}}{\#\{p < X : \#E_k(\mathbb{F}_p) \text{ is prime}\}}.$$

We might expect $\mathcal{T}_k(X) \to \frac{1}{3}$. Here is some data for the first few (non-square non-cube) values of k.

Counting Type 1 Primes

Experimentally, we find that about half the Type 1 primes give an amicable pair. It remains to count the Type 1 primes, so we let

$$\mathcal{T}_k(X) = \frac{\#\{p < X : p \text{ is a Type 1 prime for } E_k\}}{\#\{p < X : \#E_k(\mathbb{F}_p) \text{ is prime}\}}.$$

We might expect $\mathcal{T}_k(X) \to \frac{1}{3}$. Here is some data for the first few (non-square non-cube) values of k.

k	2	3	5	6	7	10
$X = 10^3$	1.000	0.615	0.533	0.417	0.571	0.333
$X = 10^4$	1.000	0.570	0.324	0.492	0.578	0.457
$X = 10^5$	1.000	0.548	0.330	0.563	0.538	0.435
$X = 10^6$	1.000	0.547	0.336	0.565	0.532	0.431

Counting Type 1 Primes

Experimentally, we find that about half the Type 1 primes give an amicable pair. It remains to count the Type 1 primes, so we let

$$\mathcal{T}_k(X) = \frac{\#\{p < X : p \text{ is a Type 1 prime for } E_k\}}{\#\{p < X : \#E_k(\mathbb{F}_p) \text{ is prime}\}}.$$

We might expect $\mathcal{T}_k(X) \to \frac{1}{3}$. Here is some data for the first few (non-square non-cube) values of k.

k	2	3	5	6	7	10
$X = 10^3$	1.000	0.615	0.533	0.417	0.571	0.333
$X = 10^4$	1.000	0.570	0.324	0.492	0.578	0.457
$X = 10^5$	1.000	0.548	0.330	0.563	0.538	0.435
$X = 10^6$	1.000	0.547	0.336	0.565	0.532	0.431

The limiting value of $\mathcal{T}_k(X)$ appears to depend on k.

Type 1 Primes and Cubic Residues

Let

$$\mathcal{O} = \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] = \mathrm{End}(E_k)$$

and let ψ be the Grössencharacter of E_k.

Theorem. Assume $q = \#\tilde{E}(\mathbb{F}_p)$ is prime, and factor

$$p\mathcal{O} = \mathfrak{p}\bar{\mathfrak{p}} \quad \text{and} \quad q\mathcal{O} = \mathfrak{q}\bar{\mathfrak{q}}.$$

Then

$$p \text{ is Type 1} \quad \Longleftrightarrow \quad \left(\frac{k}{\mathfrak{p}}\right)_3 \left(\frac{k}{\mathfrak{q}}\right)_3 = 1.$$

Type 1 Primes and Cubic Residues

Let

$$\mathcal{O} = \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] = \operatorname{End}(E_k)$$

and let ψ be the Grössencharacter of E_k.

Theorem. Assume $q = \#\tilde{E}(\mathbb{F}_p)$ is prime, and factor

$$p\mathcal{O} = \mathfrak{p}\bar{\mathfrak{p}} \quad \text{and} \quad q\mathcal{O} = \mathfrak{q}\bar{\mathfrak{q}}.$$

Then

$$p \text{ is Type } 1 \quad \Longleftrightarrow \quad \left(\frac{k}{\mathfrak{p}}\right)_3 \left(\frac{k}{\mathfrak{q}}\right)_3 = 1.$$

The proof is an involved calculation using quadratic and cubic reciprocity in $\mathbb{Q}(\sqrt{-3})$ and arithmetic properties of E_k over $\mathbb{F}_p$ and $\mathbb{F}_q$.

Applying Cubic Reciprocity

To ease notation, we let

$$\beta = \psi(\mathfrak{p}), \quad \text{so} \quad \mathfrak{p} = \beta\mathcal{O} \quad \text{and} \quad \mathfrak{q} = (1-\beta)\mathcal{O}.$$

Then one can prove that

$$\left(\frac{k}{\mathfrak{p}}\right)_3 \left(\frac{k}{\mathfrak{q}}\right)_3 = \left(\frac{k}{\beta}\right)_3 \left(\frac{k}{1-\beta}\right)_3 = \left(\frac{\beta(1-\beta)}{k}\right)_3.$$

So the distribution of Type 1 primes depends on the mod k cubic residue properties of

$$\beta(1-\beta)$$

as β ranges over $\psi(\mathfrak{p})$ values.

Applying Cubic Reciprocity

To ease notation, we let

$$\beta = \psi(\mathfrak{p}), \quad \text{so} \quad \mathfrak{p} = \beta\mathcal{O} \quad \text{and} \quad \mathfrak{q} = (1-\beta)\mathcal{O}.$$

Then one can prove that

$$\left(\frac{k}{\mathfrak{p}}\right)_3 \left(\frac{k}{\mathfrak{q}}\right)_3 = \left(\frac{k}{\beta}\right)_3 \left(\frac{k}{1-\beta}\right)_3 = \left(\frac{\beta(1-\beta)}{k}\right)_3.$$

So the distribution of Type 1 primes depends on the mod k cubic residue properties of

$$\beta(1-\beta)$$

as β ranges over $\psi(\mathfrak{p})$ values.
However, it turns out that the values of $\psi(\mathfrak{p})$ are not uniformly distributed in $(\mathcal{O}/k\mathcal{O})^*$. There are various quadratic and cubic residue conditions that they must satisfy.

A Conjectural Limit for the Density of Type 1 Primes

For ease of exposition, I restrict now to the case that k is prime. Even with this restriction, there are many cases, because our conjectural limit for $\mathcal{T}_k(X)$ depends on k modulo 36. Here is a typical case:

A Conjectural Limit for the Density of Type 1 Primes

For ease of exposition, I restrict now to the case that k is prime. Even with this restriction, there are many cases, because our conjectural limit for $\mathcal{T}_k(X)$ depends on k modulo 36. Here is a typical case:

Conjecture. Assume that $k \equiv 1 \pmod{36}$ and that k is prime. Then

$$\lim_{X\to\infty} \mathcal{T}_k(X) = \frac{\#\left\{\lambda \in \dfrac{\mathcal{O}}{k\mathcal{O}} : \begin{array}{c} \gcd(\lambda(1-\lambda), k) = 1 \\ \left(\frac{\lambda(1-\lambda)}{k}\right)_3 = 1 \\ \left(\frac{\lambda}{k}\right)_2 = -1,\ \left(\frac{\lambda}{k}\right)_3 \ne 1 \end{array}\right\}}{\#\left\{\lambda \in \dfrac{\mathcal{O}}{k\mathcal{O}} : \gcd(\lambda(1-\lambda), k) = 1\right\}}.$$

A Conjectural Limit for the Density of Type 1 Primes

For ease of exposition, I restrict now to the case that k is prime. Even with this restriction, there are many cases, because our conjectural limit for $\mathcal{T}_k(X)$ depends on k modulo 36. Here is a typical case:

Conjecture. Assume that $k \equiv 1 \pmod{36}$ and that k is prime. Then

$$\lim_{X\to\infty} \mathcal{T}_k(X) = \frac{\#\left\{\lambda \in \dfrac{\mathcal{O}}{k\mathcal{O}} : \begin{array}{c} \gcd(\lambda(1-\lambda),k)=1 \\ \left(\frac{\lambda(1-\lambda)}{k}\right)_3 = 1 \\ \left(\frac{\lambda}{k}\right)_2 = -1,\ \left(\frac{\lambda}{k}\right)_3 \ne 1 \end{array}\right\}}{\#\left\{\lambda \in \dfrac{\mathcal{O}}{k\mathcal{O}} : \gcd(\lambda(1-\lambda),k)=1\right\}}.$$

For small values of k, it is not hard to explicitly compute the fraction appearing on the right-hand side.

An Explicit Evaluation

Conditions on the cubic residue of $\lambda(1-\lambda)$ and quadratic and cubic residues of λ can be reformulated into counting points on genus 4 curves of the form

$$C : \gamma z^6(1 - \gamma z^6) = \delta x^3.$$

An Explicit Evaluation

Conditions on the cubic residue of $\lambda(1-\lambda)$ and quadratic and cubic residues of λ can be reformulated into counting points on genus 4 curves of the form

$$\boxed{C : \gamma z^6(1-\gamma z^6) = \delta x^3.}$$

The first step to obtaining an explicit formula is:

$$\boxed{\mathrm{Jac}(C) \xrightarrow{\text{isogenous}} E_{16\delta^2} \times E_{4\gamma^3\delta^4} \times E_{\gamma^5\delta^2} \times E_{-\gamma\delta^2}.}$$

An Explicit Evaluation

Conditions on the cubic residue of $\lambda(1-\lambda)$ and quadratic and cubic residues of λ can be reformulated into counting points on genus 4 curves of the form

$$\boxed{C : \gamma z^6(1-\gamma z^6) = \delta x^3.}$$

The first step to obtaining an explicit formula is:

$$\boxed{\mathrm{Jac}(C) \xrightarrow{\text{isogenous}} E_{16\delta^2} \times E_{4\gamma^3\delta^4} \times E_{\gamma^5\delta^2} \times E_{-\gamma\delta^2}.}$$

Then we use a classical formula, essentially due to Gauss, for $\#E_\alpha(\mathbb{F})$. The formulas become especially messy if $k \equiv 1 \pmod 3$, since then the ideal $k\mathcal{O}$ splits, so quantities such as $\left(\frac{\lambda}{k}\right)_2$ and $\left(\frac{\lambda}{k}\right)_3$ become products.

An Explicit Evaluation

Conditions on the cubic residue of $\lambda(1-\lambda)$ and quadratic and cubic residues of λ can be reformulated into counting points on genus 4 curves of the form

$$\boxed{C : \gamma z^6(1-\gamma z^6) = \delta x^3.}$$

The first step to obtaining an explicit formula is:

$$\boxed{\mathrm{Jac}(C) \xrightarrow{\text{isogenous}} E_{16\delta^2} \times E_{4\gamma^3\delta^4} \times E_{\gamma^5\delta^2} \times E_{-\gamma\delta^2}.}$$

Then we use a classical formula, essentially due to Gauss, for $\#E_\alpha(\mathbb{F})$. The formulas become especially messy if $k \equiv 1 \pmod 3$, since then the ideal $k\mathcal{O}$ splits, so quantities such as $\left(\frac{\lambda}{k}\right)_2$ and $\left(\frac{\lambda}{k}\right)_3$ become products.

After a certain amount of work and…

An Explicit Conjecture for $j = 0$ Curves

. . . . 12 pages of . . .

. . . . (omitted) computations . . .

. . . . we obtain

An Explicit Conjecture for $j = 0$ Curves

. . . . 12 pages of . . .

. . . . (omitted) computations . . .

. . . . we obtain

Conjecture. Let $k \neq 3$ be prime. Then the density of Type 1 primes for the curve $E_k : y^2 = x^3 + k$ is

$$\lim_{X \to \infty} \mathcal{T}_k(X) = \frac{1}{3} + R(k),$$

where $R(k) = 0$ if $k \equiv 5, 13, 25, 29 \pmod{36}$, and otherwise $R(k)$ is given by the following table:

k mod 36	$1, 19$	$17, 35$	$7, 31$	$11, 23$
$R(k)$	$\dfrac{2}{3(k-3)}$	$\dfrac{2}{3(k-1)}$	$\dfrac{2k}{3(k-2)^2}$	$\dfrac{2k}{3(k^2-2)}$

Origins of Elliptic Aliquot Sequences

Consider the Fibonacci sequence $\mathsf{F} = (F_n)_{n\geq 1}$. A number of authors have considered the question:

For which indices n is F_n divisible by n?

Origins of Elliptic Aliquot Sequences

Consider the Fibonacci sequence $\mathsf{F} = (F_n)_{n\geq 1}$. A number of authors have considered the question:

For which indices n is F_n divisible by n?

For example,

$$n \mid F_n \quad \text{for} \quad 1, 5, 12, 24, 25, 36, 48, 60, 72, 96, \ldots.$$

Origins of Elliptic Aliquot Sequences

Consider the Fibonacci sequence $\mathsf{F} = (F_n)_{n\geq 1}$. A number of authors have considered the question:

For which indices n is F_n divisible by n?

For example,

$$n \mid F_n \quad \text{for} \quad 1, 5, 12, 24, 25, 36, 48, 60, 72, 96, \ldots.$$

In general, for any integer sequence $\mathsf{A} = (A_n)_{n\geq 1}$, it is interesting to study the **Index Divisibility Set**

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

We turn $\mathcal{S}(\mathsf{A})$ into a directed graph by assigning arrows

$$\mathrm{Arrow}(\mathsf{A}) = \left\{ n \to nd : \begin{array}{l} n, nd \in \mathcal{S}(\mathsf{A}) \text{ and } ne \notin \mathcal{S}(\mathsf{A}) \\ \text{for all } e \mid d \text{ with } 1 < e < d \end{array} \right\}$$

Origins of Elliptic Aliquot Sequences

Consider the Fibonacci sequence $\mathsf{F} = (F_n)_{n \ge 1}$. A number of authors have considered the question:

For which indices n is F_n divisible by n?

For example,

$$n \mid F_n \quad \text{for} \quad 1, 5, 12, 24, 25, 36, 48, 60, 72, 96, \ldots.$$

In general, for any integer sequence $\mathsf{A} = (A_n)_{n \ge 1}$, it is interesting to study the **Index Divisibility Set**

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

We turn $\mathcal{S}(\mathsf{A})$ into a directed graph by assigning arrows

$$\mathrm{Arrow}(\mathsf{A}) = \left\{ n \to nd : \begin{array}{l} n, nd \in \mathcal{S}(\mathsf{A}) \text{ and } ne \notin \mathcal{S}(\mathsf{A}) \\ \text{for all } e \mid d \text{ with } 1 < e < d \end{array} \right\}$$

Examples of arrows in $\mathrm{Arrow}(\mathsf{F})$ include

$$(1 \to 5),\ (1 \to 12),\ (12 \to 24),\ (5 \to 60).$$

Index Divisibility of Lucas Sequences

Lucas sequences are generalizations of the Fibonaccie sequence. They are defined by recursions of the form

$$L_1 = 1, \quad L_2 = A, \quad L_{n+2} = AL_{n+1} + BL_n.$$

We will assume that $\Delta = A^2 + 4B \neq 0$.

Index Divisibility of Lucas Sequences

Lucas sequences are generalizations of the Fibonaccie sequence. They are defined by recursions of the form

$$L_1 = 1, \quad L_2 = A, \quad L_{n+2} = AL_{n+1} + BL_n.$$

We will assume that $\Delta = A^2 + 4B \neq 0$.

The index divisibility graph for general Lucas sequences has a very simple description.

Theorem. (Smyth 2009) Let L be a Lucas sequence. Then

$$\operatorname{Arrow}(\mathsf{L}) = \{n \longrightarrow np : p \mid L_n\Delta\} \cup \mathcal{B}_{A,B},$$

where $\mathcal{B}_{A,B}$ is either empty or consists of arrows of one of the forms $(n \longrightarrow 6n)$ or $(n \longrightarrow 12n)$.

Elliptic Divisibility Sequences

Consider an elliptic curve and rational point

$$E : y^2 = x^3 + ax + b, \qquad P \in E(\mathbb{Q}).$$

The multiples of P have the form

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

The sequence $\mathsf{D} = (D_n)_{n \geq 1}$ is called an

Elliptic Divisibility Sequence (EDS).

Elliptic Divisibility Sequences

Consider an elliptic curve and rational point

$$E : y^2 = x^3 + ax + b, \qquad P \in E(\mathbb{Q}).$$

The multiples of P have the form

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

The sequence $\mathsf{D} = (D_n)_{n \geq 1}$ is called an

Elliptic Divisibility Sequence (EDS).

EDS have many applications, including to cryptography and to mathematical logic.

Elliptic Divisibility Sequences

Consider an elliptic curve and rational point

$$E : y^2 = x^3 + ax + b, \qquad P \in E(\mathbb{Q}).$$

The multiples of P have the form

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

The sequence $\mathsf{D} = (D_n)_{n \geq 1}$ is called an

Elliptic Divisibility Sequence (EDS).

EDS have many applications, including to cryptography and to mathematical logic.

EDS are defined by a non-linear recursion. They are elliptic curve analogues of Lucas sequences, which are associated to the multiplicative group.

Aliquot Sequences and Index Divisibility of EDS

With these preliminaries, I can now explain how aliquot sequences appeared naturally when Kate and I studied index divisibility for elliptic divisibility sequences.

Aliquot Sequences and Index Divisibility of EDS

With these preliminaries, I can now explain how aliquot sequences appeared naturally when Kate and I studied index divisibility for elliptic divisibility sequences.

Theorem. Let D be an EDS and let $n \in \mathcal{S}(\mathsf{D})$.

(a) $p \mid D_n \implies (n \to np) \in \operatorname{Arrow}(\mathsf{D})$.

(b) Let $(p_1, p_2, \ldots, p_\ell)$ be an aliquot sequence of length $\ell \geq 2$ with $\min p_i \geq 9\ell^2$ and all $p_i \nmid n$. Then

$$n \to np_1p_2\cdots p_\ell \in \operatorname{Arrow}(\mathsf{D}).$$

(c) Conversely, if $(n \to nd)$ is an arrow with d composite and satisfying certain other conditions, then d is the product of the primes in an aliquot cycle.

Generalizations

A natural generalization is to consider an elliptic curve E over number field K. Then a sequence $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ of (degree 1) primes is an **aliquot cycle** if

$$\#E(\mathbb{F}_{\mathfrak{p}_1}) = \mathsf{N}_{K/\mathbb{Q}}\,\mathfrak{p}_2, \;\ldots\; \#E(\mathbb{F}_{\mathfrak{p}_\ell}) = \mathsf{N}_{K/\mathbb{Q}}\,\mathfrak{p}_1.$$

Generalizations

A natural generalization is to consider an elliptic curve E over number field K. Then a sequence $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ of (degree 1) primes is an **aliquot cycle** if

$$\#E(\mathbb{F}_{\mathfrak{p}_1}) = \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}_2, \ \ldots \ \#E(\mathbb{F}_{\mathfrak{p}_\ell}) = \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}_1.$$

Let $E/\mathbb{Q}$ be an elliptic curve and let $L(E,s) = \sum a_n/n^s$ be its L-series. We define an ***L*-aliqout cycle** for E to be a cycle for the recursion

$$n \longmapsto n + 1 - a_n.$$

Generalizations

A natural generalization is to consider an elliptic curve E over number field K. Then a sequence $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ of (degree 1) primes is an **aliquot cycle** if

$$\#E(\mathbb{F}_{\mathfrak{p}_1}) = \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}_2, \ \ldots \ \#E(\mathbb{F}_{\mathfrak{p}_\ell}) = \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}_1.$$

Let $E/\mathbb{Q}$ be an elliptic curve and let $L(E,s) = \sum a_n/n^s$ be its L-series. We define an **L-aliqout cycle** for E to be a cycle for the recursion

$$n \longmapsto n + 1 - a_n.$$

Similarly, we define an **N-aliqout cycle** for E to be a cycle for the recursion

$$n \longmapsto \#\mathcal{E}_0(\mathbb{Z}/n\mathbb{Z}),$$

where $\mathcal{E}_0/\mathbb{Z}$ is the identity component of the Néron model of E.

Amicable Pairs
for
Elliptic Curves

Joseph H. Silverman
(joint work with Katherine Stange)

Brown University

Palmetto Number Theory Series (PANTS XII)
Clemson University

February 20–21, 2010