Experimental Mathematics, 20(3):329–357, 2011

ISSN: 1058-6458 print / 1944-950X online
DOI: 10.1080/10586458.2011.565253

Taylor & Francis
Taylor & Francis Group

Amicable Pairs and Aliquot Cycles for Elliptic Curves

Joseph H. Silverman and Katherine E. Stange

CONTENTS

An *amicable pair* for an elliptic curve $E/\mathbb{Q}$ is a pair of primes (p, q) of good reduction for E $\#\tilde{E}_p(\mathbb{F}_p) = q$ and $\#\tilde{E}_q(\mathbb{F}_q) = p$. In this paper we study elliptic amicable pairs and analogously defined longer *elliptic aliquot cycles*. We show that there exist elliptic curves with arbitrarily long aliquot cycles, but that CM elliptic curves (with $j \neq 0$) have no aliquot cycles of length greater than two. We give conjectural formulas for the frequency of amicable pairs. For CM curves, the derivation of precise conjectural formulas involves a detailed analysis of the values of the Grössencharacter evaluated at primes $\mathfrak{p}$ in $\mathrm{End}(E)$ having the property that $\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ is prime. This is especially intricate for the family of curves with $j = 0$.

1. INTRODUCTION

Let $E/\mathbb{Q}$ be an elliptic curve. In this paper we study pairs of primes (p, q) such that E has good reduction at p and q and such that the reductions $\tilde{E}_p$ and $\tilde{E}_q$ of E at p and q satisfy

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

By analogy with a classical problem in number theory (cf. Remark 3.2), we call (p, q) an *amicable pair* for the elliptic curve $E/\mathbb{Q}$.

Example 1.1. Searching for amicable pairs using primes smaller than 10^7 on the two elliptic curves

$$E_1 : y^2 + y = x^3 - x \quad \text{and} \quad E_2 : y^2 + y = x^3 + x^2$$

yields one amicable pair on the curve E_1,

$$(1622311, 1622471),$$

and four amicable pairs on the curve E_2,

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

Example 1.2. The curve

$$E_3 : y^2 = x^3 + 2$$

2000 AMS Subject Classification: Primary 11G05, Secondary 11B99, 11G20
Keywords: elliptic divisibility sequence, elliptic curve, amicable pair, aliquot cycle

exhibits strikingly different amicable pair behavior. There are more than 800 amicable pairs for E_3 using primes smaller than 10^6, the first few of which are

$$(13,19),\ (139,163),\ (541,571),\ (613,661),\ (757,787),\ (1693,1741).$$

One objective of this note is to present theoretical and numerical evidence for the following conjecture.

Conjecture 1.3. *Let $E/\mathbb{Q}$ be an elliptic curve, let*

$$\mathcal{Q}_E(X) = \#\left\{ \begin{array}{c} \text{amicable pairs } (p,q) \text{ for } E/\mathbb{Q} \\ \text{with } p<q \text{ and } p \le X \end{array} \right\}$$

be the amicable pair counting function, and assume that there are infinitely many primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime.

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

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

where the implied constants depend on E. Here the notation $f(X) \asymp g(X)$ means that there are positive constants c_1 and c_2 such that $c_1 f(X) \le g(X) \le c_2 f(X)$ for all sufficiently large X.

(b) *If E has complex multiplication, then there is a positive constant A_E such that*

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

Here the notation $f(X) \sim g(X)$ means that $f(X)/g(X) \to 1$ as $X \to \infty$.

We do not believe that it is clear a priori why there should be such a striking difference between the CM and the non-CM cases. We first discovered this phenomenon experimentally; subsequently, we found an explanation based on Theorem 6.1, which says that if $E/\mathbb{Q}$ has CM and if $q = \#\tilde{E}_p(\mathbb{F}_p)$ is prime, then there are generally only two possible values for $\#\tilde{E}_q(\mathbb{F}_q)$, one of which is p. (The situation for $j(E) = 0$ is considerably more complicated; see Section 7.) This contrasts with the non-CM case, in which $\#\tilde{E}_q(\mathbb{F}_q)$ seems to be free to range throughout the Hasse interval. We refer the reader to Conjectures 6.9 and 7.24 for more-precise versions of the CM part of Conjecture 1.3.

The frequency of primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime or almost prime has been studied by a number of authors. In Section 2 we discuss what is known and what is conjectured concerning this problem.

Generalizing the notion of amicable pair, we define an *aliquot cycle* of length ℓ for $E/\mathbb{Q}$ to be a sequence of distinct primes $(p_1, p_2, \dots, p_\ell)$ such that E has good reduction at every p_i and such that

$$\begin{aligned} \#\tilde{E}_{p_1}(\mathbb{F}_{p_1}) = p_2, \quad \#\tilde{E}_{p_2}(\mathbb{F}_{p_2}) = p_3, \quad \dots, \\ \#\tilde{E}_{p_{\ell-1}}(\mathbb{F}_{p_{\ell-1}}) = p_\ell, \quad \#\tilde{E}_{p_\ell}(\mathbb{F}_{p_\ell}) = p_1. \end{aligned}$$

Example 1.4. The elliptic curve $y^2 = x^3 - 25x - 8$ has the aliquot triple $(83, 79, 73)$. The elliptic curve

$$\begin{aligned} E : y^2 = x^3 &+ 176209333661915432764478x \\ &+ 60625229794681596832262 \end{aligned}$$

has an aliquot cycle

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

of length 14.

In Section 4 we give a heuristic argument suggesting that the counting function for aliquot cycles of length ℓ for non-CM elliptic curves grows like $\sqrt{X}/(\log X)^\ell$. The rough idea is to assume that if $q = \#\tilde{E}_p(\mathbb{F}_p)$ is prime, then the trace values $a_q(E) = q + 1 - \#\tilde{E}_q(\mathbb{F}_q)$ are (more or less) equidistributed within the appropriate Hasse interval.

In Section 5 we give an elementary construction (Theorem 5.1) using the prime number theorem, the Chinese remainder theorem, and a result of Deuring to prove that for every ℓ there exists an elliptic curve $E/\mathbb{Q}$ with an aliquot cycle of length ℓ.

We next consider the case of elliptic curves having complex multiplication. These curves exhibit strikingly different behavior from that of their non-CM counterparts. Our first result (Theorem 6.1) says that if $E/\mathbb{Q}$ has CM with $j(E) \ne 0$, and if $q = \#\tilde{E}_p(\mathbb{F}_p)$ is prime, then there are only two possible values for $\#\tilde{E}_q(\mathbb{F}_q)$, namely p and $2q + 2 - p$. Assuming that each is equally likely (which seems to be the case experimentally), this explains why CM curves have so many amicable pairs. The proof involves first proving that p and q split in $\mathrm{End}(E)$, and then relating the values of the Grössencharacter ψ_E at primes lying above p and q.

Theorem 6.1 can also be used to show that a CM curve with $j \ne 0$ has no aliquot cycles of length 3 or greater; see Corollary 6.2. This stands in contrast to Theorem 5.1, which says that there exist curves with arbitrarily long aliquot cycles.

We finally turn to the $j = 0$ curves $y^2 = x^3 + k$, whose complicated analysis is given in the lengthy Section 7. For prime values of k, we give a precise conjectural formula for the counting function of amicable pairs that depends on the value of k modulo 36. For example, if k is prime and $k \equiv 1$ or $19 \pmod{36}$, then we conjecture that

$$\lim_{X\to\infty} \frac{\#\{p < X : p \text{ is part of an amicable pair}\}}{\#\{p < X : \#\tilde{E}_p(\mathbb{F}_p) \text{ is prime}\}} = \frac{1}{6} + \frac{1}{3k-9}, \tag{1–1}$$

while if $k \equiv 11$ or $23 \pmod{36}$, then the limiting value in (1–1) is (conjecturally) equal to $\frac{1}{6} + \frac{k}{3k^2-6}$. There are similar formulas for the other congruence classes.

The derivation of these formulas is in two parts. First, by analyzing the values of the Grössencharacter and using sextic reciprocity, we prove that (p, q) is an amicable pair if and only if

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

If the values of $\psi_E(\mathfrak{p})$ modulo k were equidistributed as p varies, we would conjecture that the number of amicable pairs is governed by the proportion of $\lambda \in \mathcal{O}/k\mathcal{O}$ satisfying $\left(\frac{\lambda(1-\lambda)}{k}\right)_6 = 1$. Here

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

This is almost true, but the allowable values of λ are often restricted by further conditions on $\left(\frac{\lambda}{k}\right)_6$. Sorting out these restrictions gives a precise conjectural value for the limit (1–1) in terms of the sizes of certain subsets of $\mathcal{O}/k\mathcal{O}$.

The second part of the proof is to derive explicit formulas for the sizes of these sets. This is done by relating the points in these sets to the $\mathcal{O}/k\mathcal{O}$-points on a certain family of curves $C^{(\gamma,\delta)}$ of genus four. We count these points by explicitly decomposing the Jacobian of $C^{(\gamma,\delta)}$ into a product of four $j = 0$ elliptic curves and using the Grössencharacter formula for the number of points on such curves. The resulting formulas are quite involved, especially in the case that k splits in $\mathcal{O}$, but eventually most of the terms cancel, leaving a relatively compact formula.

We have no good explanation for why the final formula has such a simple form; see Remark 7.22 for a discussion of the delicacy of the computation.

The conjectures in this paper are supported by heuristic arguments and, especially for CM curves, by theorems describing the allowable values of the Grössencharacter ψ_E. But heuristic arguments have been known to fail, and indeed our CM argument depends on the assumption that $\psi_E(\mathfrak{p}) \bmod k$ is uniformly distributed among its *allowable values*, where we claim to have characterized the set of allowable values. It is thus reassuring that extensive experiments are in close agreement with the conjectural values derived by theory. These experiments are described in Section 9. Finally, in Section 10 we describe some possible generalizations that deserve further study.[1]

Remark 1.5. We briefly indicate our original motivation for studying elliptic amicable pairs and aliquot cycles. They appeared in a natural fashion when we generalized to elliptic divisibility sequences Smyth's results [Smyth 10] on index divisibility of Lucas sequences. Let $(D_n)_{n\geq 1}$ be a normalized minimal regular elliptic divisibility sequence associated with an elliptic curve $E/\mathbb{Q}$ (see [Silverman and Stange 11] for definitions), and consider the set

$$\mathcal{S} = \{n \geq 1 : n \mid D_n\}.$$

The index divisibility set $\mathcal{S}$ is constructed multiplicatively by describing, for a given $n \in \mathcal{S}$, the set of minimal multiples of n that are in $\mathcal{S}$, which we denote by

$$\mathcal{A}_n = \left\{ \begin{array}{l} d \geq 1 : nd \in \mathcal{S}, \text{ and } nd' \notin \mathcal{S} \\ \text{for all } d' \mid d \text{ with } 1 < d' < d \end{array} \right\}.$$

For example, if p is a prime divisor of D_n, then $p \in \mathcal{A}_n$. We prove in [Silverman and Stange 11] that if $(p_1, \ldots, p_\ell)$ is an aliquot cycle of length $\ell \geq 2$ for $E/\mathbb{Q}$ with $p_i \nmid n$, then $p_1 p_2 \cdots p_\ell \in \mathcal{A}_n$. Conversely, let $p_1 p_2 \cdots p_\ell$ be a product of $\ell \geq 2$ distinct primes of good reduction for E not dividing n, and assume that

$$\min p_i > \left(2^{-1/2\ell} - 1\right)^{-2} \quad \text{and} \quad p_1 p_2 \cdots p_\ell \in \mathcal{A}_n.$$

Then $(p_1, \ldots, p_\ell)$ is an aliquot cycle for E. Thus any description of the index divisibility set of an elliptic divisibility sequence will, of necessity, require knowledge of aliquot cycles. See [Silverman and Stange 11] for further details.

2. HOW OFTEN IS $\#\tilde{E}_p(\mathbb{F}_p)$ PRIME?

If an elliptic curve $E/\mathbb{Q}$ is to have any amicable pairs or aliquot cycles, then it is clearly necessary that there exist primes p such that $\tilde{E}_p(\mathbb{F}_p)$ is prime. The question

[1] We also note that some supplemental material for this article is available at http://www.math.brown.edu/~jhs/amicable.html.

of existence and density of such primes has been studied by various authors.

Remark 2.1. If $E(\mathbb{Q})_{\text{tors}} \neq \{O\}$, then $\#\tilde{E}_p(\mathbb{F}_p)$ will be composite for all but finitely many p, since $E(\mathbb{Q})_{\text{tors}} \hookrightarrow \tilde{E}_p(\mathbb{F}_p)$ for all $p \nmid 2\Delta_{E/\mathbb{Q}}$. Using this observation, it is quite easy to produce curves having no nontrivial aliquot cycles, for example the curves $y^2 = x^3 + x$ and $y^2 = x^3 + 1$.

Koblitz has given a precise conjecture for the number of primes $p \le X$ such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime.

Conjecture 2.2. [Koblitz 88] *Let $E/\mathbb{Q}$ be an elliptic curve, and let*

$$\mathcal{N}_E(X) = \#\left\{ \begin{array}{c} \text{primes } p \le X \text{ such that} \\ \#\tilde{E}_p(\mathbb{F}_p) \text{ is prime} \end{array} \right\}$$

count how often E modulo p has a prime number of points. Then there is a constant $C_{E/\mathbb{Q}}$ such that

$$\mathcal{N}_E(X) = C_{E/\mathbb{Q}} \frac{X}{(\log X)^2} + o\left(\frac{X}{(\log X)^2}\right).$$

In his paper, Koblitz gave a conjectural formula for the constant $C_{E/\mathbb{Q}}$ that turned out to be incorrect in some cases. Zywina has given a corrected value for $C_{E/\mathbb{Q}}$ [Zywina 09]. The formula for $C_{E/\mathbb{Q}}$ is in terms of the image of the representation $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(E_{\text{tors}})$. In principle, this allows one to approximate $C_{E/\mathbb{Q}}$ to high precision, and Koblitz and Zywina both give a number of examples. We also note recent work of Jones showing that the condition $C_{E/\mathbb{Q}} > 0$ involves subtle properties of the curve E [Jones 10]. For additional work on the (almost) primality of $\#\tilde{E}_p(\mathbb{F}_p)$, see [Balog et al. 07, Cojocaru 05, Cojocaru et al. 09, Friedlander and Shparlinski 09, Jiménez Urroz 08].

3. ALIQUOT CYCLES AND AMICABLE PAIRS FOR ELLIPTIC CURVES

We formally give the following definitions as previously described in the introduction.

Definition 3.1. Let $E/\mathbb{Q}$ be an elliptic curve. An *aliquot cycle of length ℓ* for $E/\mathbb{Q}$ is a sequence of distinct primes $(p_1, p_2, \dots, p_\ell)$ such that E has good reduction at every p_i and such that

$$\begin{aligned} \#\tilde{E}_{p_1}(\mathbb{F}_{p_1}) = p_2, \quad \#\tilde{E}_{p_2}(\mathbb{F}_{p_2}) = p_3, \quad \dots, \\ \#\tilde{E}_{p_{\ell-1}}(\mathbb{F}_{p_{\ell-1}}) = p_\ell, \quad \#\tilde{E}_{p_\ell}(\mathbb{F}_{p_\ell}) = p_1. \end{aligned}$$

An aliquot cycle is *normalized* if $p_1 = \min p_i$. Every aliquot cycle can be normalized by a cyclic shift of its elements. An *amicable pair* is an aliquot cycle of length two.

Remark 3.2. Classically, an amicable pair is a pair of integers (m, n) satisfying $\tilde{\sigma}(m) = n$ and $\tilde{\sigma}(n) = m$, where $\tilde{\sigma}(n)$ is the sum of the proper divisors of n. Similarly, a number n is perfect if $\tilde{\sigma}(n) = n$, and a (classical) aliquot cycle is a list of distinct integers $(n_1, n_2, \dots, n_\ell)$ satisfying

$$\begin{aligned} &\tilde{\sigma}(n_1) = n_2, \ \ \tilde{\sigma}(n_2) = n_3, \ \ \dots, \ \ \tilde{\sigma}(n_{\ell-1}) = n_\ell, \\ &\tilde{\sigma}(n_\ell) = n_1. \end{aligned}$$

(Numbers appearing in an aliquot cycle are also called sociable numbers.) Perfect numbers and amicable pairs were studied in ancient Greece, and aliquot cycles of all lengths continue to attract interest to the present day. See, for example, [García et al. 04, Te Riele 82, Yan 96].

We have thus appropriated a classical name. More generally, for any arithmetic function $f(n)$, one might say that an integer n is *f-perfect* if $f(n) = n$, that a pair (m, n) is *f-amicable* if $f(m) = n$ and $f(n) = m$, and that an ℓ-tuple $(n_1, \dots, n_\ell)$ is *f-aliquot* if $f(n_{i \bmod \ell}) = n_{i+1 \bmod \ell}$. However, in our situation, a "perfect prime" for $E/\mathbb{Q}$, i.e., a prime satisfying $\#\tilde{E}_p(\mathbb{F}_p) = p$, already has a name. Such primes are called *anomalous primes* and appear as exceptional cases in diverse applications; see, for example, [Mazur 72, Olson 76]. In particular, anomalous primes are to be avoided in cryptography because the elliptic curve discrete logarithm problem (ECDLP) for anomalous primes can be solved in linear time [Satoh and Araki 98, Semaev 98, Smart 99].

Remark 3.3. Kowalski calls a pair of primes (p, q) a *twin pair for E* if $\#\tilde{E}_p(\mathbb{F}_p) = \#\tilde{E}_q(\mathbb{F}_q)$ [Kowalski 06]. He explains why they are a natural elliptic analogue of classical twin primes $(p, p+2)$, discusses their conjectural distribution, and proves some interesting results in the CM case.

We begin our study of aliquot cycles with the following general observation concerning amicable pairs.

Proposition 3.4. *Let $E/\mathbb{Q}$ be an elliptic curve, and let (p, q) be a normalized amicable pair for $E/\mathbb{Q}$ with $p \ge 5$. Then*

$$\text{End}(\tilde{E}_p/\mathbb{F}_p) \otimes \mathbb{Q} \cong \text{End}(\tilde{E}_q/\mathbb{F}_q) \otimes \mathbb{Q}.$$

Proof: The fact that p is odd and $q = \#\tilde{E}_p(\mathbb{F}_p) = p + 1 - a_p$ is prime implies in particular that $a_p \neq 0$, so E

has ordinary reduction at p. (This is where we use the assumption that $p \geq 5$; cf. [Silverman 09, Exercise 5.10].) Reversing the roles of p and q shows that E also has ordinary reduction at q.

The assumption that (p, q) is an amicable pair is equivalent to the assertions that

$$q = p + 1 - a_p \quad \text{and} \quad p = q + 1 - a_q,$$

and then a little bit of algebra shows that

$$a_p^2 - 4p = a_q^2 - 4q. \tag{3–1}$$

The field $\mathrm{End}(\tilde{E}_p/\mathbb{F}_p) \otimes \mathbb{Q}$ is generated by the Frobenius element $\mathrm{Frob}_p(x) = x^p$, which is a root of

$$T^2 - a_p T + p = 0.$$

Thus

$$\mathrm{End}(\tilde{E}_p/\mathbb{F}_p) \otimes \mathbb{Q} \cong \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right).$$

The analogous formula is true for q, and then (3–1) completes the proof of the proposition. □

4. COUNTING ALIQUOT CYCLES FOR NON-CM ELLIPTIC CURVES

In this section we study the aliquot cycle counting function

$$\mathcal{Q}_{E,\ell}(X) = \#\left\{\begin{matrix}\text{normalized aliquot cycles } (p_1, \ldots, p_\ell) \\ \text{of length } \ell \text{ for } E/\mathbb{Q} \text{ satisfying } p_1 \leq X\end{matrix}\right\}.$$

Conjecture 4.1. *Let $E/\mathbb{Q}$ be an elliptic curve that does not have complex multiplication, and assume that there are infinitely many primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime. Then the aliquot cycle counting function satisfies*

$$\mathcal{Q}_{E,\ell}(X) \asymp \frac{\sqrt{X}}{(\log X)^\ell} \quad \text{as } X \to \infty,$$

where the implied positive constants depend on E and ℓ, but are independent of X.

Remark 4.2. As noted in Section 10, an aliquot cycle (p) of length one consists of a single anomalous prime. In this case, Conjecture 4.1 follows from a general conjecture of Lang and Trotter, which predicts the stronger result

$$\mathcal{Q}_{E,1}(X) = c\frac{\sqrt{X}}{\log X} + o\left(\frac{\sqrt{X}}{\log X}\right).$$

[Lang and Trotter 76]. More generally, we have stated Conjecture 4.1 in its present form because we have a heuristic argument to support this formulation. However, as one of the referees noted, if Conjecture 4.1 is true, then most likely there will be an asymptotic formula

$$\mathcal{Q}_{E,\ell}(X) = c_{E,\ell}\frac{\sqrt{X}}{(\log X)^\ell} + o\left(\frac{\sqrt{X}}{(\log X)^\ell}\right). \tag{4–1}$$

It would be interesting to describe, even conjecturally, the value of $c_{E,\ell}$ in (4–1). We also note that for curves with CM, we give such a formula in Conjecture 6.9 (for $j(E) \neq 0$) and Conjectures 7.10 and 7.14 (for $j(E) = 0$).

We now give a heuristic argument in support of Conjecture 4.1. To ease notation, let

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

Then, setting $p_1 = p$, we have

$$\begin{aligned}&\mathrm{Prob}(p \text{ is part of an aliquot cycle of length } \ell) \qquad (4–2)\\ &= \mathrm{Prob}\left(\begin{matrix}p_2 \overset{\text{def}}{=} N_{p_1} \text{ is prime, } p_3 \overset{\text{def}}{=} N_{p_2} \text{ is prime,} \\ \ldots, p_\ell \overset{\text{def}}{=} N_{p_{\ell-1}} \text{ is prime, and } N_{p_\ell} = p_1\end{matrix}\right)\\ &\approx \left(\prod_{i=1}^{\ell-1} \mathrm{Prob}(p_{i+1} \overset{\text{def}}{=} N_{p_i} \text{ is prime})\right)\mathrm{Prob}(N_{p_\ell} = p_1).\end{aligned}$$

(We ignore the small probability that there is some $i < \ell$ such that N_{p_i} is equal to an earlier p_j.)

Under our assumption that N_p is prime for infinitely many p, Conjecture 2.2 says that

$$\mathrm{Prob}(N_p \text{ is prime}) \asymp \frac{1}{\log p},$$

and since

$$p_{i+1} = N_{p_i} = p_i + O\left(\sqrt{p_i}\right),$$

every term in the sequence $p = p_1, p_2, \ldots, p_\ell$ satisfies $p_i = p + O(\sqrt{p})$. Hence

$$\mathrm{Prob}(N_{p_i} \text{ is prime}) \asymp \frac{1}{\log p_i} \sim \frac{1}{\log p}.$$

Substituting this into (4–2) gives

$$\begin{aligned}&\mathrm{Prob}\left(p \text{ is part of an aliquot cycle of length } \ell\right)\\ &\approx \frac{1}{(\log p)^{\ell-1}} \cdot \mathrm{Prob}(N_{p_\ell} = p_1). \qquad (4–3)\end{aligned}$$

In order to estimate the last factor, we use the Sato–Tate conjecture [Silverman 09, C.21.1], which says that as q varies, the values of N_q are distributed in the interval

$\left[q+1-2\sqrt{q}, q+1+2\sqrt{q}\right]$ according to the Sato–Tate distribution,

$$\#\left\{q \le X : a \le \frac{q+1-N_q}{2\sqrt{q}} \le b\right\} \sim \pi(X)\cdot\frac{2}{\pi}\int_a^b \sqrt{1-t^2}\,dt.$$

(See [Taylor 08] for a proof of the Sato–Tate conjecture in certain cases, although our use of the conjecture is purely heuristic.) Then for primes p and $q = p + O(\sqrt{p})$, a rough estimate gives

$$\text{Prob}(N_q = p) \asymp \frac{1}{\sqrt{q}} \sim \frac{1}{\sqrt{p}}. \tag{4–4}$$

Combining (4–3) and (4–4) yields

$$\text{Prob}\,(p \text{ is part of an aliquot cycle of length } \ell) \asymp \frac{1}{\sqrt{p}(\log p)^{\ell-1}}.$$

We now estimate the number of normalized aliquot cycles of length ℓ whose initial prime is less than X:

$$\begin{aligned}\mathcal{Q}_{E,\ell}(X) &\approx \sum_{p\le X} \text{Prob}\begin{pmatrix}p \text{ is the initial element of a nor-}\\ \text{malized aliquot cycle of length } \ell\end{pmatrix}\\ &\asymp \sum_{p\le X}\frac{1}{\sqrt{p}(\log p)^{\ell-1}}.\end{aligned}$$

It remains only to use the rough approximation

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

to obtain

$$\mathcal{Q}_{E,\ell}(X) \asymp \int^X \frac{1}{\sqrt{u}(\log u)^{\ell-1}}\cdot\frac{du}{\log u} \asymp \frac{\sqrt{X}}{(\log X)^{\ell}}.$$

Remark 4.3. It seems hopeless at present to prove Conjecture 4.1 unconditionally for any particular curve. However, Balog, Cojocaru, and David have proven [Balog et al. 07] that a version of Koblitz's conjecture (Conjecture 2.2), with corrected constant as given in [Zywina 09], holds on average over families of curves $y^2 = x^3 + ax + b$ with $|a| < A$ and $|b| < B$. (See also [Jones 09, Sakagawa 08].) It would be interesting to see whether their techniques could be used to prove an average-case version of Conjecture 4.1. Of course, it would first be necessary to give an explicit estimate for the implied constants in Conjecture 4.1. (We thank Igor Shparlinski for this suggestion.)

5. ALIQUOT CYCLES OF ARBITRARY LENGTH

In this section we prove that there exist elliptic curves with aliquot cycles of arbitrary length. After submitting this paper, we became aware that our proof is similar to the proof of [Kowalski 06, Proposition 4.9], in which Kowalski constructs elliptic curves such that $\#\tilde{E}_p(\mathbb{F}_p)$ is constant for all p in a given Hasse interval.

Theorem 5.1. *For every $\ell \ge 1$ there exists an elliptic curve $E/\mathbb{Q}$ that has an aliquot cycle of length ℓ. More generally, for any positive integers $\ell_1, \dots, \ell_r$, there exists an elliptic curve $E/\mathbb{Q}$ that has distinct aliquot cycles of lengths $\ell_1, \dots, \ell_r$.*

Proof: A theorem from [Deuring 41] (vastly generalized in [Waterhouse 69]; see also [Rück 87]) says that if p is a prime and t is an integer satisfying $|t| \le 2\sqrt{p}$, then there exists an elliptic curve $\tilde{E}/\mathbb{F}_p$ satisfying

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

In other words, every Frobenius trace in the Hasse interval for p actually occurs as the trace of an elliptic curve defined over $\mathbb{F}_p$.

Now fix ℓ and let $p_1, p_2, \dots, p_\ell$ be a sequence of primes with the property that

$$|p_i + 1 - p_{i+1}| \le 2\sqrt{p_i} \quad \text{for all } 1 \le i \le \ell, \tag{5–1}$$

where by convention we set $p_{\ell+1} = p_1$. It is easy enough to find such a sequence. To be precise, we can use a weak form of the prime number theorem [Apostol 76, Theorem 4.7] that says that there are positive constants a and b such that the nth prime q_n satisfies

$$an\log(n) \le q_n \le bn\log(n).$$

It follows that for any given ℓ, if we choose n to be sufficiently large, then

$$q_{n+\ell} - q_n - 1 \le 2\sqrt{q_n}.$$

This implies that the sequence of primes $(q_{n+1}, q_{n+2}, \dots, q_{n+\ell})$ satisfies (5–1), so we take this to be our sequence $(p_1, \dots, p_\ell)$.

Applying the theorem of Deuring cited earlier, for each p_i we can find an elliptic curve $\tilde{E}_i/\mathbb{F}_{p_i}$ satisfying

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

(This includes the case $i = \ell$, in which $p_{\ell+1} = p_1$.) We now use the Chinese remainder theorem on the coefficients of the Weierstrass equations for $\tilde{E}_1, \dots, \tilde{E}_\ell$ to find an elliptic curve $E/\mathbb{Q}$ satisfying

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

Then by construction, the sequence $(p_1, \dots, p_\ell)$ is an aliquot cycle of length ℓ for $E/\mathbb{Q}$.

In a similar fashion, we can construct elliptic curves over $\mathbb{Q}$ that have aliquot cycles of any specified lengths using different sets of primes, and then we can use the Chinese remainder theorem on the coefficients of these curves to obtain a single elliptic curve over $\mathbb{Q}$ with any specified number of aliquot cycles of any specified lengths. □

Example 5.2. The algorithm described in Theorem 5.1 works well in practice, although it naturally yields equations having large coefficients. We used it in Example 1.4 to find an aliquot cycle of length 14. Here is another example. The following elliptic curve has an aliquot cycle of length 25, starting with the prime $p = 41$:

$$y^2 = x^3 + 4545482133607498579268567738514832922289740324532x + 59586726546211211829143024589437946496788579471 3.$$

6. AMICABLE PAIRS FOR CM CURVES WITH $j \neq 0$

Our next goal is to formulate and provide evidence for more-precise versions of the CM part of Conjecture 1.3. A key observation is that if E has CM, then the assumption that $q = \#\tilde{E}_p(\mathbb{F}_p)$ is prime severely limits the possible values of $\tilde{E}_q(\mathbb{F}_q)$. It turns out that the case of elliptic curves with $j(E) = 0$ is significantly more complicated than the other cases, so we deal with the $j(E) \neq 0$ curves in this section and leave the $j(E) = 0$ curves for the next section.

Theorem 6.1. *Let $E/\mathbb{Q}$ be an elliptic curve and assume:*

(1) *E has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$.*

(2) *p and q are primes of good reduction for E with $p \ge 5$ and*

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

(3) *$j(E) \neq 0$, or equivalently, $\mathcal{O} \neq \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.*

Then $D \equiv 3 \pmod 4$, and either

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

Theorem 6.1 has an interesting consequence concerning the allowable lengths of aliquot cycles for CM elliptic curves. This may be compared with Theorem 5.1, which says that there exist (necessarily non-CM) curves having aliquot cycles of arbitrary length, and with Conjecture 4.1, which implies that every non-CM elliptic curve has aliquot cycles of arbitrary length, provided that there are infinitely many primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime.

Corollary 6.2. *A CM elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0$ has no aliquot cycles of length $\ell \ge 3$ consisting of primes $p \ge 5$.*

Remark 6.3. Another way to state the conclusion of Theorem 6.1 is that either $\#\tilde{E}_q(\mathbb{F}_q) = p$, or else the nontrivial quadratic twist $\tilde{E}_q^\chi$ of $\tilde{E}_q$ satisfies $\#\tilde{E}_q^\chi(\mathbb{F}_q) = p$. This is clear, because the trace of Frobenius for a curve and its quadratic twist satisfy

$$a(\tilde{E}_q) + a(\tilde{E}_q^\chi) = 0.$$

See Remark 7.7 for the analogous statement for $j(E) = 0$ curves, which have six twists.

Remark 6.4. There are various ways in which one might generalize Theorem 6.1. For example, replacing assumption (2) by the assumption that L is an integer such that the quantity

$$q = L^2 - \big(p + 1 - \#\tilde{E}_p(\mathbb{F}_p)\big)L + p$$

is prime and splits in K leads to the following conclusion:

$$a_q(E) = \pm\big(a_p(E) + 2L\big).$$

Theorem 6.1 is the case $L = 1$. We omit the proof of the generalization, since it is similar and is not required in this paper.

Remark 6.5. Corollary 6.2 omits curves with $j(E) = 0$. It turns out that $j = 0$ curves possess a rich and complicated amicable pair structure, which will be investigated in detail in Sections 7 and 8. Corollary 7.6 gives an analogue of Theorem 6.1 saying that there are (often) six possible values for $\#\tilde{E}_q(\mathbb{F}_q)$, rather than only the two possibilities given in Theorem 6.1. Using this result, we are able to prove by a detailed case-by-case analysis that $j = 0$ curves cannot have aliquot cycles of length three; see Section 8. But we do not have a proof that there are no aliquot cycles of length greater than three when $j = 0$.

Before commencing the proofs of Theorem 6.1 and Corollary 6.2, we prove a basic result concerning the splitting of primes in CM fields.

Lemma 6.6. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by K, let $p \ge 5$ be a prime of good reduction for $E/\mathbb{Q}$, and suppose that $\#\tilde{E}_p(\mathbb{F}_p)$ is odd. Then p splits in K.*

Proof: We have

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

so the assumptions that $p \ne 2$ and $\#\tilde{E}_p(\mathbb{F}_p)$ is odd imply that a_p is odd, so in particular $a_p \ne 0$. Hence E has ordinary reduction at p. (Note that our assumption that $p \ge 5$ and Hasse's bound $|a_p| \le 2\sqrt{p}$ imply that $p \mid a_p$ if and only if $a_p = 0$.) It follows that the field K is isomorphic to $\mathrm{End}(\tilde{E}_p) \otimes \mathbb{Q}$, which is generated by a root of the characteristic polynomial $T^2 - a_pT + p$ of Frobenius. Therefore $K = \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right)$, and

$$p = \left(\frac{a_p + \sqrt{a_p^2 - 4p}}{2}\right)\left(\frac{a_p - \sqrt{a_p^2 - 4p}}{2}\right)$$

either splits or is ramified in K. But we can rule out the latter case by noting that

$$p \text{ ramified in } K \Longrightarrow p \mid a_p^2 - 4p \Longrightarrow p \mid a_p \Longrightarrow a_p = 0.$$

This contradicts the fact that a_p is odd, and hence p splits in K. □

Proof of Theorem 6.1: Up to $\bar{\mathbb{Q}}$-isomorphism, there are 13 elliptic curves defined over $\mathbb{Q}$ that have complex multiplication. For a list, see, for example, [Silverman 94, A §3]. There are three isomorphism classes whose conductor N_E is a power of two:

$$\begin{aligned} &E : y^2 = x^3 + x, \quad N_E = 2^6,\\ &E : y^2 = x^3 + 6x^2 + x, \quad N_E = 2^5,\\ &E : y^2 = x^3 + 4x^2 + 2x, \quad N_E = 2^8. \end{aligned}$$

All three of these curves have a nontrivial two-torsion point, as do all of their $\bar{\mathbb{Q}}/\mathbb{Q}$ twists, so $\#E(\mathbb{F}_p)$ is even for all $p \ge 3$. Hence none of these curves admit an amicable pair; cf. Remark 2.1. The remaining CM curves have complex multiplication by a field $\mathbb{Q}(\sqrt{-D})$ with $D \equiv 3 \pmod 4$.

The endomorphism ring of E is an order in the field $K = \mathbb{Q}(\sqrt{-D})$, where $D \equiv 3 \pmod 4$, so it has the form

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

for some integer $f \ge 1$, which is called the conductor of $\mathcal{O}$. In particular, we have $\mathcal{O}^* = \{\pm 1\}$, since our assumption that $j(E) \ne 0$ excludes the case $(D, f) = (3, 1)$.

The theory of complex multiplication says that there is a Grössencharacter ψ_E such that for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ of residue characteristic $p \ge 5$ at which E has good reduction, we have

(i) $\psi_E(\mathfrak{p}) \in \mathcal{O}$ with $\psi_E(\mathfrak{p})\mathcal{O}_K = \mathfrak{p}$.

(ii) $\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) + 1 - \mathrm{Tr}\big(\psi_E(\mathfrak{p})\big)$.

See, for example, [Rubin and Silverberg 09, Proposition 4.1] or [Silverman 94, II §9]. (Note that our assumption that $\mathfrak{p}$ has residue characteristic $p \ge 5$ implies that p does not divide the conductor of $\mathcal{O}$, since the fact that E has CM and is defined over $\mathbb{Q}$ forces $\mathcal{O}$ to have class number one, which in turn means that the conductor of $\mathcal{O}$ is at most 3.)

We are given that $p \ge 5$ and that $\#\tilde{E}_p(\mathbb{F}_p) = q$ is prime. It follows from Lemma 6.6 that p splits in K, say

$$p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}.$$

Then $\mathbb{F}_p = \mathbb{F}_{\mathfrak{p}}$, so

$$q = \#\tilde{E}_p(\mathbb{F}_p) = \#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) = \mathrm{N}_{K/\mathbb{Q}}\big(1 - \psi_E(\mathfrak{p})\big). \quad (6\text{–}1)$$

Notice that this implies, in particular, that q splits in K. So writing $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$, we have

$$q = \mathrm{N}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{q})\big). \quad (6\text{–}2)$$

Comparing (6–1) and (6–2), and using the fact that $\psi_E(\mathfrak{p})$ and $\psi_E(\mathfrak{q})$ are in $\mathcal{O}$, we see that there is a unit $u \in \mathcal{O}^*$ such that either

$$\psi_E(\mathfrak{q}) = u\big(1 - \psi_E(\mathfrak{p})\big) \quad \text{or} \quad \psi_E(\mathfrak{q}) = u\overline{\big(1 - \psi_E(\mathfrak{p})\big)}. \quad (6\text{–}3)$$

(This follows from the fact that the factorization of the ideal $q\mathcal{O}$ is unique, up to switching the factors.)

As noted earlier, we have $\mathcal{O}^* = \{\pm 1\}$, so

$$\begin{aligned} &\mathrm{Tr}\big(\psi_E(\mathfrak{q})\big)\\ &\quad = \pm\,\mathrm{Tr}\big(1 - \psi_E(\mathfrak{p})\big) && \text{from (6–3) with } u = \pm 1\\ &\quad = \pm\,\big(2 - \mathrm{Tr}\big(\psi_E(\mathfrak{p})\big)\big) && \text{linearity}\\ &\quad = \pm\big(2 - (p + 1 - q)\big) && \text{since } \#\tilde{E}_p(\mathbb{F}_p) = q\\ &\quad = \pm(q + 1 - p). \end{aligned}$$

Hence

$$\begin{aligned} \#\tilde{E}_q(\mathbb{F}_q) = \#\tilde{E}_{\mathfrak{q}}(\mathbb{F}_{\mathfrak{q}}) &= q + 1 - \mathrm{Tr}\big(\psi_E(\mathfrak{q})\big)\\ &= q + 1 \pm (q + 1 - p). \end{aligned}$$

This completes the proof of Theorem 6.1. □

Proof of Corollary 6.2: Let $(p_1, p_2, \dots, p_\ell)$ be a normalized aliquot cycle of length $\ell \ge 3$ for $E/\mathbb{Q}$ such that all $p_i \ge 3$. Since the primes in the cycle are distinct, Theorem 6.1 tells us that

$$p_i - p_{i-1} = p_{i-1} - p_{i-2} + 2 \quad \text{for } 3 \le i \le \ell. \tag{6–4}$$

Further, since the term in the aliquot cycle following p_ℓ is p_1, Theorem 6.1 gives

$$p_1 - p_\ell = p_\ell - p_{\ell-1} + 2. \tag{6–5}$$

We have assumed that the cycle is normalized, i.e., $p_2 - p_1 > 0$. Induction using (6–4) shows that $p_i - p_{i-1} > 0$ for all $2 \le i \le \ell$, and then (6–5) says that $p_1 - p_\ell > 0$. Hence $(p_1, \dots, p_\ell, p_1)$ is a strictly increasing list of integers, a contradiction that completes the proof of Corollary 6.2. □

Remark 6.7. Suppose that $E/\mathbb{Q}$ has CM and that $(p_1, \dots, p_\ell)$ satisfies $\#\tilde{E}_{p_i}(\mathbb{F}_{p_i}) = p_{i+1}$ for $1 \le i < \ell$, but we do not require that the sequence form a cycle. Then (6–4) gives a (degenerate) linear recurrence for the p_i whose solution is

$$p_i = (i-1)p_2 - (i-2)p_1 + (i-1)(i-2). \tag{6–6}$$

If the sequence (p_i) did cycle, then we would have $p_{\ell+1} = p_1$ and $p_{\ell+2} = p_2$. Putting first $i = \ell + 1$ and then $i = \ell + 2$ into (6–6) yields (after some algebra) $p_1 = p_2 + \ell - 1$ and $p_1 = p_2 + \ell + 1$, a contradiction that provides an alternative proof of Corollary 6.2.

Remark 6.8. Let $E/\mathbb{Q}$ be an elliptic curve having no rational torsion, having CM by $\mathbb{Q}(\sqrt{-D})$, and satisfying $j \ne 0$. Suppose that p is a prime for which $\#\tilde{E}_p(\mathbb{F}_p) = q$ is prime, and suppose that $\mathfrak{p}$ lies over p. Write

$$\psi_E(\mathfrak{p}) = \left(m + \frac{1}{2}\right) + \frac{\ell}{2}\sqrt{-D},$$

where m and ℓ are integers. (This is always possible, since $D \equiv 3 \pmod 4$.) Then

$$p = N(\psi_E(\mathfrak{p})) = m^2 + m + \frac{1 + \ell^2 D}{4},$$
$$q = N(1 - \psi_E(\mathfrak{p})) = (m-1)^2 + (m-1) + \frac{1 + \ell^2 D}{4}.$$

(If $\psi_E(\mathfrak{q})$ for $\mathfrak{q}$ above q has trace $-2m + 1$, then this will result in an amicable pair.) Thus prime reduction is related to the occurrence of "twin primes" in the quadratic progression of values of a quadratic polynomial of the form $x^2 + x + a$. See [Olson 79] for more about this connection. For example, it is well known that the polynomial $x^2 + x + 41$ is prime for the 40 values of x between 0 and 39, and we find the following amicable pairs in the range $1 < p \le 1600$ for the elliptic curve

$$y^2 = x^3 + x^2 - 2174420x + 1234136692$$

having CM by $\mathbb{Q}(\sqrt{-163})$:

$$(\mathbf{41}, \mathbf{43}),\ (61, 71),\ (97, 113),\ (\mathbf{151}, \mathbf{173}),\ (197, 223),$$
$$(347, 383),\ (503, 547),\ (673, 709),\ (\mathbf{853}, \mathbf{911}),$$
$$(971, 1033),\ (1039, 1049),\ (1097, 1163),\ (1129, 1151),$$
$$(\mathbf{1301}, \mathbf{1373}),\ (1423, 1489),\ (\mathbf{1523}, \mathbf{1601}).$$

In this list, the pairs that are in bold appear in the list of prime values of $x^2 + x + 41$.

Write $\mathrm{Twin}(a)$ for the set of such "quadratic twin primes" in the values of $x^2 + x + a$. Conjecture 1.3(b), or Conjecture 2.2 of Koblitz, then implies the existence of a constant C such that

$$\#\bigcup_{\ell \ge 0} \mathrm{Twin}\left(\frac{1 + \ell^2 D}{4}\right) \sim C\frac{X}{(\log X)^2}.$$

See [Baier and Zhao 08] for background on primes in quadratic progression.

We now use Theorem 6.1 to give a heuristic justification for the following conjecture.

Conjecture 6.9. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication, and assume that $j(E) \ne 0$. Define counting functions*

$$\mathcal{N}_E(X) = \#\left\{ \begin{array}{c} \text{primes } p \le X \text{ such that} \\ \#\tilde{E}_p(\mathbb{F}_p) \text{ is prime} \end{array} \right\},$$
$$\mathcal{Q}_E(X) = \#\left\{ \begin{array}{c} \text{amicable pairs } (p,q) \text{ for } E/\mathbb{Q} \\ \text{with } p < q \text{ and } p \le X \end{array} \right\}.$$

Then either $\mathcal{N}_E(X)$ is bounded, or else

$$\lim_{X \to \infty} \frac{\mathcal{Q}_E(X)}{\mathcal{N}_E(X)} = \frac{1}{4}.$$

We note that Conjecture 2.2 says that if $\mathcal{N}_E(X)$ is unbounded, then it is asymptotic to $C_{E/\mathbb{Q}}X/(\log X)^2$. So the combination of Conjectures 2.2 and 6.9 gives a strengthened version of the CM part of Conjecture 1.3.

Our justification for Conjecture 6.9 is to observe that Theorem 6.1 says that if $\#\tilde{E}_p(\mathbb{F}_p) = q$ is prime, then there are two possibilities for $\#\tilde{E}_q(\mathbb{F}_q)$, one of which is p. Experiments indicate that each possibility occurs with equal probability, and we have no theoretical reasons for expecting otherwise, so we will accept the hypothesis that

$$\mathrm{Prob}\left(\#\tilde{E}_q(\mathbb{F}_q) = p \;\middle|\; \#\tilde{E}_p(\mathbb{F}_p) = q \text{ is prime}\right) = \frac{1}{2}.$$

Further, if we assume Conjecture 2.2, then

$$\text{Prob}\left(\#\tilde{E}_p(\mathbb{F}_p) \text{ is prime} \;\middle|\; p \le X\right) \sim \frac{\mathcal{N}_E(X)}{\pi(X)}.$$

Combining these estimates yields

$$\begin{aligned}
&\#\left\{p \le X : \#\tilde{E}_p(\mathbb{F}_p) = q \text{ is prime and } \#\tilde{E}_q(\mathbb{F}_q) = p\right\} \\
&\quad\approx \sum_{p\le X} \text{Prob}\left(\begin{array}{l}\#\tilde{E}_p(\mathbb{F}_p) = q \text{ is prime} \\ \text{and } \#E_q(\mathbb{F}_q) = p\end{array}\right) \\
&\quad\approx \sum_{p\le X} \text{Prob}\left(\#\tilde{E}_q(\mathbb{F}_q) = p \;\middle|\; \#\tilde{E}_p(\mathbb{F}_p) = q \text{ is prime}\right) \\
&\qquad\qquad \times \text{Prob}\left(\#\tilde{E}_p(\mathbb{F}_p) \text{ is prime}\right) \\
&\quad\approx \sum_{p\le X} \frac{1}{2}\cdot\frac{\mathcal{N}_E(X)}{\pi(X)} = \frac{\mathcal{N}_E(X)}{2}.
\end{aligned}$$

Finally, we need to divide by 2, because $\mathcal{Q}_E(X)$ counts only amicable pairs (p,q) that are normalized to satisfy $p < q$.

Remark 6.10. The referee has pointed out that if $E/\mathbb{Q}$ has CM, then one can show that

$$\mathcal{N}_E(X) \ll \frac{X}{(\log X)^2},$$

which of course yields the same upper bound for $\mathcal{Q}_E(X)$. This at least gives an upper bound of the right order of magnitude in Conjecture 1.3(b). The proof is a basic application of sieve theory, but lacking a reference, we briefly sketch the proof as shown to us by Ram Murty.

Let A be a finite multiset, and for each d, let A_d be the subset of A of elements divisible by d. Suppose that we write $\#A_d = \#A/f(d) + R_d$ for some function f. In order to give an upper bound for the number of elements in A that are not divisible by primes $p < z$, sieve theory says that we need to have a good estimate for the error sum

$$\sum_{d<z^2} |R_d|. \tag{6–7}$$

We now take A to be the multiset of $\#\tilde{E}(\mathbb{F}_p)$ with $p < X$. Then an estimate for (6–7) is obtained in the CM case using a version of the Bombieri–Vinogradov theorem for imaginary quadratic fields with $z = x^t$ with $t < \frac{1}{4}$. (See [Murty and Murty 87] for the Bombieri–Vinogradov-type theorem for number fields that is required.) This easily leads to estimates of the form $\mathcal{N}_E(X) \ll \pi(X)/\log X$. Indeed, it would suffice to have a good estimate for (6–7) with $z = x^t$ for any fixed $t > 0$.

7. AMICABLE PAIRS FOR CM CURVES WITH $j = 0$

In this section we study elliptic curves having j-invariant zero. The analysis of amicable pairs on these curves is significantly more complicated than that on all other CM elliptic curves, due primarily to the extra units in the endomorphism ring. In particular, experiments described in Section 9 suggest that the limiting value of $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ for the curve $y^2 = x^3 + k$ varies for different values of k; see Conjecture 7.24.

We continue with the Grössencharacter notation from the previous section and set some additional notation that will remain in effect for this section. We let

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

so ω is a primitive sixth root of unity. We note that the unit group $(\mathcal{O}_K/3\mathcal{O}_K)^*$ is a group of order 6, and that the natural map

$$\boldsymbol{\mu}_6 = \mathcal{O}_K^* \xrightarrow{\sim} (\mathcal{O}_K/3\mathcal{O}_K)^*$$

is an isomorphism. Further, for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that is relatively prime to 3 and any $\alpha \in \mathcal{O}_K \smallsetminus \mathfrak{p}$, we recall that the sextic residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_6$ is defined by the conditions

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_6 \in \boldsymbol{\mu}_6 \quad\text{and}\quad \left(\frac{\alpha}{\mathfrak{p}}\right)_6 \equiv \alpha^{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p}-1)/6} \pmod{\mathfrak{p}}.$$

Theorem 7.1. *Let $k \in \mathbb{Z}$ be a nonzero integer, let $E/\mathbb{Q}$ be the elliptic curve*

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

so E has CM by $\mathcal{O}_K$, and let ψ_E be the Grössencharacter associated to E. Suppose that $p \ge 5$ and $q \ge 5$ are primes of good reduction for E such that

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

Then:

(a) *The prime p splits in K, say $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, and satisfies*

$$\psi_E(\mathfrak{p})\big(1-\psi_E(\mathfrak{p})\big) \equiv 1 \pmod{3\mathcal{O}_K}.$$

(b) *The ideal defined by $\mathfrak{q} = \big(1-\psi_E(\mathfrak{p})\big)\mathcal{O}_K$ satisfies $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$. In particular, the prime q splits in K.*

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

$$1 - \psi_E(\mathfrak{p}) = \left(\frac{4k}{\mathfrak{p}}\right)_6 \left(\frac{4k}{\mathfrak{q}}\right)_6 \psi_E(\mathfrak{q}). \tag{7–1}$$

(d) *Let* $\epsilon \in \{\pm 1\}$. *Then the trace* $a_q(E) = q+1-\#\tilde{E}_q(\mathbb{F}_q)$ *satisfies*

$$a_q(E) = \epsilon(q+1-p) \Longleftrightarrow \left(\frac{4k}{\mathfrak{p}}\right)_6 \left(\frac{4k}{\mathfrak{q}}\right)_6 = \epsilon. \quad (7\text{–}2)$$

Remark 7.2. The expressions in (c) and (d) appear naturally in the course of proving Theorem 7.1, but we note that they may be simplified using Proposition 7.5, which says that $\left(\frac{4}{\mathfrak{p}}\right)_6 \left(\frac{4}{\mathfrak{q}}\right)_6 = 1$. This allows us to rewrite (7–1) and (7–2) as

$$1 - \psi_E(\mathfrak{p}) = \left(\frac{k}{\mathfrak{p}}\right)_6 \left(\frac{k}{\mathfrak{q}}\right)_6 \psi_E(\mathfrak{q}), \quad (7\text{–}1')$$

$$a_q(E) = \pm(q+1-p) \Longleftrightarrow \left(\frac{k}{\mathfrak{p}}\right)_6 \left(\frac{k}{\mathfrak{q}}\right)_6 = \pm 1. \quad (7\text{–}2')$$

Proof: The fact that p splits in $\mathcal{O}_K$ follows from Lemma 6.6, which proves the first part of (a). Next, as noted during the proof of Theorem 6.1, the Grössencharacter of a CM elliptic curve satisfies

$$\#\tilde{E}_p(\mathbb{F}_p) = \mathrm{N}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{p})\big) + 1 - \mathrm{Tr}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{p})\big).$$

Using the given value $q = \#\tilde{E}_p(\mathbb{F}_p)$, this can be written as

$$q = \mathrm{N}_{K/\mathbb{Q}}\big(1 - \psi_E(\mathfrak{p})\big).$$

Hence $\mathfrak{q} = \big(1-\psi_E(\mathfrak{p})\big)\mathcal{O}_K$ satisfies $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$, which proves (b).

Further, both $\psi_E(\mathfrak{p})$ and $1-\psi_E(\mathfrak{p})$ have norms that are relatively prime to 3. This implies first that $\psi_E(\mathfrak{p}) \equiv \omega^j \pmod 3$ for some $j \in \mathbb{Z}$, and second that j is odd, since otherwise, $1-\omega^j$ would be divisible by $\sqrt{-3}$. On the other hand, for any odd value of j it is easy to check that

$$(1-\omega^j)\omega^j \equiv 1 \pmod{3\mathcal{O}_K},$$

so we find that

$$\psi_E(\mathfrak{p})\big(1-\psi_E(\mathfrak{p})\big) \equiv 1 \pmod{3\mathcal{O}_K}. \quad (7\text{–}3)$$

This proves the second assertion in (a).

For the proof of (c), we use the explicit formula for the Grössencharacter of curves of the form $y^2 = x^3 + k$ in terms of sextic residue symbols. This formula says that $\psi_E(\mathfrak{p}) = -\left(\frac{4k}{\mathfrak{p}}\right)_6^{-1}\pi$, where the generator π is a primary generator for $\mathfrak{p}$, i.e., $\pi \equiv 2 \pmod{3\mathcal{O}_K}$. (See [Ireland and Rosen 90, Chapter 18, Theorem 4, and Section 7] or [Rubin and Silverberg 09, Proposition 4.1].) Reducing this formula for ψ_E modulo 3 and applying it to both of the primes $\mathfrak{p}$ and $\mathfrak{q}$, we obtain

$$\psi_E(\mathfrak{p}) \equiv \left(\frac{4k}{\mathfrak{p}}\right)_6^{-1} \pmod{3\mathcal{O}_K}, \quad (7\text{–}4)$$
$$\psi_E(\mathfrak{q}) \equiv \left(\frac{4k}{\mathfrak{q}}\right)_6^{-1} \pmod{3\mathcal{O}_K}.$$

By definition, the ideal $\mathfrak{q}$ is generated by $1-\psi_E(\mathfrak{p})$. On the other hand, the Grössencharacter has the property that $\psi_E(\mathfrak{q})$ generates the ideal $\mathfrak{q}$. It follows that there is a unit $u \in \mathcal{O}_K^* = \boldsymbol{\mu}_6$ such that $1-\psi_E(\mathfrak{p}) = u\psi_E(\mathfrak{q})$. Using (7–3) and (7–4), we find that

$$u = \frac{1-\psi_E(\mathfrak{p})}{\psi_E(\mathfrak{q})} \equiv \frac{1}{\psi_E(\mathfrak{p})\psi_E(\mathfrak{q})} \equiv \left(\frac{4k}{\mathfrak{p}}\right)_6 \left(\frac{4k}{\mathfrak{q}}\right)_6 \pmod{3\mathcal{O}_K}.$$

Since a sixth root of unity is determined by its residue modulo 3, this last congruence is an equality, which completes the proof of (c).

Using the defining property of the Grössencharacter and formula (7–1) from (c), we have

$$\begin{aligned} a_q(E) &= \mathrm{Tr}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{q})\big) \\ &= \mathrm{Tr}_{K/\mathbb{Q}}\left(\left(\frac{4k}{\mathfrak{p}}\right)_6^{-1}\left(\frac{4k}{\mathfrak{q}}\right)_6^{-1}\big(1-\psi_E(\mathfrak{p})\big)\right). \end{aligned}$$

Similarly, using the assumption that $\#\tilde{E}_p(\mathbb{F}_p) = q$, we find that

$$\begin{aligned} \mathrm{Tr}_{E/\mathbb{Q}}\big(1-\psi_E(\mathfrak{p})\big) &= 2 - \mathrm{Tr}_{E/\mathbb{Q}}\big(\psi_E(\mathfrak{p})\big) \\ &= 2 - (p+1-q) = q+1-p. \end{aligned}$$

Hence for $\epsilon \in \{\pm 1\}$, we have

$$\begin{aligned} &a_q(E) = \epsilon(q+1-p) \Longleftrightarrow \\ &\quad \mathrm{Tr}_{K/\mathbb{Q}}\left(\epsilon\left(\frac{4k}{\mathfrak{p}}\right)_6^{-1}\left(\frac{4k}{\mathfrak{q}}\right)_6^{-1}\big(1-\psi_E(\mathfrak{p})\big)\right) \\ &\quad = \mathrm{Tr}_{E/\mathbb{Q}}\big(1-\psi_E(\mathfrak{p})\big). \end{aligned}$$

We now use the following lemma, which may be applied because the quantity $\mathrm{N}_{E/\mathbb{Q}}\big(1-\psi_E(\mathfrak{p})\big) = q$ is neither a square nor 3 times a square. The lemma allows us to conclude that

$$a_q(E) = \epsilon(q+1-p) \Longleftrightarrow \epsilon\left(\frac{4k}{\mathfrak{p}}\right)_6^{-1}\left(\frac{4k}{\mathfrak{q}}\right)_6^{-1} = 1,$$

which completes the proof of (e). □

Lemma 7.3. *Let* $\alpha \in \mathcal{O}_K$ *have the property that* $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ *is neither a square nor* 3 *times a square. Then*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \quad \textit{with } \zeta \in \boldsymbol{\mu}_6 \Longleftrightarrow \zeta = 1.$$

Proof: We have

$$\begin{aligned}
&\mathrm{Tr}_{K/\mathbb{Q}}(\zeta\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)\\
&\quad\iff \mathrm{Tr}_{K/\mathbb{Q}}\big((\zeta-1)\alpha\big) = 0\\
&\quad\iff (\zeta-1)\alpha = c\sqrt{-3} \qquad \text{for some } c\in\mathbb{Z}\\
&\quad\iff \zeta = 1 \text{ or } \alpha = c\frac{\sqrt{-3}}{\zeta-1}.
\end{aligned}$$

(Note that c is in $\mathbb{Z}$ because ζ and α are in $\mathcal{O}_K = \mathbb{Z}[\omega]$.) Suppose that $\zeta \ne 1$. We observe that as ζ ranges over $\boldsymbol{\mu}_6 \smallsetminus \{1\}$, the quantity $\sqrt{-3}/(\zeta-1)$ takes on the five values

$$\left\{2-\omega, 1-\omega, \frac{1}{2}-\omega, -\omega, -1-\omega\right\}.$$

The norms of these five numbers form the set $\left\{1, 3, \frac{3}{4}\right\}$, so the norm of α would have the form c^2, $3c^2$, or $3(c/2)^2$, contradicting the assumption on $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$. □

We can use Theorem 7.1 to show that for some curves with $j(E) = 0$, the conclusion of Theorem 6.1 is true, i.e., there are only two possible values for $\#\tilde{E}_q(\mathbb{F}_q)$.

Corollary 7.4. *Let $d \in \mathbb{Z}$ be a nonzero integer, and let E be the elliptic curve $E : y^2 = x^3 + 2d^3$. Let p be a prime with $p \nmid 6d$ such that $q = \#\tilde{E}_p(\mathbb{F}_p)$ is also prime and satisfies $q \nmid 6d$. Then*

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

Proof: Using notation from Theorem 7.1, we have $k = 2d^3$, so

$$\left(\frac{4k}{\mathfrak{p}}\right)_6 = \left(\frac{2d}{\mathfrak{p}}\right)_6^3 = \pm 1 \quad \text{and} \quad \left(\frac{4k}{\mathfrak{q}}\right)_6 = \left(\frac{2d}{\mathfrak{q}}\right)_6^3 = \pm 1.$$

It follows from Theorem 7.1(d) that $a_q(E)$ is equal to $\pm(q+1-p)$. □

We next prove two useful facts.

Proposition 7.5. *Let k, E, p, q, $\mathfrak{p}$, and $\mathfrak{q}$ be as in the statement of Theorem 7.1.*

(a) $\left(\frac{k}{\mathfrak{p}}\right)_6 = \omega$ *or* ω^5.

(b) $\left(\frac{2}{\mathfrak{p}}\right)_6\left(\frac{2}{\mathfrak{q}}\right)_6 = \left(\frac{2}{p}\right)_{\mathbb{Q}}\left(\frac{2}{q}\right)_{\mathbb{Q}}$, *so in particular,* $\left(\frac{2}{\mathfrak{p}}\right)_6\left(\frac{2}{\mathfrak{q}}\right)_6 = \pm 1$.

In (b), $\left(\frac{\cdot}{\cdot}\right)_{\mathbb{Q}}$ *denotes the usual quadratic residue symbol in* $\mathbb{Z}$.)

Proof: (a) If k is a square modulo $\mathfrak{p}$, then $\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ has a nontrivial 3-torsion point, so $\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ cannot be prime. Similarly, if k is a cube modulo $\mathfrak{p}$, then $\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ has a nontrivial 2-torsion point, so again $\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ cannot be prime. Hence

$$\left(\frac{k}{\mathfrak{p}}\right)_6^3 = \left(\frac{k}{\mathfrak{p}}\right)_2 \ne 1 \quad \text{and} \quad \left(\frac{k}{\mathfrak{p}}\right)_6^2 = \left(\frac{k}{\mathfrak{p}}\right)_3 \ne 1.$$

This means that $\left(\frac{k}{\mathfrak{p}}\right)_6$ cannot equal 1, ω^2, ω^3, or ω^4, so it must be either ω or ω^5.

(b) We first note that for any $\alpha, \beta \in \mathcal{O}_K$ with $\gcd(6, \beta) = 1$, we have

$$\left(\frac{\alpha}{\beta}\right)_6^{-1} = \left(\frac{\alpha}{\beta}\right)_6^5 = \left(\frac{\alpha}{\beta}\right)_6^3\left(\frac{\alpha}{\beta}\right)_6^2 = \left(\frac{\alpha}{\beta}\right)_2\left(\frac{\alpha}{\beta}\right)_3. \quad (7\text{–}5)$$

If, in addition, $\alpha \in \mathbb{Z}$, then [Ireland and Rosen 90, Chapter 18, Section 7, Lemma 2] says that $\left(\frac{\alpha}{\beta}\right)_2 = \left(\frac{\alpha}{\mathrm{N}_{K/\mathbb{Q}}(\beta)}\right)_{\mathbb{Q}}$.

In order to prove (b), we use cubic reciprocity [Ireland and Rosen 90, Chapter 9, Section 3]. We recall that an element $\alpha \in \mathcal{O}_K$ is said to be *primary* if $\alpha \equiv 2 \pmod{3\mathcal{O}_K}$. Since $\psi_E(\mathfrak{p})$ is relatively prime to 3, there is a (unique) sixth root of unity $\zeta \in \boldsymbol{\mu}_6$ such that $\zeta\psi_E(\mathfrak{p})$ is primary. It follows from Theorem 7.1(a) that $\zeta^{-1}\big(1-\psi_E(\mathfrak{p})\big)$ is also primary, and of course, the number 2 is primary. Hence cubic reciprocity yields

$$\begin{aligned}
\left(\frac{2}{\mathfrak{p}}\right)_3\left(\frac{2}{\mathfrak{q}}\right)_3 &= \left(\frac{2}{\psi_E(\mathfrak{p})}\right)_3\left(\frac{2}{1-\psi_E(\mathfrak{p})}\right)_3\\
&= \left(\frac{2}{\zeta\psi_E(\mathfrak{p})}\right)_3\left(\frac{2}{\zeta^{-1}(1-\psi_E(\mathfrak{p}))}\right)_3\\
&= \left(\frac{\zeta\psi_E(\mathfrak{p})}{2}\right)_3\left(\frac{\zeta^{-1}(1-\psi_E(\mathfrak{p}))}{2}\right)_3\\
&= \left(\frac{\psi_E(\mathfrak{p})(1-\psi_E(\mathfrak{p}))}{2}\right)_3. \qquad (7\text{–}6)
\end{aligned}$$

The primes $\psi_E(\mathfrak{p})$ and $1-\psi_E(\mathfrak{p})$ are relatively prime to 2, so $\psi_E(\mathfrak{p})$ is congruent to either ω or $1+\omega$ modulo 2. (Note that $\mathcal{O}_K/2\mathcal{O}_K = \{0, 1, \omega, 1+\omega\}$.) Hence

$$\psi_E(\mathfrak{p})\big(1-\psi_E(\mathfrak{p})\big) \equiv \omega(1+\omega) \equiv 1 \pmod{2\mathcal{O}_K}.$$

Substituting into (7–6) shows that $\left(\frac{2}{\mathfrak{p}}\right)_3\left(\frac{2}{\mathfrak{q}}\right)_3 = 1$. Using (7–5) and its accompanying remark, we find that

$$\left(\frac{2}{\mathfrak{p}}\right)_6^{-1}\left(\frac{2}{\mathfrak{q}}\right)_6^{-1} = \left(\frac{2}{\mathfrak{p}}\right)_2\left(\frac{2}{\mathfrak{q}}\right)_2\left(\frac{2}{\mathfrak{p}}\right)_3\left(\frac{2}{\mathfrak{q}}\right)_3 = \left(\frac{2}{p}\right)_{\mathbb{Q}}\left(\frac{2}{q}\right)_{\mathbb{Q}},$$

which completes the proof of (b). □

Corollary 7.6. *Let $E/\mathbb{Q}$, p, and q be as in the statement of Theorem 7.1.*

(a) *There exists an integer A satisfying*

$$A^2 = \frac{2pq + 2p + 2q - p^2 - q^2 - 1}{3}. \qquad (7\text{–}7)$$

(b) *The trace* $a_q(E) = q + 1 - \#\tilde{E}_q(\mathbb{F}_q)$ *equals one of the following six values:*

$$\pm(q+1-p), \quad \frac{\pm(q+1-p) \pm 3A}{2}. \tag{7–8}$$

Remark 7.7. The six possible values of $\#\tilde{E}_q(\mathbb{F}_q)$ described in Corollary 7.6(b) are $\#\tilde{E}_q^{(d)}(\mathbb{F}_q)$ for the sextic twists of $\tilde{E}_q$ corresponding to the elements of $H^1\big(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}(\tilde{E}_q)\big) \cong H^1\big(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \boldsymbol{\mu}_6\big) \cong \mathbb{F}_q^*/(\mathbb{F}_q^*)^6$.

Remark 7.8. Using Corollary 7.6 and a case-by-case analysis, we will prove in Section 8 that $j = 0$ elliptic curves have no aliquot cycles of length three.

Proof: (a) We know that $\mathrm{Tr}\big(\psi_E(\mathfrak{p})\big) = a_p(E)$, so writing $\psi_E(\mathfrak{p})$ as an element of $\mathcal{O}_K = \mathbb{Z}[\omega]$, it has the form

$$\psi_E(\mathfrak{p}) = \frac{a_p(E) + A\sqrt{-3}}{2} \quad \text{for some } A \in \mathbb{Z}. \tag{7–9}$$

Since we also know that $\mathrm{N}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{p})\big) = p$, we find that

$$\frac{a_p(E)^2 + 3A^2}{4} = p. \tag{7–10}$$

Finally, the assumption $\#\tilde{E}_p(\mathbb{F}_p) = q$ is equivalent to $a_p(E) = p + 1 - q$. We substitute this value into (7–10), and then a little bit of algebra shows that A has the form specified by (7–7).

(b) Applying (7–1) from Theorem 7.1, we find that

$$\mathrm{Tr}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{q})\big) = \mathrm{Tr}_{K/\mathbb{Q}}\big(\zeta(1 - \psi_E(\mathfrak{p}))\big)$$

for some $\zeta \in \boldsymbol{\mu}_6$. Using the value of $\psi_E(\mathfrak{p})$ from (7–9) with the substitution $a_p(E) = p + 1 - q$ yields

$$\mathrm{Tr}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{q})\big) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\zeta\left(\frac{q+1-p-A\sqrt{-3}}{2}\right)\right).$$

Substituting in each of the six possible values $\zeta \in \boldsymbol{\mu}_6$ and taking the trace yields the six values listed in (7–8). □

Definition 7.9. Fix a nonzero integer k and let E be the curve $E : y^2 = x^3 + k$. We let $\mathcal{N}_k$ denote the set

$$\mathcal{N}_k = \left\{ \begin{array}{c} \text{primes } p \geq 5 \text{ of good reduction for} \\ E \text{ such that } q = \#\tilde{E}_p(\mathbb{F}_p) \text{ is also} \\ \text{a prime of good reduction for } E \end{array} \right\}.$$

(This differs slightly from our earlier notation in that we are now excluding a few primes, but this does not affect our asymptotic formulas.) We define a subset of $\mathcal{N}_k$ by

$$\mathcal{N}_k^{[1]} = \big\{p \in \mathcal{N}_k : a_q(E) = \pm(q+1-p)\big\},$$

and we say that the primes in $\mathcal{N}_k^{[1]}$ are of type 1 for E. We write $\mathcal{N}_k(X)$ for the number of primes in $\mathcal{N}_k$ that are less than X, and similarly for $\mathcal{N}_k^{[1]}(X)$.

Only type-1 primes can be amicable, and based on experiments, we expect that about half of the type-1 primes will be part of an amicable pair. Let

$$\mathcal{Q}_k(X) = \# \left\{ \begin{array}{c} p < X : p < q \text{ and } (p,q) \\ \text{is an amicable pair for } E \end{array} \right\},$$

i.e., $\mathcal{Q}_k(X)$ is the number of normalized amicable pairs (p, q) on E with $p < X$. Then we have the following conjecture, where the conjectured limit is $\frac{1}{4}$, rather than $\frac{1}{2}$, because $\mathcal{Q}_k(X)$ counts amicable pairs (p, q) with $p < q$, while $\mathcal{N}_k^{[1]}(X)$ counts both (p, q) and (q, p).

Conjecture 7.10. *With notation as above, the proportion of type-1 primes that are part of a normalized amicable pair is given by*

$$\lim_{X\to\infty} \frac{\mathcal{Q}_k(X)}{\mathcal{N}_k^{[1]}(X)} = \frac{1}{4}.$$

Thus in order to understand the distribution of amicable pairs on E, we need to study the density of the type-1 primes in $\mathcal{N}_k$.

Remark 7.11. According to Corollary 7.6, there are six possible values for $a_q(E)$, two of which give type-1 primes, so one might expect $\mathcal{N}_k^{[1]}$ to have density $\frac{1}{3}$ inside $\mathcal{N}_k$. This turns out not to be the case. At the extreme end, Corollary 7.4 says that $\mathcal{N}_{2d^3}^{[1]} = \mathcal{N}_{2d^3}$ for any nonzero $d \in \mathbb{Z}$. The rest of this section is devoted to developing tools for calculating a conjectural value for $\lim_{X\to\infty} \mathcal{N}_k^{[1]}(X)/\mathcal{N}_k(X)$. This value depends on k in quite a complicated way; see Conjecture 7.14. For precise formulas when k is prime, see Conjecture 7.24, which says that the limit should equal $\frac{1}{3} + R(k)$, where $R(k)$ is a rational function of k that depends on k modulo 36.

Definition 7.12. We set the notation

$$n \overset{\mathrm{pr}}{\equiv} a \pmod{m} \iff p \equiv a \pmod{m}$$
$$\text{for every prime } p \mid n.$$

Further, for any ideal $\mathfrak{K} \subset \mathcal{O}_K$, we define

$$\mathcal{O}_{K,\mathfrak{K}}^\sharp = \left\{\lambda \in \frac{\mathcal{O}_K}{\mathfrak{K}} : \gcd\big(\lambda(1-\lambda), \mathfrak{K}\big) = 1\right\}.$$

If $\mathfrak{K} = k\mathcal{O}_K$ is principal, we write simply $\mathcal{O}_{K,k}^\sharp$.

Now let $k \in \mathbb{Z}$ satisfy $\gcd(6,k)=1$. We define a set M_k that depends on k modulo 4 and on the primes dividing k modulo 9. The definition for the four cases is as follows:

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

$$M_k = \left\{ \lambda \in \mathcal{O}_{K,k}^\sharp : \left(\frac{\lambda}{k}\right)_2 = -1 \text{ and } \left(\frac{\lambda}{k}\right)_3 \neq 1 \right\}.$$

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

$$M_k = \left\{ \lambda \in \mathcal{O}_{K,k}^\sharp : \left(\frac{\lambda}{k}\right)_2 = -1 \right\}.$$

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

$$M_k = \left\{ \lambda \in \mathcal{O}_{K,k}^\sharp : \left(\frac{\lambda}{k}\right)_3 \neq 1 \right\}.$$

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

$$M_k = \mathcal{O}_{K,k}^\sharp.$$

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

$$M_k^{[1]} = \left\{ \lambda \in M_k : \left(\frac{\lambda(1-\lambda)}{k}\right)_3 = 1 \right\}.$$

Remark 7.13. It is easy to check that $k \overset{\text{pr}}{\equiv} \pm 1 \pmod 9$ if and only if every cube root of unity in $\mathcal{O}_K/k\mathcal{O}_K$ is itself a cube. For example, suppose that $k \in \mathbb{Z}$ is prime. If $k \equiv -1 \pmod 9$, then $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_{k^2}$ is a finite field with k^2 elements, and $\boldsymbol{\mu}_9 \subset \mathbb{F}_{k^2}$. Similarly, if $k \equiv 1 \pmod 9$, then $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_k \times \mathbb{F}_k$, and $\boldsymbol{\mu}_9 \subset \mathbb{F}_k$. Thus in both cases, every cube root of unity in $\mathcal{O}_K/k\mathcal{O}_K$ is itself a cube.

Conjecture 7.14. *Let $k \in \mathbb{Z}$ be an integer satisfying $\gcd(6,k)=1$. Then*

$$\lim_{X\to\infty} \frac{\mathcal{N}_k^{[1]}(X)}{\mathcal{N}_k(X)} = \frac{\#\mathcal{M}_k^{[1]}}{\#\mathcal{M}_k}. \tag{7–11}$$

Remark 7.15. For small values of k, it is not difficult to compute the sets $\mathcal{M}_k$ and $\mathcal{M}_k^{[1]}$, thereby obtaining an explicit (conjectural) value for the limit (7–11). Table 1 gives some examples corresponding to the four cases (a)–(d) used to define $\mathcal{M}_k$, further divided according to the value of k modulo 3. (The notation (x.n) after each value of k indicates the case x = (a), ..., (d) and the congruence class $k \equiv n \pmod 3$.)

Our justification for Conjecture 7.14 uses the following weak form of quadratic and cubic reciprocity for the field $\mathbb{Q}(\omega)$.

k	$\#\mathcal{O}_{K,k}^\sharp$	$\#M_k$	$\#M_k^{[1]}$	$\#M_k^{[1]}/\#M_k$
37 (a.1)	1225	408	144	$\frac{6}{17} = 0.3529$
17 (a.2)	287	96	36	$\frac{3}{8} = 0.3750$
13 (b.1)	121	60	20	$\frac{1}{3} = 0.3333$
5 (b.2)	23	12	4	$\frac{1}{3} = 0.3333$
19 (c.1)	289	192	72	$\frac{3}{8} = 0.3750$
71 (c.2)	5039	3360	1152	$\frac{12}{35} = 0.3429$
7 (d.1)	25	25	13	$\frac{13}{25} = 0.5200$
11 (d.2)	119	119	47	$\frac{47}{119} = 0.3950$

TABLE 1. The sets $\mathcal{O}_{K,k}^\sharp$, M_k, and $M_k^{[1]}$.

Lemma 7.16. *Let $k \in \mathbb{Z}$ satisfy $\gcd(k,6)=1$, and let $\lambda \in \mathbb{Z}[\omega]$ satisfy $\gcd(6k,\lambda)=1$. Then:*

(a) (Quadratic reciprocity in $\mathbb{Q}(\omega)$.)

$$\left(\frac{k}{\lambda}\right)_2 = (-1)^{\frac{\mathrm{N}(\lambda)-1}{2}\cdot\frac{k-1}{2}} \left(\frac{\lambda}{k}\right)_2.$$

(b) (Cubic reciprocity in $\mathbb{Q}(\omega)$.) *Let $\zeta \in \boldsymbol{\mu}_3$ be the unique cube root of unity such that*

$$\zeta\lambda \equiv \pm 1 \pmod{3\mathcal{O}_K}.$$

Then

$$\left(\frac{k}{\lambda}\right)_3 = \left(\frac{\zeta}{k}\right)_3 \left(\frac{\lambda}{k}\right)_3.$$

Proof: Let $\alpha, \beta \in \mathbb{Z}[\omega]$ satisfy $\gcd(\alpha,\beta) = \gcd(\alpha\beta, 6) = 1$. We start with the sextic reciprocity law for $\mathbb{Q}(\omega)$ as stated in [Lemmermeyer 00, Theorem 7.10]. This says that if α and β are "E-primary" (see [Lemmermeyer 00] for terminology), then

$$\left(\frac{\alpha}{\beta}\right)_6 \left(\frac{\beta}{\alpha}\right)_6^{-1} = (-1)^{\frac{\mathrm{N}(\alpha)-1}{2}\cdot\frac{\mathrm{N}(\beta)-1}{2}}. \tag{7–12}$$

Let $\rho = \omega^2$ denote a primitive cube root of unity. Then for $\alpha \in \mathcal{O}_K$ satisfying $\gcd(6,\alpha)=1$, we have by definition

$$\alpha \text{ is } E\text{-primary} \Longleftrightarrow \alpha \equiv \pm 1 \pmod 3 \text{ and } \alpha^3 = A + B\rho \text{ with } A + B \equiv 1 \pmod 4.$$

(This is a corrected version of [Lemmermeyer 00, Lemma 7.9], which omits the $\alpha \equiv \pm 1 \pmod 3$ condition and includes a superfluous $3 \mid B$ requirement.)

We note that if $\alpha \equiv \pm 1 \pmod 3$, then exactly one of $\pm\alpha$ is E-primary.

We now consider $k \in \mathbb{Z}$ and $\lambda \in \mathcal{O}_K$ as in the statement of the lemma. Since k is an integer and satisfies $\gcd(6,k)=1$, we have

$$\begin{aligned} k \text{ is } E\text{-primary} &\iff k \equiv \pm 1 \pmod 3 \text{ and} \\ &\qquad k^3 \equiv 1 \pmod 4 \\ &\iff k \equiv 1 \pmod 4, \end{aligned}$$

so $(-1)^{(k-1)/2}k$ is E-primary. We also note that for any $\alpha \in \mathcal{O}_K$ satisfying $\gcd(6,\alpha)=1$, Euler's formula says that

$$\left(\frac{-1}{\alpha}\right)_6 \equiv (-1)^{(\mathrm{N}(\alpha)-1)/6} \pmod{\alpha\mathcal{O}_K}, \tag{7–13}$$

and since both sides of (7–13) are sixth roots of unity, the congruence (7–13) is an equality. In particular,

$$\left(\frac{-1}{k}\right)_6 = (-1)^{(\mathrm{N}(k)-1)/6} = (-1)^{(k^2-1)/6} = 1. \tag{7–14}$$

It is an easy exercise to verify that there is a unique $\zeta \in \boldsymbol{\mu}_3$ such that $\zeta\lambda \equiv \pm 1 \pmod 3$; cf. [Ireland and Rosen 90, Proposition 9.3.5].

Then one of $\pm\zeta\lambda$ is E-primary, so we can apply (7–12) to the E-primary numbers $\alpha = (-1)^{(k-1)/2}k$ and $\beta = \pm\zeta\lambda$. Then (7–12) becomes

$$\left(\frac{(-1)^{(k-1)/2}k}{\lambda}\right)_6 \left(\frac{\pm\zeta\lambda}{k}\right)_6^{-1} = (-1)^{\frac{k^2-1}{2}\cdot\frac{\mathrm{N}(\lambda)-1}{2}} = 1.$$

(The second equality comes from the fact that $k^2 \equiv 1 \pmod 4$.) Hence

$$\left(\frac{-1}{\lambda}\right)_6^{(k-1)/2} \left(\frac{k}{\lambda}\right)_6 \left(\frac{\pm 1}{k}\right)_6^{-1} \left(\frac{\zeta}{k}\right)_6^{-1} \left(\frac{\lambda}{k}\right)_6^{-1} = 1.$$

Using (7–13) and (7–14) gives

$$\left(\frac{k}{\lambda}\right)_6 = (-1)^{\frac{\mathrm{N}(\lambda)-1}{2}\cdot\frac{k-1}{2}} \left(\frac{\zeta}{k}\right)_6 \left(\frac{\lambda}{k}\right)_6. \tag{7–15}$$

(We note in particular that the sign used to ensure that $\zeta\lambda$ is E-primary turns out to be irrelevant because $\left(\frac{-1}{k}\right)_6 = 1$.) Cubing (7–15) and using $\zeta^3 = 1$ gives the quadratic reciprocity formula in (a), and similarly, squaring (7–15) gives the cubic reciprocity formula in (b). □

Justification for Conjecture 7.14: Let $p \in \mathcal{N}_k$, so Theorem 7.1(a) tells us that p splits in $\mathcal{O}_K$, say $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. As in that theorem, we let $\mathfrak{q} = \big(1-\psi_E(\mathfrak{p})\big)\mathcal{O}_K$. Then squaring Theorem 7.1(d) yields

$$p \in \mathcal{N}_k^{[1]} \iff \left(\frac{4k}{\mathfrak{p}}\right)_3 \left(\frac{4k}{\mathfrak{q}}\right)_3 = 1.$$

Further, Proposition 7.5 implies that $\left(\frac{2}{\mathfrak{p}}\right)_3 \left(\frac{2}{\mathfrak{q}}\right)_3 = 1$, so we find that

$$p \in \mathcal{N}_k^{[1]} \iff \left(\frac{k}{\mathfrak{p}}\right)_3 \left(\frac{k}{\mathfrak{q}}\right)_3 = 1.$$

The (prime) ideals $\mathfrak{p}$ and $\mathfrak{q}$ are generated, respectively, by the elements $\psi_E(\mathfrak{p})$ and $1-\psi_E(\mathfrak{p})$, and Theorem 7.1(a) says that these elements satisfy

$$\psi_E(\mathfrak{p})\big(1-\psi_E(\mathfrak{p})\big) \equiv 1 \pmod{3\mathcal{O}_K}. \tag{7–16}$$

Hence if we choose $\xi \in \boldsymbol{\mu}_6$ to satisfy

$$\xi\psi_E(\mathfrak{p}) \equiv \pm 1 \pmod{3\mathcal{O}_K},$$

then (7–16) says that we also have

$$\xi^{-1}\big(1-\psi_E(\mathfrak{p})\big) \equiv \pm 1 \pmod{3\mathcal{O}_K}.$$

This allows us to apply cubic reciprocity (Lemma 7.16(b), or [Ireland and Rosen 90, Chapter 9, Section 3, Theorem 1]) to compute

$$\begin{aligned} \left(\frac{k}{\mathfrak{p}}\right)_3 \left(\frac{k}{\mathfrak{q}}\right)_3 &= \left(\frac{k}{\xi\psi_E(\mathfrak{p})\mathcal{O}_K}\right)_3 \left(\frac{k}{\xi^{-1}(1-\psi_E(\mathfrak{p}))\mathcal{O}_K}\right)_3 \\ &= \left(\frac{\xi\psi_E(\mathfrak{p})}{k\mathcal{O}_K}\right)_3 \left(\frac{\xi^{-1}(1-\psi_E(\mathfrak{p}))}{k\mathcal{O}_K}\right)_3 \\ &= \left(\frac{\psi_E(\mathfrak{p})}{k\mathcal{O}_K}\right)_3 \left(\frac{1-\psi_E(\mathfrak{p})}{k\mathcal{O}_K}\right)_3. \end{aligned}$$

Hence

$$p \in \mathcal{N}_k^{[1]} \iff \left(\frac{\psi_E(\mathfrak{p})\big(1-\psi_E(\mathfrak{p})\big)}{k\mathcal{O}_K}\right)_3 = 1. \tag{7–17}$$

We now consider how the values $\psi_E(\mathfrak{p})$ are distributed in $\mathcal{O}_K/k\mathcal{O}_K$ as p varies in $\mathcal{N}_k$. If p were chosen completely randomly, subject only to $p \equiv 1 \pmod 3$, then we might expect the values of $\psi_E(\mathfrak{p})$ to be uniformly distributed among the congruence classes in $\mathcal{O}_K/k\mathcal{O}_K$. However, Proposition 7.6(a) tells us that $\left(\frac{k}{\mathfrak{p}}\right)_6$ equals either ω or ω^5, i.e., it is a primitive sixth root of unity. Equivalently,

$$\left(\frac{k}{\mathfrak{p}}\right)_2 = -1 \quad \text{and} \quad \left(\frac{k}{\mathfrak{p}}\right)_3 = \omega^2 \text{ or } \omega^4, \tag{7–18}$$

i.e., neither $\left(\frac{k}{\mathfrak{p}}\right)_2$ nor $\left(\frac{k}{\mathfrak{p}}\right)_3$ equals 1. This gives a constraint on the values of $\psi_E(\mathfrak{p})$ for $p \in \mathcal{N}_k$. Discarding finitely many elements of $\mathcal{N}_k$, we may assume that $p \nmid 6k$, and then reciprocity (Lemma 7.16) tells us that

$$\left(\frac{k}{\mathfrak{p}}\right)_2 = (-1)^{\frac{p-1}{2}\cdot\frac{k-1}{2}} \left(\frac{\psi_E(\mathfrak{p})}{k}\right)_2$$

and

$$\left(\frac{k}{\mathfrak{p}}\right)_3 = \left(\frac{\zeta}{k}\right)_3 \left(\frac{\psi_E(\mathfrak{p})}{k}\right)_3,$$

where $\zeta \in \boldsymbol{\mu}_3$ satisfies $\zeta\psi_E(\mathfrak{p}) \equiv \pm 1 \pmod 3$. (Note that $\mathrm{N}\big(\psi_E(\mathfrak{p})\big) = p$.) Hence the constraints (7–18) on $\psi_E(\mathfrak{p})$ from Proposition 7.6(a) become

$$\left(\frac{\psi_E(\mathfrak{p})}{k}\right)_2 = -(-1)^{\frac{p-1}{2}\cdot\frac{k-1}{2}}, \tag{7–19}$$

$$\left(\frac{\zeta}{k}\right)_3 \left(\frac{\psi_E(\mathfrak{p})}{k}\right)_3 = \omega^2 \text{ or } \omega^4.$$

We now make the following two assumptions, which are supported by experiments:

(i) For $p \in \mathcal{N}_k$, the value of $p \bmod 4$ is equally likely to be 1 or 3.

(ii) For $p \in \mathcal{N}_k$, the value of ζ in (7–19) is equally likely to be 1, ω^2, or ω^4.

These assumptions have the following consequences:

1. If $k \equiv 3 \pmod 4$, then the first equation in (7–19) has no effect on the value of $\psi_E(\mathfrak{p}) \bmod k$.
2. If $k \overset{\text{pr}}{\not\equiv} \pm 1 \pmod 9$, i.e., if cube roots of unity in $\mathcal{O}_K/k\mathcal{O}_K$ are not necessarily cubes, then the second equation in (7–19) has no effect on the value of $\psi_E(\mathfrak{p}) \bmod k$.

On the other hand, if $k \equiv 1 \pmod 4$, then the first equation in (7–19) gives the constraint $\left(\frac{\psi_E(\mathfrak{p})}{k}\right)_2 = -1$; and similarly, if $k \overset{\text{pr}}{\equiv} \pm 1 \pmod 9$, then the second equation in (7–19) imposes the condition $\left(\frac{\psi_E(\mathfrak{p})}{k}\right)_3 \neq 1$.

Thus considering the four cases, we see that $\psi_E(\mathfrak{p})$ is in the set M_k. Further, we note that (7–17) says that $p \in \mathcal{N}_k^{[1]}$ if and only if $\psi_E(\mathfrak{p}) \in \mathcal{M}_k^{[1]}$. Hence it is reasonable to conjecture that the density of $\mathcal{N}_k^{[1]}$ in $\mathcal{N}_k$ is given by the ratio $\#\mathcal{M}_k^{[1]}/\#\mathcal{M}_k$. □

Conjecture 7.14 is reasonably satisfactory in that the sets $\mathcal{M}_k$ and $\mathcal{M}_k^{[1]}$ are easy to compute for any particular (not-too-large) value of k. In the remainder of this section we derive explicit formulas for $\#\mathcal{M}_k$ and $\#\mathcal{M}_k^{[1]}$ when k is prime. We do this by breaking them up into subsets of the following sort. For any ideal $\mathfrak{K} \subset \mathcal{O}_K$ and any roots of unity $\zeta \in \boldsymbol{\mu}_6$ and $\xi \in \boldsymbol{\mu}_3$, we define

$$\begin{aligned} M_{\mathfrak{K}}(\zeta) &= \left\{\lambda \in \mathcal{O}_{K,\mathfrak{K}}^{\sharp} : \left(\frac{\lambda}{\mathfrak{K}}\right)_6 = \zeta\right\} \\ &= \left\{\lambda \in \mathcal{O}_{K,\mathfrak{K}}^{\sharp} : \left(\frac{\lambda}{\mathfrak{K}}\right)_2 = \zeta^3 \text{ and } \left(\frac{\lambda}{\mathfrak{K}}\right)_3 = \zeta^2\right\}, \\ M_{\mathfrak{K}}^{[1]}(\zeta,\xi) &= \left\{\lambda \in M_{\mathfrak{K}}(\zeta) : \left(\frac{\lambda(1-\lambda)}{\mathfrak{K}}\right)_3 = \xi\right\}. \end{aligned}$$

As before, if $\mathfrak{K} = k\mathcal{O}_K$ is principal, we write $M_k(\zeta)$ and $M_k^{[1]}(\zeta,\xi)$. Further, if $S \subset \boldsymbol{\mu}_6$ is any set of roots of unity, we write $M_{\mathfrak{K}}(S)$ for the union of $M_{\mathfrak{K}}(\zeta)$ with $\zeta \in S$. With this notation, the four cases defining M_k are given by

(a) $M_k = M_k\big(\{\omega, \omega^5\}\big)$,

(b) $M_k = M_k\big(\{\omega, \omega^3, \omega^5\}\big)$,

(c) $M_k = M_k\big(\{\omega, \omega^2, \omega^4, \omega^5\}\big)$,

(d) $M_k = M_k(\boldsymbol{\mu}_6)$,

and in all cases, $M_k^{[1]} = M_k^{[1]}(S,1)$, where $S \subset \boldsymbol{\mu}_6$ is the set for the appropriate case.

We now restrict attention to the case that $k \in \mathbb{Z}$ is a rational *prime* with $\gcd(6,k) = 1$. If $k \equiv 2 \pmod 3$, so k is inert in K, then the computation of M_k and $M_k^{[1]}$ takes place in the field $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_{k^2}$ with k^2 elements. On the other hand, if $k \equiv 1 \pmod 3$, so k splits as $k\mathcal{O}_K = \mathfrak{K}\bar{\mathfrak{K}}$, then

$$\frac{\mathcal{O}_K}{k\mathcal{O}_K} \cong \frac{\mathcal{O}_K}{\mathfrak{K}} \times \frac{\mathcal{O}_K}{\bar{\mathfrak{K}}} \cong \mathbb{F}_k \times \mathbb{F}_k.$$

In this case, a condition such as $\left(\frac{\lambda}{k}\right)_3 \neq 1$ becomes more complicated, since there are many ways for the product $\left(\frac{\lambda}{\mathfrak{K}}\right)_3 \left(\frac{\lambda}{\bar{\mathfrak{K}}}\right)_3$ to be different from 1.

Proposition 7.17. *Let $k \geq 5$ be a rational prime. The following table gives the values of $\#M_k(S)$ for various subsets $S \subset \boldsymbol{\mu}_6$, divided into cases according to whether k is split or inert in $K = \mathbb{Q}(\sqrt{-3}\,)$:*

		$k \equiv 1 \pmod 3$	$k \equiv 2 \pmod 3$
(a)	$\#M_k\big(\{\omega,\omega^5\}\big)$	$\frac{1}{3}(k-1)(k-3)$	$\frac{1}{3}(k^2-1)$
(b)	$\#M_k\big(\{\omega,\omega^3,\omega^5\}\big)$	$\frac{1}{2}(k-1)(k-3)$	$\frac{1}{2}(k^2-1)$
(c)	$\#M_k\big(\{\omega,\omega^2,\omega^4,\omega^5\}\big)$	$\frac{2}{3}(k-1)(k-3)$	$\frac{2}{3}(k^2-1)$
(d)	$\#M_k(\boldsymbol{\mu}_6)$	$(k-2)^2$	k^2-2

Proof: Suppose first that k is inert, so $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_{k^2}$. Then $\#M_k(\boldsymbol{\mu}_6)$ simply counts the $\lambda \in \mathbb{F}_{k^2}$ such that λ and $1-\lambda$ are units, so is equal to k^2-2. Next, $\#M_k\big(\{\omega,\omega^3,\omega^5\}\big)$ counts the quadratic nonresidues in $\mathbb{F}_{k^2}$, of which there are $\frac{1}{2}(k^2-1)$. (Here the condition that $1-\lambda$ be a unit is irrelevant, since 1 is a quadratic residue.) Similarly, $\#M_k\big(\{\omega,\omega^2,\omega^4,\omega^5\}\big)$ counts cubic nonresidues in $\mathbb{F}_{k^2}$, of which there are $\frac{2}{3}(k^2-1)$. Finally, $\#M_k\big(\{\omega,\omega^5\}\big)$ counts the elements that are neither quadratic nor cubic residues, of which there are $\frac{1}{3}(k^2-1)$.

Next suppose that k splits, so $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_k \times \mathbb{F}_k$. Then $\#M_k(\boldsymbol{\mu}_6)$ counts $(a,b) \in \mathbb{F}_k^2$ with neither a nor b equal to 0 or 1. This gives $k-2$ possibilities for each of a and b, so $\#M_k(\boldsymbol{\mu}_6) = (k-2)^2$.

The required calculations for each of the remaining cases have much in common, so we will illustrate

only the case of $M_k\big(\{\omega,\omega^3,\omega^5\}\big)$. Exactly $\frac{1}{2}$ of invertible (a,b) are quadratic nonresidues. Therefore, there are $\frac{1}{2}(k-1)^2$ such elements. Of these, there are $\frac{1}{2}(k-1)$ of the form $(1,b)$ and $\frac{1}{2}(k-1)$ of the form $(a,1)$. The set $M_k\big(\{\omega,\omega^3,\omega^5\}\big)$ counts invertible (a,b) that are quadratic nonresidues having $a\neq 1$ and $b\neq 1$. Therefore

$$\begin{aligned}\#M_k\big(\{\omega,\omega^3,\omega^5\}\big) &= \frac{1}{2}(k-1)^2 - 2\left(\frac{1}{2}(k-1)\right)\\ &= \frac{1}{2}(k-1)(k-3).\end{aligned}$$

(Note that $(1,1)$ is a quadratic residue, so the invertible nonresidues of the form $(a,1)$ and $(1,b)$ are disjoint.) A similar argument applies to the two remaining cases, where we rely on the fact that invertible elements of $\mathbb{F}_k\times\mathbb{F}_k$ and of $\mathbb{F}_k$ fall evenly into the six sextic residue classes. □

The table in Proposition 7.17 gives the value of $\#M_k(S)$ for the four subsets $S\subset\boldsymbol{\mu}_6$ that appear in Conjecture 7.14. It remains to construct a similar table for the values of $\#M_k^{[1]}(S)$. It turns out that these values can be expressed in terms of the number of points on a certain curve of genus four over various finite fields. We begin with a description of the curve that we need, after which we count points in order to compute the desired values.

Proposition 7.18. *Let $\mathbb{F}$ be a perfect field of characteristic not equal to 2 or 3. For $\kappa\in\mathbb{F}^*$ we define $E^{(\kappa)}$ to be the elliptic curve*

$$E^{(\kappa)}: y^2 = x^3+\kappa,$$

and for $\gamma,\delta\in\mathbb{F}^*$, we define $C_6^{(\gamma,\delta)}$ to be a smooth projective model for the algebraic curve given by the affine equation

$$C_6^{(\gamma,\delta)}: \gamma z^6(1-\gamma z^6) = \delta x^3.$$

Then:

(a) *The curve $C_6^{(\gamma,\delta)}$ has genus four.*

(b) *There are finite maps from $C_6^{(\gamma,\delta)}$ to curves of the form $E^{(\kappa)}$ given by the following formulas*:

$$\begin{aligned}
&C_6^{(\gamma,\delta)}\to E^{(16\delta^2)},\ \ (x,z)\mapsto(-4\delta x, 8\gamma\delta z^6-4\delta),\\
&C_6^{(\gamma,\delta)}\to E^{(4\gamma^3\delta^4)},\ \ (x,z)\mapsto\left(\frac{\delta^2x^2}{z^6},\gamma^2\delta^2z^3+\frac{\gamma\delta^2}{z^3}\right),\\
&C_6^{(\gamma,\delta)}\to E^{(\gamma^5\delta^2)},\ \ (x,z)\mapsto\left(\frac{\gamma\delta x}{z^4},\frac{\gamma^2\delta}{z^3}\right),\\
&C_6^{(\gamma,\delta)}\to E^{(-\gamma\delta^2)},\ \ (x,z)\mapsto\left(-\frac{\delta x}{z^2},\gamma\delta z^3\right).
\end{aligned}$$

(c) *The maps in* (b) *are independent; hence they induce an isogeny*

$$E^{(16\delta^2)}\times E^{(4\gamma^3\delta^4)}\times E^{(\gamma^5\delta^2)}\times E^{(-\gamma\delta^2)}\longrightarrow J_6^{(\gamma,\delta)}\ \stackrel{\text{def}}{=}\ \mathrm{Jac}(C_6^{(\gamma,\delta)}).$$

(d) *For any prime ℓ different from the characteristic of $\mathbb{F}$, we have isomorphisms of $\mathrm{Gal}(\bar{\mathbb{F}}/\mathbb{F})$-modules,*

$$\begin{aligned}
&H^1_{\text{ét}}\big(C^{(\gamma,\delta)}_{6/\mathbb{F}},\mathbb{Q}_\ell\big)\\
&\quad\cong H^1_{\text{ét}}\big(J^{(\gamma,\delta)}_{6/\mathbb{F}},\mathbb{Q}_\ell\big)\\
&\quad\cong H^1_{\text{ét}}\big(E^{(16\delta^2)}_{/\mathbb{F}},\mathbb{Q}_\ell\big)\times H^1_{\text{ét}}\big(E^{(4\gamma^3\delta^4)}_{/\mathbb{F}},\mathbb{Q}_\ell\big)\\
&\qquad\times H^1_{\text{ét}}\big(E^{(\gamma^5\delta^2)}_{/\mathbb{F}},\mathbb{Q}_\ell\big)\times H^1_{\text{ét}}\big(E^{(-\gamma\delta^2)}_{/\mathbb{F}},\mathbb{Q}_\ell\big).
\end{aligned}$$

Proof: (a) All of the $C_6^{(\gamma,\delta)}$ curves are geometrically isomorphic, so it suffices to calculate the genus of $C_6^{(1,1)}$, which for convenience we denote by C_6. A simple calculation shows that the projective closure of C_6 in $\mathbb{P}^2$ is singular at $(0,0)$ and at the point at infinity, and that each of these singular points resolves to three points on the smooth model. (See Proposition 7.19 for details.) We let C_1 be the elliptic curve

$$C_1: z(1-z)=x^3,$$

and we consider the natural degree-6 map

$$\psi: C_6\longrightarrow C_1,\quad (x,z)\longmapsto(x,z^6).$$

The map ψ is ramified only at $(0,0)$ and ∞, the sets $\psi^{-1}(0,0)$ and $\psi^{-1}(\infty)$ each consist of three points, and each of these points has ramification index 2. Applying the Riemann–Hurwitz genus formula to ψ gives

$$\begin{aligned}2g(C_6)-2 &= 6\big(2g(C_1)-2\big)+\sum_{P\in C_1}\big(e_P(\psi)-1\big)\\ &= 6(2-2)+6(2-1)=6.\end{aligned}$$

Hence $g(C_6)=4$.

(b) It is an exercise to verify that the given maps are well defined, but we briefly comment on their origin. The automorphism group of the curve $C_6^{(\gamma,\delta)}$ is fairly large, since

$$\boldsymbol{\mu}_3\times\boldsymbol{\mu}_6\subset\mathrm{Aut}(C_6^{(\gamma,\delta)}),\quad [\zeta,\xi](x,z)=(\zeta x,\xi z).$$

Taking quotients of $C_6^{(\gamma,\delta)}$ by various subgroups of $\boldsymbol{\mu}_3\times\boldsymbol{\mu}_6$ gives maps to curves of lower genus, which in turn give the four maps described in (b).

(c) From general principles, the maps in (b) induce isogenies $E^{(\kappa)}\to J_6^{(\gamma,\delta)}$ for the given values of κ. There are various ways to see that these isogenies are independent. For example, one can use the fact that the

four $E^{(\kappa)}$ are nonisogenous over $\mathbb{C}(\gamma,\delta)$, treating γ and δ as indeterminates. Alternatively, at least in characteristic 0, one can take $\gamma=\delta=1$, untwist to get four maps $C_6^{(1,1)}\to E^{(1)}$ defined over $\bar{\mathbb{Q}}$, and use the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the maps to show that they are independent. Or for a purely geometric proof, one can use intersection theory and the fact that the pairing

$$\begin{aligned}&\langle\,\cdot\,,\,\cdot\,\rangle : \mathrm{Map}(C_6^{(1,1)},E^{(1)})/E^{(1)}\to\mathbb{Z},\\ &\langle\phi,\psi\rangle=\deg(\phi+\psi)-\deg\phi-\deg\psi,\end{aligned}$$

is a positive definite quadratic form. (The $E^{(1)}$ in the denominator is shorthand for the right action of the group of translations.) We sketch the characteristic-zero Galois-theoretic proof, so we assume that $\mathrm{char}(\mathbb{F})=0$.

Independence of maps is geometric, so it suffices to prove independence for $\gamma=\delta=1$. Let $\psi_1,\dots,\psi_4$ be the four maps in (b), so

$$\begin{aligned}&\psi_1 : C_6^{(1,1)}\longrightarrow E^{(16)}, \qquad \psi_2 : C_6^{(1,1)}\longrightarrow E^{(4)},\\ &\psi_3 : C_6^{(1,1)}\longrightarrow E^{(1)}, \qquad \psi_4 : C_6^{(1,1)}\longrightarrow E^{(-1)}.\end{aligned}$$

We compose these maps with untwisting maps $E^{(\kappa)}\to E^{(1)}$, so we get four maps

$$\begin{aligned}\phi_1 : C_6^{(1,1)} &\xrightarrow{\psi_1} E^{(16)} \xrightarrow{(x,y)\to\left(\frac{1}{2\sqrt[3]{2}}x,\frac{1}{4}y\right)} E^{(1)},\\ \phi_2 : C_6^{(1,1)} &\xrightarrow{\psi_2} E^{(4)} \xrightarrow{(x,y)\to\left(\frac{1}{\sqrt[3]{4}}x,\frac{1}{2}y\right)} E^{(1)},\\ \phi_3 : C_6^{(1,1)} &\xrightarrow{\psi_3} E^{(1)} \xrightarrow{(x,y)\to(x,y)} E^{(1)},\\ \phi_4 : C_6^{(1,1)} &\xrightarrow{\psi_4} E^{(-1)} \xrightarrow{(x,y)\to(-x,iy)} E^{(1)}.\end{aligned}$$

The maps $\psi_1,\dots,\psi_4$ are defined over $\mathbb{Q}$, but the maps $\phi_1,\dots,\phi_4$ are defined only over $\bar{\mathbb{Q}}$, not $\mathbb{Q}$. We consider the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on these maps. To do this, we choose elements $\sigma,\tau\in\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ satisfying

$$\begin{aligned}&\sigma(\sqrt[3]{2})=\rho\sqrt[3]{2}, \quad \sigma(i)=i,\\ &\tau(\sqrt[3]{2})=\sqrt[3]{2}, \quad \tau(i)=-i.\end{aligned}$$

Here $\rho=\frac{1}{2}(-1+\sqrt{-3})$ is a fixed primitive cube root of unity. We also note that $\boldsymbol{\mu}_3$ acts on $E^{(1)}$ via $[\rho](x,y)=(\rho x,y)$. Looking at the explicit formulas for $\phi_1,\dots,\phi_4$, we find that

$$\begin{aligned}&\phi_1^\sigma=[\rho^2]\circ\phi_1, \quad \phi_2^\sigma=[\rho]\circ\phi_2, \quad \phi_3^\sigma=\phi_3, \quad \phi_4^\sigma=\phi_4,\\ &\phi_1^\tau=\phi_1, \quad \phi_2^\tau=\phi_2, \quad \phi_3^\tau=\phi_3, \quad \phi_4^\tau=[-1]\circ\phi_4.\end{aligned}$$

Now suppose that we have a relation

$$[n_1]\circ\phi_1+[n_2]\circ\phi_2+[n_3]\circ\phi_3+[n_4]\circ\phi_4=0. \quad (7\text{–}20)$$

Applying the transformation τ to (7–20) has the effect of replacing ϕ_4 by $[-1]\circ\phi_4$, so subtracting the two equations yields $[2n_4]\circ\phi_4=0$. Since the map $\phi_4 : C_6^{(1,1)}\to E^{(1)}$ is a finite map, it follows that $n_4=0$.

Applying σ and σ^2 to (7–20), we end up with three equations:

$$\begin{aligned}[n_1]\circ\phi_1+[n_2]\circ\phi_2+[n_3]\circ\phi_3&=0, \quad (7\text{–}21)\\ [n_1]\circ[\rho^2]\circ\phi_1+[n_2]\circ[\rho]\circ\phi_2+[n_3]\circ\phi_3&=0, \quad (7\text{–}22)\\ [n_1]\circ[\rho]\circ\phi_1+[n_2]\circ[\rho^2]\circ\phi_2+[n_3]\circ\phi_3&=0. \quad (7\text{–}23)\end{aligned}$$

Adding (7–21), (7–22), and (7–23) and using $1+\rho+\rho^2=0$ gives $[3n_3]\circ\phi_3=0$, which implies $n_3=0$. Similarly, adding (7–21) to $[\rho]$ times (7–22) to $[\rho^2]$ times (7–23) gives $[3n_1]\circ\phi_1=0$, so $n_1=0$. Finally, since $n_1=n_3=0$, the equation (7–21) gives $n_2=0$. This completes the proof that $\phi_1,\dots,\phi_4$ are independent.

(d) It is a standard fact that $H^1_{\text{ét}}$ of a curve and its Jacobian are isomorphic. This gives the first isomorphism, and the second follows from (c) and the fact that an isogeny between abelian varieties induces an isomorphism of their étale cohomologies. □

Proposition 7.19. *Let $\mathfrak{K}$ be a prime ideal in $\mathcal{O}_K$ such that $\boldsymbol{\mu}_6\subset\mathcal{O}_K/\mathfrak{K}$, i.e., $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{K})\equiv 1 \pmod 6$. Let $\zeta\in\boldsymbol{\mu}_6$ and $\xi\in\boldsymbol{\mu}_3$, choose elements $\gamma,\delta\in\mathcal{O}_K$ satisfying $\left(\frac{\gamma}{\mathfrak{K}}\right)_6=\zeta$ and $\left(\frac{\delta}{\mathfrak{K}}\right)_3=\xi$, and let $C_6^{(\delta,\gamma)}$ be the smooth projective curve from Proposition 7.18 given by the affine equation*

$$C_6^{(\gamma,\delta)} : \gamma z^6(1-\gamma z^6)=\delta x^3.$$

Then

$$\#M_{\mathfrak{K}}^{[1]}(\zeta,\xi)=\frac{1}{18}\left(\#C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right)-e(\zeta,\xi)\right),$$

where the error term $e(\zeta,\xi)$ is given by the formula

$$e(\zeta,\xi)=\begin{bmatrix}6 \text{ if } \zeta=1\\ 0 \text{ if } \zeta\ne 1\end{bmatrix}+\begin{bmatrix}3 \text{ if } \zeta^2=\xi\\ 0 \text{ if } \zeta^2\ne\xi\end{bmatrix}+\begin{bmatrix}3 \text{ if } \zeta^4=\xi\\ 0 \text{ if } \zeta^4\ne\xi\end{bmatrix}.$$

Proof: Our choices of γ and δ imply that for any $\lambda\in\mathcal{O}_K$,

$$\begin{aligned}&\left(\frac{\lambda}{\mathfrak{K}}\right)_6=\zeta\\ &\quad\Longleftrightarrow \gamma^{-1}\lambda\equiv\text{a nonzero sixth power} \pmod{\mathfrak{K}}\end{aligned}$$

and

$$\begin{aligned}&\left(\frac{\lambda(1-\lambda)}{\mathfrak{K}}\right)_3=\xi\\ &\quad\Longleftrightarrow \delta^{-1}\lambda(1-\lambda)\equiv\text{a nonzero cube} \pmod{\mathfrak{K}}.\end{aligned}$$

We thus get a natural map

$$\begin{aligned}\left\{(x,z)\in C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right) : x\ne 0,\infty\right\}&\longrightarrow M_{\mathfrak{K}}(\zeta,\xi),\\ (x,z)&\longmapsto \gamma z^6. \quad (7\text{–}24)\end{aligned}$$

We claim that the map (7–24) is exactly 18-to-1. To see this, let $\lambda \in M_{\mathfrak{K}}(\zeta,\xi)$. Then $\lambda \equiv \gamma v^6 \pmod{\mathfrak{K}}$ and $\lambda(1-\lambda) \equiv \delta u^3 \pmod{\mathfrak{K}}$ for some $u, v \in (\mathcal{O}_K/\mathfrak{K})^*$, so λ is the image of the point $(u,v) \in C_6^{(\gamma,\delta)}(\mathcal{O}_K/\mathfrak{K})$. Further, for a given value of λ, there are six choices for v and three choices for u. (Note that $\mathcal{O}_K/\mathfrak{K}$ contains $\boldsymbol{\mu}_6$.) Hence

$$\#M_{\mathfrak{K}}(\zeta,\xi) = \frac{1}{18}\#\left(C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right) \smallsetminus \{x = 0 \text{ or } \infty\}\right).$$

It remains to count the number of $\mathcal{O}_K/\mathfrak{K}$-rational points with $x = 0$ or ∞ on a smooth model of $C_6^{(\gamma,\delta)}$.

To ease notation, we let $C = C_6^{(\gamma,\delta)}$, and we let C' be the curve

$$C' : \gamma(1-\gamma z^6) = \delta x^3. \tag{7–25}$$

The birational map

$$C \longrightarrow C', \quad (x,z) \longmapsto (xz^{-2}, z),$$

is a bijection on the set of points

$$C \smallsetminus \{x = 0 \text{ or } \infty\} \xleftrightarrow{\sim} C' \smallsetminus \{x = 0 \text{ or } \infty\} \cup \{z = 0\},$$

and the affine piece of C' defined by equation (7–25) is smooth, so the points with $x = 0$ on C become the points with $x = 0$ or $z = 0$ on C'. (More precisely, we will see that the singular point $(0,0) \in C$ is blown up to three points on C', while there are six smooth points of the form $(0, \gamma^{-1/6})$ on both C and C'.) The points on C' with $x = 0$ or $z = 0$ are characterized by

$$(0,z) \in C' \Longleftrightarrow z^6 = \gamma^{-1}$$

and

$$(x,0) \in C' \Longleftrightarrow x^3 = \gamma\delta^{-1}.$$

Thus there are points of the form $(0,z)$ if and only if $\left(\frac{\gamma}{\mathfrak{K}}\right)_6 = 1$, and there are points of the form $(0,x)$ if and only if $\left(\frac{\gamma\delta^{-1}}{\mathfrak{K}}\right)_3 = 1$. Using the values $\left(\frac{\gamma}{\mathfrak{K}}\right)_6 = \zeta$ and $\left(\frac{\gamma\delta^{-1}}{\mathfrak{K}}\right)_3 = \left(\frac{\gamma}{\mathfrak{K}}\right)_6^2\left(\frac{\delta^{-1}}{\mathfrak{K}}\right)_3 = \zeta^2\xi^{-1}$, we find that

$$\#\left\{(0,z) \in C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right)\right\} = \begin{cases} 6 & \text{if } \zeta = 1, \\ 0 & \text{if } \zeta \neq 1, \end{cases}$$

$$\#\left\{(x,0) \in C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right)\right\} = \begin{cases} 3 & \text{if } \zeta^2 = \xi, \\ 0 & \text{if } \zeta^2 \neq \xi. \end{cases}$$

It remains to count the points at infinity on C'. Homogenizing the equation for C' gives the curve $\gamma y^6 - \gamma^2 z^6 = \delta x^3 y^3$. The unique (singular) point at infinity is $[x,y,z] = [1,0,0]$, so dehomogenizing by setting $x = 1$ gives the curve

$$\gamma y^6 - \gamma^2 z^6 = \delta y^3.$$

We blow up the singular point $(0,0)$ by setting $y = z^2 u$. (This corresponds to blowing up twice. One can check that the other coordinate charts do not yield any additional points.) The resulting curve has affine equation

$$\gamma z^6 u^6 - \gamma^2 = \delta u^3.$$

This affine curve is smooth, and the points that map to the point at infinity on C' are the points with $z = 0$ and $u^3 = -\gamma^2\delta^{-1}$. Using $\left(\frac{\gamma^2\delta^{-1}}{\mathfrak{K}}\right)_3 = \left(\frac{\gamma}{\mathfrak{K}}\right)_6^4\left(\frac{\delta^{-1}}{\mathfrak{K}}\right)_3$, we see that

$$\#\left\{\text{points at infinity on } C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right)\right\} = \begin{cases} 3 & \text{if } \zeta^4 = \xi, \\ 0 & \text{if } \zeta^4 \neq \xi. \end{cases}$$

This completes the proof of the proposition. □

The next step is to count the number of points on $C_6^{(\gamma,\delta)}$ defined over a finite field. This is done using the decomposition of $J_6^{(\gamma,\delta)}$ into a product of elliptic curves.

Proposition 7.20. *With notation as in the statement of Proposition 7.19, choose an element $\pi \in \mathcal{O}_K$ satisfying $\mathfrak{K} = \pi\mathcal{O}_K$ and $\pi \equiv 2 \pmod 3$. Further, let $\epsilon = \left(\frac{2}{\mathfrak{K}}\right)_3$. Then*

$$\begin{aligned} &\#C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right) \\ &\quad = \mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K} + 1 + \mathrm{Tr}_{K/\mathbb{Q}}(\xi\bar{\pi}) \\ &\qquad + \mathrm{Tr}_{K/\mathbb{Q}}(\epsilon^2\zeta^3\xi^2\bar{\pi}) + \mathrm{Tr}_{K/\mathbb{Q}}(\epsilon\zeta^5\xi\bar{\pi}) \\ &\qquad + (-1)^{\frac{1}{2}(\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K}-1)}\,\mathrm{Tr}_{K/\mathbb{Q}}(\epsilon\zeta\xi\bar{\pi}). \end{aligned}$$

If $\mathfrak{K}$ is an inert prime, say $\mathfrak{K} = k\mathcal{O}_K$ with $k \in \mathbb{Z}$ satisfying $k \equiv 2 \pmod 3$, and if we take $\delta = 1$, then the formula simplifies to

$$\#C_6^{(\gamma,1)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right) = \begin{cases} k^2 + 1 + 8k & \text{if } \zeta = 1, \\ k^2 + 1 - 4k & \text{if } \zeta = -1, \\ k^2 + 1 + 2k & \text{if } \zeta \neq \pm 1. \end{cases}$$

Proof: To ease notation, let $\mathbb{F}_{\mathfrak{K}} = \mathcal{O}_K/\mathfrak{K}$, so $\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K} = \#\mathbb{F}_{\mathfrak{K}}$. Further, let $F_{\mathfrak{K}}$ be the $(\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K})$th-power Frobenius map on $\bar{\mathbb{F}}_{\mathfrak{K}}$. Then the number of points in $C_6^{(\gamma,\delta)}(\mathbb{F}_{\mathfrak{K}})$ is given by the trace formula [Hartshorne 77, C.4.2]

$$\#C_6^{(\gamma,\delta)}(\mathbb{F}_{\mathfrak{K}}) = \mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K} + 1 - \mathrm{Tr}\Big(F_{\mathfrak{K}} \;\Big|\; H^1_{\text{ét}}(C^{(\gamma,\delta)}_{6/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big). \tag{7–26}$$

We compute the trace using Proposition 7.18, which splits the representation for $C_6^{(\gamma,\delta)}$ into a product of representations on elliptic curves with zero j-invariant.

Thus

$$\begin{aligned}
&\mathrm{Tr}\Big(F_{\mathfrak{K}} \mid H^1_{\text{ét}}(C^{(\gamma,\delta)}_{6/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) \\
&\quad = \mathrm{Tr}\Big(F_{\mathfrak{K}} \mid H^1_{\text{ét}}(E^{(16\delta^2)}_{/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) \\
&\qquad + \mathrm{Tr}\Big(F_{\mathfrak{K}} \mid H^1_{\text{ét}}(E^{(4\gamma^3\delta^4)}_{/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) \\
&\qquad + \mathrm{Tr}\Big(F_{\mathfrak{K}} \mid H^1_{\text{ét}}(E^{(\gamma^5\delta^2)}_{/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) \\
&\qquad + \mathrm{Tr}\Big(F_{\mathfrak{K}} \mid H^1_{\text{ét}}(E^{(-\gamma\delta^2)}_{/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big).
\end{aligned} \tag{7–27}$$

We now apply [Ireland and Rosen 90, Chapter 18, Section 3, Theorem 4], which gives a formula for the trace in terms of residue symbols. Writing $\mathfrak{K} = \pi\mathcal{O}_K$ with $\pi \equiv 2 \pmod 3$, we find that

$$\begin{aligned}
&\mathrm{Tr}\Big(F_{\mathfrak{K}} \mid H^1_{\text{ét}}(C^{(\gamma,\delta)}_{6/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) \\
&\quad = -\left(\frac{2^6\delta^2}{\mathfrak{K}}\right)_6^{-1}\pi - \left(\frac{2^6\delta^2}{\mathfrak{K}}\right)_6\bar{\pi} - \left(\frac{2^4\gamma^3\delta^4}{\mathfrak{K}}\right)_6^{-1}\pi \\
&\qquad - \left(\frac{2^4\gamma^3\delta^4}{\mathfrak{K}}\right)_6\bar{\pi} - \left(\frac{2^2\gamma^5\delta^2}{\mathfrak{K}}\right)_6^{-1}\pi \\
&\qquad - \left(\frac{2^2\gamma^5\delta^2}{\mathfrak{K}}\right)_6\bar{\pi} - \left(\frac{-2^2\gamma\delta^2}{\mathfrak{K}}\right)_6^{-1}\pi - \left(\frac{-2^2\gamma\delta^2}{\mathfrak{K}}\right)_6\bar{\pi} \\
&\quad = -\xi^{-1}\pi - \xi\bar{\pi} - \left(\frac{2}{\mathfrak{K}}\right)_3^{-2}\zeta^{-3}\xi^{-2}\pi - \left(\frac{2}{\mathfrak{K}}\right)_3^{2}\zeta^{3}\xi^{2}\bar{\pi} \\
&\qquad - \left(\frac{2}{\mathfrak{K}}\right)_3^{-1}\zeta^{-5}\xi^{-1}\pi - \left(\frac{2}{\mathfrak{K}}\right)_3\zeta^{5}\xi\bar{\pi} \\
&\qquad - \left(\frac{-1}{\mathfrak{K}}\right)_2\left(\frac{2}{\mathfrak{K}}\right)_3^{-1}\zeta^{-1}\xi^{-1}\pi - \left(\frac{-1}{\mathfrak{K}}\right)_2\left(\frac{2}{\mathfrak{K}}\right)_3\zeta\xi\bar{\pi}.
\end{aligned} \tag{7–28}$$

Noting that $\left(\frac{-1}{\mathfrak{K}}\right)_2 = (-1)^{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{K}-1)/2}$, we combine (7–26) and (7–28) to obtain the desired result.

In the case that $\mathfrak{K} = k\mathcal{O}_K$ is an inert prime, we have $(-1)^{\frac{1}{2}(k^2-1)} = 1$, since k is odd. Further, both 2 and k are primary, so cubic reciprocity gives $\left(\frac{2}{\mathfrak{K}}\right)_3 = \left(\frac{2}{k}\right)_3 = \left(\frac{k}{2}\right)_3 = 1$. Further taking $\delta = 1$ implies that $\xi = 1$, so the formula for $\#C_6^{(\gamma,1)}(\mathcal{O}_K/\mathfrak{K})$ becomes

$$\begin{aligned}
&k^2 + 1 + \big(\mathrm{Tr}_{K/\mathbb{Q}}(1) + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta^3) + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta^5) \\
&\quad + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta)\big)k.
\end{aligned}$$

Taking the six possible values $\zeta \in \boldsymbol{\mu}_6$ yields the stated formula. □

Proposition 7.21. *Let $k \geq 5$ be a rational prime. The following table gives the values of $\#M_k^{[1]}(S,1)$ for various subsets $S \subset \boldsymbol{\mu}_6$, divided into cases according to whether k is split or inert in $K = \mathbb{Q}(\sqrt{-3})$; cf. Proposition 7.17:*

		$k \equiv 1 \pmod 3$	$k \equiv 2 \pmod 3$
(a)	$\#M_k^{[1]}(\{\omega, \omega^5\}, 1)$	$\frac{1}{9}(k-1)^2$	$\frac{1}{9}(k+1)^2$
(b)	$\#M_k^{[1]}(\{\omega, \omega^3, \omega^5\}, 1)$	$\frac{1}{6}(k-1)(k-3)$	$\frac{1}{6}(k^2-1)$
(c)	$\#M_k^{[1]}(\{\omega, \omega^2, \omega^4, \omega^5\}, 1)$	$\frac{2}{9}(k-1)^2$	$\frac{2}{9}(k+1)^2$
(d)	$\#M_k^{[1]}(\boldsymbol{\mu}_6, 1)$	$\frac{1}{3}(k^2-2k+4)$	$\frac{1}{3}(k^2+2k-2)$

Proof: We begin with the case that $k \equiv 2 \pmod 3$, so $\mathfrak{K} = k\mathcal{O}_K$ is a prime ideal with $\mathrm{N}_{K/\mathbb{Q}}\mathfrak{K} = k^2$. We let $\omega = \frac{1}{2}(1+\sqrt{-3})$ be the usual sixth root of unity, and we choose some $\gamma \in \mathcal{O}_K$ satisfying

$$\left(\frac{\gamma}{\mathfrak{K}}\right)_6 = \omega.$$

Then for any $0 \leq i \leq 5$, we have

$$\begin{aligned}
&18\#M_k^{[1]}(\omega^i, 1) \\
&\quad = \#C_6^{(\gamma^i,1)}(\mathbb{F}_{\mathfrak{K}}) - \begin{bmatrix} 12 & \text{if } i = 0 \\ 6 & \text{if } i = 3 \\ 0 & \text{otherwise} \end{bmatrix} \\
&\quad \text{(from Proposition 7.19 with } \zeta = \omega^i \text{ and } \xi = 1) \\
&\quad = \begin{bmatrix} k^2+1+8k & \text{if } i = 0 \\ k^2+1-4k & \text{if } i = 3 \\ k^2+1+2k & \text{otherwise} \end{bmatrix} - \begin{bmatrix} 12 & \text{if } i = 0 \\ 6 & \text{if } i = 3 \\ 0 & \text{otherwise} \end{bmatrix} \\
&\quad \text{(from Proposition 7.20 with } \zeta = \omega^i \text{ and } \xi = 1) \\
&\quad = \begin{cases} k^2+8k-11 & \text{if } i = 0, \\ k^2-4k-5 & \text{if } i = 3, \\ k^2+2k+1 & \text{otherwise.} \end{cases}
\end{aligned}$$

It is now easy to compute

$$\#M_k^{[1]}(S,1) = \sum_{\zeta \in S} \#M_k^{[1]}(\zeta, 1)$$

for the four cases of the proposition. For example,

$$\begin{aligned}
\#M_k^{[1]}(\boldsymbol{\mu}_6, 1) &= \frac{1}{18}\big((k^2+8k-11) + (k^2-4k-5) \\
&\qquad + 4(k^2+2k+1)\big) \\
&= \frac{1}{3}(k^2+2k-2).
\end{aligned}$$

Next we consider the case that $k \equiv 1 \pmod 3$, so $k\mathcal{O}_K = \mathfrak{K}\bar{\mathfrak{K}}$ splits. The definition of the residue symbol says that

$$\begin{aligned}
\left(\frac{\lambda}{k\mathcal{O}_K}\right)_6 &= \left(\frac{\lambda}{\mathfrak{K}}\right)_6\left(\frac{\lambda}{\bar{\mathfrak{K}}}\right)_6, \\
\left(\frac{\lambda(1-\lambda)}{k\mathcal{O}_K}\right)_3 &= \left(\frac{\lambda(1-\lambda)}{\mathfrak{K}}\right)_3\left(\frac{\lambda(1-\lambda)}{\bar{\mathfrak{K}}}\right)_3,
\end{aligned}$$

so using the Chinese remainder theorem,

$$\mathcal{O}_K/k\mathcal{O}_K = \mathcal{O}_K/\mathfrak{K}\mathcal{O}_K \times \mathcal{O}_K/\bar{\mathfrak{K}}\mathcal{O}_K,$$

a quantity such as $M_k^{[1]}(\zeta,\xi)$ breaks up into a sum of products,

$$M_k^{[1]}(\zeta,\xi)=\sum_{u=0}^{5}\sum_{v=0}^{2}M_{\mathfrak{K}}^{[1]}(\omega^u,\omega^{2v})M_{\bar{\mathfrak{K}}}^{[1]}(\zeta\omega^{-u},\xi\omega^{-2v}).$$

Hence for $0\le i\le 5$, we have

$$\begin{aligned}M_k^{[1]}(\omega^i,1)&=\sum_{u=0}^{5}\sum_{v=0}^{2}M_{\mathfrak{K}}^{[1]}(\omega^u,\omega^{2v})M_{\bar{\mathfrak{K}}}^{[1]}(\omega^{i-u},\omega^{-2v})\\&=\sum_{u=0}^{5}\sum_{v=0}^{2}M_{\mathfrak{K}}^{[1]}(\omega^u,\omega^{2v})M_{\mathfrak{K}}^{[1]}(\omega^{u-i},\omega^{2v}).\end{aligned}\tag{7–29}$$

(For the second equality we have used the identity $M_{\mathfrak{K}}^{[1]}(\zeta,\xi)=M_{\bar{\mathfrak{K}}}^{[1]}(\bar\zeta,\bar\xi)$.) We choose γ and δ to satisfy

$$\left(\frac{\gamma}{\mathfrak{K}}\right)_6=\omega\quad\text{and}\quad\left(\frac{\delta}{\mathfrak{K}}\right)_3=\omega^2.$$

Then Proposition 7.19 gives us the formula

$$18M_{\mathfrak{K}}^{[1]}(\omega^u,\omega^{2v})=\#C_6^{(\gamma^u,\delta^v)}(\mathbb{F}_{\mathfrak{K}})-e(\omega^u,\omega^{2v}),\tag{7–30}$$

where

$$\begin{aligned}e(\omega^u,\omega^{2v})=&\begin{bmatrix}6&\text{if } u\equiv 0 \pmod 6\\0&\text{otherwise}\end{bmatrix}\\&+\begin{bmatrix}3&\text{if } u\equiv v \pmod 3\\0&\text{otherwise}\end{bmatrix}\\&+\begin{bmatrix}3&\text{if } 2u\equiv v \pmod 3\\0&\text{otherwise}\end{bmatrix}.\end{aligned}\tag{7–31}$$

Further, Proposition 7.20 gives us the number of points on the curve:

$$\begin{aligned}&\#C_6^{(\gamma^u,\delta^v)}(\mathbb{F}_{\mathfrak{K}})\\&\quad=k+1+\operatorname{Tr}_{K/\mathbb{Q}}(\omega^{2v}\bar\pi)+\operatorname{Tr}_{K/\mathbb{Q}}(\epsilon^2\omega^{3u+4v}\bar\pi)\\&\qquad+\operatorname{Tr}_{K/\mathbb{Q}}(\epsilon\omega^{5u+2v}\bar\pi)+(-1)^{\frac12(k-1)}\operatorname{Tr}_{K/\mathbb{Q}}(\epsilon\omega^{u+2v}\bar\pi),\end{aligned}\tag{7–32}$$

where $\epsilon=\left(\frac{2}{\mathfrak{K}}\right)_3$.

Combining (7–29), (7–30), (7–31), and (7–32) gives an explicit, albeit quite complicated, formula for $M_k^{[1]}(\omega^i,1)$. In principle, this formula could be computed by hand, but we evaluated it using PARI in both the $k\equiv 1 \pmod 4$ and $k\equiv 3 \pmod 4$ cases.[2] The results are listed in Table 2.[3]

Examining Table 2, we see that the value of $\#M_k^{[1]}(\omega^i,1)$ is independent of k modulo 4 and can be summarized as follows:

$$18\#M_k^{[1]}(\omega^i,1)=\begin{cases}k^2+4k+13 & \text{if } i=0,\\ k^2-8k+7 & \text{if } i=3,\\ k^2-2k+1 & \text{otherwise.}\end{cases}$$

It is now a simple matter to compute the value of $\#M_k^{[1]}(S,1)$ for the four cases, as shown in Table 2. For example,

$$\begin{aligned}\#M_k^{[1]}(\boldsymbol{\mu}_6,1)&=\frac{1}{18}\big((k^2+4k+13)+(k^2-8k+7)\\&\qquad+4(k^2-2k+1)\big)\\&=\frac13(k^2-2k+4).\end{aligned}$$

This completes the proof of Proposition 7.21. □

Remark 7.22. As noted earlier, we used PARI to compute $M_k^{[1]}(\omega^i,1)$ by evaluating formulas (7–29), (7–30), (7–31), and (7–32), where we treated k, π, and ϵ as indeterminates, and we formally set $\bar\pi=k/\pi$ and $\bar\epsilon=1/\epsilon$. The value of $M_k^{[1]}(\omega^i,1)$ turns out to be a quadratic polynomial in k that is independent of k mod 4. We do not have an a priori explanation for why this should be the case. In order to illustrate the delicacy of the argument, we suppose for a moment that the isogeny decomposition of the Jacobian of $C_6^{(\gamma,\delta)}$ in Proposition 7.18 looks like

$$E^{(16\delta^2)}\times E^{(4\gamma^4\delta^4)}\times E^{(\gamma^5\delta^2)}\times E^{(-\gamma\delta^2)}\longrightarrow \operatorname{Jac}(C_6^{(\gamma,\delta)}).$$

(All that we have done is change the second elliptic factor from $E^{(4\gamma^3\delta^4)}$ to $E^{(4\delta^4)}$.) This would have the effect in formula (7–32) of changing the second trace term from $\operatorname{Tr}_{K/\mathbb{Q}}(\epsilon^2\omega^{3u+4v}\bar\pi)$ to $\operatorname{Tr}_{K/\mathbb{Q}}(\epsilon^2\omega^{4v}\bar\pi)$. But with this small modification, there is less cancellation in the computation of $M_k^{[1]}(\omega^i,1)$, so for example, $\#M_k^{[1]}\big(\{\omega,\omega^5\},1\big)$ would equal

$$\frac19\left(k^2+2k+1+2\operatorname{Tr}\left(\left(\frac{2}{\mathfrak{K}}\right)_3^2\bar\pi^2\right)\right).$$

Thus $\#M_k^{[1]}\big(\{\omega,\omega^5\},1\big)$ would depend on both $\left(\frac{2}{\mathfrak{K}}\right)_3$ and the factorization of k in $\mathcal{O}_K$.

Remark 7.23. Many of the cases of Proposition 7.21 can be obtained somewhat more easily by working on elliptic curves $z(1-z)=\delta x^3$ or genus-two curves $\gamma z^2(1-\gamma z^2)=\delta x^3$. However, some cases require the curves $\gamma z^6(1-\gamma z^6)=\delta x^3$ of genus four, so for unity of exposition and to save space, we have derived all cases using these latter curves.

Combining Conjecture 7.14 with the computations in Propositions 7.17 and 7.21 yields precise formulas for the

[2] PARI is available at http://pari.math.u-bordeaux.fr/.

[3] See http://www.math.brown.edu/~jhs/amicable.html for the PARI script that we used, and Remark 7.22 for further information about this computation.

$$\begin{aligned}
&\boldsymbol{k \equiv 1 \pmod 4} && \boldsymbol{k \equiv 3 \pmod 4}\\
&18\#M_k^{[1]}(\omega^0,1) = k^2+4k+13 && 18\#M_k^{[1]}(\omega^0,1) = k^2+4k+13\\
&18\#M_k^{[1]}(\omega^1,1) = k^2-2k+1 && 18\#M_k^{[1]}(\omega^1,1) = k^2-2k+1\\
&18\#M_k^{[1]}(\omega^2,1) = k^2-2k+1 && 18\#M_k^{[1]}(\omega^2,1) = k^2-2k+1\\
&18\#M_k^{[1]}(\omega^3,1) = k^2-8k+7 && 18\#M_k^{[1]}(\omega^3,1) = k^2-8k+7\\
&18\#M_k^{[1]}(\omega^4,1) = k^2-2k+1 && 18\#M_k^{[1]}(\omega^4,1) = k^2-2k+1\\
&18\#M_k^{[1]}(\omega^5,1) = k^2-2k+1 && 18\#M_k^{[1]}(\omega^5,1) = k^2-2k+1
\end{aligned}$$

$$\begin{aligned}
\#M_k^{[1]}\big(\{\omega^1,\omega^5\},1\big) &= (1/9)(k^2-2k+1)\\
\#M_k^{[1]}\big(\{\omega^1,\omega^3,\omega^5\},1\big) &= (1/6)(k^2-4k+3)\\
\#M_k^{[1]}\big(\{\omega^1,\omega^2,\omega^4,\omega^5\},1\big) &= (2/9)(k^2-2k+1)\\
\#M_k^{[1]}\big(\{\omega^0,\omega^1,\omega^2,\omega^3,\omega^4,\omega^5\},1\big) &= (1/3)(k^2-2k+4)
\end{aligned}$$

TABLE 2. Results of computing $M_k^{[1]}(S,1)$ using PARI.

conjectural density of type-1 primes on $y^2 = x^3 + k$ when k is prime.

Conjecture 7.24. *Let $k \geq 5$ be a rational prime. Then*

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

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

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

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

In particular, $R(k) = O(1/k)$.

We do not have an intrinsic explanation for why $R(k)$ is the same in cases (a) and (c), nor do we know why $R(k) = 0$ in case (b).

8. CURVES WITH $j = 0$ HAVE NO ALIQUOT TRIPLES

In this section we use Corollary 7.6 and a detailed case-by-case analysis to show that an elliptic curve with $j = 0$ has no normalized aliquot triples (p, q, r) with $p > 7$. The details are sufficiently intricate that it seems likely a different argument would be needed to prove that there are no aliquot cycles of length greater than three.

Proposition 8.1. *Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) = 0$. Then E has no normalized aliquot triples (p, q, r) with $p > 7$.*

Proof: We use Corollary 7.6, which says that if p and $q = \#\tilde{E}_p(\mathbb{F}_p)$ are prime, then $r = \#\tilde{E}_q(\mathbb{F}_q)$ takes one of six possible values. One of these six possible values is p, which is not allowed, since we are assuming that p, q, r are distinct. Hence r has one of the following forms:

$$\begin{aligned}
r &= 2q + 2 - p && \text{(Case 1)},\\
r &= \frac{\pm(q+1-p) \pm 3A_{p,q}}{2} && \text{(Case 2)},
\end{aligned}$$

where $A_{x,y}$ satisfies

$$A_{x,y}^2 = \frac{4xy - (x+y-1)^2}{3}.$$

(Of course, Case 2 is really four cases, depending on the choice of signs.)

For the moment letting $s = \#\tilde{E}_r(\mathbb{F}_r)$, we can apply the same reasoning to (q, r, s) to deduce that

$$\begin{aligned} s &= 2r + 2 - q && \text{(Case A)},\\ s &= \frac{\pm(r+1-q) \pm 3A_{q,r}}{2} && \text{(Case B)}. \end{aligned}$$

To ease notation, we let

$$F(x,y) = \frac{\pm(y+1-x) \pm 3A_{x,y}}{2}.$$

Then the two cases for r followed by the two cases for s give four possibilities for s in terms of p and q:

$$\begin{aligned} s &= 3q + 6 - 2p && \text{(Case 1A)},\\ s &= 2F(p,q) + 2 - q && \text{(Case 2A)},\\ s &= F(q, 2q+2-p) && \text{(Case 1B)},\\ s &= F\big(q, F(p,q)\big) && \text{(Case 2B)}. \end{aligned}$$

(Of course, each case is really several cases depending on the choice of signs for each occurrence of F.)

The assumption that (p, q, r) is an aliquot triple is equivalent to saying that $s = p$. Suppose first we are in Case 1A. Then $s = p$ is equivalent to

$$3q + 6 - 2p = p,$$

so $p = q + 2$. This contradicts our assumption that the triple is normalized, i.e., that p is the smallest element of the triple. Hence Case 1A is not possible.

Next we consider Case 2A. Then the assumption $s = p$ implies that $2F(p,q) = p + q - 2$. Using the definition of F, this can be written as

$$\pm(q+1-p) \pm 3A_{p,q} = p + q - 2,$$

which (using the definition of A) implies that

$$\begin{aligned} \big((p+q-2) \pm (q+1-p)\big)^2 &= 9A_{p,q}^2\\ &= 3\big(4pq - (p+q-1)^2\big). \end{aligned} \tag{8–1}$$

This gives two subcases, which we denote by $2A^+$ and $2A^-$ according to the choice of sign. A little bit of algebra yields

$$\begin{aligned} 28p^2 - 24pq + 12q^2 - 72p - 24q + 48 = 0 \quad &\text{(Case 2A}^+\text{)},\\ 12p^2 - 24pq + 28q^2 - 24p - 40q + 16 = 0 \quad &\text{(Case 2A}^-\text{)}. \end{aligned}$$

Both of the functions on the left-hand sides have leading quadratic forms that are positive definite, so there are only finitely many integral solutions (p, q). A more careful analysis shows that the first is positive for $p > 5$ and the second is positive for $p > 7$.

Next comes Case 1B, where the assumption that $s = p$ leads to the formula

$$F(q, 2q+2-p) = p.$$

Writing this out in terms of $A_{q,2q+2-p}$, moving all the other terms to the other side, squaring, and simplifying, we again get two cases depending on a choice of sign. Thus

$$\begin{aligned} 12p^2 - 12pq + 4q^2 - 24p + 12 = 0 \quad &\text{(Case 1B}^+\text{)},\\ 4p^2 - 4pq + 4q^2 + 12 = 0 \quad &\text{(Case 1B}^-\text{)}. \end{aligned}$$

The quadratic function for Case $1B^+$ is positive for $p > 7$, and the quadratic function for Case $1B^-$ is positive for $p > 0$.

Finally we turn to Case 2B, which is somewhat more complicated because it is given by the formula

$$F\big(q, F(p,q)\big) = p,$$

which involves two iterations of the function F. The signs on the $A_{x,y}$ terms are irrelevant, since we square them, but the other signs in the definition of F do affect the eventual equation. After a bunch of algebra, we find that the p and q values for an amicable triple coming from Case 2B must satisfy one of the following equations:

Case $2B^{++}$:

$$\begin{aligned} &4p^4 + 2p^3q + 3p^2q^2 - pq^3 + q^4 - 6p^3 - 15p^2q\\ &\quad - 15pq^2 + 3p^2 + 3pq + 3q^2 = 0; \end{aligned}$$

Case $2B^{+-}$:

$$\begin{aligned} &9p^2q^2 - 9pq^3 + 9q^4 + 9p^2q - 27pq^2 + 3p^2 - 21pq\\ &\quad - 3q^2 - 6p + 6q + 4 = 0; \end{aligned}$$

Case $2B^{-+}$:

$$3p^2q^2 - 3pq^3 + q^4 + 9p^2q - 9pq^2 + 9p^2 - 9pq + 3q^2 = 0;$$

Case $2B^{--}$:

$$\begin{aligned} &4p^4 - 18p^3q + 33p^2q^2 - 27pq^3 + 9q^4 - 10p^3 + 33p^2q\\ &\quad - 21pq^2 + 21p^2 - 21pq - 3q^2 - 10p + 6q + 4 = 0. \end{aligned}$$

All of these quartic functions are positive if $0 < p < q$ with p sufficiently large. More precisely, it suffices to take $p > 3$ for Cases $2B^{++}$ and $2B^{+-}$, $p > 4$ for Case $2B^{-+}$, and $p > 2$ for Case $2B^{--}$.

This completes the proof that E has no aliquot triples. □

9. AMICABLE PAIRS FOR ELLIPTIC CURVES: EXPERIMENTS

In this section we present the results of experiments that test the reasonableness of our conjectures. We begin with Conjecture 1.3, which deals with the case of CM curves having nonzero j-invariant.

We computed the number $\mathcal{Q}_E(X)$ of amicable pairs up to X for elliptic curves with CM by the imaginary quadratic order of discriminant $-D$ and conductor f. Theorem 6.1 says that it suffices to consider $D \equiv 3 \pmod 4$. Further, the assumption that E is defined over $\mathbb{Q}$ means that $\mathcal{O}$ has class number one, so the classification of imaginary quadratic fields of class number one combined with an elementary formula for the class number of an order [Shimura 94, Exercise 4.12] implies that the only possibilities for D are $D \in \{3, 7, 11, 19, 43, 67, 163\}$, and the possible values of f are given by $f \in \{1, 2, 3\}$ if $D = 3$, $f \in \{1, 2\}$ if $D = 7$, and $f = 1$ in all other cases. See [Silverman 94, A §3] for a Weierstrass equation for each CM type.

We ignore for the moment the case $(D, f) = (3, 1)$. As noted in the proof of Theorem 6.1, the curves with (D, f) equal to $(3, 2)$, $(7, 1)$, and $(7, 2)$ have nontrivial 2-torsion, so neither they nor any of their (necessarily quadratic) twists have amicable pairs. The curve with $(D, f) = (3, 3)$ listed in [Silverman 94, A §3] has nontrivial 3-torsion, but it has quadratic twists with trivial torsion, so is a candidate to have amicable pairs. Table 3 lists the number $\mathcal{Q}_E(X)$ of amicable pairs up to the given bound and the ratio of $\mathcal{Q}_E(X)$ to the number $\mathcal{N}_E(X)$ of primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime. For this table we used the following Weierstrass equations.[4]

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

The results in Table 3 are consistent with Conjecture 6.9, which predicts that the ratio $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ should approach $\frac{1}{4}$.

We next considered the curves $y^2 = x^3 + k$ with $j(E) = 0$. Table 4, which is included for historical reasons, was our first intimation that the limiting value of $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ behaves differently for different values of k, with no obvious pattern for $2 \le k \le 10$. (Note that we do not list values of k that are squares or cubes, since in those cases $E(\mathbb{Q})_{\text{tors}}$ is nontrivial, so there are no amicable pairs.)

We recall the notation $\mathcal{N}_k^{[1]}$ for the set of type-1 primes for the curve $y^2 = x^3 + k$; see Section 7 for the precise definition. Conjecture 7.10 predicts that $\mathcal{Q}_k(X) \sim \frac{1}{4}\mathcal{N}_k^{[1]}(X)$, and in the case that k is prime, Conjecture 7.24 says that

$$\mathcal{N}_k^{[1]}(X) \sim \left(\frac{1}{3} + R(k)\right)\mathcal{N}_k(X),$$

where $R(k)$ is given by an explicit formula that depends on k modulo 36. We tested these two conjectures by computing $\mathcal{Q}_k(X)$, $\mathcal{N}_k^{[1]}(X)$, and $\mathcal{N}_k(X)$ for $X = 10^8$. The results are listed in Table 5. Column 5 provides convincing evidence for Conjecture 7.10, and the final two columns show that Conjecture 7.24 is in good agreement with experiment in all eight cases. (The notation (x.n) after each value of k indicates the case x = (a), ..., (d) and the congruence class $k \equiv n \pmod 3$ from Conjecture 7.24.)

We also checked Conjecture 7.14 experimentally for composite values of k. The results are listed in Table 6, where the conjectural limiting ratio is obtained by explicitly counting the size of the sets $\mathcal{M}_k$ and $\mathcal{M}_k^{[1]}$. The top eight k-entries in this table are products of two primes covering the usual eight cases; the final four entries include two values that are not square-free ($175 = 5 \cdot 7^2$ and $245 = 5 \cdot 7^2$) and two values that are products of three distinct primes ($385 = 5 \cdot 7 \cdot 11$ and $455 = 5 \cdot 7 \cdot 13$).

In order to test further the validity of Conjecture 7.14, we recomputed the final entry in the table with $X = 10^9$ and obtained

$$\frac{\mathcal{N}_{455}^{[1]}(10^9)}{\mathcal{N}_{455}(10^9)} = 0.3380.$$

This is in excellent agreement with the theoretical value of $4699/13915 = 0.3377$.

Finally, we consider Conjecture 4.1, which deals with non-CM curves. This conjecture is much harder to check numerically, because the function $\sqrt{X}/(\log X)^2$ grows quite slowly. We performed an extended search for amicable pairs on the elliptic curve

$$E : y^2 + y = x^3 + x^2 \tag{9–1}$$

of conductor 43, which we studied in Example 1.1. We used PARI to compute all normalized amicable pairs (p, q) with $p < 10^{11}$, and Andrew Sutherland subsequently extended our list to $p < 10^{12}$. Table 7 gives the first few and last few pairs.[5]

[4] Calculations on quadratic twists of the listed curves yielded virtually identical results.

[5] The complete list is available at http://www.math.brown.edu/~jhs/amicable.html.

(D, f)	$(3,3)$	$(11,1)$	$(19,1)$	$(43,1)$	$(67,1)$	$(163,1)$
$\mathcal{Q}_E(10^5)$	124	48	103	205	245	395
$\mathcal{Q}_E(10^5)/\mathcal{N}_E(10^5)$	0.251	0.238	0.248	0.260	0.238	0.246
$\mathcal{Q}_E(10^6)$	804	303	709	1330	1671	2709
$\mathcal{Q}_E(10^6)/\mathcal{N}_E(10^6)$	0.250	0.247	0.253	0.255	0.245	0.247
$\mathcal{Q}_E(10^7)$	5581	2267	5026	9353	12190	19691
$\mathcal{Q}_E(10^7)/\mathcal{N}_E(10^7)$	0.249	0.251	0.250	0.251	0.250	0.252

TABLE 3. $\mathcal{Q}_E(X)$ and $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ for elliptic curves with CM by $\mathbb{Q}(\sqrt{-D})$.

k	2	3	5	6	7	10
$X = 10^5$	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	0.1394	0.129	0.107

TABLE 4. $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ for elliptic curves $y^2 = x^3 + k$.

					$\mathcal{N}_k^{[1]}(X)/\mathcal{N}_k(X)$	
k	$\mathcal{Q}_k(X)$	$\mathcal{N}_k^{[1]}(X)$	$\mathcal{N}_k(X)$	$\mathcal{Q}/\mathcal{N}^{[1]}$	experiment	conjecture
5 (b.2)	14595	58594	175703	0.249	0.3335	$\frac{1}{3} = 0.3333$
7 (d.1)	21897	87825	168743	0.249	0.5205	$\frac{13}{25} = 0.5200$
11 (d.2)	16760	66698	169062	0.251	0.3945	$\frac{47}{119} = 0.3950$
13 (b.1)	13921	55766	167333	0.250	0.3333	$\frac{1}{3} = 0.3333$
17 (a.2)	15899	63810	169226	0.249	0.3771	$\frac{3}{8} = 0.3750$
19 (c.1)	15760	63066	168196	0.250	0.3750	$\frac{3}{8} = 0.3750$
23 (d.2)	15138	61210	168512	0.247	0.3632	$\frac{191}{527} = 0.3624$
29 (b.2)	13945	56286	168642	0.248	0.3338	$\frac{1}{3} = 0.3333$
31 (d.1)	15054	60349	168344	0.249	0.3585	$\frac{301}{841} = 0.3579$
37 (a.1)	14765	59430	168471	0.248	0.3528	$\frac{6}{17} = 0.3529$
41 (b.2)	13938	56381	168567	0.247	0.3345	$\frac{1}{3} = 0.3333$
43 (d.1)	14711	58807	168410	0.250	0.3492	$\frac{589}{1681} = 0.3504$
47 (d.2)	14513	58400	168365	0.249	0.3469	$\frac{767}{2207} = 0.3475$
53 (a.2)	14534	58257	168353	0.249	0.3460	$\frac{9}{26} = 0.3462$
59 (d.2)	14588	58422	168783	0.250	0.3461	$\frac{1199}{3479} = 0.3446$
61 (b.1)	13919	55816	168197	0.249	0.3318	$\frac{1}{3} = 0.3333$
67 (d.1)	14522	57944	168239	0.251	0.3444	$\frac{1453}{4225} = 0.3439$
71 (c.2)	14295	57661	168508	0.248	0.3422	$\frac{12}{35} = 0.3429$
73 (a.1)	14389	57828	168614	0.249	0.3430	$\frac{12}{35} = 0.3429$
79 (d.1)	14458	57937	168690	0.250	0.3435	$\frac{2029}{5929} = 0.3422$
83 (d.2)	14415	57871	168435	0.249	0.3436	$\frac{2351}{6887} = 0.3414$
89 (a.2)	14349	57634	168737	0.249	0.3416	$\frac{15}{44} = 0.3409$
97 (b.1)	13908	55880	168457	0.249	0.3317	$\frac{1}{3} = 0.3333$

TABLE 5. Density of amicable and type-1 primes with $p \le X$ for the curve $y^2 = x^3 + k$, for prime k and $X = 10^8$.

					$\mathcal{N}_k^{[1]}(X)/\mathcal{N}_k(X)$	
k	$\mathcal{Q}_k(X)$	$\mathcal{N}_k^{[1]}(X)$	$\mathcal{N}_k(X)$	$\mathcal{Q}/\mathcal{N}^{[1]}$	experiment	conjecture
35 (d.2)	15616	63169	168666	0.247	0.3745	$\frac{43}{115} = 0.3739$
55 (d.1)	14725	58718	168870	0.251	0.3477	$\frac{949}{2737} = 0.3467$
77 (b.2)	13977	56251	168921	0.248	0.3330	$\frac{1}{3} = 0.3333$
85 (b.1)	13994	56142	168767	0.249	0.3327	$\frac{1}{3} = 0.3333$
323 (c.2)	14095	56609	168585	0.249	0.3358	$\frac{43}{128} = 0.3359$
629 (a.2)	14001	56269	168042	0.249	0.3349	$\frac{3267}{9766} = 0.3345$
703 (c.1)	14181	56754	168817	0.250	0.3362	$\frac{1097}{3278} = 0.3347$
901 (a.1)	14060	56384	168411	0.249	0.3348	$\frac{3738}{11189} = 0.3341$
175 (d.1)	15662	63177	168840	0.248	0.3742	$\frac{43}{115} = 0.3739$
245 (b.2)	14792	58848	175934	0.251	0.3345	$\frac{1}{3} = 0.3333$
385 (b.1)	13934	56158	168393	0.248	0.3335	$\frac{1}{3} = 0.3333$
455 (d.2)	14072	56627	168342	0.249	0.3364	$\frac{4699}{13915} = 0.3377$

TABLE 6. Density of amicable and type-1 primes with $p \le X$ for the curve $y^2 = x^3 + k$, for composite k and $X = 10^8$.

$(853, 883)$	$(77761, 77999)$
$(1147339, 1148359)$	$(1447429, 1447561)$
$(82459561, 82471789)$	$(109165543, 109180121)$
$(253185307, 253194619)$	$(320064601, 320079131)$
$\vdots$	$\vdots$
$(811569419461, 811569591827)$	$(838059794239, 838061257667)$
$(851273574199, 851274251683)$	$(885227547847, 885227943451)$
$(916134576373, 916134747943)$	$(948135054247, 948136458277)$
$(954115635797, 954115645823)$	$(977575750447, 977576865637)$

TABLE 7. Some amicable pairs for $y^2 + y = x^3 + x^2$.

Conjectures 1.3(a) and 4.1 say that $\mathcal{Q}_E(X)$, the number of amicable pairs up to X, should grow like a multiple of $\sqrt{X}/(\log X)^2$. Table 8 tests this conjecture by computing the ratios

$$\frac{\mathcal{Q}_E(X)}{\sqrt{X}/(\log X)^2} \quad \text{and} \quad \frac{\log \mathcal{Q}_E(X)}{\log X}$$

for various values of X. The third column of Table 8 provides some small support for the conjecture that $\mathcal{Q}_E(X)$ grows like a multiple of $\sqrt{X}/(\log X)^2$. On the other hand, although the fourth column of the table suggests that $\mathcal{Q}_E(X)$ grows like X^δ for some $\delta > 0$, it is far from clear that δ is as large as $\frac{1}{2}$. We suspect the problem is that we are able to compute $\mathcal{Q}_E(X)$ only up to $X = 10^{12}$, and although 10^{12} is a moderately large number in terms of computation time, it is comparatively small compared to the likely error terms in any putative asymptotic formula for $\mathcal{Q}_E(X)$.[6]

Finally, we searched for normalized aliquot triples (p, q, r) on the curve (9–1). We found no examples with $p < 10^{11}$, and Andrew Sutherland found that there is exactly one such triple with $p < 10^{12}$, namely

$$(658501858783, 658502719313, 658502576161).$$

10. GENERALIZATIONS

As we have defined them, aliquot cycles for elliptic curves differ in a significant way from classical aliquot cycles associated with the sum of divisors function. In the classical case, every integer n leads to a possibly nonrepeating aliquot sequence $\big(n, \tilde{\sigma}(n), \tilde{\sigma}^2(n), \tilde{\sigma}^3(n), \dots\big)$, and it is an aliquot cycle if some iterate $\tilde{\sigma}^k(n)$ eventually returns to

[6] For additional data on two other curves, see http://www.math.brown.edu/~jhs/amicable.html.

X	$\mathcal{Q}_E(X)$	$\mathcal{Q}_E(X)/\frac{\sqrt{X}}{(\log X)^2}$	$\frac{\log \mathcal{Q}_E(X)}{\log X}$
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
$2 \cdot 10^{11}$	70	0.106	0.163
$4 \cdot 10^{11}$	88	0.099	0.168
$6 \cdot 10^{11}$	97	0.092	0.169
$8 \cdot 10^{11}$	109	0.092	0.171
10^{12}	117	0.089	0.172

TABLE 8. Counting amicable pairs for $y^2 + y = x^3 + x^2$.

n. (A major open problem for $\tilde{\sigma}$ is whether there are starting values for which the sequence is unbounded.) But for elliptic curves, if we arrive at a prime p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is not prime, then the sequence cannot be continued. We propose here two alternative definitions of elliptic aliquot sequences that more closely resemble the classical definition. We leave the investigation of these generalized sequences to a future paper.

Definition 10.1. Let $E/\mathbb{Q}$ be an elliptic curve, let $L(E/\mathbb{Q}, s) = \sum_{n\geq 1} a_n/n^s$ be the L-series of E, and define a function

$$F_E : \mathbb{N} \longrightarrow \mathbb{N}, \quad F_E(n) = n + 1 - a_n.$$

A *type-L aliquot sequence* for $E/\mathbb{Q}$ is a sequence obtained by starting at some $n \in \mathbb{N}$ and repeatedly applying the map F_E. A *type-L aliquot cycle* is a type-L aliquot sequence that returns to its starting value.

Definition 10.2. Let $E/\mathbb{Q}$ be an elliptic curve, let $\mathcal{E}^0/\mathbb{Z}$ be the open subset of the Néron model for $E/\mathbb{Q}$ consisting of the connected components of each fiber, and define a function

$$G_E : \mathbb{N} \longrightarrow \mathbb{N}, \quad G_E(n) = \#\mathcal{E}^0(\mathbb{Z}/n\mathbb{Z}).$$

A *type-N aliquot sequence* for $E/\mathbb{Q}$ is a sequence obtained by starting at some $n \in \mathbb{N}$ and repeatedly applying the map G_E. A *type-N aliquot cycle* is a type-N aliquot sequence that returns to its starting value.

Remark 10.3. There is a natural way to generalize the notion of elliptic amicable pairs and aliquot cycles to elliptic curves defined over number fields. Thus let $F/\mathbb{Q}$ be a number field and E/F an elliptic curve. We will say that a sequence of distinct degree-one prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_\ell$ is an *aliquot cycle* of length ℓ for E/F if E has good reduction at every $\mathfrak{p}_i$ and

$$\#\tilde{E}_{\mathfrak{p}_1}(\mathbb{F}_{\mathfrak{p}_1}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2), \ \ \#\tilde{E}_{\mathfrak{p}_2}(\mathbb{F}_{\mathfrak{p}_2}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_3), \ \ \ldots,$$
$$\#\tilde{E}_{\mathfrak{p}_{\ell-1}}(\mathbb{F}_{\mathfrak{p}_{\ell-1}}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_\ell), \ \ \#\tilde{E}_{\mathfrak{p}_\ell}(\mathbb{F}_{\mathfrak{p}_\ell}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1).$$

Many of the methods and results in this paper carry over in a straightforward manner to the number field case. For example, the following analogue of Theorem 6.1 holds.

Theorem 10.4. *Let $F/\mathbb{Q}$ be a number field, and let E/F be an elliptic curve with complex multiplication by an order in the quadratic imaginary field K. Suppose that $\mathfrak{p}$ and $\mathfrak{q}$ are degree-one primes of F at which E has good reduction, that $\mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{p} \geq 5$, and that*

$$\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) = \mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{q}.$$

Assume further that $j(E) \neq 0$. Then

$$\#\tilde{E}_{\mathfrak{q}}(\mathbb{F}_{\mathfrak{q}}) = \mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{p}$$

or

$$\#\tilde{E}_{\mathfrak{q}}(\mathbb{F}_{\mathfrak{q}}) = 2\,\mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{q} + 2 - \mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{p}.$$

It would be interesting to see to what extent the other results in this paper are valid over number fields, including especially the analysis of amicable pairs on curves with $j(E) = 0$.

ACKNOWLEDGMENTS

The authors would like to thank Franz Lemmermeyer, Jonathan Wise, and Soroosh Yazdani for their assistance, Igor Shparlinski and Antonella Perucca for their comments on the initial draft of this article, and the referees and Ram Murty for the observation in Remark 6.10, as well as many other helpful suggestions. The authors would also like to thank Andrew Sutherland for extending our original list of amicable pairs in Table 7 from 10^{11} to 10^{12}, as well as for finding an amicable triple on $y^2 + y = x^3 + x^2$.

The research in this note was performed while the first author was a long-term visiting researcher at Microsoft Research New England and included a short visit by the second author. Both authors thank MSR for its hospitality during their visits. The second author's research was supported by NSERC PDF-373333.

REFERENCES

[Apostol 76] T. M. Apostol. *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics. New York: Springer-Verlag, 1976.

[Baier and Zhao 08] S. Baier and L. Zhao. "On Primes Represented by Quadratic Polynomials." In *Anatomy of Integers*, CRM Proc. Lecture Notes 46, pp. 159–166. Providence: Amer. Math. Soc., 2008.

[Balog et al. 07] A. Balog, A. Cojocaru, and C. David. "Average Twin Prime Conjecture for Elliptic Curves." arXiv:0709.1461, 2007.

[Cojocaru 05] A. C. Cojocaru. "Reductions of an Elliptic Curve with Almost Prime Orders." *Acta Arith.* 119:3 (2005), 265–289.

[Cojocaru et al. 09] A. C. Cojocaru, F. Luca, and I. E. Shparlinski. "Pseudoprime Reductions of Elliptic Curves." *Math. Proc. Cambridge Philos. Soc.* 146:3 (2009), 513–522.

[Deuring 41] M. Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper." *Abh. Math. Sem. Hansischen Univ.* 14 (1941), 197–272.

[Friedlander and Shparlinski 09] J. Friedlander and I. Shparlinski. "Elliptic Twin Prime Conjecture." In *Proc. 2nd Intern. Workshop Coding and Cryptology, Zhangjiajie*, Lecture Notes in Comput. Sci. 5557, pp. 77–81. Berlin: Springer, 2009.

[García et al. 04] M. García, J. M. Pedersen, and H. te Riele. "Amicable Pairs, a Survey." In *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Inst. Commun. 41, pp. 179–196. Providence: Amer. Math. Soc., 2004.

[Hartshorne 77] R. Hartshorne. *Algebraic Geometry*, Graduate Texts in Mathematics 52. New York: Springer-Verlag, 1977.

[Ireland and Rosen 90] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, 2nd edition, Graduate Texts in Mathematics 84. New York: Springer-Verlag, 1990.

[Jiménez Urroz 08] J. Jiménez Urroz. "Almost Prime Orders of CM Elliptic Curves Modulo p." In *Algorithmic Number Theory*, Lecture Notes in Comput. Sci. 5011, pp. 74–87. Berlin: Springer, 2008.

[Jones 09] N. Jones. "Averages of Elliptic Curve Constants." *Math. Ann.* 345:3 (2009), 685–710.

[Jones 10] N. Jones. "Almost Prime Orders of Elliptic Curves with CM Modulo p," an appendix to "Geometry and Arithmetic of Verbal Dynamical Systems on Simple Groups," by T. Bandman, F. Grunewald, and B. Kunyaavskii. *Groups Geom. Dyn.* 4 (2010), 607–655.

[Koblitz 88] N. Koblitz. "Primality of the Number of Points on an Elliptic Curve over a Finite Field." *Pacific J. Math.* 131:1 (1988), 157–165.

[Kowalski 06] E. Kowalski. "Analytic Problems for Elliptic Curves." *J. Ramanujan Math. Soc.* 21:1 (2006), 19–114.

[Lang and Trotter 76] S. Lang and H. Trotter. *Frobenius Distributions in* GL_2*-Extensions*, Lecture Notes in Mathematics 504. Berlin: Springer-Verlag, 1976.

[Lemmermeyer 00] F. Lemmermeyer. *Reciprocity Laws: From Euler to Eisenstein*, Springer Monographs in Mathematics. Berlin: Springer-Verlag, 2000.

[Mazur 72] B. Mazur. "Rational Points of Abelian Varieties with Values in Towers of Number Fields." *Invent. Math.* 18 (1972), 183–266.

[Murty and Murty 87] M. R. Murty and V. K. Murty. "A Variant of the Bombieri–Vinogradov Theorem." In *Number Theory (Montreal, Que., 1985)*, CMS Conf. Proc. 7, pp. 243–272. Providence: Amer. Math. Soc., 1987.

[Olson 76] L. D. Olson. "Hasse Invariants and Anomalous Primes for Elliptic Curves with Complex Multiplication." *J. Number Theory* 8:4 (1976), 397–414.

[Olson 79] L. D. Olson. "The Trace of Frobenius for Elliptic Curves with Complex Multiplication." In *Algebraic Geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, Lecture Notes in Math. 732, pp. 454–476. Berlin: Springer, 1979.

[Rubin and Silverberg 09] K. Rubin and A. Silverberg. "Point Counting on Reductions of CM Elliptic Curves." *J. Number Theory* 129:12 (2009), 2903–2923.

[Rück 87] H.-G. Rück. "A Note on Elliptic Curves over Finite Fields." *Math. Comp.* 49:179 (1987), 301–304.

[Sakagawa 08] H. Sakagawa. "Study of Group Orders of Elliptic Curves." *J. Math. Kyoto Univ.* 48:4 (2008), 725–746.

[Satoh and Araki 98] T. Satoh and K. Araki. "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves." *Comment. Math. Univ. St. Paul.* 47:1 (1998), 81–92.

[Semaev 98] I. A. Semaev. "Evaluation of Discrete Logarithms in a Group of p-Torsion Points of an Elliptic Curve in Characteristic p." *Math. Comp.* 67:221 (1998), 353–356.

[Shimura 94] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*, Publications of the Mathematical Society of Japan 11. Princeton: Princeton University Press, 1994.

[Silverman 94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151. New York: Springer-Verlag, 1994.

[Silverman 09] J. H. Silverman. *The Arithmetic of Elliptic Curves*, second edition, Graduate Texts in Mathematics 106. New York: Springer, 2009.

[Silverman and Stange 11] J. H. Silverman and K. E. Stange. "Terms in Elliptic Divisibility Ssequences Divisible by Their Indices." *Acta Arithmetica* 146:4 (2011), 355–378.

[Smart 99] N. P. Smart. "The Discrete Logarithm Problem on Elliptic Curves of Trace One." *J. Cryptology* 12:3 (1999), 193–196.

[Smyth 10] C. Smyth. "Lucas Sequence Terms Divisible by Their Indices." *Journal of Integer Sequences* 13 (2010), Article 10.2.4, available online (http://www.cs.uwaterloo.ca/journals/JIS/VOL13/Smyth/smyth2.html).

[Taylor 08] R. Taylor. "Automorphy of Some ℓ-adic Lifts of Automorphic Mod-ℓ Representations II." *Pub. Math. IHES* 108 (2008), 183–239.

[Te Riele 82] H. J. J. te Riele. "Perfect Numbers and Aliquot Sequences." In *Computational Methods in Number Theory, Part I*, Math. Centre Tracts 154, pp. 141–157. Amsterdam: Math. Centrum, 1982.

[Waterhouse 69] W. C. Waterhouse. "Abelian Varieties over Finite Fields." *Ann. Sci. École Norm. Sup. (4)* 2 (1969), 521–560.

[Yan 96] S. Y. Yan. *Perfect, Amicable and Sociable Numbers: A Computational Approach*. River Edge, NJ: World Scientific, 1996.

[Zywina 09] D. Zywina. "A Refinement of Koblitz's Conjecture." arXiv:0909.5280, 2009.

Joseph H. Silverman, Mathematics Department, Box 1917 Brown University, Providence, RI 02912, USA (jhs@math.brown.edu)

Katherine E. Stange, Department of Mathematics, Stanford University, 450 Serra Mall, Building 380, Stanford, CA 94305, USA (stange@math.stanford.edu)

Received December 22, 2009; accepted July 8, 2010.