ELLIPTIC ALIQUOT CYCLES OF FIXED LENGTH

NATHAN JONES

Abstract. Silverman and Stange define the notion of an aliquot cycle of length L for a fixed elliptic curve E over $\mathbb{Q}$, and conjecture an order of magnitude for the function which counts such aliquot cycles. In the present note, we combine heuristics of Lang-Trotter with those of Koblitz to refine their conjecture to a precise asymptotic formula by specifying the appropriate constant. We give a criterion for positivity of the conjectural constant, as well as some numerical evidence for our conjecture.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and fix a positive integer $L \geq 2$. In analogy with the classical notion of an aliquot cycle, Silverman and Stange [10] define an L-tuple $(p_1, p_2, \dots, p_L)$ of distinct positive integers to be an **aliquot cycle of length L for** E if each p_i is a prime number of good reduction for E and

$$p_{i+1} = |E(\mathbb{F}_{p_i})| \quad \forall i \in \{1, 2, \dots, L-1\} \quad \text{and} \quad p_1 = |E(\mathbb{F}_{p_L})|,$$

which may be more succinctly written as

$$p_{i+1} = |E(\mathbb{F}_{p_i})|, \quad \forall i \in \mathbb{Z}/L\mathbb{Z}. \tag{1}$$

When $L = 2$, an aliquot cycle is also referred to as an **amicable pair for** E. As observed in [10, Remark 1.5], there is an intimate connection between aliquot cycles for E and elliptic divisibility sequences, which relate to generalizations of classical index divisibility questions about Lucas sequences. Thus, it is of interest to know how common such aliquot cycles are, so we consider the function which counts aliquot cycles of fixed length for a fixed elliptic curve E over $\mathbb{Q}$. More precisely, define an aliquot cycle $(p_1, p_2, \dots, p_L)$ to be **normalized** if $p_1 = \min\{p_i : 1 \leq i \leq L\}$, and then write

$$\pi_{E,L}(x) := |\{p_1 \leq x : \exists \text{ a normalized aliquot cycle } (p_1, p_2, \dots, p_L) \text{ for } E\}|.$$

Conjecture 1.1. *(Silverman-Stange) Let E be an elliptic curve over $\mathbb{Q}$ and $L \geq 2$ a fixed integer, and assume that there are infinitely many primes p such that $|E(\mathbb{F}_p)|$ is prime. Then, as $x \to \infty$, one has*

$$\pi_{E,L}(x) \quad \begin{cases} \asymp \frac{\sqrt{x}}{(\log x)^L} & \text{if } E \text{ has no CM} \\ \sim A_E \frac{x}{(\log x)^2} & \text{if } E \text{ has CM and } L = 2, \end{cases}$$

where the implied constants in $\asymp$ are both positive and depend only on E and L, and A_E is a precise positive constant.

Remark 1.2. We may interpret the $L = 1$ case of (1) as describing primes p_1 for which $p_1 = |E(\mathbb{F}_{p_1})|$. Such primes are called **anomalous** primes and have been considered by Mazur [7]. The asymptotic count for anomalous primes up to x is a special case of a conjecture of Lang and Trotter [6].

In [10], Silverman and Stange focus on the intricacies of the CM case, proving that if E has CM, $j_E \neq 0$ and $L \geq 3$, then E any normalized aliquot cycle $(p_1, p_2, \dots, p_L)$ for E must have $p_1 < 5$ (so in particular, $\pi_{E,L}(x) = O(1)$). The case $j_E = 0$ is apparently more complicated, and no proof is given that $\pi_{E,L}(x) = O(1)$ when $j_E = 0$ and $L > 3$.

In this note, we refine Conjecture 1.1 to an asymptotic formula in the non-CM case. Heuristics will be developed which lead to the following conjecture.

E	$x = 10^6$	$x = 10^8$	$x = 10^{10}$	$x = 10^{12}$
$E_1 : y^2 + y = x^3 - x$	0	1	16	115
$E_2 : y^2 = x^3 + 6x - 2$	0	5	32	208
$E_3 : y^2 = x^3 - 3x + 4$	0	0	0	0

Table 1: Values of $\pi_{E,2}(x)$

Conjecture 1.3. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and $L \geq 2$ a fixed integer. Then there is a non-negative real constant $C_{E,L} \geq 0$ (see (7) below) so that, as $x \longrightarrow \infty$,*

$$\pi_{E,L}(x) \sim C_{E,L} \int_2^x \frac{1}{2\sqrt{t}(\log t)^L} dt. \tag{2}$$

Remark 1.4. It is possible for the constant $C_{E,L}$ to be zero, in which case $\lim_{x\to\infty} \pi_{E,L}(x)$ is provably finite. Thus, in case $C_{E,L} = 0$, let us interpret the above asymptotic to mean that $\lim_{x\to\infty} \pi_{E,L}(x) < \infty$.

Remark 1.5. By integration by parts, one has

$$\int_2^x \frac{1}{2\sqrt{t}(\log t)^L} dt \ = \ \frac{\sqrt{x}}{(\log x)^L} + O\left(\frac{\sqrt{x}}{(\log x)^{L+1}}\right).$$

Thus, Conjecture 1.3 is consistent with Conjecture 1.1. In practice, the error term $\left|\pi_{E,L}(x) - C_{E,L} \displaystyle\int_2^x \frac{1}{2\sqrt{t}(\log t)^L} dt\right|$ should be smaller than $\left|\pi_{E,L}(x) - C_{E,L} \dfrac{\sqrt{x}}{(\log x)^L}\right|$, just as in the case of the prime number theorem.

Consider Table 1, which lists the values of $\pi_{E,2}(x)$ for a few non-CM curves E and various magnitudes x. Note that $\pi_{E_2,2}(x)$ is larger than $\pi_{E_1,2}(x)$. This difference is explained by the associated constants appearing in Conjecture 1.3. Indeed, a computation shows that

$$\frac{C_{E_2,2}}{C_{E_1,2}} \approx 1.714.$$

Also note that $\pi_{E_3,2}(10^{12}) = 0$. The additional fact that $|\{p \leq 10^6 : |E_3(\mathbb{F}_p)| \text{ is prime}\}| = 3236$ indicates that there probably are infinitely many primes p for which $|E_3(\mathbb{F}_p)|$ is prime, in which case the above data suggests that E_3 might be a counterexample to Conjecture 1.1. We will later see that $C_{E_3,2} = 0$, and that E_3 is indeed a counterexample, assuming a conjecture of Koblitz on the primality of $|E(\mathbb{F}_p)|$.

Remark 1.6. The heuristics which lead to Conjecture 1.3 are in the style of Koblitz and Lang-Trotter, whose conjectures have been proven "on average over elliptic curves E" (see [1] and [2]). It might be interesting to see if one could also prove an average version of Conjecture 1.3.

1.1. **Positivity of $C_{E,L}$ and a directed graph $\mathcal{G}_E$.** In the interest of characterizing the elliptic curves which have infinitely many aliquot cycles of length L, we will state a graph-theoretic criterion for positivity of $C_{E,L}$. Recall that a **directed graph** $\mathcal{G}$ is a pair $(\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \mathcal{V}(\mathcal{G})$ is an arbitrary set of **vertices** and $\mathcal{E} = \mathcal{E}(\mathcal{G}) \subseteq \mathcal{V} \times \mathcal{V}$ is a subset of **directed edges**. Finally, the sequence of vertices $(v_1, v_2, v_3, \ldots, v_n)$ is a **closed walk of length** n if and only if $(v_i, v_{i+1}) \in \mathcal{E}$, for each $i \in \mathbb{Z}/n\mathbb{Z} = \{1, 2, 3, \ldots, n\}$. Note that closed walks may have repeated vertices. For instance, if $(v, v) \in \mathcal{E}$ for some vertex v (i.e. if $\mathcal{G}$ has a *loop* at a vertex v), then $\mathcal{G}$ has closed walks of any length.

We will associate to an elliptic curve E a directed graph $\mathcal{G}_E$. First, consider the n-th division field $\mathbb{Q}(E[n])$ of E, obtained by adjoining to $\mathbb{Q}$ the x and y-coordinates of the n-torsion $E[n]$ of a given Weierstrass model of E. The extension $\mathbb{Q}(E[n])$ is Galois over $\mathbb{Q}$, and once we fix a basis over $\mathbb{Z}/n\mathbb{Z}$ of $E[n]$, we may view

$$\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \subseteq GL_2(\mathbb{Z}/n\mathbb{Z}). \tag{3}$$

We will now attach to $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ a directed graph $\mathcal{G}_E(n)$. Viewing Galois automorphisms as 2×2 matrices via (3), the vertex set $\mathcal{V}(n)$ of our graph $\mathcal{G}_E(n)$ is

$$\mathcal{V}(n) := \{(t, d) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times : \exists g \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \text{ with } \mathrm{tr}\, g = t, \det g = d\}.$$

We define the edge set $\mathcal{E}(n)$ by declaring that $(v_1, v_2) \in \mathcal{E}$ if and only if $d_1 + 1 - t_1 = d_2$, where $v_i = (t_i, d_i) \in \mathcal{V}(n)$.

Let m_E denote the **torsion conductor** of E, which is defined as the smallest positive integer m for which

$$\forall n \in \mathbb{Z}_{>0}, \quad \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) = \pi^{-1}(\mathrm{Gal}(\mathbb{Q}(E[\gcd(m,n)])/\mathbb{Q})),$$

where $\pi : GL_2(\mathbb{Z}/n\mathbb{Z}) \to GL_2(\mathbb{Z}/\gcd(m,n)\mathbb{Z})$ is the canonical projection. (The existence of a torsion conductor m_E for a non-CM elliptic curve E is a celebrated theorem of Serre [9].) Finally, we define the directed graph $\mathcal{G}_E$ to be the above graph at level m_E:

$$\mathcal{G}_E := \mathcal{G}_E(m_E).$$

The following version of Conjecture 1.3 states a criterion for positivity of $C_{E,L}$ in terms of the directed graph $\mathcal{G}_E$.

Conjecture 1.7. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and $L \geq 2$ a fixed integer. Suppose that the directed graph $\mathcal{G}_E$ has a closed walk of length L. Then there are infinitely many aliquot cycles of length L for E. More precisely, there is a positive constant $C_{E,L} > 0$ so that, as $x \longrightarrow \infty$,*

$$\pi_{E,L}(x) \sim C_{E,L} \int_2^x \frac{1}{2\sqrt{t}(\log t)^L} dt.$$

Remark 1.8. If $\mathcal{G}_E$ does not have a closed walk of length L, then $C_{E,L} = 0$ and there are at most finitely many aliquot cycles of length L for E (see Proposition 2.6 below).

In Section 2, we will write down the constant $C_{E,L}$ explicitly as an "almost Euler product" and discuss its positivity in terms of the graph $\mathcal{G}_E$. In Section 3, we will develop the heuristics which lead to Conjecture 1.3. In Section 4, we will provide some numerical evidence for Conjecture 1.3 by examining the order of magnitude of $\pi_{E,L}(x) - C_{E,L} \displaystyle\int_2^x \frac{1}{2\sqrt{t}\log^L t}\, dt$ for various elliptic curves E and $L = 2$.

2. The constant

We now describe in detail the constant $C_{E,L}$. The following lemma allows us to interpret (1) in terms of the Frobenius automorphisms[1] $\mathrm{Frob}_{\mathbb{Q}(E[n])}(p_i) \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ attached to the various primes p_i. Recall the trace of Frobenius $a_p(E) \in \mathbb{Z}$, which is defined by

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

Lemma 2.1. *For any positive integer n and any prime p of good reduction for E which does not divide n, p is unramified in $\mathbb{Q}(E[n])$ and for any Frobenius automorphism $\mathrm{Frob}_{\mathbb{Q}(E[n])}(p) \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$, we have*

$$\mathrm{tr}(\mathrm{Frob}_{\mathbb{Q}(E[n])}(p)) \equiv a_E(p) \mod n$$

and

$$\det(\mathrm{Frob}_{\mathbb{Q}(E[n])}(p)) \equiv p \mod n.$$

Proof. See [8, IV-4–IV-5]. □

For any subset $G \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$, define

$$G^L_{\text{ali-cycle}} := \left\{(g_1, g_2, \ldots, g_L) \in G^L : \ \forall i \in \mathbb{Z}/L\mathbb{Z}, \det(g_{i+1}) = \det(g_i) + 1 - \mathrm{tr}(g_i)\right\}. \tag{4}$$

Note that, by Lemma 2.1, if $(p_1, p_2, \ldots, p_L)$ is an aliquot cycle of length L for E, then

$$(\mathrm{Frob}_{\mathbb{Q}(E[n])}(p_1), \mathrm{Frob}_{\mathbb{Q}(E[n])}(p_2), \ldots, \mathrm{Frob}_{\mathbb{Q}(E[n])}(p_L)) \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-cycle}}. \tag{5}$$

[1]The Frobenius automorphism in $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ attached to an unramified rational prime p is only defined up to conjugation in $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. Here and throughout the paper, we understand $\mathrm{Frob}_{\mathbb{Q}(E[n])}(p)$ to be any choice of such a Frobenius automorphism.

Next, let $\phi(x) := \frac{2}{\pi}\sqrt{1-x^2}$ be the distribution function of Sato-Tate, which (assuming E has no CM) conjecturally[2] satisfies

$$\lim_{x\to\infty} \frac{|\{p \le x : \frac{a_p(E)}{2\sqrt{p}} \in I \subseteq [-1,1]\}|}{|\{p \le x\}|} = \int_I \phi(x)dx.$$

In other words, ϕ is the density function of $a_p(E)/2\sqrt{p}$, viewed as a random variable. Denote by $\phi_L := \phi * \phi * \cdots * \phi$ the L-fold convolution of ϕ with itself, which is the density function of the random variable

$$\sum_{i=1}^{L} \frac{a_{p_i}(E)}{2\sqrt{p_i}},$$

provided the various terms $a_{p_i}(E)/2\sqrt{p_i}$ are statistically independent. Finally, for a positive integer k, put

$$n_k := \prod_{p \le k} p^k. \tag{6}$$

In Section 3, we will develop heuristics which predict Conjecture 1.3, with

$$C_{E,L} := \frac{\phi_L(0)}{L} \cdot \lim_{k\to\infty} \frac{n_k^L |\operatorname{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L_{\text{ali-cycle}}|}{|\operatorname{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L|}. \tag{7}$$

2.1. **The constant as a product.** We will presently prove the following proposition, which gives a more explicit expression of $C_{E,L}$ as a convergent Euler product. Recall that m_E denotes the torsion conductor of E, i.e. the smallest positive integer m for which

$$\forall n \in \mathbb{Z}_{>0}, \quad \operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) = \pi^{-1}(\operatorname{Gal}(\mathbb{Q}(E[\gcd(m,n)])/\mathbb{Q})),$$

where $\pi : GL_2(\mathbb{Z}/n\mathbb{Z}) \to GL_2(\mathbb{Z}/\gcd(m,n)\mathbb{Z})$ is the canonical projection.

Proposition 2.2. *For a positive integer k, let $n_k := \prod_{p\le k} p^k$. Then one has*

$$\lim_{k\to\infty} \frac{n_k^L |\operatorname{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L_{ali\text{-}cycle}|}{|\operatorname{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L|} = \frac{m_E^L |\operatorname{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{ali\text{-}cycle}|}{|\operatorname{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L|} \cdot \prod_{\ell \nmid m_E} \frac{\ell^L |GL_2(\mathbb{F}_\ell)^L_{ali\text{-}cycle}|}{|GL_2(\mathbb{F}_\ell)^L|}$$

Furthermore,

$$0 < \frac{\ell^L |GL_2(\mathbb{F}_\ell)^L_{ali\text{-}cycle}|}{|GL_2(\mathbb{F}_\ell)^L|} = 1 + O_L\left(\frac{1}{\ell^2}\right), \tag{8}$$

so the infinite product $\prod_{\ell\nmid m_E} \frac{\ell^L |GL_2(\mathbb{F}_\ell)^L_{ali\text{-}cycle}|}{|GL_2(\mathbb{F}_\ell)^L|}$ converges absolutely.

The proof of Proposition 2.2 involves the following two lemmas.

Lemma 2.3. *Let n_1 and n_2 be relatively prime positive integers, and pick any subgroups $G_1 \subseteq GL_2(\mathbb{Z}/n_1\mathbb{Z})$ and $G_2 \subseteq GL_2(\mathbb{Z}/n_2\mathbb{Z})$. Then, viewing $G_1 \times G_2 \subseteq GL_2(\mathbb{Z}/n_1n_2\mathbb{Z})$, one has*

$$(G_1 \times G_2)^L_{ali\text{-}cycle} = (G_1)^L_{ali\text{-}cycle} \times (G_2)^L_{ali\text{-}cycle}.$$

Proof of Lemma 2.3. Let $\iota : GL_2(\mathbb{Z}/n_1\mathbb{Z}) \times GL_2(\mathbb{Z}/n_2\mathbb{Z}) \to GL_2(\mathbb{Z}/n_1n_2\mathbb{Z})$ be the isomorphism of the chinese remainder theorem, and set $G := \iota(G_1 \times G_2)$. For each L-tuple $(g_i)_i \in G^L$, we have

$$\forall i \in \mathbb{Z}/L\mathbb{Z} \ \det g_{i+1} \equiv \det g_i + 1 - \operatorname{tr} g_i \pmod{n_1n_2} \iff \forall i \in \mathbb{Z}/L\mathbb{Z} \begin{array}{l} \det g_{i+1} \equiv \det g_i + 1 - \operatorname{tr} g_i \pmod{n_1} \\ \det g_{i+1} \equiv \det g_i + 1 - \operatorname{tr} g_i \pmod{n_2}. \end{array}$$

This implies the conclusion of Lemma 2.3. □

[2]Assuming E has non-integral j-invariant, the Sato-Tate conjecture is now a theorem of L. Clozel, M. Harris, N. Shepherd-Barron, and R. Taylor (see [11] and the references therein).

Lemma 2.4. *Let n be a positive integer and n' any multiple of n such that, for every prime numbur ℓ, $\ell \mid n' \Rightarrow \ell \mid n$. Let $\pi : GL_2(\mathbb{Z}/n'\mathbb{Z}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$ denote the canonical projection and let $G \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$ be any subgroup. Then one has*

$$\frac{(n')^L|(\pi^{-1}(G))^L_{ali\text{-}cycle}|}{|\pi^{-1}(G)^L|} = \frac{n^L|G^L_{ali\text{-}cycle}|}{|G^L|}. \tag{9}$$

Proof of Lemma 2.4. By induction, it suffices to check the case $n' = \ell n$, where ℓ is some prime dividing n. In this case, since $|\pi^{-1}(G)| = \ell^4|G|$, (9) is equivalent to

$$|(\pi^{-1}(G))^L_{\text{ali-cycle}}| = \ell^{3L}|G^L_{\text{ali-cycle}}|, \tag{10}$$

which we now show. Fix an element $g = (g_1, g_2, \ldots, g_L) \in G^L_{\text{ali-cycle}}$, and note that any element $g' \in \pi^{-1}(g)$ has the form

$$g' = (g'_1, g'_2, \ldots, g'_L) = (\tilde{g}_1(I + nA_1), \tilde{g}_2(I + nA_2), \ldots, \tilde{g}_L(I + nA_L)) \in \pi^{-1}(g),$$

where for each i, $\tilde{g}_i$ is any fixed lift to $GL_2(\mathbb{Z}/\ell n\mathbb{Z})$ of g_i, and $A_i \in M_{2\times 2}(\mathbb{F}_\ell)$ is arbitrary. We will presently determine the exact conditions on the A_i which force $(g'_1, g'_2, \ldots, g'_L) \in (\pi^{-1}(G))^L_{\text{ali-cycle}}$. First note that, since $(g_1, g_2, \ldots, g_L) \in G^L_{\text{ali-cycle}}$, we must have

$$\forall i \in \mathbb{Z}/L\mathbb{Z}, \quad g_i \pmod{\ell} \notin \{0, I\}, \tag{11}$$

and furthermore, the quantity

$$\gamma_i := \frac{\det \tilde{g}_{i+1} - \det \tilde{g}_i - 1 + \operatorname{tr} \tilde{g}_i}{n} \in \mathbb{F}_\ell$$

is well-defined. One checks that

$$\det g'_{i+1} \equiv \det g'_i + 1 - \operatorname{tr} g'_i \mod \ell n \iff \gamma_i \equiv -\det g_{i+1} \cdot \operatorname{tr} A_{i+1} + \det g_i \cdot \operatorname{tr} A_i - \operatorname{tr}(g_i A_i) \mod \ell. \tag{12}$$

The condition on the right-hand side is (affine) linear in the coefficients of A_{i+1} and A_i. We consider the linear transformation

$$\begin{aligned} T : \mathbb{F}_\ell^{4L} \simeq M_{2\times 2}(\mathbb{F}_\ell)^L &\to \mathbb{F}_\ell^L \\ (A_i) &\mapsto (-\det g_{i+1} \cdot \operatorname{tr} A_{i+1} + \det g_i \cdot \operatorname{tr} A_i - \operatorname{tr}(g_i A_i)). \end{aligned}$$

In light of (12), the condition (10) will follow from the surjectivity of the above linear transformation, which we now verify. Writing coordinates as

$$g_i =: \begin{pmatrix} x_i & y_i \\ z_i & w_i \end{pmatrix} \quad \text{and} \quad A_i =: \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix},$$

we have

$$T((A_i)) = ((\det g_i - x_i)a_i + (\det g_i - w_i)d_i - y_i c_i - z_i b_i - \det g_{i+1} a_{i+1} - \det g_{i+1} d_{i+1}).$$

By (11), at least one of $\det g_i - x_i$, $\det g_i - w_i$, y_i and z_i must be non-zero modulo ℓ, and so

$$T(\{0\} \times \cdots \times \{0\} \times M_{2\times 2}(\mathbb{F}_\ell) \times \{0\} \times \cdots \times \{0\}) = \{0\} \times \cdots \times \{0\} \times \mathbb{F}_\ell \times \{0\} \times \cdots \times \{0\},$$

where the non-zero entries correspond to the same index i. In particular, the linear transformation in question is surjective and we have verified (10), finishing the proof of Lemma 2.4. □

Proof of Proposition 2.2. Choose k large enough so that $m_E \mid n_k$, and write $n_k = n_k^{(1)} \cdot n_k^{(2)}$, where $n_k^{(1)}$ is divisible by primes dividing m_E and $\gcd(m_E, n_k^{(2)}) = 1$. By definition of m_E, we then have

$$\operatorname{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q}) \simeq \pi^{-1}(\operatorname{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})) \times \prod_{\substack{\ell^k \| n_k \\ \ell \nmid m_E}} GL_2(\mathbb{Z}/\ell^k\mathbb{Z}),$$

where $\pi : GL_2(\mathbb{Z}/n_k^{(1)}\mathbb{Z}) \to GL_2(\mathbb{Z}/m_E\mathbb{Z})$ is the canonical projection. By Lemmas 2.3 and 2.4, we have

$$\frac{n_k^L|\operatorname{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L_{\text{ali-cycle}}|}{|\operatorname{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L|} = \frac{m_E^L|\operatorname{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}}|}{|\operatorname{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L|} \cdot \prod_{\substack{\ell \mid n_k \\ \ell \nmid m_E}} \frac{\ell^L|\operatorname{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})^L_{\text{ali-cycle}}|}{|\operatorname{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})^L|}.$$

Taking the limit as $k \to \infty$, we arrive at the product representation of $C_{E,L}$ stated in Proposition 2.2. We leave the verification of (8) as an exercise. □

2.2. **Positivity of the constant.** We will now discuss the positivity of $C_{E,L}$. The following corollary of Proposition 2.2 is immediate.

Corollary 2.5. *One has*

$$C_{E,L} > 0 \iff \mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{ali\text{-}cycle} \neq \emptyset. \tag{13}$$

We will now prove the following proposition, which allows one to deduce Conjecture 1.7 from Conjecture 1.3.

Proposition 2.6. *For any non-CM elliptic curve E over $\mathbb{Q}$, one has*

$$C_{E,L} > 0 \iff \mathcal{G}_E \text{ has a closed walk of length } L. \tag{14}$$

Furthermore, if $\mathcal{G}_E$ has no closed walks of length L, then there are only finitely many aliquot cycles $(p_1, p_2, \ldots, p_L)$ of length L for E.

Proof. First we prove (14). By Corollary 2.5, we are reduced to showing that

$$\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} \neq \emptyset \iff \mathcal{G}_E \text{ has a closed walk of length } L. \tag{15}$$

The mapping

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q}) &\to \mathcal{V}(\mathcal{G}_E) \\ g &\mapsto (\operatorname{tr} g, \det g) \end{aligned}$$

induces a mapping $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} \longrightarrow \{\text{closed walks of length } L \text{ in } \mathcal{G}_E\}$. Thus, if $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} \neq \emptyset$ then $\mathcal{G}_E$ has a closed walk of length L. Conversely, suppose $\mathcal{G}_E$ has a closed walk $(v_1, v_2, v_3, \ldots, v_L)$ of length L. Recall that $\mathcal{V} = \mathbb{Z}/m_E\mathbb{Z} \times (\mathbb{Z}/m_E\mathbb{Z})^\times$ and write $v_i = (t_i, d_i)$. Choosing any element $g_i \in \mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})$ with $\operatorname{tr} g_i = t_i$ and $\det g_i = d_i$, we have then constructed an element $(g_1, g_2, \ldots, g_L) \in \mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}}$, so that $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} \neq \emptyset$. By Corollary 2.5, we conclude the proof of (14).

To see why the nonexistence of closed walks of length L in $\mathcal{G}_E$ implies that $\lim_{x\to\infty} \pi_{E,L}(x) < \infty$, note first that, by (15), one has that $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} = \emptyset$. But then (5) implies that $\lim_{x\to\infty} \pi_{E,L}(x) < \infty$, and the proof of Proposition 2.6 is complete. □

3. Heuristics

We will construct a probabilistic model in the style of Koblitz [5] and Lang-Trotter [6]. We shall call the L-tuple $(p_1, p_2, \ldots, p_L)$ of distinct prime numbers an **aliquot sequence of length L for E** if it satisfies

$$p_{i+1} = |E(\mathbb{F}_{p_i})| \quad \forall i \in \{1, 2, \ldots L-1\}.$$

Thus, an aliquot cycle of length L is an aliquot sequence of length L which additionally satisfies $p_1 = |E(\mathbb{F}_{p_L})|$. Suppose that $(p_1, p_2, \ldots, p_L)$ is an aliquot sequence of length L for E. By substituting $p_2 = p_1 + 1 - a_{p_1}(E)$ into the equation $p_3 = p_2 + 1 - a_{p_2}(E)$, one finds that $p_3 = p_1 + 2 - (a_{p_1}(E) + a_{p_2}(E))$, and continuing in this manner one obtains

$$p_1 = |E(\mathbb{F}_{p_L})| \iff \sum_{j=1}^{L} a_{p_j}(E) = L. \tag{16}$$

Thus, a given L-tuple $(p_1, p_2, \ldots, p_L)$ of positive integers is an aliquot cycle of length L for E if and only if the following conditions hold:

(1_L) The L-tuple $(p_1, p_2, \ldots, p_L)$ is an aliquot sequence of length L for E.

(2_L) One has $\displaystyle\sum_{j=1}^{L} a_{p_j}(E) = L$.

Consider the following condition, which generalizes condition (2_L) above by replacing L with an arbitrary fixed integer r:

$(2'_L)$ One has $\displaystyle\sum_{j=1}^{L} a_{p_j}(E) = r.$

We will now develop the heuristic "probability" that a given L-tuple $(p_1, p_2, \ldots, p_L)$ of positive integers satisfies (1_L) and $(2'_L)$. First, we must gather some notation. Fix a positive integer n and elements $a, b \in \mathbb{Z}/n\mathbb{Z}$. For any subset $S \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$, let

$$\begin{aligned} S_{\mathcal{N}=a} &:= \{g \in S : \det(g) + 1 - \operatorname{tr}(g) = a\} \\ S^{\det=b} &:= \{g \in S : \det(g) = b\} \\ S^{\det=b}_{\mathcal{N}=a} &:= S_{\mathcal{N}=a} \cap S^{\det=b}. \end{aligned}$$

Finally, for $L \geq 1$ and $G \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$, put

$$G^L_{\text{ali-sequence}} := \left\{(g_1, g_2, \ldots, g_L) \in G^L : \forall i \in \{1, 2, \ldots, L-1\}, \det(g_{i+1}) = \det(g_i) + 1 - \operatorname{tr}(g_i)\right\}.$$

Note that if $L = 1$, the defining conditions become empty and we have $G^{L=1}_{\text{ali-seqence}} = G$. For a general $L \geq 1$, note that any aliquot sequence $(p_1, p_2, \ldots, p_L)$ for E will satisfy

$$(\operatorname{Frob}_{\mathbb{Q}(E[n])}(p_1), \operatorname{Frob}_{\mathbb{Q}(E[n])}(p_2), \ldots \operatorname{Frob}_{\mathbb{Q}(E[n])}(p_L)) \in \operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-sequence}}.$$

Finally, for a fixed integer r, define

$$G^{L,\sum \operatorname{tr}=r}_{\text{ali-sequence}} := \left\{(g_1, g_2, \ldots, g_L) \in G^L_{\text{ali-sequence}} : \sum_{i=1}^{L} \operatorname{tr}(g_i) \equiv r \mod n\right\}.$$

We will presently derive an expression for the probability

$$\mathcal{P}_{(1_L),(2'_L)}(t) := \operatorname{Prob}\left((p_1, p_2, \ldots, p_L) \text{ satisfies } (1_L) \text{ and } (2'_L), \text{ given that } p_1 \approx t\right),$$

Putting $\mathcal{P}_{(1_L)}(t)$ for the probability that $(p_1, p_2, \ldots, p_L)$ satisfies (1_L) above, and $\mathcal{P}^{\text{given } (1_L)}_{(2'_L)}(t)$ for the conditional probability that $(p_1, p_2, \ldots, p_L)$ satisfies $(2'_L)$, given that it satisfies (1_L), we have

$$\mathcal{P}_{(1_L),(2'_L)}(t) = \mathcal{P}_{(1_L)}(t) \cdot \mathcal{P}^{\text{given } (1_L)}_{(2'_L)}(t). \tag{17}$$

In Section 3.1 below, we will derive the probability formula

$$\mathcal{P}_{(1_L)}(t) \approx \frac{n^{L-1} \cdot |\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-sequence}}|}{|\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L|} \cdot \frac{1}{(\log t)^L}. \tag{18}$$

Following this, in Section 3.2, we will derive

$$\mathcal{P}^{\text{given } (1_L)}_{(2'_L)}(t) \approx \phi_L\left(\frac{r}{2\sqrt{t}}\right) \frac{n \cdot |\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{L,\sum \operatorname{tr}=r}_{\text{ali-sequence}}|}{|\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-sequence}}|} \cdot \frac{1}{2\sqrt{t}}. \tag{19}$$

Before deriving (18) and (19), we will now observe that, taken together, they lead to Conjecture 1.3. Indeed, using (17), (18) and (19), one concludes

$$\mathcal{P}_{(1_L),(2'_L)}(t) \approx \phi_L\left(\frac{r}{2\sqrt{t}}\right) \cdot \frac{n^L |\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{L,\sum \operatorname{tr}=r}_{\text{ali-sequence}}|}{|\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L|} \cdot \frac{1}{2\sqrt{t}(\log t)^L}$$

Just as with (16), one verifies that, for each $(g_1, g_2, \ldots, g_L) \in GL_2(\mathbb{Z}/n\mathbb{Z})^L_{\text{ali-sequence}}$, one has

$$\det(g_L) + 1 - \operatorname{tr}(g_L) = \det g_1 \iff \sum_{i=1}^{L} \operatorname{tr}(g_i) \equiv L \mod n.$$

It follows that $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-cycle}} = \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{L,\sum \mathrm{tr}=L}_{\text{ali-sequence}}$. Thus, putting $r = L$, $n = n_k$ and taking the limit as $k \to \infty$, one arrives at

$$\mathcal{P}_{(1_L),(2_L)}(t) \approx \phi\left(\frac{L}{2\sqrt{t}}\right) \cdot \lim_{k\to\infty} \frac{n_k^L |\,\mathrm{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L_{\text{ali-cycle}}|}{|\,\mathrm{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L|} \cdot \frac{1}{2\sqrt{t}(\log t)^L}.$$

Thus, using

$$\pi_{E,L}(x) \approx \frac{1}{L}\int_2^x \mathcal{P}_{(1_L),(2_L)}(t)\,dt,$$

one arrives at Conjecture 1.3. The reason for the extra factor of L in the denominator above is that $\pi_{E,L}(x)$ counts *normalized* aliquot cycles, whereas the heuristic probabilities above do not take normalization into account. Also, since L is fixed, one verifies that the estimation $\phi(L/(2\sqrt{t})) \approx \phi(0)$ does not affect the asymptotic.

3.1. **The probability that $(p_1, p_2, \ldots, p_L)$ satisfies (1_L).** We will now derive a refined probability formula which implies (18). Fix a vector $\mathbf{a} = (a_2, a_3, \ldots, a_L) \in ((\mathbb{Z}/n\mathbb{Z})^\times)^{L-1}$, and consider the probability

$$\mathcal{P}^{\mathbf{a}}_{(1_L)}(t) := \mathrm{Prob}((p_1, p_2, \ldots p_L) \text{ satisfies } (1_L) \text{ and } \forall i \in \{2,3,\ldots,L\},\ p_i \equiv a_i \mod n)$$

and (for any subset $G \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$) the subset

$$G^{L,\mathbf{a}}_{\text{ali-sequence}} := \{(g_1, g_2, \ldots, g_L) \in G^L_{\text{ali-sequence}} : \forall i \in \{2,3,\ldots,L\},\ \det(g_i) = a_i\}.$$

In case $L = 1$, the vector $\mathbf{a} \in ((\mathbb{Z}/n\mathbb{Z})^\times)^0$ is non-existent, and as before we interpret the empty condition as $G^{1,\mathbf{a}}_{\text{ali-sequence}} = G$. Also note the decomposition

$$G^{L,\mathbf{a}}_{\text{ali-sequence}} = G_{\mathcal{N}=a_2} \times G^{\det=a_2}_{\mathcal{N}=a_3} \times G^{\det=a_3}_{\mathcal{N}=a_4} \times \cdots \times G^{\det=a_{L-1}}_{\mathcal{N}=a_L} \times G^{\det=a_L}. \tag{20}$$

Finally, note that if $\mathbf{a_1} \neq \mathbf{a_2}$, then $G^{L,\mathbf{a_1}}_{\text{ali-sequence}} \cap G^{L,\mathbf{a_2}}_{\text{ali-sequence}} = \emptyset$, and so we have a disjoint union

$$G^L_{\text{ali-sequence}} = \bigsqcup_{\mathbf{a}\in((\mathbb{Z}/n\mathbb{Z})^\times)^{L-1}} G^{L,\mathbf{a}}_{\text{ali-sequence}}.$$

For similar reasons, we have

$$\mathcal{P}_{(1_L)}(t) = \sum_{\mathbf{a}\in((\mathbb{Z}/n\mathbb{Z})^\times)^{L-1}} \mathcal{P}^{\mathbf{a}}_{(1_L)}(t).$$

Thus, (18) will follow from

$$\mathcal{P}^{\mathbf{a}}_{(1_L)}(t) \approx \frac{n^{L-1} \cdot |\,\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{L,\mathbf{a}}_{\text{ali-sequence}}|}{|\,\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L|} \cdot \frac{1}{(\log t)^L}, \tag{21}$$

which we will now derive by induction on L.

Base case: $L = 1$. Suppose that p_1 is a positive integer of size about t. One may interpret the prime number theorem as the probabilistic statement that

$$\mathcal{P}_{(1_{L=1})}(t) = \mathrm{Prob}(p_1 \text{ is prime}) \approx \frac{1}{\log t},$$

which is base case $L = 1$ of (21).

Induction step. Assume now that (21) holds for some fixed $L \geq 1$, and fix any vector $\mathbf{a} = (a_2, a_3, \ldots, a_{L+1}) \in ((\mathbb{Z}/n\mathbb{Z})^\times)^L$. Since the statement

$$\text{“}(p_1, p_2, \ldots p_{L+1}) \text{ satisfies } (1_{L+1}) \text{ and } \forall i \in \{2,3,\ldots,L+1\},\ p_i \equiv a_i \mod n\text{”}$$

is equivalent to

$$(p_1, p_2, \ldots p_L) \text{ satisfies } (1_L) \text{ and } \forall i \in \{2,3,\ldots,L\},\ p_i \equiv a_i \mod n$$
$$\text{and}$$
$$p_{L+1} := p_L + 1 - a_{p_L}(E) \text{ is prime, and } p_{L+1} \equiv a_{L+1} \mod n,$$

we see that

$$\mathcal{P}_{(1_{L+1})}^{(a_2,a_3,\ldots,a_L,a_{L+1})}(t) = \mathcal{P}_{(1_L)}^{(a_2,a_3,\ldots,a_L)}(t) \cdot \mathcal{P}(t), \tag{22}$$

where $\mathcal{P}(t)$ is the conditional probability that $p_{L+1} := p_L + 1 - a_{p_L}(E)$ is prime, and that $p_{L+1} \equiv a_{L+1} \mod n$, given that (1_L) holds. To estimate $\mathcal{P}(t)$, let us assume that (1_L) holds. First note that, by the Hasse bound $|a_p(E)| \leq 2\sqrt{p}$, one has

$$p_{L+1} = p_1 + L - \sum_{i=1}^{L} a_{p_i}(E) \in [p_1 + L - 2L\sqrt{p_{\max}}, p_1 + L + 2L\sqrt{p_{\max}}],$$

where $p_{\max} := \max\{p_i : i = 1, 2, \ldots, L\}$. By induction we have $p_{\max} = t + O_L(\sqrt{t})$, and so $p_{L+1} \approx t$, with an error of $O_L(\sqrt{t})$. Now, if p_{L+1} were a positive integer of size about t selected independently of $(p_1, p_2, \ldots, p_L)$, then

$$\text{Prob}(p_{L+1} \text{ is prime and } p_{L+1} \equiv a_{L+1} \mod n) \approx \frac{1}{\varphi(n)\log t}, \tag{23}$$

by the prime number theorem in arithmetic progressions. If the positive integer p_{L+1} were chosen randomly and independently of the previous primes, then the probability that $p_{L+1} \equiv a_{L+1} \mod n$ would be $1/n$. However, p_{L+1} is not chosen independently of $(p_1, p_2, \ldots, p_L)$; it is related to p_L by the formula $p_{L+1} = p_L + 1 - a_{p_L}(E)$. Thus, the congruence $p_{L+1} \equiv a_{L+1} \mod n$ is really the demand that $\text{Frob}_{\mathbb{Q}(E[n])}(p_L) \in \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})_{\mathcal{N}=a_{L+1}}$. Since we assume that (1_L) holds, we know that $\text{Frob}_{\mathbb{Q}(E[n])}(p_L) \in GL_2(\mathbb{Z}/n\mathbb{Z})^{\det=a_L}$. It is thus natural to multiply (23) by the correction factor

$$\frac{|\,\text{Gal}(\mathbb{Q}(E[n])\mathbb{Q})_{\mathcal{N}=a_{L+1}}^{\det=a_L}|/|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{\det=a_L}|}{1/n},$$

obtaining

$$\mathcal{P}(t) \approx \frac{|\,\text{Gal}(\mathbb{Q}(E[n])\mathbb{Q})_{\mathcal{N}=a_{L+1}}^{\det=a_L}|/|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{\det=a_L}|}{1/n} \cdot \frac{1}{\varphi(n)\log t} = \frac{n|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})_{\mathcal{N}=a_{L+1}}^{\det=a_L}|}{|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})|} \cdot \frac{1}{\log t}. \tag{24}$$

By (20), we may re-write (21) as

$$\mathcal{P}_{(1_L)}^{\mathbf{a}}(t) \approx n^{L-1} \cdot \frac{|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})_{\mathcal{N}=a_2}|}{|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})|} \cdot \left(\prod_{i=2}^{L-1} \frac{|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})_{\mathcal{N}=a_{i+1}}^{\det=a_i}|}{|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})|} \right) \cdot \frac{|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{\det=a_L}|}{|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})|} \cdot \frac{1}{(\log t)^L}.$$

Plugging this expression and (24) into (22), and using the fact that

$$|\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{\det=a_L}| = |\,\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{\det=a_{L+1}}|,$$

one concludes the induction step, completing the derivation of (21), and thus of (18).

As a byproduct of our analysis, we have motivated the following conjecture, wherein

$$\pi_E^{L\text{-ali-sequence}}(x) := |\{p_1 \leq x : \exists \text{ an aliquot sequence } (p_1, p_2, \ldots, p_L) \text{ for } E\}|$$

and

$$C_E^{L\text{-ali-sequence}} := \lim_{k \to \infty} \frac{n_k^{L-1} \cdot |\,\text{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})_{\text{ali-sequence}}^{L}|}{|\,\text{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^{L}|}.$$

Conjecture 3.1. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and $L \geq 2$ a fixed integer. Then as $x \longrightarrow \infty$, one has*

$$\pi_E^{L\text{-ali-sequence}}(x) \sim C_E^{L\text{-ali-sequence}} \int_2^x \frac{1}{(\log t)^L} dt. \tag{25}$$

Similarly to Proposition 2.6, one has

$$C_E^{L\text{-ali-sequence}} > 0 \iff \mathcal{G}_E \text{ has a (directed) walk of length } L.$$

3.2. **The conditional probability that $(p_1, p_2, \ldots, p_L)$ satisfies $(2'_L)$.** We will now derive (19), completing the heuristic derivation of Conjecture 1.3. Suppose that $(p_1, p_2, \ldots, p_L)$ is an aliquot sequence of length L for E, i.e. that it satisfies (1_L). What is the conditional probability that $\sum_{i=1}^{L} a_{p_i}(E) = r$? In the case $L = 1$, condition (1_L) is empty, and our question becomes identical to the Lang-Trotter conjecture for fixed Frobenius trace. In what follows, we will develop a probabilistic model in the same style as theirs.

Fixing a level n, the number $f_n(r, p) \geq 0$ will estimate the probability of the event that $\sum_{i=1}^{L} a_{p_i}(E) = r$, given that $(p = p_1, p_2, \ldots, p_L)$ is an aliquot sequence of length L for E. We will model the situation by assuming that the vector

$$(\mathrm{Frob}_{\mathbb{Q}(E[n])}(p_1), \mathrm{Frob}_{\mathbb{Q}(E[n])}(p_2), \ldots \mathrm{Frob}_{\mathbb{Q}(E[n])}(p_L)) \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-sequence}} \tag{26}$$

is randomly distributed according to counting measure, and we will assume that the various $\dfrac{a_{p_i}(E)}{2\sqrt{p_i}}$ are independent at infinity, i.e. that ϕ_L is the distribution function for $\sum_{i=1}^{L} \dfrac{a_{p_i}(E)}{2\sqrt{p_i}}$. We will also assume independence of the random variables $\sum_{i=1}^{L} \dfrac{a_{p_i}(E)}{2\sqrt{p_i}}$ and (26). Finally, in order to simplify our model, we will also regard all of the various primes p_i as having the same size, namely p. These considerations lead us to the following assumptions about the probabilities $f_n(r, p)$:

$$\begin{aligned} &f_n(r,p) = 0 \ \text{ if } \ |r| > 2L\sqrt{p} \\ &f_n(r,p) = \phi_L\left(\frac{r}{2\sqrt{p}}\right) \cdot \frac{n|\,\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{L,\sum \mathrm{tr}=r}_{\text{ali-sequence}}|}{|\,\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{L}_{\text{ali-sequence}}|} \cdot c_p \ \text{ if } \ |r| \leq 2L\sqrt{p}, \end{aligned} \tag{27}$$

where c_p is some constant chosen so that $\sum_{r \in \mathbb{Z}} f_n(r, p) = 1$. Then, similarly to [6, pp. 31–32], one concludes that $c_p \sim \dfrac{1}{2\sqrt{p}}$, as $p \to \infty$. This leads to (19), completing the derivation of Conjecture 1.3.

4. Examples

We will now give some numerical evidence for Conjecture 1.3.

4.1. **Elliptic curves with $C_{E,2} > 0$.** Table 2 displays some data for four elliptic curves. The column labelled "Predicted" lists the values of $C_{E,2} \displaystyle\int_2^{10^{12}} \frac{dt}{2\sqrt{t}(\log t)^2}$; "Actual" lists the values of $\pi_{E,2}(10^{12})$; "% error" lists as a percentage the values of

$$\frac{C_{E,2} \int_2^{10^{12}} \frac{dt}{2\sqrt{t}(\log t)^2} - \pi_{E,2}(10^{12})}{C_{E,2} \int_2^{10^{12}} \frac{dt}{2\sqrt{t}(\log t)^2}}.$$

The first and third curves were already considered in [10], and are included here largely to show the contrast with the second curve. A detailed list of all of the amicable pairs for each of these curves may be found in the appendix.

The elliptic curves E appearing in Table 2 satisfy the property that, for each $n \geq 1$,

$$[GL_2(\mathbb{Z}/n\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})] \leq 2 \tag{29}$$

(See [8, pp. 309–311] and [6, p. 51]). As shown in [8, pp. 310–311], this is the smallest index that one can have for general n when the elliptic curve E is defined over $\mathbb{Q}$. We call any elliptic curve E satisfying (29) a

E	Predicted	Actual	% error
$y^2+y=x^3-x$	120.445	115	4.52%
$y^2=x^3+6x-2$	206.464	208	−0.74%
$y^2+y=x^3+x^2$	120.442	117	2.86%
$y^2+xy+y=x^3-x^2$	120.437	112	7.01%

(28)

Table 2: Data on $\pi_{E,2}(10^{12})$ for various E

E	$C_{E,2}$	$\Delta_{sf}(E)$
$y^2+y=x^3-x$	≈ 0.077093219	37
$y^2=x^3+6x-2$	≈ 0.132151070	−3
$y^2+y=x^3+x^2$	≈ 0.077091320	−43
$y^2+xy+y=x^3-x^2$	≈ 0.077088124	−53

Table 3: Values of $C_{E,2}$ and $\Delta_{sf}(E)$

Serre curve. Serre curves are thus elliptic curves for which $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is "as large as possible for all n," and it has been shown that, when ordered by height, almost all elliptic curves are Serre curves (see [3]). One can show that for any Serre curve E, one has $C_{E,L}>0$. In fact, if we define the constant C_L by

$$C_L := \frac{\phi_L(0)}{L}\cdot\lim_{k\to\infty}\frac{n_k^L|GL_2(\mathbb{Z}/n_k\mathbb{Z})^L_{\text{ali-cycle}}|}{|GL_2(\mathbb{Z}/n_k\mathbb{Z})^L|}=\frac{\phi_L(0)}{L}\cdot\prod_{\ell\text{ prime}}\frac{\ell^L|GL_2(\mathbb{F}_\ell)^L_{\text{ali-cycle}}|}{|GL_2(\mathbb{F}_\ell)^L|},$$

then for any Serre curve E one has that

$$C_{E,L}=C_L\cdot f_L(\Delta_{sf}(E)),$$

where $\Delta_{sf}(E)$ denotes the square-free part of the discriminant of any Weierstrass model of E and f_L is a positive function which approaches 1 as $|\Delta_{sf}(E)|$ approaches infinity. When $L=2$ one has

$$\begin{aligned}C_2&=\frac{\phi_2(0)}{2}\cdot\prod_{\ell\text{ prime}}\frac{\ell^2|GL_2(\mathbb{F}_\ell)^2_{\text{ali-cycle}}|}{|GL_2(\mathbb{F}_\ell)^2|}\\&=\frac{8}{3\pi^2}\cdot\prod_{\ell\text{ prime}}\frac{\ell^2(\ell^4-2\ell^3-2\ell^2+3\ell+3)}{[(\ell^2-1)(\ell-1)]^2}\approx 0.077088124.\end{aligned}$$

Table 3 gives the values of $C_{E,2}$ and $\Delta_{sf}(E)$ for each of the curves in (28). The reason the second curve has a larger value of $C_{E,2}$ is that $|\Delta_{sf}(E)|$ is smaller for this curve than for the others.

4.2. **An elliptic curve with $C_{E,L}=0$.** We will now discuss briefly the elliptic curve

$$E\ :\ y^2=x^3-3x+4 \tag{30}$$

which was mentioned in the introduction, for which $\pi_{E,L}(x)\equiv 0$ since the associated graph $\mathcal{G}_E$ contains no closed walks at all. We will presently describe the Galois group $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$, which is an index 4 subgroup of $GL_2(\mathbb{Z}/4\mathbb{Z})$. First, define the subgroup $H(4)\subseteq GL_2(\mathbb{Z}/4\mathbb{Z})$ by

$$H(4):=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\-1&-1\end{pmatrix},\begin{pmatrix}-1&-1\\1&0\end{pmatrix},\begin{pmatrix}-1&-1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\-1&-1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}.$$

We then have

$$\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})=H(4)\cdot\left(I+2\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}\right). \tag{31}$$

(To see that the right-hand expression defines a subgroup of $GL_2(\mathbb{Z}/4\mathbb{Z})$, note that

$$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}$$

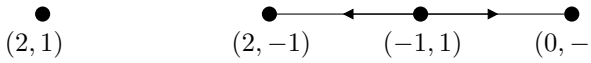
is closed under addition and under $GL_2(\mathbb{Z}/2\mathbb{Z})$-conjugation.)

Since $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$ is a proper subgroup of $GL_2(\mathbb{Z}/4\mathbb{Z})$ (even though $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = GL_2(\mathbb{Z}/2\mathbb{Z})$) one has $4 \mid m_E$, and the restriction map $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$ induces a graph morphism

$$\mathcal{G}_E = \mathcal{G}_E(m_E) \twoheadrightarrow \mathcal{G}_E(4), \tag{32}$$

which is surjective in the sense that it carries the vertex set $\mathcal{V}(m_E)$ onto $\mathcal{V}(4)$ and likewise carries $\mathcal{E}(m_E)$ onto $\mathcal{E}(4)$.

On the other hand, using (31), one finds that the directed graph $\mathcal{G}_E(4)$ is as follows.



(33)

4.2.1. *Infinitely many primes p for which $E(\mathbb{F}_p)$ is prime.* The non-CM case of a conjecture of Koblitz (see [5] and also [12]) expresses (in our terminology) that for any non-CM elliptic curve E, the existence of a single directed edge in $\mathcal{G}_E$ implies the existence of infinitely many primes p for which $|E(\mathbb{F}_p)|$ is prime. Taking E to be the elliptic curve given by (30) we see by the surjectivity of (32) together with (33) that $\mathcal{G}_E$ contains at least one directed edge. Thus, assuming Koblitz's conjecture, there are infinitely many primes p for which $|E(\mathbb{F}_p)|$ is prime.

4.2.2. *Finitely many amicable pairs (p_1, p_2) for E.* Continuing with the example (30), by the surjectivity of (32) together with (33), we see that $\mathcal{G}_E$ contains no closed walks at all. By Proposition 2.6, there are only finitely many amicable pairs (p_1, p_2) for E. In this particular example, the reason is that, whenever $p_2 = |E(\mathbb{F}_{p_1})|$ for some prime p_1, we see from (33) that $(\mathrm{tr}(\mathrm{Frob}_{\mathbb{Q}(E[4])}(p_1)), \det(\mathrm{Frob}_{\mathbb{Q}(E[4])}(p_1))) = (-1, 1)$ (otherwise, $|E(\mathbb{F}_{p_1})|$ would be even). But then $(\mathrm{tr}\,\mathrm{Frob}_{\mathbb{Q}(E[4])}(p_2), \det \mathrm{Frob}_{\mathbb{Q}(E[4])}(p_2) \in \{(0, -1), (2, -1)\}$, in which case $|E(\mathbb{F}_{p_2})|$ must be even. Thus, E has no aliquot cycles of length 2, except possibly one with $p_1 = 2$.

Remark 4.1. There is a modular curve X of level 4 whose $\mathbb{Q}$-rational points correspond to j-invariants of elliptic curves E for which $-\Delta_E$ is a perfect square. Above each such j-invariant, one may find an appropriate twist E for which (31) holds, and thus for which $\pi_E^{2-\mathrm{aliquot}}(x) = 0$. The elliptic curve (30) is one such example.

5. Acknowledgments

The author gratefully acknowledges A.C. Cojocaru, who first brought this question to my attention, and also J. Silverman for a stimulating discussion. Also thanks to A. Sutherland, who provided help with the computations (a description of the software used therein may be found in [4]).

References

[1] A. Balog, A.C. Cojocaru and C. David, Average twin prime conjecture for elliptic curves, *Amer. J. Math.*, **133** no. 5 (2011) 1179–1229.
[2] C. David and F. Pappalardi, Average Frobenius distributions of elliptic curves, *Int. Math. Res. Not. IMRN*, **1999** (1999), 165–183.
[3] N. Jones, Almost all elliptic curves are Serre curves, *Trans. Amer. Math. Soc.*, **362** (2010), 1547–1570.
[4] K. Kedyala and A. Sutherland, Computing L-series of hyperelliptic curves, *Algorithmic Number Theory 8th International Symposium* (ANTS VIII), LNCS 5011, Springer, 312–326, 2008.
[5] N. Koblitz, Primality of the number of points on an elliptic curve over a finite field, *Pacific J. Math.* **131** (1988), 157–165.
[6] S. Lang and H. Trotter, *Frobenius Distributions in GL_2-Extensions*, Lecture Notes in Mathematics **504**, Springer, Berlin 1976.
[7] B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18** (1972), 183–266.
[8] J-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York–Amsterdam 1968.
[9] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[10] J. H. Silverman and K. Stange, Amicable pairs and aliquot cycles for elliptic curves, *Experiment. Math.* **20** (2011), no. 3, 329–357.
[11] R. Taylor, Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations, *Pub. Math. IHES* **108** (2008), 183–239.
[12] D. Zywina, A refinement of Koblitz's Conjecture, *Int. J. Number Theory*, **7** (2011), no. 3, 739–769.

6. Appendix: explicit lists of amicable pairs

The following tables list explicitly the aliquot cycles of length 2 up to 10^{12} for each elliptic curve in (28). As mentioned before, the list for the first and third elliptic curves already appear in the literature.

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

(1622311, 1622471)	(209051131, 209065277)	(435197207, 435203627)
(1039959127, 1040001691)	(1129509221, 1129533787)	(1226864057, 1226882263)
(2352481871, 2352558343)	(2611684883, 2611740823)	(2948995759, 2949055441)
(3694651133, 3694724861)	(3700382359, 3700422013)	(5683068649, 5683159501)
(6349942217, 6349993721)	(6914519077, 6914622391)	(7780832797, 7780990501)
(7860919111, 7861056859)	(11661099739, 11661236029)	(13190078443, 13190190973)
(17715766063, 17715919189)	(18474017909, 18474073067)	(20141992589, 20142034597)
(27533596327, 27533695253)	(30088680781, 30088865197)	(30219540259, 30219626189)
(35165094271, 35165277859)	(39781723027, 39781892179)	(40193486233, 40193590513)
(53243937647, 53244180001)	(66112307671, 66112681087)	(75220327627, 75220824407)
(79547451029, 79547941961)	(82972540933, 82973007269)	(91481681563, 91481831167)
(135209380513, 135209499589)	(136915494109, 136915595393)	(157257407323, 157257693611)
(158984455501, 158984688949)	(167039564669, 167040084401)	(177684339499, 177684824747)
(180834082483, 180834577073)	(220572066031, 220572215359)	(222615955253, 222616408523)
(225553569541, 225554322289)	(232147447429, 232147688077)	(237450526301, 237450906587)
(242306352073, 242306848111)	(254431324111, 254431871483)	(266978335579, 266979154129)
(278362825919, 278362984259)	(310815976057, 310816715611)	(313411448689, 313411783339)
(337937547001, 337937666239)	(346014872941, 346015802347)	(349091231189, 349091456213)
(355874233339, 355875011273)	(374395351147, 374395833101)	(389045160211, 389046040597)
(410216001667, 410216487617)	(425054768539, 425055365503)	(433264475593, 433265271421)
(447995295149, 447995753581)	(450962487379, 450963499751)	(452460382313, 452460690173)
(458893417501, 458893876037)	(459730791547, 459731977339)	(467750074973, 467750803543)
(479317568749, 479317690799)	(487450330357, 487451102659)	(492300415627, 492300923243)
(492804132581, 492804306977)	(495444691993, 495445905593)	(512761175929, 512762306323)
(512831724641, 512832427781)	(535685535181, 535685802473)	(541205932447, 541206076321)
(542986795411, 542987777977)	(543698127899, 543698612339)	(548910506773, 548911500937)
(582293306269, 582294364021)	(594593079499, 594593130487)	(616357100551, 616357962947)
(621398107639, 621398159887)	(637853583649, 637853929663)	(662264439119, 662265469751)
(667090336879, 667090628623)	(668446398773, 668446550483)	(677386393447, 677387660891)
(691941147839, 691941897841)	(715473741821, 715474531417)	(716974038541, 716975043439)
(731061198019, 731061747727)	(736836558559, 736836756037)	(739367967629, 739368490373)
(747470186753, 747471096839)	(747741940633, 747742621163)	(787050974509, 787051054799)
(788049803507, 788050962247)	(791043347177, 791043576221)	(814883538661, 814884311611)
(828555018217, 828556059601)	(829762693999, 829763438291)	(834436212079, 834437146787)
(836460556301, 836460725687)	(844964045659, 844965469009)	(846341290477, 846341935993)
(855505476433, 855505945837)	(875067239093, 875068051043)	(880220286991, 880220771851)
(882103493123, 882104446687)	(904777224133, 904777406573)	(931427616797, 931428699827)
(941072287627, 941072777989)	(947754240637, 947755837411)	(975303777571, 975304270909)
(988356964733, 988357609933)		

$$E : y^2 = x^3 + 6x - 2$$

(1548181, 1549957)	(8418001, 8420869)	(27020971, 27023203)
(41099887, 41102779)	(55475983, 55485487)	(103188703, 103189183)
(103560409, 103562257)	(247178983, 247205683)	(311333227, 311334547)
(313230349, 313253617)	(356804113, 356827567)	(422576281, 422601397)
(519858049, 519859897)	(532921261, 532948789)	(695441821, 695470429)
(909516679, 909537679)	(1041003277, 1041034381)	(1285610191, 1285666111)
(1323964627, 1324003501)	(1460968087, 1460999563)	(1573023853, 1573036789)
(2228730391, 2228739319)	(2856670207, 2856729307)	(2884015957, 2884076497)
(3487502743, 3487556353)	(3637904731, 3637909417)	(3698023993, 3698087053)
(5738542567, 5738600821)	(6133051201, 6133153483)	(6752045479, 6752144557)
(7132897549, 7132989307)	(7856869717, 7856980249)	(10651831501, 10651905937)
(11245617703, 11245732123)	(11895069451, 11895081379)	(12556864459, 12556881829)
(12961854553, 12961959823)	(14028936853, 14028997627)	(17819373163, 17819395123)
(19374492091, 19374504559)	(20002813219, 20002997401)	(20043073867, 20043079489)
(21309214687, 21309268879)	(21365073151, 21365086591)	(21392159689, 21392351269)
(21634673911, 21634735261)	(23716596619, 23716760269)	(25262268439, 25262298301)
(25588885939, 25588919803)	(28359161143, 28359242143)	(34599021349, 34599359077)
(34992582463, 34992729643)	(35528890741, 35529091189)	(35994010963, 35994101401)
(36220685653, 36220823053)	(37203130933, 37203226117)	(38998338619, 38998409209)
(39895808779, 39896029939)	(43060037287, 43060236229)	(45077531659, 45077823727)
(45996173803, 45996256021)	(48663034831, 48663094723)	(50138991919, 50139094801)
(50274637603, 50274713833)	(61616410483, 61616553619)	(62645351809, 62645575891)
(69076161499, 69076484017)	(75420226099, 75420328603)	(91815723319, 91815916921)
(95856852841, 95857110871)	(97300695241, 97300912453)	(101838416089, 101838631711)
(104860147387, 104860414207)	(105129527617, 105129547609)	(110933234197, 110933366851)
(113007291079, 113007693451)	(118034554213, 118034711017)	(121458837607, 121459013983)
(122121727729, 122122035571)	(123043281511, 123043417417)	(127164399319, 127164716047)
(129776642731, 129777043213)	(130375783231, 130376242357)	(134543151409, 134543156239)
(136033853041, 136034432371)	(139803425491, 139803584803)	(140398380691, 140398878517)
(141371775949, 141372134119)	(143625540313, 143625910663)	(146984081467, 146984107561)
(154455052183, 154455447337)	(154558154293, 154558266547)	(154589048881, 154589146171)
(160477931953, 160478402197)	(169100913031, 169101408187)	(170157172567, 170157425161)
(176093570269, 176093594137)	(180683118661, 180683512459)	(180918695641, 180919056559)
(181661826109, 181662063151)	(193624195909, 193624275049)	(197728432483, 197728647073)
(200346558421, 200346908953)	(206169275317, 206169892651)	(208532319661, 208532649307)
(209288525629, 209288889991)	(214444029871, 214444663267)	(218963657833, 218964291703)
(223263181027, 223263280729)	(230300519569, 230300669971)	(241404945073, 241405363681)
(251761334491, 251761616599)	(253721388703, 253721923513)	(257773331401, 257773671427)
(258262219483, 258262725001)	(258290107969, 258291005671)	(263287907227, 263288596171)
(264118967857, 264119109511)	(267424290457, 267424717363)	(271213201957, 271213641901)
(281252697337, 281252884639)	(281308871953, 281309112493)	(282505134739, 282505672369)
(286455303427, 286455801883)	(290995669561, 290996513623)	(295016767207, 295017062383)

(continued on next page)

($E : y^2 = x^3 + 6x - 2$, continued)

(304611562393, 304611905011)	(316426926331, 316427396851)	(320194228441, 320194439881)
(323392992001, 323393683099)	(323759613889, 323759796799)	(338730801697, 338731733731)
(339933813691, 339933979057)	(369205061077, 369205230841)	(370101477787, 370101545599)
(372063948853, 372064610173)	(377383236409, 377383778599)	(381651061711, 381651855967)
(385133497741, 385134282067)	(387439552267, 387439963693)	(394584712183, 394585469767)
(416569428133, 416569871587)	(419068686397, 419069355931)	(427471260409, 427472032921)
(432809199301, 432810098419)	(438923378953, 438923590843)	(452117698771, 452118519019)
(480996157987, 480996939901)	(491663527261, 491663719213)	(493862867191, 493863140227)
(496495770301, 496496069977)	(497423088763, 497423596921)	(503412302287, 503412574603)
(508725587593, 508726001809)	(509175117817, 509176307413)	(514535068759, 514535497039)
(523540389637, 523541126389)	(523542025147, 523543103947)	(529110442891, 529110568849)
(530665482229, 530665688353)	(534353032483, 534353959813)	(549968382823, 549968390329)
(550105241731, 550106356699)	(554960009509, 554960226913)	(583282615459, 583283214121)
(588292030849, 588292139647)	(601289295913, 601289609563)	(618553274137, 618553734361)
(627259045531, 627259840177)	(641812301983, 641813638393)	(658785056563, 658786238197)
(675907216669, 675907700131)	(676669802719, 676670932747)	(684967404067, 684968499517)
(685269294349, 685269771181)	(685573828441, 685574444917)	(691921122031, 691921263751)
(695361639307, 695362458157)	(724138195909, 724139642449)	(745941844117, 745942115407)
(751323994363, 751324293919)	(759503735437, 759503759251)	(764977801831, 764979218077)
(771520756183, 771521557333)	(777427080589, 777427099777)	(785945109151, 785946501919)
(797321303083, 797322101827)	(800217573139, 800218603939)	(800232048799, 800233233139)
(807079605733, 807080354401)	(810955125037, 810955878367)	(838120137769, 838120638049)
(844929845209, 844930800097)	(854376423709, 854377562827)	(878892886021, 878893049557)
(901292660053, 901293027631)	(901938239287, 901938376201)	(903067276537, 903067840579)
(924895719301, 924896722261)	(947036364709, 947037146329)	(951922236313, 951922594213)
(957843151099, 957844425523)	(959131543543, 959132519413)	(961955322421, 961955801899)
(962692820833, 962693488201)	(966784833601, 966785085457)	(971826907483, 971828106541)
(988941171109, 988942616029)		

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

$(853, 883)$	$(77761, 77999)$	$(1147339, 1148359)$
$(1447429, 1447561)$	$(82459561, 82471789)$	$(109165543, 109180121)$
$(253185307, 253194619)$	$(320064601, 320079131)$	$(794563993, 794571803)$
$(797046407, 797057473)$	$(2185447367, 2185504261)$	$(2382994403, 2383029443)$
$(4101180511, 4101190039)$	$(4686466159, 4686510971)$	$(5293671709, 5293749623)$
$(6677602471, 6677694539)$	$(7074693823, 7074704971)$	$(7806306133, 7806380963)$
$(9395537549, 9395559011)$	$(9771430993, 9771433303)$	$(9849225103, 9849306373)$
$(10574564857, 10574619851)$	$(12657210407, 12657303353)$	$(13003880317, 13003900901)$
$(13789895011, 13790023199)$	$(14436076927, 14436180091)$	$(14976551207, 14976590371)$
$(15597047659, 15597075937)$	$(15679549877, 15679688491)$	$(16322301811, 16322366867)$
$(17725049203, 17725142719)$	$(17841395323, 17841406601)$	$(20780607817, 20780797927)$
$(23338053773, 23338135543)$	$(28358243743, 28358411071)$	$(29859516131, 29859782089)$
$(31615097957, 31615194739)$	$(33266376239, 33266419807)$	$(33963999907, 33964128017)$
$(34525477799, 34525684639)$	$(39287748091, 39287808559)$	$(40136806357, 40137038941)$
$(46438194193, 46438453213)$	$(51838270219, 51838493561)$	$(51881025571, 51881167549)$
$(52011956957, 52012184953)$	$(55823622193, 55823919169)$	$(57920520199, 57920640709)$
$(62765305697, 62765625749)$	$(62995853671, 62996152237)$	$(66252308051, 66252349753)$
$(67177409329, 67177631771)$	$(69449506103, 69449741239)$	$(75002612911, 75002660263)$
$(77264683829, 77264993327)$	$(77635421531, 77635670141)$	$(79067605783, 79067881429)$
$(81263083703, 81263204563)$	$(94248260597, 94248586591)$	$(104544108049, 104544364087)$
$(111287830573, 111288274567)$	$(118206158729, 118206360829)$	$(120791219099, 120791323493)$
$(132962516737, 132962703661)$	$(142574237383, 142574369533)$	$(144750903551, 144751137469)$
$(155467666099, 155467836031)$	$(161226480901, 161227124081)$	$(173164057399, 173164630033)$
$(178633373617, 178633516081)$	$(213013688359, 213013931239)$	$(218475851959, 218475922267)$
$(222335132807, 222335345521)$	$(225529688431, 225529987157)$	$(232349609983, 232349658979)$
$(234896302009, 234896350369)$	$(240677586449, 240678201091)$	$(241352193611, 241352273849)$
$(265340194039, 265340401483)$	$(277515892207, 277516507711)$	$(287800715711, 287801137609)$
$(299486604371, 299487430807)$	$(302166243187, 302166581251)$	$(323643851647, 323644499221)$
$(356299878281, 356300493907)$	$(378008294449, 378008508961)$	$(383399841217, 383399894341)$
$(392864677427, 392865349441)$	$(415381769743, 415381922953)$	$(421953112561, 421953604103)$
$(425072615243, 425073437039)$	$(438722917471, 438723215947)$	$(475655912713, 475656729419)$
$(477171588461, 477171935243)$	$(509779650181, 509780267947)$	$(519205252403, 519205488493)$
$(580562183213, 580562489173)$	$(605229610571, 605229758977)$	$(614484897889, 614485486079)$
$(637355743513, 637356846673)$	$(649999477469, 649999993999)$	$(655455388397, 655456255439)$
$(658459698947, 658460090441)$	$(662097699853, 662098655233)$	$(705006602177, 705006769807)$
$(723299067853, 723299355619)$	$(775857545861, 775859048443)$	$(793725967891, 793727339077)$
$(794925473327, 794926023761)$	$(811569419461, 811569591827)$	$(838059794239, 838061257667)$
$(851273574199, 851274251683)$	$(885227547847, 885227943451)$	$(916134576373, 916134747943)$
$(948135054247, 948136458277)$	$(954115635797, 954115645823)$	$(977575750447, 977576865637)$

$$E : y^2 + xy = y = x^3 - x^2$$

$(15782639, 15784843)$	$(190661353, 190664659)$	$(502321091, 502327927)$
$(623231569, 623231993)$	$(848089241, 848132891)$	$(867592309, 867624829)$
$(3416538269, 3416597377)$	$(3717074213, 3717173309)$	$(4238113591, 4238209777)$
$(5152594561, 5152642949)$	$(6089286341, 6089340407)$	$(9570960601, 9571090813)$
$(10307814653, 10308007673)$	$(12344104739, 12344173241)$	$(12716284769, 12716356283)$
$(13176256817, 13176313231)$	$(16346940559, 16347177017)$	$(17446634749, 17446866277)$
$(17640097129, 17640202039)$	$(17813465101, 17813616323)$	$(20236386439, 20236522001)$
$(25399397321, 25399525139)$	$(28962287951, 28962407993)$	$(44498254369, 44498268181)$
$(44505831763, 44506130107)$	$(46349770567, 46349853013)$	$(46458108131, 46458263461)$
$(50111710081, 50111715697)$	$(50358110393, 50358130913)$	$(53101240499, 53101392913)$
$(53479634651, 53479832557)$	$(58314298151, 58314604273)$	$(61023254293, 61023633193)$
$(63927854251, 63928173559)$	$(69324497167, 69324768649)$	$(72719208101, 72719547421)$
$(74695294579, 74695303807)$	$(77163314573, 77163565477)$	$(87909792151, 87910126273)$
$(89232374177, 89232642671)$	$(90765908473, 90765993701)$	$(104578431757, 104578692593)$
$(106490241971, 106490439611)$	$(117092369503, 117092709313)$	$(119750886781, 119751206593)$
$(136259885981, 136260396247)$	$(147752621281, 147752621473)$	$(152386047371, 152386399289)$
$(159205542883, 159205941493)$	$(162082190863, 162082739993)$	$(162228888733, 162229099127)$
$(176417856691, 176418563047)$	$(181356597949, 181356724279)$	$(189892739581, 189893224141)$
$(203800207903, 203800471873)$	$(211513919011, 211514727163)$	$(220708027751, 220708595369)$
$(229639371653, 229639954039)$	$(232087576949, 232087869109)$	$(241147849703, 241148516573)$
$(244618491253, 244619163127)$	$(257901424217, 257901714461)$	$(261006203473, 261006566413)$
$(276349180903, 276349242947)$	$(284018293907, 284018841541)$	$(292321566133, 292322062051)$
$(303417636943, 303418534169)$	$(330731874709, 330732406447)$	$(335698096693, 335698400441)$
$(352360579243, 352360813999)$	$(355468546691, 355469258233)$	$(362673106891, 362673597557)$
$(370230266191, 370230703417)$	$(378965271283, 378965623903)$	$(380261411263, 380262381227)$
$(390135772571, 390136652989)$	$(390799130147, 390800011621)$	$(400024457279, 400025502673)$
$(402493970449, 402495159901)$	$(414985447453, 414985542637)$	$(418036669879, 418037202859)$
$(421489291187, 421489882091)$	$(444533520989, 444534760079)$	$(487236963173, 487237982267)$
$(520046808691, 520046846843)$	$(526535611213, 526535898193)$	$(542199064171, 542199898081)$
$(570305518229, 570306739627)$	$(578863687643, 578864208623)$	$(584693259547, 584694507781)$
$(604132829593, 604133190781)$	$(612708244831, 612708811523)$	$(633641436079, 633641528089)$
$(634237451317, 634237815037)$	$(646610210237, 646611215177)$	$(661780097659, 661780284409)$
$(662587649869, 662587671379)$	$(675497678743, 675497762833)$	$(707189418797, 707190256169)$
$(726804340441, 726804853387)$	$(729011769121, 729011923819)$	$(763258759231, 763259788957)$
$(780058611379, 780059712277)$	$(789194123593, 789194848801)$	$(792144114521, 792144583487)$
$(800068081357, 800068897333)$	$(824682365453, 824683788449)$	$(896499439369, 896500153051)$
$(897964354531, 897965047027)$	$(910331668333, 910332505723)$	$(938116069703, 938116887583)$
$(992075415607, 992076747499)$		