Pacific
Journal of
Mathematics

ELLIPTIC ALIQUOT CYCLES OF FIXED LENGTH

NATHAN JONES

Volume 263 No. 2 June 2013

PACIFIC JOURNAL OF MATHEMATICS
Vol. 263, No. 2, 2013
dx.doi.org/10.2140/pjm.2013.263.353

ELLIPTIC ALIQUOT CYCLES OF FIXED LENGTH

NATHAN JONES

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 [2011] define an L-tuple $(p_1, p_2, \ldots, p_L)$ 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,

$$p_1 = |E(\mathbb{F}_{p_L})| \qquad \text{and} \qquad p_{i+1} = |E(\mathbb{F}_{p_i})| \text{ for all } i \in \{1, 2, \ldots, L-1\},$$

which may be more succinctly written as

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

When $L = 2$, an aliquot cycle is also referred to as an *amicable pair for E*. As observed in [Silverman and Stange 2011, 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 (see also [Gottschlich 2012], which studies some distributional aspects of elliptic divisibility sequences).

It is of interest to know how common such aliquot cycles are, so we presently 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 $(p_1, p_2, \ldots, p_L)$ to be *normalized* if $p_1 = \min\{p_i : 1 \leq i \leq L\}$, and then write

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

Work partially supported by the National Security Agency under grant H98230-12-1-0210.
MSC2010: 11G05.
Keywords: elliptic curve, aliquot cycle, amicable pair.

The behavior of $\pi_{E,L}(x)$ for large x depends heavily on whether or not E has complex multiplication (CM), as the following conjecture indicates.

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

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

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

Remark 1.2. We may interpret the case $L = 1$ 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 in [Mazur 1972]. The asymptotic count for anomalous primes up to x is a special case of a conjecture of Lang and Trotter [1976].

Silverman and Stange [2011] focus on the intricacies of the CM case, proving that if E has CM, $j_E \neq 0$ and $L \geq 3$, then 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.

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 nonnegative real constant $C_{E,L} \geq 0$ (see (5) below) so that, as $x \longrightarrow \infty$,

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

Remark 1.4. It is possible for the constant $C_{E,L}$ to be zero, in which case the limit $\lim_{x\to\infty} \pi_{E,L}(x)$ 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

$$\left|\pi_{E,L}(x) - C_{E,L} \int_2^x \frac{1}{2\sqrt{t}(\log t)^L}\, dt\right|$$

E	$x=10^6$	$x=10^8$	$x=10^{10}$	$x=10^{12}$	$x=10^{13}$
$E_1: y^2+y=x^3-x$	0	1	16	115	332
$E_2: y^2=x^3+6x-2$	0	5	32	208	564
$E_3: y^2=x^3-3x+4$	0	0	0	0	0

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

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 $\pi_{E_3,2}(10^{13}) = 0$. The additional fact that

$$\left|\left\{p \le 10^{12} : p \text{ is of good reduction for } E_3 \text{ and } |E_3(F_p)| \text{ is prime}\right\}\right| = 715, 698, 540$$

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 [Balog et al. 2011; David and Pappalardi 1999]). 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 $\mathscr{G}_E$.* In the interest of characterizing the non-CM 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* $\mathscr{G}$ is a pair $(\mathscr{V}, \mathscr{E})$, where $\mathscr{V} = \mathscr{V}(\mathscr{G})$ is an arbitrary set of *vertices* and $\mathscr{E} = \mathscr{E}(\mathscr{G}) \subseteq \mathscr{V} \times \mathscr{V}$ is a subset of *directed edges*. The sequence of vertices $(v_1, v_2, v_3, \ldots, v_n)$ is a *closed walk of length n* if and only if $(v_i, v_{i+1}) \in \mathscr{E}$ 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 $(v, v) \in \mathscr{E}$ for some vertex v (i.e., if $\mathscr{G}$ has a *loop* at a vertex v), then $\mathscr{G}$ has closed walks of any length.

We will associate to an elliptic curve E a directed graph $\mathscr{G}_E$. 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

$$\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}). \tag{2}$$

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 (2), the vertex set $\mathcal{V}(n)$ of our graph $\mathcal{G}_E(n)$ is

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

We define the set $\mathcal{E}(n) \subseteq \mathcal{V}(n) \times \mathcal{V}(n)$ of directed edges by declaring that $(v_1, v_2) \in \mathcal{E}(n)$ 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

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

where $\pi : \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/\gcd(m, n)\mathbb{Z})$ 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 [1972].) 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).

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 $\pi_{E,L}(x) - C_{E,L} \int_2^x \frac{1}{2\sqrt{t}(\log t)^L}\, dt$ for various elliptic curves E and $L \in \{2, 3\}$.

2. The constant

We now describe in detail the constant $C_{E,L}$. The next 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 satisfies the equation

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

as well as the Hasse bound

$$|a_p(E)| \le 2\sqrt{p}. \tag{3}$$

Lemma 2.1 [Serre 1968, IV-4–IV-5]. *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*

$$\mathrm{tr}(\mathrm{Frob}_{\mathbb{Q}(E[n])}(p)) \equiv a_p(E) \bmod n \quad \text{and} \quad \det(\mathrm{Frob}_{\mathbb{Q}(E[n])}(p)) \equiv p \bmod n.$$

For any subset $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, define

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

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

$$\begin{aligned}\bigl(\mathrm{Frob}_{\mathbb{Q}(E[n])}(p_1), \mathrm{Frob}_{\mathbb{Q}(E[n])}(p_2), \dots, \mathrm{Frob}_{\mathbb{Q}(E[n])}(p_L)\bigr)&\\ \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-cycle}}&.\end{aligned} \tag{4}$$

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

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

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,

[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.

[2] Assuming E has nonintegral j-invariant, the Sato–Tate conjecture is now a theorem of L. Clozel, M. Harris, N. Shepherd-Barron, and R. Taylor (see [Taylor 2008] and the references therein).

which (again assuming the Sato–Tate conjecture) 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." Since the primes $p_1, p_2, \dots, p_L$ belonging to an aliquot cycle must be close to one another (i.e., within $\approx L\sqrt{t}$ of one another where $p_1 \approx t$, by the Hasse bound (3)), we are really assuming statistical independence *in short intervals* of the various terms $a_{p_i}(E)/2\sqrt{p_i}$. Finally, for a positive integer k, put

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

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

$$C_{E,L} := \frac{\phi_L(0)}{L} \cdot \lim_{k\to\infty} \frac{n_k^L \left|\mathrm{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L_{\text{ali-cycle}}\right|}{\left|\mathrm{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L\right|}. \tag{5}$$

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

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

where $\pi : \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/\gcd(m,n)\mathbb{Z})$ is the canonical projection.

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

$$\lim_{k\to\infty} \frac{n_k^L \left|\mathrm{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L_{\text{ali-cycle}}\right|}{\left|\mathrm{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q})^L\right|} = \frac{m_E^L \left|\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}}\right|}{\left|\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L\right|} \cdot \prod_{l \nmid m_E} \frac{l^L \left|\mathrm{GL}_2(\mathbb{F}_l)^L_{\text{ali-cycle}}\right|}{\left|\mathrm{GL}_2(\mathbb{F}_l)^L\right|}.$$

Furthermore,

$$0 < \frac{l^L \left|\mathrm{GL}_2(\mathbb{F}_l)^L_{\text{ali-cycle}}\right|}{\left|\mathrm{GL}_2(\mathbb{F}_l)^L\right|} = 1 + O_L\left(\frac{1}{l^2}\right), \tag{6}$$

so the infinite product $\prod_{l \nmid m_E} \frac{l^L \left|\mathrm{GL}_2(\mathbb{F}_l)^L_{\text{ali-cycle}}\right|}{\left|\mathrm{GL}_2(\mathbb{F}_l)^L\right|}$ *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 $G_1 \subseteq \mathrm{GL}_2(\mathbb{Z}/n_1\mathbb{Z})$ and $G_2 \subseteq \mathrm{GL}_2(\mathbb{Z}/n_2\mathbb{Z})$. Then, viewing $G_1 \times G_2 \subseteq \mathrm{GL}_2(\mathbb{Z}/n_1n_2\mathbb{Z})$, one has*

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

Proof. Let $\iota : \mathrm{GL}_2(\mathbb{Z}/n_1\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/n_2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n_1n_2\mathbb{Z})$ 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

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

This implies the conclusion of Lemma 2.3. □

Lemma 2.4. *Let n be a positive integer and n' any multiple of n such that, for every prime number l, $l \mid n' \Rightarrow l \mid n$. Let $\pi : \mathrm{GL}_2(\mathbb{Z}/n'\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ denote the canonical projection and let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be any subgroup. Then one has*

$$\frac{(n')^L \left|(\pi^{-1}(G))^L_{\text{ali-cycle}}\right|}{|\pi^{-1}(G)^L|} = \frac{n^L \left|G^L_{\text{ali-cycle}}\right|}{|G^L|}. \tag{7}$$

Proof. By induction, it suffices to check the case $n' = ln$, where l is some prime dividing n. In this case, since $|\pi^{-1}(G)| = l^4|G|$, (7) is equivalent to

$$\left|(\pi^{-1}(G))^L_{\text{ali-cycle}}\right| = l^{3L} \left|G^L_{\text{ali-cycle}}\right|, \tag{8}$$

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

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

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

$$g_i \pmod{l} \notin \{0, I\} \quad \text{for each } i \in \mathbb{Z}/L\mathbb{Z} \tag{9}$$

and furthermore, the quantity

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

is well-defined. One checks that

$$\begin{aligned} &\det g'_{i+1} \equiv \det g'_i + 1 - \operatorname{tr} g'_i \bmod ln \\ &\iff \quad \gamma_i \equiv -\det g_{i+1} \cdot \operatorname{tr} A_{i+1} + \det g_i \cdot \operatorname{tr} A_i - \operatorname{tr}(g_i A_i) \bmod l. \end{aligned} \tag{10}$$

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

$$T : \mathbb{F}_l^{4L} \simeq M_{2\times 2}(\mathbb{F}_l)^L \to \mathbb{F}_l^L,$$

given by

$$(A_i)_{i=1}^L \mapsto \bigl(-\det g_{i+1} \cdot \operatorname{tr} A_{i+1} + \det g_i \cdot \operatorname{tr} A_i - \operatorname{tr}(g_i A_i)\bigr)_{i=1}^L.$$

In light of (10), the condition (8) 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

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

By (9), at least one of $\det g_i - x_i$, $\det g_i - w_i$, y_i and z_i must be nonzero modulo l, and so

$$T\bigl(\{0\} \times \cdots \times \{0\} \times M_{2\times 2}(\mathbb{F}_l) \times \{0\} \times \cdots \times \{0\}\bigr) = \{0\} \times \cdots \times \{0\} \times \mathbb{F}_l \times \{0\} \times \cdots \times \{0\},$$

where the nonzero entries correspond to the same index i. In particular, the linear transformation in question is surjective and we have verified (8), finishing the proof of Lemma 2.4. $\square$

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

$$\operatorname{Gal}(\mathbb{Q}(E[n_k])/\mathbb{Q}) \simeq \pi^{-1}\bigl(\operatorname{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})\bigr) \times \prod_{\substack{l^k \parallel n_k \\ l \nmid m_E}} \operatorname{GL}_2(\mathbb{Z}/l^k\mathbb{Z}),$$

where $\pi : \operatorname{GL}_2(\mathbb{Z}/n_k^{(1)}\mathbb{Z}) \to \operatorname{GL}_2(\mathbb{Z}/m_E\mathbb{Z})$ is the canonical projection. By Lemmas 2.3 and 2.4, we have

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

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 (6) as an exercise. $\square$

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*

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

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*

$$C_{E,L} > 0 \iff \mathscr{G}_E \text{ has a closed walk of length } L. \tag{11}$$

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

Proof. First we prove (11). By Corollary 2.5, we are reduced to showing that

$$\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} \neq \varnothing \iff \mathscr{G}_E \text{ has a closed walk of length } L. \tag{12}$$

The mapping

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

induces a mapping $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} \longrightarrow \{\text{closed walks of length } L \text{ in } \mathscr{G}_E\}$. Thus, if $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} \neq \varnothing$ then $\mathscr{G}_E$ has a closed walk of length L. Conversely, suppose $\mathscr{G}_E$ has a closed walk $(v_1, v_2, v_3, \dots, v_L)$ of length L. Recall that $\mathscr{V} = \mathbb{Z}/m_E\mathbb{Z} \times (\mathbb{Z}/m_E\mathbb{Z})^\times$ 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 $(g_1, g_2, \dots, g_L) \in \mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}}$, so $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} \neq \varnothing$. By Corollary 2.5, we conclude the proof of (11).

To see why the nonexistence of closed walks of length L in $\mathscr{G}_E$ implies that $\lim_{x\to\infty} \pi_{E,L}(x) < \infty$, note that, by (12), one has $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})^L_{\text{ali-cycle}} = \varnothing$. But then (4) 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 1988] and [Lang and Trotter 1976]. We shall call the L-tuple $(p_1, p_2, \dots, p_L)$ of distinct prime numbers an *aliquot sequence of length L for E* if it satisfies

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

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 $(p_1, p_2, \dots, p_L)$ 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

$$p_1 = |E(\mathbb{F}_{p_L})| \iff \sum_{j=1}^{L} a_{p_j}(E) = L. \tag{13}$$

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 $\sum_{j=1}^{L} a_{p_j}(E) = L$.

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

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

We 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 $S \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let

$$S_{\mathcal{N}=a} := \{g \in S : \det(g) + 1 - \mathrm{tr}(g) = a\} = \{g \in S : \det(I - g) = a\},$$
$$S^{\det=b} := \{g \in S : \det(g) = b\}, \quad S^{\det=b}_{\mathcal{N}=a} := S_{\mathcal{N}=a} \cap S^{\det=b}.$$

Finally, for $L \geq 1$ and $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, put

$$G^L_{\text{ali-sequence}} := \bigl\{(g_1, g_2, \ldots, g_L) \in G^L : \\ \text{for all } i \in \{1, 2, \ldots, L-1\}, \det(g_{i+1}) = \det(g_i) + 1 - \mathrm{tr}(g_i)\bigr\}.$$

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

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

Finally, for a fixed integer r, define

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

We will presently derive an expression for the probability

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

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

$$\mathcal{P}_{(1_L),(2'_L)}(t) = \mathcal{P}_{(1_L)}(t) \cdot \mathcal{P}^{\text{given }(1_L)}_{(2'_L)}(t). \tag{14}$$

In Section 3.1 below, we will derive the probability formula

$$\mathcal{P}_{(1_L)}(t) \approx \frac{n^{L-1} \cdot \left|\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-sequence}}\right|}{\left|\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L\right|} \cdot \frac{1}{(\log t)^L}. \tag{15}$$

Following this, in Section 3.2, we will derive

$$\mathcal{P}^{\text{given }(1_L)}_{(2'_L)}(t) \approx \phi_L\left(\frac{r}{2\sqrt{t}}\right) \frac{n \cdot \left|\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{L, \sum \mathrm{tr} = r}_{\text{ali-sequence}}\right|}{\left|\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-sequence}}\right|} \cdot \frac{1}{2\sqrt{t}}. \tag{16}$$

Before deriving (15) and (16), we will now observe that, taken together, they lead to Conjecture 1.3. Indeed, using (14), (15) and (16), one concludes

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

Just as with (13), one verifies that, for each $(g_1, g_2, \ldots, g_L) \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})^L_{\text{ali-sequence}}$, one has

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

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

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

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 $\phi_L(L/(2\sqrt{t})) \approx \phi_L(0)$ does not affect the asymptotic.

3.1. ***The probability that*** $(p_1, p_2, \dots, p_L)$ ***satisfies*** (1_L)**.** We will now derive a refined probability formula which implies (15). Fix a vector $\boldsymbol{a} = (a_2, a_3, \dots, a_L) \in ((\mathbb{Z}/n\mathbb{Z})^\times)^{L-1}$, and consider the probability

$$\mathcal{P}^{\boldsymbol{a}}_{(1_L)}(t) := \mathrm{Prob}\big((p_1, p_2, \dots p_L) \text{ satisfies } (1_L) \text{ and for all } i \in \{2, 3, \dots, L\},\ p_i \equiv a_i \bmod n\big)$$

and (for any subset $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$) the subset

$$G^{L,\boldsymbol{a}}_{\text{ali-sequence}} := \big\{(g_1, g_2, \dots, g_L) \in G^L_{\text{ali-sequence}} : \text{for all } i \in \{2, 3, \dots, L\},\ \det(g_i) = a_i\big\}.$$

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

$$G^{L,\boldsymbol{a}}_{\text{ali-sequence}} = G_{\mathcal{N}=a_2} \times G^{\det=a_2}_{\mathcal{N}=a_3} \times G^{\det=a_3}_{\mathcal{N}=a_4} \times \cdots \times G^{\det=a_{L-1}}_{\mathcal{N}=a_L} \times G^{\det=a_L}. \tag{17}$$

Finally, note that if $\boldsymbol{a}_1 \neq \boldsymbol{a}_2$, then $G^{L,\boldsymbol{a}_1}_{\text{ali-sequence}} \cap G^{L,\boldsymbol{a}_2}_{\text{ali-sequence}} = \varnothing$, and so we have a disjoint union

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

For similar reasons, we have

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

Thus, (15) will follow from

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

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 (18).

Induction step. Assume now that (18) holds for some fixed $L \geq 1$, and fix any vector $\boldsymbol{a} = (a_2, a_3, \dots, a_{L+1}) \in ((\mathbb{Z}/n\mathbb{Z})^\times)^L$. Since the statement

$$(p_1, p_2, \dots, p_{L+1}) \text{ satisfies } (1_{L+1}) \text{ and for all } i \in \{2, 3, \dots, L+1\},\ p_i \equiv a_i \bmod n$$

is equivalent to

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

we see that

$$\mathcal{P}^{(a_2, a_3, \dots, a_L, a_{L+1})}_{(1_{L+1})}(t) = \mathcal{P}^{(a_2, a_3, \dots, a_L)}_{(1_L)}(t) \cdot \mathcal{P}(t), \tag{19}$$

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

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

where $p_{\max} := \max\{p_i : i = 1, 2, \dots, L\}$. 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 $(p_1, p_2, \dots, p_L)$, then

$$\operatorname{Prob}(p_{L+1} \text{ is prime and } p_{L+1} \equiv a_{L+1} \bmod n) \approx \frac{1}{\varphi(n)\log t}, \tag{20}$$

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 $p_{L+1} \equiv a_{L+1} \bmod n$ would be $1/n$. However, p_{L+1} is not chosen independently of $(p_1, p_2, \dots, p_L)$; it is related to p_L by the formula $p_{L+1} = p_L + 1 - a_{p_L}(E)$. Thus, the congruence $p_{L+1} \equiv a_{L+1} \bmod n$ is really the demand that

$$\operatorname{Frob}_{\mathbb{Q}(E[n])}(p_L) \in \operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})_{\mathcal{N} = a_{L+1}}.$$

Since we assume that (1_L) holds, we know that $\operatorname{Frob}_{\mathbb{Q}(E[n])}(p_L) \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})^{\det = a_L}$. It is thus natural to multiply (20) by the correction factor

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

obtaining

$$\begin{aligned} \mathcal{P}(t) &\approx \frac{\left|\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{\det=a_L}_{\mathcal{N}=a_{L+1}}\right| \big/ \left|\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{\det=a_L}\right|}{1/n} \cdot \frac{1}{\varphi(n)\log t} \\ &= \frac{n\left|\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{\det=a_L}_{\mathcal{N}=a_{L+1}}\right|}{|\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})|} \cdot \frac{1}{\log t}. \end{aligned} \tag{21}$$

By (17), we may rewrite (18) as

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

Plugging this expression and (21) into (19), and using the fact that

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

one concludes the induction step, completing the derivation of (18), and thus of (15).

Our analysis has motivated the following conjecture, wherein

$$\pi^{\text{ali-sequence}}_{E,L}(x) := \left|\left\{p_1 \le x : \exists \text{ an aliquot sequence } (p_1, p_2, \dots, p_L) \text{ for } E\right\}\right|,$$

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

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

$$\pi^{\text{ali-sequence}}_{E,L}(x) \sim C^{\text{ali-sequence}}_{E,L} \int_2^x \frac{1}{(\log t)^L}\, dt.$$

Similarly to Proposition 2.6, one has

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

3.2. ***The conditional probability that $(p_1, p_2, \dots, p_L)$ satisfies $(2'_L)$.*** We will now derive (16), completing the heuristic derivation of Conjecture 1.3. Suppose that $(p_1, p_2, \dots, p_L)$ 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 $f_n(r, p) \ge 0$ will estimate the probability of the event that $\sum_{i=1}^{L} a_{p_i}(E) = r$, given that $(p = p_1, p_2, \dots, p_L)$ is an aliquot sequence of length L for E. We will model the situation by assuming that the vector

$$\left(\mathrm{Frob}_{\mathbb{Q}(E[n])}(p_1), \mathrm{Frob}_{\mathbb{Q}(E[n])}(p_2), \dots \mathrm{Frob}_{\mathbb{Q}(E[n])}(p_L)\right) \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^L_{\text{ali-sequence}} \tag{22}$$

is randomly distributed according to counting measure, and we will assume that the various $a_{p_i}(E)/(2\sqrt{p_i})$ are independent at infinity, i.e., that ϕ_L is the distribution function for their sum. We will also assume independence of the random variables $\sum_{i=1}^{L} a_{p_i}(E)/(2\sqrt{p_i})$ and (22). 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 $f_n(r, p)$:

$$f_n(r, p) = 0 \quad \text{if } |r| > 2L\sqrt{p},$$

$$f_n(r, p) = \phi_L\left(\frac{r}{2\sqrt{p}}\right) \cdot \frac{n\left|\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{L,\sum \mathrm{tr}=r}_{\text{ali-sequence}}\right|}{\left|\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})^{L}_{\text{ali-sequence}}\right|} \cdot c_p \quad \text{if } |r| \le 2L\sqrt{p},$$

where c_p is some constant chosen so that $\sum_{r\in\mathbb{Z}} f_n(r, p) = 1$. Then, similarly to [Lang and Trotter 1976, pp. 31–32], one concludes that $c_p \sim \frac{1}{2\sqrt{p}}$, as $p \to \infty$. This leads to (16), 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 $C_{E,L} > 0$.*** Table 2 and Table 3 display some data for four elliptic curves. In each table, the column labeled "predicted" lists the approximate values of

$$C_{E,L} \int_2^{10^{13}} \frac{dt}{2\sqrt{t}(\log t)^L},$$

"actual" lists the values of $\pi_{E,L}(10^{13})$, and "% error" lists as a percentage the approximate values of

$$\frac{C_{E,L} \displaystyle\int_2^{10^{13}} \frac{dt}{2\sqrt{t}(\log t)^L} - \pi_{E,L}(10^{13})}{C_{E,L} \displaystyle\int_2^{10^{13}} \frac{dt}{2\sqrt{t}(\log t)^L}}.$$

The first and third curves were already considered in [Silverman and Stange 2011], and are included here largely to show the contrast with the second curve. For each of these curves, a detailed list of the aliquot cycles with $p_1 \le 10^{13}$ may be found in an expanded version of this paper [Jones 2012].

E	predicted	actual	% error
$y^2 + y = x^3 - x$	318.98	332	-4.08%
$y^2 = x^3 + 6x - 2$	546.78	564	-2.97%
$y^2 + y = x^3 + x^2$	318.97	328	-2.83%
$y^2 + xy + y = x^3 - x^2$	318.95	331	-3.78%

Table 2. Data on $\pi_{E,2}(10^{13})$ for various E.

E	predicted	actual	% error
$y^2+y=x^3-x$	3.03	3	1.05%
$y^2=x^3+6x-2$	12.59	12	4.66%
$y^2+y=x^3+x^2$	3.04	2	34.10%
$y^2+xy+y=x^3-x^2$	3.02	4	−32.48%

Table 3. Data on $\pi_{E,3}(10^{13})$ for various E.

The four elliptic curves E under consideration satisfy

$$\big[\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}):\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})\big]\le 2 \tag{23}$$

for each $n\ge 1$ (see [Serre 1972, pp. 309–311; Lang and Trotter 1976, p. 51]). As shown in [Serre 1972, 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 (23) a *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 [Jones 2010; Radhakrishnan 2008]). 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

$$C_L:=\frac{\phi_L(0)}{L}\cdot\lim_{k\to\infty}\frac{n_k^L\big|\mathrm{GL}_2(\mathbb{Z}/n_k\mathbb{Z})^L_{\text{ali-cycle}}\big|}{\big|\mathrm{GL}_2(\mathbb{Z}/n_k\mathbb{Z})^L\big|}=\frac{\phi_L(0)}{L}\cdot\prod_{l\text{ prime}}\frac{l^L\big|\mathrm{GL}_2(\mathbb{F}_l)^L_{\text{ali-cycle}}\big|}{\big|\mathrm{GL}_2(\mathbb{F}_l)^L\big|},$$

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. For $L=2$ one has

$$\begin{aligned}C_2&=\frac{\phi_2(0)}{2}\cdot\prod_{l\text{ prime}}\frac{l^2\big|\mathrm{GL}_2(\mathbb{F}_l)^2_{\text{ali-cycle}}\big|}{\big|\mathrm{GL}_2(\mathbb{F}_l)^2\big|}=\frac{8}{3\pi^2}\cdot\prod_{l\text{ prime}}\frac{l^2(l^4-2l^3-2l^2+3l+3)}{[(l^2-1)(l-1)]^2}\\&\approx 0.077088124,\end{aligned}$$

whereas for $L=3$ one has

$$\begin{aligned}C_3&=\frac{\phi_3(0)}{3}\prod_{l\text{ prime}}\frac{l^3\big|\mathrm{GL}_2(\mathbb{F}_l)^3_{\text{ali-cycle}}\big|}{\big|\mathrm{GL}_2(\mathbb{F}_l)^3\big|}\\&=\frac{\phi_3(0)}{3}\prod_{l\text{ prime}}\frac{l^3\big[l^6-3l^5-3l^4+14l^3+(3+\chi(l))l^2-(19+3\chi(l))l-10-3\chi(l)\big]}{[(l^2-1)(l-1)]^3}\\&\approx 0.019759298,\end{aligned}$$

E	$C_{E,2}$	$C_{E,3}$	$\Delta_{sf}(E)$
$y^2+y=x^3-x$	≈ 0.077093	≈ 0.019841	37
$y^2=x^3+6x-2$	≈ 0.132151	≈ 0.082365	-3
$y^2+y=x^3+x^2$	≈ 0.077091	≈ 0.019861	-43
$y^2+xy+y=x^3-x^2$	≈ 0.077088	≈ 0.019759	-53

Table 4. Values of $C_{E,2}$, $C_{E,3}$ and $\Delta_{sf}(E)$.

where $\chi(l)=\left(\frac{-3}{l}\right)$ denotes the character of conductor 3. Table 4 gives the values of $C_{E,2}$, $C_{E,3}$ and $\Delta_{sf}(E)$ for each of the four curves under consideration. The reason the second curve has a larger value of $C_{E,L}$ 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

$$E\ :\ y^2=x^3-3x+4 \tag{24}$$

which was mentioned in the introduction, for which $\pi_{E,L}(x)\equiv 0$ and whose 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 $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. First, define the subgroup $H(4)\subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ 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

$$\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})=H(4)\cdot\left(I+2\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}\right). \tag{25}$$

(To see that the right-hand expression defines a subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, note that

$$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}\subseteq M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$$

is closed under addition and under $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$-conjugation.)

Even though $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})=\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$ is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, and so one has $4\mid m_E$. Furthermore, in this case 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

$$\mathcal{G}_E=\mathcal{G}_E(m_E)\twoheadrightarrow\mathcal{G}_E(4), \tag{26}$$

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 (25), one finds that the directed graph $\mathcal{G}_E(4)$ is:

$$(2, 1) \qquad\qquad (2, -1) \longleftarrow (-1, 1) \longrightarrow (0, -1) \tag{27}$$

Infinitely many primes p for which $|E(\mathbb{F}_p)|$ is prime. The non-CM case of a conjecture of Koblitz (see [Koblitz 1988] and also [Zywina 2011]) 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 (24), we see by the surjectivity of (26) together with (27) 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.

Finitely many aliquot cycles for E. Continuing with the example (24), by the surjectivity of (26) together with (27), we see that $\mathcal{G}_E$ contains no closed walks at all. By Proposition 2.6, there are only finitely many aliquot cycles $(p_1, p_2, \dots, p_L)$ for E. This particular example may be explained as follows. Whenever $p_2 = |E(\mathbb{F}_{p_1})|$ for some prime p_1, we see from (27) 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

$$\big(\mathrm{tr}(\mathrm{Frob}_{\mathbb{Q}(E[4])}(p_2)), \det(\mathrm{Frob}_{\mathbb{Q}(E[4])}(p_2))\big) \in \{(0, -1), (2, -1)\},$$

in which case $|E(\mathbb{F}_{p_2})|$ must be even. One deduces that E has no aliquot cycles of length $L \geq 2$, and indeed no aliquot *sequences* of length $L \geq 3$.

Remark 4.1. There is a modular curve X of level 4 and genus 0 with $|X(\mathbb{Q})| = \infty$, whose noncuspidal $\mathbb{Q}$-rational points correspond to elliptic curves E' for which $-\Delta_{E'}$ is a perfect square. For almost all such elliptic curves E', one may find an appropriate twist E of E' for which (25) holds, and thus for which $\lim_{x\to\infty} \pi_{E,L}(x) < \infty$ for $L \geq 2$. The elliptic curve (24) is one such example.

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 many thanks to A. Sutherland, who provided help with the computations (a description of the software used therein may be found in [Kedlaya and Sutherland 2008]). Finally, thanks to the anonymous referee for a careful reading of the manuscript and several helpful comments.

References

[Balog et al. 2011] A. Balog, A.-C. Cojocaru, and C. David, "Average twin prime conjecture for elliptic curves", *Amer. J. Math.* **133**:5 (2011), 1179–1229. MR 2012j:11118 Zbl 05969056

[David and Pappalardi 1999] C. David and F. Pappalardi, "Average Frobenius distributions of elliptic curves", *Internat. Math. Res. Notices* 4 (1999), 165–183. MR 2000g:11045 Zbl 0934.11033

[Gottschlich 2012] A. Gottschlich, "On positive integers n dividing the nth term of an elliptic divisibility sequence", *New York J. Math.* **18** (2012), 409–420. MR 2928585 Zbl 06098855

[Jones 2010] N. Jones, "Almost all elliptic curves are Serre curves", *Trans. Amer. Math. Soc.* **362**:3 (2010), 1547–1570. MR 2011d:11130 Zbl 1204.11088

[Jones 2012] N. Jones, "Elliptic aliquot cycles of fixed length", preprint, 2012. arXiv 1212.1010

[Kedlaya and Sutherland 2008] K. S. Kedlaya and A. V. Sutherland, "Computing L-series of hyperelliptic curves", pp. 312–326 in *Algorithmic number theory*, edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, Berlin, 2008. MR 2010d:11070 Zbl 1232.11078

[Koblitz 1988] N. Koblitz, "Primality of the number of points on an elliptic curve over a finite field", *Pacific J. Math.* **131**:1 (1988), 157–165. MR 89h:11023 Zbl 0608.10010

[Lang and Trotter 1976] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions: Distribution of Frobenius automorphisms in* $\mathrm{G}L_2$*-extensions of the rational numbers*, Lecture Notes in Mathematics **504**, Springer, Berlin, 1976. MR 58 #27900 Zbl 0329.12015

[Mazur 1972] B. Mazur, "Rational points of abelian varieties with values in towers of number fields", *Invent. Math.* **18** (1972), 183–266. MR 56 #3020 Zbl 0245.14015

[Radhakrishnan 2008] V. Radhakrishnan, *An asymptotic formula for the number of non–Serre curves in a two-parameter family of elliptic curves*, Ph.D. thesis, University of Colorado at Boulder, 2008, Available at http://search.proquest.com/docview/304629348. MR 2711545

[Serre 1968] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, New York, 1968. MR 41 #8422 Zbl 0186.25701

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. In French. MR 52 #8126 Zbl 0235.14012

[Silverman and Stange 2011] J. H. Silverman and K. E. Stange, "Amicable pairs and aliquot cycles for elliptic curves", *Exp. Math.* **20**:3 (2011), 329–357. MR 2012g:11109

[Taylor 2008] R. Taylor, "Automorphy for some l-adic lifts of automorphic mod l Galois representations, II", *Publ. Math. Inst. Hautes Études Sci.* 108 (2008), 183–239. MR 2010j:11085 Zbl 1169.11021

[Zywina 2011] D. Zywina, "A refinement of Koblitz's conjecture", *Int. J. Number Theory* **7**:3 (2011), 739–769. MR 2012e:11107 Zbl 05913798

Received July 16, 2012. Revised December 10, 2012.

NATHAN JONES
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF MISSISSIPPI
HUME HALL 305
P.O. BOX 1848
UNIVERSITY, MS 38677
UNITED STATES

ncjones@olemiss.edu

PACIFIC JOURNAL OF MATHEMATICS

msp.org/pjm

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2013 is US $400/year for the electronic version, and $485/year for print and electronic.
Subscriptions, requests for back issues and changes of subscribers address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and the Science Citation Index.

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published monthly except July and August. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 263 No. 2 June 2013

0030-8730(201306)263:2;1-5