Baier, S., and N. Jones. (2009) "A Refined Version of the Lang-Trotter Conjecture,"
International Mathematics Research Notices, Vol. 2009, No. 3, pp. 433–461
Advance Access publication December 30, 2008
doi:10.1093/imrn/rnn136

A Refined Version of the Lang–Trotter Conjecture

Stephan Baier[1] and Nathan Jones[2]

[1]Jacobs University Bremen, School of Engineering and Science, P.O. Box 750 561, 28725 Bremen, Germany and [2]Centre de Recherches Mathématiques, Université de Montréal, P.O. Box 6128, Centre-ville Station, Montréal, Québec H3C 3J7, Canada

Correspondence to be sent to: s.baier@jacobs-university.de

Let E be an elliptic curve defined over the rational numbers and r a fixed integer. Using a probabilistic model consistent with the Chebotarev density theorem for the division fields of E and the Sato–Tate distribution, Lang and Trotter conjectured an asymptotic formula for the number of primes up to x which have Frobenius trace equal to r, where r is a *fixed* integer. However, as shown in this note, this asymptotic estimate cannot hold for *all* r in the interval $|r| \leq 2\sqrt{x}$ with a uniform bound for the error term, because an estimate of this kind would contradict the Chebotarev density theorem as well as the Sato–Tate conjecture. The purpose of this note is to refine the Lang–Trotter conjecture, by taking into account the "semicircular law," to an asymptotic formula that conjecturally holds for arbitrary integers r in the interval $|r| \leq 2\sqrt{x}$, with a uniform error term. We demonstrate consistency of our refinement with the Chebotarev density theorem for a fixed division field, and with the Sato–Tate conjecture. We also present numerical evidence for the refined conjecture.

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ of minimal discriminant Δ_E. For any prime number p not dividing Δ_E, let E_p denote the reduction of E modulo p and

$$a_E(p) := p + 1 - \#E_p(\mathbb{Z}/p\mathbb{Z})$$

Received January 25, 2008; Revised October 9, 2008; Accepted October 20, 2008
Communicated by Prof. Barry Mazur

the trace of Frobenius at p. For a fixed integer r, define the prime-counting function

$$\pi_{E,r}(x) := \sum_{\substack{p \le x, p \nmid \Delta_E \\ a_E(p) = r}} 1.$$

By studying a probabilistic model consistent with the Chebotarev density theorem for the division fields of E and the Sato–Tate distribution, Lang and Trotter formulated the following conjecture.

Conjecture 1. (Lang–Trotter) Let E be an elliptic curve over $\mathbb{Q}$ and $r \in \mathbb{Z}$ a fixed integer. If $r = 0$ then assume additionally that E has no complex multiplication. Then

$$\pi_{E,r}(x) = C_{E,r} \int_2^x \frac{dt}{2\sqrt{t}\log t} + o\left(\frac{\sqrt{x}}{\log x}\right) = C_{E,r}\,\frac{\sqrt{x}}{\log x} + o\left(\frac{\sqrt{x}}{\log x}\right) \tag{1}$$

as $x \to \infty$, where $C_{E,r}$ is a specific non-negative constant. □

Remark 1. It is possible that the constant $C_{E,r} = 0$, in which case we interpret the asymptotic to mean that there are only finitely many primes p for which $a_E(p) = r$. □

We note that if $r = 0$ and E has complex multiplication, Deuring [3] showed that half of the primes p satisfy $a_E(p) = 0$, i.e.

$$\pi_{E,0}(x) \sim \frac{\pi(x)}{2} \quad \text{as } x \to \infty.$$

More precisely, for any constant $C > 1$, we have

$$\pi_{E,0}(x) = \frac{1}{2} Li(x) + O\left(\frac{x}{(\log x)^C}\right), \tag{2}$$

where the implied O-constant depends only on E and C, and

$$Li(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} \quad \text{as } x \to \infty.$$

Primes p with $a_E(p) = 0$ are known as "supersingular primes."

We point out that Conjecture 1 is formulated for *fixed* numbers r. The purpose of this note is to refine Conjecture 1 to an asymptotic formula, which conjecturally holds for

arbitrary integers r in the interval $-2\sqrt{x} \le r \le 2\sqrt{x}$, with a uniform error term, where the case $r = 0$ is excluded if E has complex multiplication. Our refinement is stated below.

Conjecture 2. Let E be an elliptic curve over $\mathbb{Q}$. Fix any $C > 1$. Then, uniformly for $|r| \le 2\sqrt{x}$, where the case $r = 0$ is excluded if E has CM, we have

$$\pi_{E,r}(x) = C_{E,r} \int_{\max\{2,r^2/4\}}^{x} \frac{\Phi_E(r/(2\sqrt{t}))}{2\sqrt{t}\log t} dt + O_{E,C}\left(\frac{\sqrt{x}}{(\log x)^C}\right), \tag{3}$$

where $C_{E,r}$ is the same constant appearing in Conjecture 1, and

$$\Phi_E(z) := \begin{cases} \sqrt{1-z^2} & \text{if } E \text{ does not have CM} \\ \frac{1}{\sqrt{1-z^2}} & \text{if } E \text{ has CM.} \end{cases} \tag{4}$$

□

For convenience, throughout the sequel, we denote the main term on the right-hand side of (3) by $F_{E,r}(x)$, i.e. we set

$$F_{E,r}(x) := C_{E,r} \int_{\max\{2,r^2/4\}}^{x} \frac{\Phi_E(r/(2\sqrt{t}))}{2\sqrt{t}\log t} dt \tag{5}$$

if $x \ge \max\{2, r^2/4\}$. We note that this term is bounded from above by the main term in Conjecture 1, i.e.

$$F_{E,r}(x) \ll C_{E,r} \frac{\sqrt{x}}{\log x}. \tag{6}$$

Conjecture 2 is rather "conservative" in the sense that the O-term bounding the error is smaller than the main term by no more than a factor of a power of logarithm. In Section 3, we shall give a heuristic suggesting the following sharpening of Conjecture 2, which essentially states that the the error term in (3) should not be much larger than the square root of the main term.

Conjecture 3. Let E be an elliptic curve over $\mathbb{Q}$ and $\varepsilon > 0$. Assume that $|r| \le 2\sqrt{x}$. Assume further that $r \ne 0$ if E has CM. Then

$$\pi_{E,r}(x) = F_{E,r}(x) + O_{E,\varepsilon}(x^{\varepsilon}\sqrt{1 + F_{E,r}(x)}), \tag{7}$$

where the function $F_{E,r}(x)$ is defined as in (5). □

Our work is motivated by the natural desire to sum the prime-counting function $\pi_{E,r}(x)$ over r in a fixed residue class and recover the Chebotarev density theorem for the appropriate division field of E. More precisely, fix a modulus q and denote by $\mathbb{Q}(E[q])$ the qth division field of E, i.e. the field obtained by adjoining to $\mathbb{Q}$ the x and y coordinates of the q-torsion points of a given Weierstrass model of E. Fixing a basis

$$E[q] \simeq \mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$$

of $E[q]$ over $\mathbb{Z}/q\mathbb{Z}$, we may view the Galois group

$$\mathrm{Gal}\,(\mathbb{Q}(E[q])/\mathbb{Q}) \leq GL_2(\mathbb{Z}/q\mathbb{Z})$$

as a subgroup of $GL_2(\mathbb{Z}/q\mathbb{Z})$. Finally, let us denote by

$$\delta_{a,q} := \frac{|\{g \in \mathrm{Gal}\,(\mathbb{Q}(E[q])/\mathbb{Q}) : \mathrm{tr}\, g \equiv a \mod q\}|}{|\mathrm{Gal}\,(\mathbb{Q}(E[q])/\mathbb{Q})|}$$

the Chebotarev factor. The Chebotarev density theorem for the field $\mathbb{Q}(E[q])$ implies that, for any fixed constant $C > 1$, we have

$$\sum_{\substack{p \leq x, p \nmid q\Delta_E \\ a_E(p) \equiv a \mod q}} 1 \quad = \quad \delta_{a,q}\, Li(x) + O\left(\frac{x}{(\log x)^C}\right). \tag{8}$$

We begin by observing that

$$\sum_{\substack{r \equiv a \mod q \\ |r| \leq 2\sqrt{x}}} \left(\sum_{\substack{p \leq x, p \nmid \Delta_E \\ a_E(p) = r}} 1 \right) \quad = \quad \left(\sum_{\substack{p \leq x, p \nmid q\Delta_E \\ a_E(p) \equiv a \mod q}} 1 \right) + O_q(1).$$

Thus, paying attention only to the main terms in (8) and Conjecture 1, and taking (2) in the CM case into account, it is natural to hope that

$$\left(\sum_{\substack{r \equiv a \mod q \\ 0 < |r| \leq 2\sqrt{x}}} C_{E,r} \right) \frac{\sqrt{x}}{\log x} \quad \sim \quad \left(\delta_{a,q} - \frac{\gamma(E,a,q)}{2} \right) \frac{x}{\log x},$$

where

$$\gamma(E,a,q) = \begin{cases} 1 & \text{if } E \text{ has CM and } a \equiv 0 \mod q, \\ 0 & \text{otherwise.} \end{cases}$$

However, this is not the case. In fact, as proved in Section 4, one has the following.

Proposition 1. Let A be any integer and B any positive integer. Set $M := \max\{|A|, |A+B|\}$. Then

$$\sum_{\substack{r \equiv a \bmod q \\ A < r \leq A+B \\ r \neq 0}} C_{E,r} = \begin{cases} \frac{1}{\pi}\left(\delta_{a,q} - \frac{\gamma(E,a,q)}{2}\right) B + O_E(q \log^3 M) & \text{if } E \text{ has CM} \\ \frac{2}{\pi}\delta_{a,q} B + O_E(q) & \text{if } E \text{ has no CM.} \end{cases} \tag{9}$$

□

It follows that

$$\left(\sum_{\substack{r \equiv a \bmod q \\ 0 < |r| \leq 2\sqrt{x}}} C_{E,r}\right) \frac{\sqrt{x}}{\log x} \sim \frac{1}{\lambda_E} \frac{8}{\pi}\left(\delta_{a,q} - \frac{\gamma(E,a,q)}{2}\right) \frac{x}{\log x} \tag{10}$$

as $x \to \infty$, where

$$\lambda_E := \begin{cases} 2 & \text{if } E \text{ has CM} \\ 1 & \text{if } E \text{ has no CM.} \end{cases}$$

Hence, the conjectural asymptotic estimate (1) cannot hold for all r in the interval $|r| \leq 2\sqrt{x}$ with a uniform bound for the error term of size $o(\sqrt{x}/\log x)$. We shall further see that (1) with a uniform bound for the error term also contradicts the Sato–Tate conjecture (this follows from Theorem 4, proved in Section 6). We shall show that our refined Conjecture 2 (resp. Conjecture 3) remedies these discrepancies. Moreover, in Section 6 we shall demonstrate that in a certain sense, the main term in Conjectures 2 (resp. Conjecture 3) is the only possibility.

The paper is organized as follows. In Section 2, we motivate Conjectures 2 and 3. We also discuss briefly in which regions of the (x,r)-plane our main term differs significantly from that in Conjecture 1 and under which circumstances (3) (resp. (7)) is actually an *asymptotic* estimate. In Section 3, we give a detailed description of the constants $C_{E,r}$. In Section 4, we provide a proof of Proposition 1, which will serve as a key tool in what follows. In Section 5, we prove that Conjecture 2 is consistent with the Chebotarev density theorem, and in Section 6, we demonstrate the consistency with the distribution of $a_E(p)/(2\sqrt{p}) \in [-1,1]$. Finally, in Section 7, we present numerical evidence for Conjectures 2 and 3.

2 The Refinement

The work of Lang-Trotter takes account of algebraic and analytic information in coming up with the factor $C_{E,r}$. However, the analytic part of their heuristic replaces the "semi-circular law" of Sato-Tate with a limiting constant value. This works well for fixed (or small) r's, as considered in their work. However, when we consider arbitrary r's in the interval $-2\sqrt{x} \le r \le 2\sqrt{x}$, it becomes necessary to introduce an analytic factor corresponding to the Sato-Tate distribution in the non-CM case and to another characteristic distribution in the CM case.

Roughly speaking, the heuristics of Lang and Trotter predict that the probability that a large natural number p is prime and satisfies $a_E(p) = r$ is

$$\approx C_{E,r} \frac{1}{2\sqrt{p}\log p}. \tag{11}$$

Thus, one expects that

$$\pi_{E,r}(x) = C_{E,r} \sum_{2\le n\le x} \frac{1}{2\sqrt{n}\log n} + o\left(\frac{\sqrt{x}}{\log x}\right) = C_{E,r} \int_2^x \frac{dt}{2\sqrt{t}\log t} + o\left(\frac{\sqrt{x}}{\log x}\right),$$

as $x \to \infty$. We note that

$$\int_2^x \frac{dt}{2\sqrt{t}\log t} \sim \frac{\sqrt{x}}{\log x}, \quad \text{as } x \to \infty.$$

To be precise, the reason for the apparent inconsistency (10) between Conjecture 1 and (8) is two-fold:

R1 When r is not very small compared with $\sqrt{x}$, the heuristic (11) needs to be corrected by a factor accounting for the distribution of

$$\frac{a_E(p)}{2\sqrt{p}} \in [-1, 1].$$

R2 Since $\pi_{E,r}(x)$ only counts primes p that are $\ge r^2/4$, the interval of integration in Conjecture 1 should be $[r^2/4, x]$ rather than $[2, x]$.

Note that for fixed r and large x, neither of these observations affect the asymptotic.

2.1 The distribution of $a_E(p)/(2\sqrt{p}) \in [-1,1]$

The appropriate measure for equidistribution of the quantity

$$\frac{a_E(p)}{2\sqrt{p}} \in [-1,1]$$

is $\phi_E(z)dz$, where $\phi_E(z)$ is defined by

$$\phi_E(z) := \begin{cases} \frac{2}{\pi}\sqrt{1-z^2} & \text{if } E \text{ does not have CM} \\ \frac{1}{2\pi}\,\frac{1}{\sqrt{1-z^2}} & \text{if } E \text{ has CM.} \end{cases} \tag{12}$$

In the CM case, this distribution law is a classical theorem of Deuring [3].

Theorem 1. (Deuring) Suppose that K is an imaginary quadratic field and that E has complex multiplication by an order in K, i.e.

$$\mathrm{End}_{\overline{\mathbb{Q}}}(E) \otimes \mathbb{Q} \simeq K.$$

Then for any prime number p of good reduction for E, we have

$$a_E(p) = 0 \iff p \text{ is inert in } K.$$

Furthermore, if $I \subset [-1,1]$ is some interval with $0 \notin I$, then

$$\lim_{x\to\infty} \frac{\left|\left\{p \le x : p \nmid \Delta_E, \frac{a_E(p)}{2\sqrt{p}} \in I\right\}\right|}{\pi(x)} = \int_I \phi_E(z)dz, \tag{13}$$

where

$$\phi_E(z) = \frac{1}{2\pi}\,\frac{1}{\sqrt{1-z^2}}. \qquad \square$$

In the non-CM case, the distribution law was conjectured independently by Sato and Tate (see [10]).

Conjecture 4. (Sato–Tate) For an elliptic curve E over $\mathbb{Q}$ without complex multiplication and any subinterval $I \subseteq [-1,1]$, we have

$$\lim_{x\to\infty} \frac{\left|\left\{p \le x : p \nmid \Delta_E, \frac{a_E(p)}{2\sqrt{p}} \in I\right\}\right|}{\pi(x)} \sim \int_I \phi_E(z)dz,$$

where $\phi_E(z) = \frac{2}{\pi}\sqrt{1-z^2}$. □

We note that the Sato–Tate conjecture has been proved by L. Clozel, M. Harris, N. Shepherd-Barron, and R. Taylor for all elliptic curves E over totally real fields (in particular, over the rationals) satisfying the mild condition of having multiplicative reduction at some prime (see [11] and the references therein).

2.2 Modifying the heuristic

Observation R1 and the above facts on the distribution of $a_E(p)/(2\sqrt{p})$ suggest that the heuristic (11) should be corrected by the factor $\phi_E(r/(2\sqrt{p}))$ and then be normalized by an appropriate constant factor $\mathfrak{C}$, which we specify later. Hence, the probability that a large natural number p is a prime with $a_E(p) = r$ should be

$$\sim \mathfrak{C}C_{E,r}\frac{\phi_E(r/(2\sqrt{p}))}{2\sqrt{p}\log p}.$$

This modified heuristic, taken together with observation R2, suggests that the prime counting function $\pi_{E,r}(x)$ behaves approximately like

$$\mathfrak{C}C_{E,r}\int_{\max\{2,r^2/4\}}^{x} \frac{\phi_E(r/(2\sqrt{t}))}{2\sqrt{t}\log t}dt.$$

For this approximation to be consistent with Conjecture 1, the normalization factor must be $\mathfrak{C} = 1/\phi_E(0)$. This leads us to the main term in Conjecture 2 upon noting that $\Phi_E(z) = \phi_E(z)/\phi_E(0)$.

Furthermore, taking the bound (6) and the order of magnitude of the O-term in (8) into account, it seems reasonable to conjecture that the error in our approximation of

$\pi_{E,r}(x)$ is smaller than $\sqrt{x}/\log x$ by at least a factor of $(\log x)^C$, which gives the error term in Conjecture 2.

We are not only interested in the correct form of the main term in the approximation of $\pi_{E,r}(x)$ but also in the true order of magnitude of the error term. We note that, assuming the generalized Riemann hypothesis, the true order of magnitude of the error term in (8) is $O\left(x^{1/2+\varepsilon}\right)$, which is by almost a factor of $\sqrt{x}$ smaller than $x/(\log x)^C$. Similarly, a much sharper bound than $O(\sqrt{x}/(\log x)^C)$ should hold for the error term in (1). Indeed, if we assume that the events "p is prime with $a_E(p) = r$" are independent as p runs over the natural numbers, then Chebyshev's law of large numbers suggests that the error term should not be much larger than the square root of the main term. This leads us to the error term

$$O_{E,\varepsilon}(x^{\varepsilon}\sqrt{1 + F_{E,r}(x)}) \tag{14}$$

in Conjecture 3. The reason we include the term 1 in the error bound is so that the statement continues to hold true even when $C_{E,r} = 0$.

We point out that the implied constant in (14) cannot be independent of the elliptic curve E. To see this, pick any large integer r and then for any prime p in the range $r^2/4 < p < x$, find $E_p \pmod p$ such that $a_p(E_p) = r$. Then select an elliptic curve E over $\mathbb{Q}$ with $E \equiv E_p \pmod p$ for all such p. Hence, if one desires to state a conjecture which is uniform in E, one certainly needs to bring into the error term some information about E. It is conceivable that one might replace (14) with

$$O_{\varepsilon}((N_E x)^{\varepsilon}\sqrt{1 + F_{E,r}(x)}),$$

where N_E is the conductor of E.

2.3 Comparison of the main term and error term

In the following, we compare the sizes of the main term $F_{E,r}(x)$ and the error terms in (3) and (7), respectively. We begin with some comments on the constants (see Section 3 for details).

If $C_{E,r} = 0$, then it is conjectured that only finitely many primes satisfy $a_E(p) = r$ in which case (3) is trivial. In the following, we assume that $C_{E,r} \neq 0$. If E has CM by an order in an imaginary quadratic field K, then (as we will see in Section 3) the nonzero

values of the constant satisfy the bound

$$C_{E,r} \neq 0 \Longrightarrow \frac{1}{\log\log(3+|r|)} \ll_E C_{E,r} \ll_E \log\log(3+|r|). \tag{15}$$

It follows that in this case the main term $F_{E,r}(x)$ satisfies the bound

$$\frac{\sqrt{4x-r^2}}{\log x \log\log(3+|r|)} \ll_E F_{E,r}(x) \ll_E \frac{\sqrt{4x-r^2}}{\log x} \log\log(3+|r|).$$

If E has no CM, then the nonzero values of the constant $C_{E,r}$ are uniformly bounded from below and above as r varies, i.e. there exist positive constants c_E and C_E for which

$$C_{E,r} \neq 0 \Longrightarrow \quad c_E \leq C_{E,r} \leq C_E. \tag{16}$$

Hence, in this case the main term in $F_{E,r}(x)$ satisfies the bound

$$F_{E,r}(x) \asymp_E \frac{(4x-r^2)^{3/2}}{x\log x}.$$

Now, let $B > 0$ be arbitrarily given. By the above observations, if the constant C is chosen large enough, then the error term $O(\sqrt{x}/(\log x)^C)$ in (3) is small compared to the main term if $|r| \leq 2\sqrt{x}(1-1/(\log x)^B)$ and x is sufficiently large. Hence, in this case, (3) is an asymptotic estimate. In all other cases, (3) implies an estimate for $\pi_{E,r}(x)$ which is still nontrivial.

Similarly, (7) is an asymptotic estimate if x is large and $|r| \leq 2\sqrt{x}(1-x^{-\delta})$, where δ is a fixed positive number satisfying $\delta < 1$ in the CM case and $\delta < 1/3$ in the non-CM case (provided ε is chosen small enough).

We also note that (3) as well as (7) imply (1) if $r = o(\sqrt{x})$. Hence, Conjecture 1 is contained in Conjecture 2 as well as in Conjecture 4. If $|r| > D\sqrt{x}$ for some fixed positive D, then the main term in (1) is significantly larger than the main term $F_{E,r}(x)$ in (3) and (7).

3 The constants $C_{E,r}$

We now give a description of the constants $C_{E,r}$. The reader may find more details in [6].

We first introduce the notation

$$G_E(n) := \begin{cases} \mathrm{Gal}\,(K(E[n])/K) & \text{if } E \text{ has CM by the imaginary quadratic field } K \\ \mathrm{Gal}\,(\mathbb{Q}(E[n])/\mathbb{Q}) & \text{if } E \text{ has no CM.} \end{cases}$$

We further set

$$H_E(n) := \begin{cases} (\mathcal{O}/n\mathcal{O})^* & \text{if } E \text{ has CM by an order } \mathcal{O} \text{ in } K \\ GL_2(\mathbb{Z}/n\mathbb{Z}) & \text{if } E \text{ has no CM.} \end{cases}$$

We note that $G_E(n)$ can be viewed as a subgroup of $H_E(n)$. With this in mind, for any subgroup G of $H_E(n)$ and any integer r, we write

$$G_r := \{g \in G \,:\, \mathrm{tr}\, g \equiv r \mod n\}.$$

Following Lang and Trotter [6], we now define the constant $C_{E,r}$ by

$$C_{E,r} := \phi_E(0)\frac{m_E|G_E(m_E)_r|}{|G_E(m_E)|}\prod_{\substack{\ell \text{ prime} \\ \ell \nmid m_E}} \frac{\ell|H_E(\ell)_r|}{|H_E(\ell)|}, \tag{17}$$

where the positive integer m_E is given by the following theorem, the celebrated non-CM case of which is due to Serre [8].

Theorem 2. Suppose that E is an elliptic curve over $\mathbb{Q}$. Then there exists a positive integer m_E so that, for any positive integer n, we have

$$G_E(n) \simeq \pi^{-1}(G_E(\gcd(n, m_E))),$$

where $\pi : H_E(n) \longrightarrow H_E(\gcd(n, m_E))$ denotes the canonical projection. In particular, if ℓ is a prime not dividing m_E, then $G_E(\ell) \simeq H_E(\ell)$. □

Note that the conclusion of Theorem 2 and (17) continue to hold if one replaces the integer m_E by any multiple. For notational convenience, we will assume in the CM case that

$$\left(4 \prod_{\ell \text{ ramified in } \mathcal{O}} \ell\right) \quad \text{divides } m_E. \tag{18}$$

Under this assumption, we further have the following explicit description of the cardinalities of $H_E(\ell)$ and $H_E(\ell)_r$ if $\ell \nmid m_E$.

Lemma 1. Let r be any integer and ℓ be a prime not dividing m_E (in particular, ℓ does not ramify in $\mathcal{O}$ if E has CM by $\mathcal{O}$). If E does not have CM, then

$$|H_E(\ell)| = l(l-1)^2(l+1) \tag{19}$$

and

$$|H_E(\ell)_r| = \begin{cases} \ell^2(\ell-1) & \text{if } r \equiv 0 \mod \ell \\ \ell(\ell^2-\ell-1) & \text{otherwise.} \end{cases} \tag{20}$$

If E has CM by an order $\mathcal{O}$ in an imaginary quadratic field K, then

$$|H_E(\ell)| = (\ell-1)(\ell-\chi_{\mathcal{O}}(\ell)) \tag{21}$$

and

$$|H_E(\ell)_r| = \begin{cases} \ell-1 & \text{if } r \equiv 0 \mod \ell \\ \ell-(1+\chi_{\mathcal{O}}(\ell)) & \text{otherwise,} \end{cases} \tag{22}$$

where $\chi_{\mathcal{O}}(\ell)$ is the character determining the splitting of ℓ in the order $\mathcal{O}$, namely

$$\chi_{\mathcal{O}}(\ell) := \begin{cases} 1 & \text{if } \ell \text{ splits in } \mathcal{O} \\ -1 & \text{if } \ell \text{ is inert in } \mathcal{O}. \end{cases}$$ □

Proof. We leave the proofs of (19) and (20) to the reader and deal only with the CM case. We note that since E is defined over $\mathbb{Q}$, the class number $h(\mathcal{O})$ of the order $\mathcal{O}$ equals 1 (see [9, p. 99, Proposition1.2 (b)], which works out the case where $\mathcal{O}$ is the full ring of integers). Now for any prime ℓ that is not ramified in $\mathcal{O}$, we have

$$\mathcal{O}/\ell\mathcal{O} \simeq \begin{cases} \mathbb{F}_\ell \oplus \mathbb{F}_\ell & \text{if } \ell \text{ splits in } \mathcal{O} \\ \mathbb{F}_{\ell^2} & \text{if } \ell \text{ is inert in } \mathcal{O}. \end{cases} \tag{23}$$

This implies (21) and (22). ■

Thus, if E has CM, then

$$C_{E,r} = \frac{1}{2\pi} \frac{m_E |G_E(m_E)_r|}{|G_E(m_E)|} \prod_{\substack{\ell \nmid m_E \\ \ell \mid r}} \left(1 + \frac{\chi_{\mathcal{O}}(\ell)}{\ell - \chi_{\mathcal{O}}(\ell)}\right) \prod_{\substack{\ell \nmid m_E \\ \ell \nmid r}} \left(1 - \frac{\chi_{\mathcal{O}}(\ell)}{(\ell-1)\,(\ell - \chi_{\mathcal{O}}(\ell))}\right).$$

Noting that, for fixed E, the factor $\frac{m_E |G_E(m_E)_r|}{|G_E(m_E)|}$ takes on only finitely many values as r varies, we obtain the bounds (15). If E does not have CM, then we have

$$C_{E,r} = \frac{2}{\pi} \frac{m_E |G_E(m_E)_r|}{|G_E(m_E)|} \prod_{\substack{\ell \nmid m_E \\ \ell \mid r}} \left(1 + \frac{1}{\ell^2 - 1}\right) \prod_{\substack{\ell \nmid m_E \\ l \nmid r}} \left(1 - \frac{1}{(\ell-1)(\ell^2-1)}\right).$$

Notice that the Euler product converges absolutely and (16) follows.

4 Averaging the Constants over Residue Classes

Proposition 1 will serve as a key tool in the following sections. We now provide a proof of this proposition, which has some similarity to the proof of Lemma 9 in [1], where certain constants related to $C_{E,r}$ were averaged as well. However, the algebraic structure of the relevant constants in [1] is much simpler than that of the original Lang–Trotter constants $C_{E,r}$, which we deal with in the present paper.

Our goal is to obtain an asymptotic formula for the average

$$\sum_{\substack{r \equiv a \bmod q \\ A < r \leq A+B \\ r \neq 0}} C_{E,r}.$$

As observed in the previous section, (17) continues to hold if the integer m_E appearing on the right-hand side of this equation is replaced by any multiple. Therefore, we may assume that m_E is divisible by q throughout the following. Moreover, Theorem 2 and Lemma 1 tell us that if ℓ is a prime not dividing m_E, then

$$|G_E(\ell)_r| = \begin{cases} |H_E(\ell)_1| & \text{if } \ell \nmid r \\ |H_E(\ell)_0| & \text{if } \ell \mid r. \end{cases}$$

Hence, we can write the constant in the form

$$C_{E,r} = \phi_E(0)\frac{m_E|G_E(m_E)_r|}{|G_E(m_E)|}C f(r), \tag{24}$$

where

$$C := \prod_{\ell\nmid m_E} \frac{\ell|H_E(\ell)_1|}{|H_E(\ell)|} \quad \text{and} \quad f(r) := \prod_{\substack{\ell\nmid m_E\\ \ell\mid r}} \frac{|H_E(\ell)_0|}{|H_E(\ell)_1|}.$$

Thus we have

$$\begin{aligned}\sum_{\substack{r\equiv a \bmod q\\ A<r\le A+B\\ r\neq 0}} C_{E,r} &= \phi_E(0)m_E C \sum_{\substack{r\equiv a \bmod q\\ A<r\le A+B\\ r\neq 0}} f(r)\frac{|G_E(m_E)_r|}{|G_E(m_E)|}\\ &= \phi_E(0)m_E C \sum_{\substack{b \bmod m_E\\ b\equiv a \bmod q}} \frac{|G_E(m_E)_b|}{|G_E(m_E)|} \sum_{\substack{r\equiv b \bmod m_E\\ A<r\le A+B\\ r\neq 0}} f(r).\end{aligned} \tag{25}$$

We use the Dirichlet convolution $g = f * \mu$ to rewrite the inner sum as

$$\sum_{\substack{r\equiv b \bmod m_E\\ A<r\le A+B\\ r\neq 0}} f(r) = \sum_{\substack{r\equiv b \bmod m_E\\ A<r\le A+B\\ r\neq 0}} \sum_{d\mid r} g(d) = \sum_{d=1}^{\infty} g(d) \sum_{\substack{A<r\le A+B\\ r\equiv b \bmod m_E\\ r\equiv 0 \bmod d\\ r\neq 0}} 1. \tag{26}$$

It is straightforward to show that

$$g(d) = \begin{cases} \mu^2(d)\prod_{\ell\mid d}\frac{|H_E(\ell)_0|-|H_E(\ell)_1|}{|H_E(\ell)_1|} & \text{if } \gcd(d,m_E)=1\\ 0 & \text{if } \gcd(d,m_E)>1.\end{cases} \tag{27}$$

Using Lemma 1, we see that

$$\sum_{d=1}^{\infty} g(d) = \begin{cases} \sum_{\gcd(d,m_E)=1}\frac{\mu^2(d)\cdot\chi_{\mathcal{O}}(d)}{\prod_{\ell\mid d}(\ell-1-\chi_{\mathcal{O}}(\ell))} & \text{if } E \text{ has CM by } \mathcal{O}\\ \sum_{\gcd(d,m_E)=1}\frac{\mu^2(d)}{\prod_{\ell\mid d}(\ell^2-\ell-1)} & \text{if } E \text{ has no CM.}\end{cases}$$

Note in particular that the sum $\sum_{d=1}^{\infty} g(d)$ is convergent, albeit only conditionally in the CM case. Using (26) and the Chinese Remainder Theorem, we deduce in the non-CM case

that

$$\sum_{\substack{r\equiv b \bmod m_E\\ A<r\le A+B\\ r\neq 0}} f(r) = \sum_{d=1}^{\infty} g(d)\left(\frac{B}{dm_E} + O(1)\right) = \frac{B}{m_E}\sum_{d=1}^{\infty}\frac{g(d)}{d} + O(1).$$

In the CM case, the error term is more delicate, and so (recalling that $M := \max\{|A|, |A+B|\}$), we write

$$\begin{aligned}\sum_{\substack{r\equiv b \bmod m_E\\ A<r\le A+B\\ r\neq 0}} f(r) &= \sum_{d\le M} g(d)\left(\frac{B}{dm_E} + O(1)\right)\\ &= \frac{B}{m_E}\sum_{d=1}^{\infty}\frac{g(d)}{d} + O\left(\frac{B}{m_E}\sum_{d>M}\frac{|g(d)|}{d} + \sum_{d\le M}|g(d)|\right)\\ &= \frac{B}{m_E}\sum_{d=1}^{\infty}\frac{g(d)}{d} + O((\log M)^3),\end{aligned}$$

where we have used the fact that, for $\gcd(d, m_E) = 1$ (note that then d must be odd by (18)), one has

$$|g(d)| \le \frac{1}{d}\prod_{\ell\mid d}\left(1+\frac{2}{\ell-2}\right) \ll \frac{1}{d}\prod_{\ell\mid d}\left(1+\frac{2}{\ell}\right) \ll \frac{(\log d)^2}{d} \text{ and } B \ll M.$$

Also, by (27), and noting that the sum $\sum_{d=1}^{\infty}\frac{g(d)}{d}$ converges absolutely in either case, we have

$$\sum_{d=1}^{\infty}\frac{g(d)}{d} = \prod_{\ell\nmid m_E}\left(1+\frac{g(\ell)}{\ell}\right) = \prod_{\ell\nmid m_E}\frac{|H_E(\ell)_0| + (\ell-1)|H_E(\ell)_1|}{\ell|H_E(\ell)_1|} = C^{-1}.$$

Inserting this into (25) and using the fact that

$$\sum_{\substack{b \bmod m_E\\ b\equiv a \bmod q}}\frac{|G_E(m_E)_b|}{|G_E(m_E)|} = \frac{|G_E(q)_a|}{|G_E(q)|},$$

we conclude that

$$\sum_{\substack{r\equiv a \bmod q \\ A<r\le A+B}} C_{E,r} = \phi_E(0)B\frac{|G_E(q)_a|}{|G_E(q)|} + \begin{cases} O_E(q\log^3 M) & \text{if } E \text{ has CM} \\ O_E(q) & \text{if } E \text{ has no CM.} \end{cases}$$

Proposition 1 now follows at once from the next

Lemma 2. We have

$$\frac{|G_E(q)_a|}{|G_E(q)|} = \lambda_E\left(\delta_{a,q} - \frac{\gamma(E,a,q)}{2}\right),$$

where

$$\lambda_E := \begin{cases} 2 & \text{if } E \text{ has CM} \\ 1 & \text{if } E \text{ has no CM.} \end{cases}$$ □

Proof of Lemma 2. In case E has no CM, the result is immediate. We turn to the CM case. Suppose first that $K \subseteq \mathbb{Q}(E[q])$. Noting the disjoint union

$$\mathrm{Gal}\,(\mathbb{Q}(E[q])/\mathbb{Q}) = \mathrm{Gal}\,(\mathbb{Q}(E[q])/K) \sqcup (\mathrm{Gal}\,(\mathbb{Q}(E[q])/\mathbb{Q}) - \mathrm{Gal}\,(\mathbb{Q}(E[q])/K)),$$

and that every matrix in $(\mathrm{Gal}\,(\mathbb{Q}(E[q])/\mathbb{Q}) - \mathrm{Gal}\,(\mathbb{Q}(E[q])/K))$ has trace zero, Lemma 2 follows in this case. If K is not contained in $\mathbb{Q}(E[q])$, then we must have either $q = 1$ or $q = 2$ (see [7, Lemma 6], for example). The case $q = 1$ is trivial, and if $q = 2$, we see that

$$\mathrm{Gal}\,(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq \mathrm{Gal}\,(K(E[2])/K) \hookrightarrow (\mathcal{O}/2\mathcal{O})^*.$$

By (23), it follows that $\mathrm{Gal}\,(\mathbb{Q}(E[2])/\mathbb{Q})$ is cyclic of order 1, 2, or 3, corresponding to whether 2 splits, ramifies, or remains inert in $\mathcal{O}$, respectively. We will now argue that the "cyclic of order 3" case never occurs. To see this, first note that if $\mathrm{Gal}\,(\mathbb{Q}(E[2])/\mathbb{Q})$ is cyclic of order 3, then the discriminant of E is a perfect square. Indeed, one may identify $\mathrm{Aut}(E[2])$ with S_3, the symmetric group on *three* letters, by considering its action on the nonidentity 2-torsion points

$$E[2] - \{(\infty,\infty)\} = \{(e_1,0),(e_2,0),(e_3,0)\},$$

where E is given by the Weierstrass model $y^2 = (x - e_1)(x - e_2)(x - e_3)$. If $\mathrm{Gal}\,(\mathbb{Q}(E[2])/\mathbb{Q})$ is cyclic of order three, then under this association it must correspond to the alternating group A_3. But then by Galois theory,

$$\sqrt{\Delta_E} = (e_1 - e_2)(e_1 - e_3)(e_2 - e_3) \in \mathbb{Q},$$

and so Δ_E is a perfect square. Now consider the explicit Weierstrass equations

$$y^2 = x^3 + ax, \quad y^2 = x^3 + b, \quad y^2 = x^3 - 3j(j - 1728)^3x + 2j(j - 1728)^5$$

with j-invariants 1728, 0, and

$$j \in \{54000, -12288000, 287496, -3375, 16581375, 8000, -32768, -884736,$$
$$-884736000, -147197952000, -262537412640768000\},$$

respectively. Any CM elliptic curve over $\mathbb{Q}$ is $\overline{\mathbb{Q}}$-isomorphic to one of these models, and except for the curves with j-invariant 1728, the square-free part of the discriminant $\Delta = -16(4a^3 + 27b^2)$ is independent of the model chosen. One computes the discriminants to be

$$-2^8a^3, \quad -2^4 3^3 b^2, \quad 2^{12}3^6 j^2(j - 1728)^9.$$

The only time any of these is a perfect square is for the curve $y^2 = x^3 + ax$, when $a = -t^2$, in which case $E[2]$ is rational. Thus, $\mathrm{Gal}\,(\mathbb{Q}(E[2])/\mathbb{Q})$ is never cyclic of order 3, and so must be cyclic of order 1 or 2, representable by matrices as

$$\mathrm{Gal}\,(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\} \text{ or } \left\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}.$$

In either case, we have

$$\frac{|G_E(2)_0|}{|G_E(2)|} = \delta_{0,2} = 1 \quad \text{and} \quad \frac{|G_E(2)_1|}{|G_E(2)|} = \delta_{1,2} = 0,$$

upon which Lemma 2 follows in this case. ■

We have now completed the proof of Proposition 1. □

5 Consistency with Chebotarev Density

We will now verify the consistency of our refinement with the Chebotarev density theorem for the qth division field of E. More precisely, we establish the following.

Theorem 3. Conjecture 2 implies the asymptotic (8). □

Proof. Let $F_{E,r}(x)$ be defined as in (5), i.e. $F_{E,r}(x)$ is the main term in (3). The statement of the theorem follows from (2) and the asymptotic estimate

$$\sum_{\substack{r\equiv a \bmod q\\ 0<|r|\leq 2\sqrt{x}}} F_{E,r}(x) = \left(\delta_{a,q} - \frac{\gamma(E,a,q)}{2}\right) Li(x) + O_E(q\sqrt{x}\log^3 x),$$

which we shall prove in the following. We remark that, in the (more straightforward) non-CM case, one may obtain the stronger error term $O_E(q\sqrt{x}/\log x)$. The CM case is complicated a bit by the fact that ϕ_E has a singularity at the point 1, which necessitates a truncation parameter $\delta > 0$ that will eventually approach zero. We will prove the CM case, noting that the non-CM case follows in much the same way, but without the parameter δ.

We begin by splitting the left-hand sum as

$$\sum_{\substack{r\equiv a \bmod q\\ 0<|r|\leq 2\sqrt{x}}} F_{E,r}(x) = \sum_{\substack{r\equiv a \bmod q\\ 2<r\leq 2\sqrt{x}}} F_{E,r}(x) + \sum_{\substack{r\equiv a \bmod q\\ -2\sqrt{x}<r\leq -3}} F_{E,r}(x) + O\left(\frac{\sqrt{x}}{\log x}\right).$$

We will now show that

$$\sum_{\substack{r\equiv a \bmod q\\ 2<r\leq 2\sqrt{x}}} F_{E,r}(x) = \frac{1}{2}\left(\delta_{a,q} - \frac{\gamma(E,a,q)}{2}\right) Li(x) + O_E(q\sqrt{x}\log^3 x), \tag{28}$$

the proof that

$$\sum_{\substack{r\equiv a \bmod q\\ -2\sqrt{x}<r\leq -3}} F_{E,r}(x) = \frac{1}{2}\left(\delta_{a,q} - \frac{\gamma(E,a,q)}{2}\right) Li(x) + O_E(q\sqrt{x}\log^3 x)$$

being essentially the same. Remembering that $\Phi_E(z) = \phi_E(z)/\phi_E(0)$, the left-hand side of (28) is the limit as $\delta \to 0^+$ of

$$\frac{1}{\phi_E(0)} \sum_{\substack{r \equiv a \bmod q \\ 2 < r \leq 2\sqrt{x}}} C_{E,r} \int_{r^2/4+\delta}^{x+\delta} \frac{\phi_E(r/(2\sqrt{t}))}{2\sqrt{t}\log t} dt.$$

By partial summation and by integration by parts, the above expression is equal to

$$-\frac{1}{\phi_E(0)} \int_3^{2\sqrt{x}} \left(\sum_{\substack{r \equiv a \bmod q \\ 2 < r \leq y}} C_{E,r} \right) \frac{d}{dy} \left(\int_{y^2/4+\delta}^{x+\delta} \frac{\phi_E(y/(2\sqrt{t}))}{2\sqrt{t}\log t} dt \right) dy.$$

We now invoke the estimate (9), obtaining

$$-\lambda_E \left(\delta_{a,q} - \frac{\gamma(E,a,q)}{2} \right) \int_3^{2\sqrt{x}} (y-3) \frac{d}{dy} \left(\int_{y^2/4+\delta}^{x+\delta} \frac{\phi_E(y/(2\sqrt{t}))}{2\sqrt{t}\log t} dt \right) dy + O_E(q\sqrt{x+\delta}\log^3 x), \tag{29}$$

where

$$\lambda_E := \begin{cases} 2 & \text{if } E \text{ has CM} \\ 1 & \text{if } E \text{ has no CM,} \end{cases}$$

and for the error bound, we have used the fact that

$$\int_{9/4+\delta}^{x+\delta} \frac{\phi_E(3/(2\sqrt{t}))}{2\sqrt{t}\log t} dt \ll \sqrt{x+\delta}.$$

Integrating by parts, we see that the integral in the main term is then equal to

$$\begin{aligned} \int_3^{2\sqrt{x}} \int_{y^2/4+\delta}^{x+\delta} \frac{\phi_E(y/(2\sqrt{t}))}{2\sqrt{t}\log t} dt\, dy &= \int_{9/4+\delta}^{x+\delta} \frac{1}{2\sqrt{t}\log t} \int_3^{2\sqrt{t-\delta}} \phi_E(y/(2\sqrt{t})) dy\, dt \\ &= \int_{9/4+\delta}^{x+\delta} \frac{1}{\log t} \int_{3/(2\sqrt{t})}^{2\sqrt{t-\delta}/(2\sqrt{t})} \phi_E(z) dz\, dt \\ &= \int_{9/4+\delta}^{x+\delta} \frac{dt}{\log t} \cdot \int_0^1 \phi_E(z) dz + O\left(\frac{\sqrt{x+\delta}}{\log x} \right), \end{aligned}$$

where we have made use of the facts that, for (say) $0 \le \lambda \le 1/2$,

$$2\pi \int_0^{\lambda} \phi_E(t)dt = \arcsin(\lambda) = \lambda + O(\lambda^3)$$

and

$$\arcsin(1) - \arcsin(1-\lambda) = O(\sqrt{\lambda}),$$

which imply that

$$\int_{9/4+\delta}^{x+\delta} \frac{1}{\log t} \int_0^{3/(2\sqrt{t})} \phi_E(z)dzdt = O\left(\frac{\sqrt{x+\delta}}{\log x}\right)$$

and

$$\int_{9/4+\delta}^{x+\delta} \frac{1}{\log t} \int_{1-\delta/t}^{1} \phi_E(z)dzdt = O\left(\frac{\sqrt{\delta}\sqrt{x+\delta}}{\log x}\right).$$

Inserting this into (29), using that

$$\int_0^1 \phi_E(z)dz = \begin{cases} 1/4 & \text{if } E \text{ has CM} \\ 1/2 & \text{if } E \text{ has no CM} \end{cases} = \frac{1}{2\lambda_E},$$

and letting $\delta \to 0^+$, the asymptotic estimate (28) and hence Theorem 3 is proved. ■

6 Consistency with Sato–Tate

In this section, we will establish that Conjecture 2 implies the Sato–Tate conjecture. We deduce this from the following stronger result, which implies that the correcting factor $\Phi_E(z)$ in the main term in (3) is the only possibility, i.e. it *must* be of the form given in (4).

Theorem 4. Let E be an elliptic curve over $\mathbb{Q}$, $\phi_E(z)$ be defined by (12) and $C > 1$ be any constant. Assume that there exists a continuously differentiable function $\Phi : (-1, 1) \to \mathbb{R}$

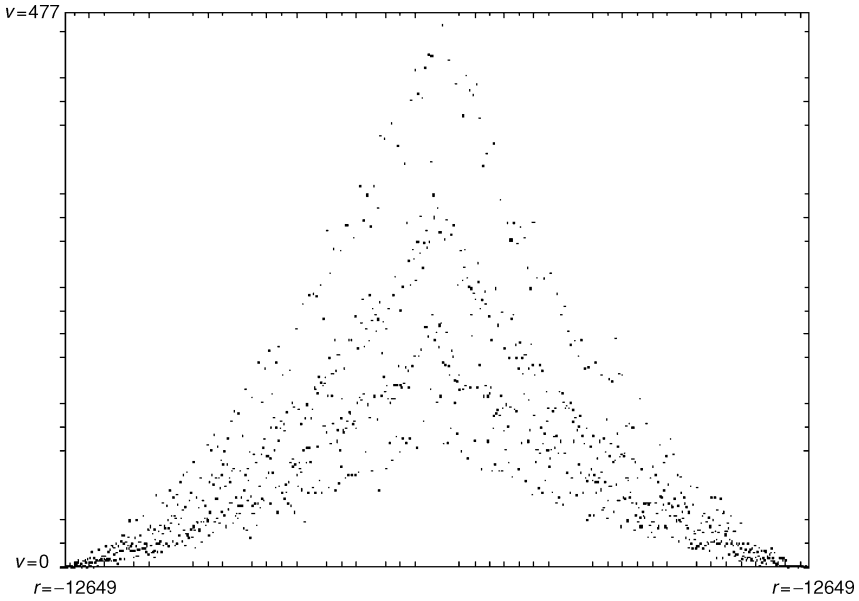

Fig. 1. The function $v = \pi_{E,r}(4 \times 10^7)$, as a function of r.

such that, uniformly for $|r| \leq 2\sqrt{x}$ (excluding $r = 0$ if E has CM),

$$\pi_{E,r}(x) = C_{E,r} \int_{\max\{2,r^2/4\}}^{x} \frac{\Phi(r/(2\sqrt{t}))}{2\sqrt{t}\log t} dt + O\left(\frac{\sqrt{x}}{(\log x)^C}\right). \tag{30}$$

Then the Sato–Tate conjecture (resp. (13) if E has CM) holds if and only if $\Phi(z) = \Phi_E(z)$ for all $z \in (-1, 1)$, where $\Phi_E(z)$ is defined as in (4). □

Proof. By continuity of Φ, we have $\Phi(z) = \Phi_E(z)$ for all $z \in (-1, 1)$ if and only if

$$\int_\alpha^\beta \Phi(z)dz = \int_\alpha^\beta \Phi_E(z)dz \tag{31}$$

for all α, β with $-1 < \alpha < \beta < 1$ and $0 \notin [\alpha, \beta]$. Moreover, equation (31) is equivalent with

$$\int_\alpha^\beta \phi(z)dz = \int_\alpha^\beta \phi_E(z)dz,$$

where we set

$$\phi(z) := \phi_E(0)\Phi(z),$$

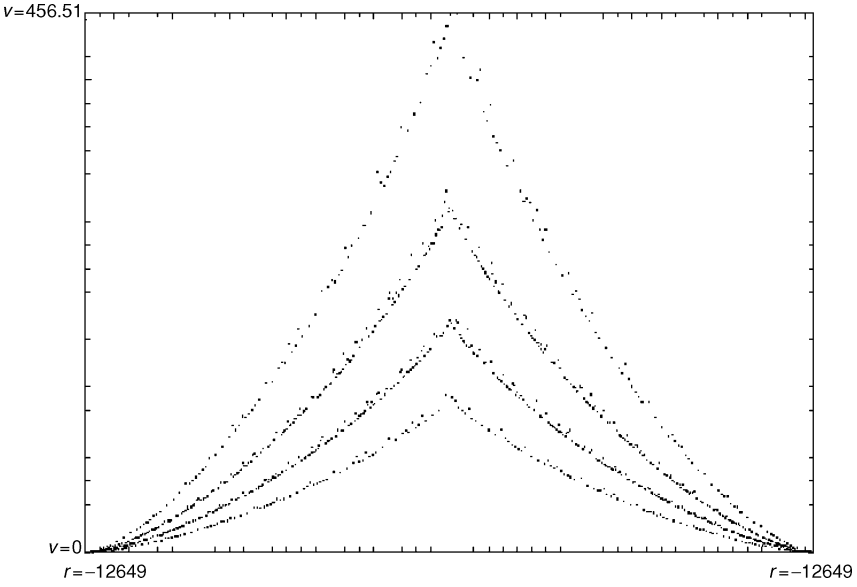

Fig. 2. The approximation $v = F_{E,r}(4 \times 10^7)$, as a function of r.

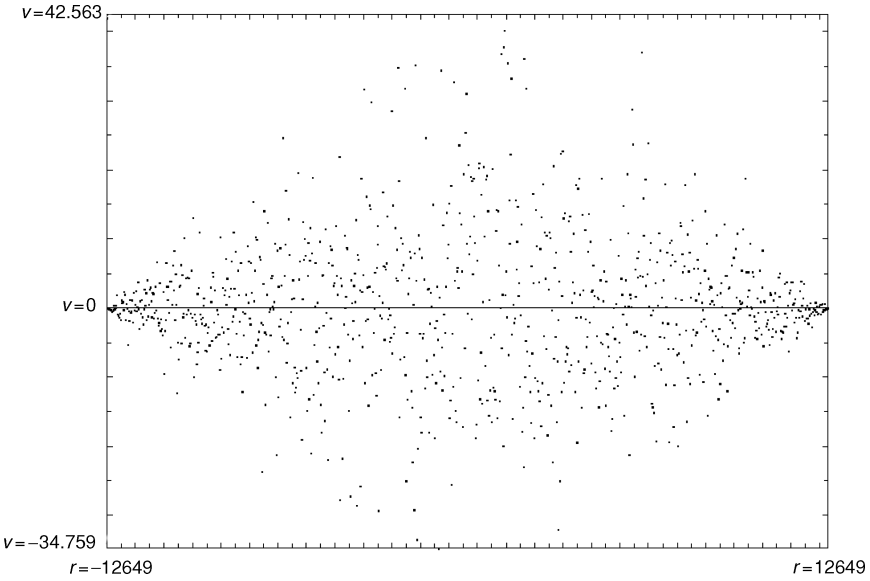

Fig. 3. The absolute error $v = \pi_{E,r}(4 \times 10^7) - F_{E,r}(4 \times 10^7)$.

and $\phi_E(z)$ is defined as in (12). Therefore, to establish the equivalence claimed in the theorem, it suffices to prove that if (30) holds, then

$$\sum_{\substack{p \le x \\ \alpha \le \frac{a_E(p)}{2\sqrt{p}} < \beta}} 1 \sim Li(x) \int_\alpha^\beta \phi(z) dz \quad \text{as } x \to \infty \tag{32}$$

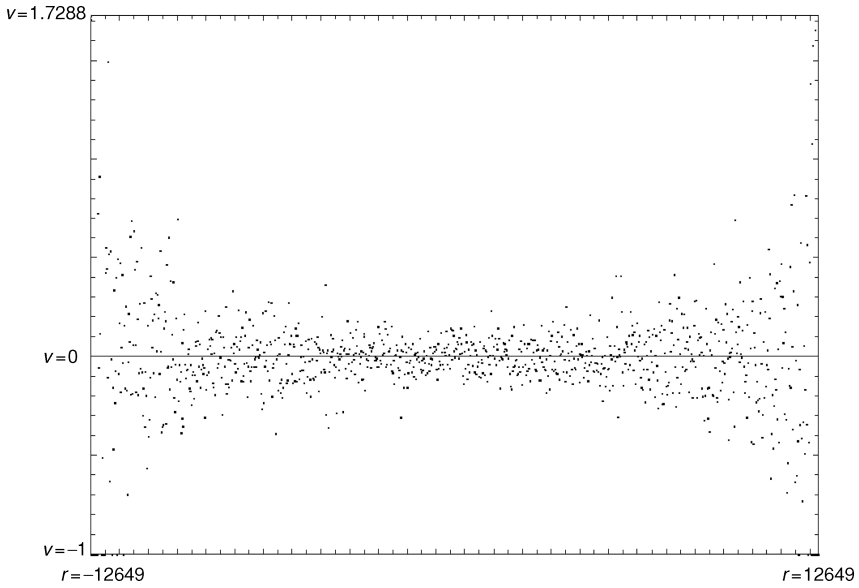

Fig. 4. The relative error $v = \frac{\pi_{E,r}(4\cdot 10^7) - F_{E,r}(4\cdot 10^7)}{F_{E,r}(4\cdot 10^7)}$.

for all fixed α, β satisfying $-1 < \alpha < \beta < 1$ and $0 \notin [\alpha, \beta]$. In the sequel, we assume that $0 < \alpha < \beta < 1$. In the complementary case $-1 < \alpha < \beta < 0$, (32) can be proved similarly.

We note that, for $a_E(p) > 0$ one has

$$\alpha \leq \frac{a_E(p)}{2\sqrt{p}} < \beta \quad \Longleftrightarrow \quad \frac{a_E(p)^2}{4\beta^2} < p \leq \frac{a_E(p)^2}{4\alpha^2}.$$

Thus,

$$\sum_{\substack{p \leq x \\ \alpha \leq \frac{a_E(p)}{2\sqrt{p}} < \beta}} 1 = \sum_{0 < r \leq 2\sqrt{x}\alpha} \left(\pi_{E,r}\left(\frac{r^2}{4\alpha^2}\right) - \pi_{E,r}\left(\frac{r^2}{4\beta^2}\right)\right) + \sum_{2\sqrt{x}\alpha < r \leq 2\sqrt{x}\beta} \left(\pi_{E,r}(x) - \pi_{E,r}\left(\frac{r^2}{4\beta^2}\right)\right). \tag{33}$$

We observe that (32) follows from (30), (33), and the asymptotic estimate

$$\sum_{2 < r \leq 2\sqrt{x}\alpha} \frac{C_{E,r}}{\phi_E(0)} \int_{r^2/4\beta^2}^{r^2/4\alpha^2} \frac{\phi(r/(2\sqrt{t}))}{2\sqrt{t}\log t} dt + \sum_{2\sqrt{x}\alpha < r \leq 2\sqrt{x}\beta} \frac{C_{E,r}}{\phi_E(0)} \int_{r^2/4\beta^2}^{x} \frac{\phi(r/(2\sqrt{t}))}{2\sqrt{t}\log t} dt = Li(x) \int_\alpha^\beta \phi(z) dz + O_{\alpha,\beta}(\sqrt{x}\log^2 x), \tag{34}$$

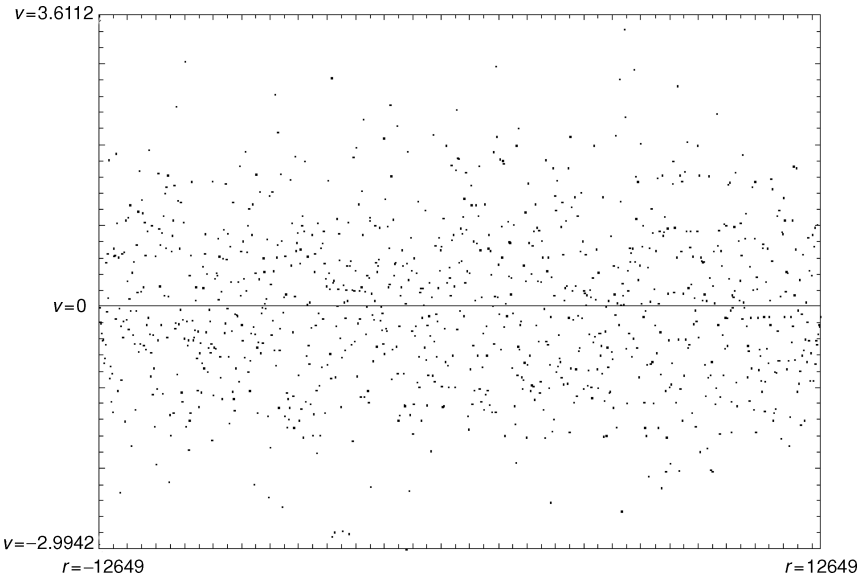

Fig. 5. $v = \frac{\text{Error}}{\sqrt{\text{Main term}}} = \frac{\pi_{E,r}(4\times 10^7) - F_{E,r}(4\times 10^7)}{\sqrt{F_{E,r}(4\times 10^7)}}$.

which we shall prove in the following. Reversing the order of summation and integration, the left-hand side of (34) becomes

$$\int_2^x \frac{1}{2\sqrt{t}\log t}\left(\sum_{2\alpha\sqrt{t}<r\le 2\beta\sqrt{t}} \frac{C_{E,r}}{\phi_E(0)}\phi\left(\frac{r}{2\sqrt{t}}\right)\right) dt \; + O_{\alpha,\beta}(1). \tag{35}$$

We note that by $\delta_{1,0} = 1$ and the definition of $\phi_E(z)$ in (12), the main term on the right-hand side of (9) coincides with $\phi(0)B$ if $q = 1$ and $a = 0$. Now using partial summation, Proposition 1 with $q = 1$, $a = 0$, and integration by parts, we have

$$\begin{aligned}
&\sum_{2\alpha\sqrt{t}<r\le 2\beta\sqrt{t}} C_{E,r}\phi\left(\frac{r}{2\sqrt{t}}\right)\\
&= \phi(\beta)\sum_{2\alpha\sqrt{t}<r\le 2\beta\sqrt{t}} C_{E,r} - \int_{2\alpha\sqrt{t}}^{2\beta\sqrt{t}}\left(\sum_{2\alpha\sqrt{t}<r\le y} C_{E,r}\right)\frac{d}{dy}\phi\left(\frac{y}{2\sqrt{t}}\right) dy\\
&= \phi_E(0)(2\beta\sqrt{t} - 2\alpha\sqrt{t})\phi(\beta) - \phi_E(0)\int_{2\alpha\sqrt{t}}^{2\beta\sqrt{t}}(y - 2\alpha\sqrt{t})\frac{d}{dy}\phi\left(\frac{y}{2\sqrt{t}}\right) dy + O_{\alpha,\beta}(\log^3 t)\\
&= \phi_E(0)\int_{2\alpha\sqrt{t}}^{2\beta\sqrt{t}}\phi\left(\frac{y}{2\sqrt{t}}\right) dy + O_{\alpha,\beta}(\log^3 t),
\end{aligned}$$

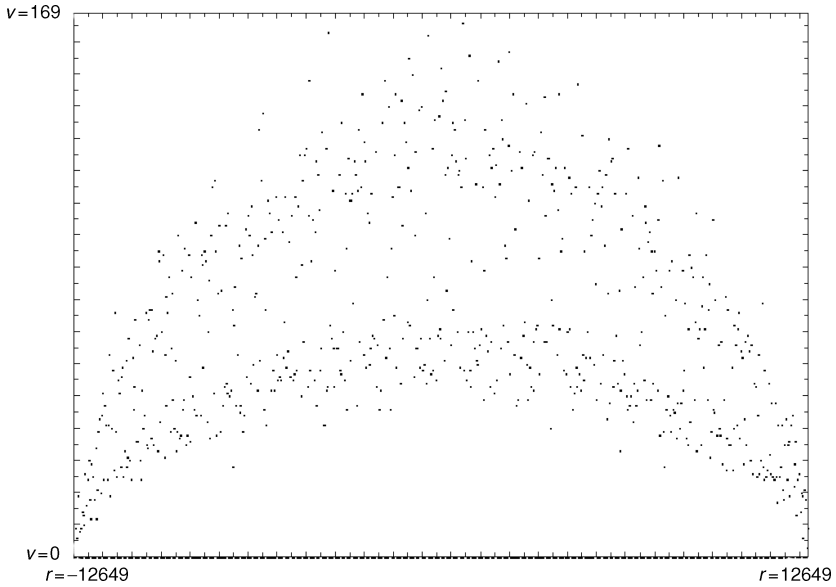

Fig. 6. The function $v = \pi_{E,r}(4 \times 10^7)$, as a function of r.

where for the estimation of the error term, we have used that the derivative of ϕ is continuous and hence bounded on $[\alpha, \beta]$. Thus, (35) equals

$$\int_2^x \frac{1}{2\sqrt{t}\log t} \int_{2\alpha\sqrt{t}}^{2\beta\sqrt{t}} \phi\left(\frac{y}{2\sqrt{t}}\right) dy dt + O_{\alpha,\beta}(\sqrt{x}\log^2 x).$$

Making the change of variables $y/(2\sqrt{t}) \to z$, the main term above becomes

$$Li(x) \int_\alpha^\beta \phi(z) dz,$$

which proves (34) and hence Theorem 4. ■

7 Numerical Evidence

We conclude with some supporting numerical evidence. Figures 1–5 display data for the single elliptic curve E given by the Weierstrass equation

$$Y^2 = X^3 + 6X - 2.$$

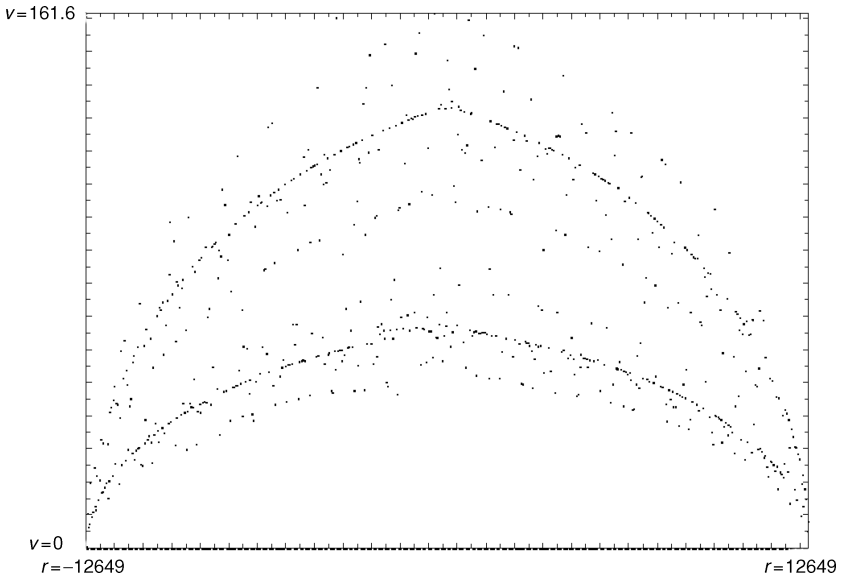

Fig. 7. The approximation $v = F_{E,r}(4 \times 10^7)$, as a function of r.

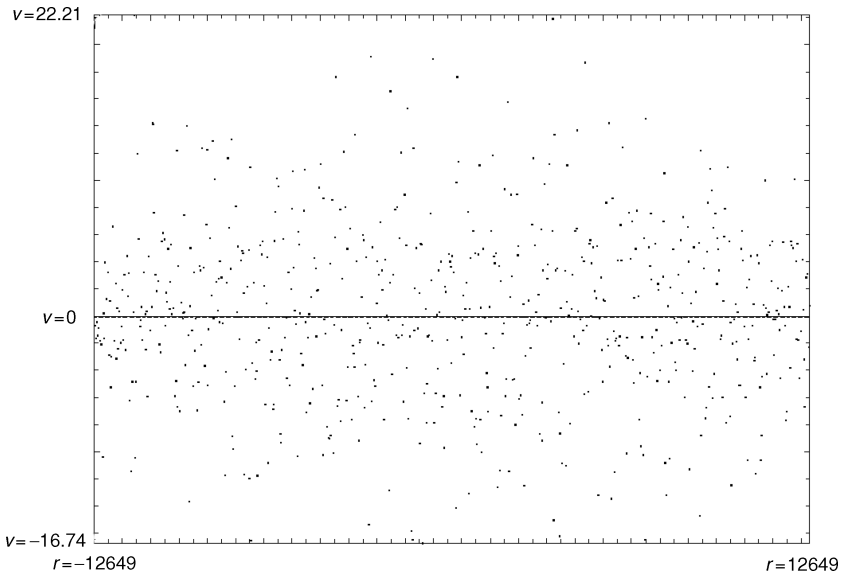

Fig. 8. The absolute error $v = \pi_{E,r}(4 \times 10^7) - F_{E,r}(4 \times 10^7)$.

In Figure 1, we plot the function $v := \pi_{E,r}(4 \times 10^7)$ as a function of the variable r. In Figure 2, we plot our approximation $v := F_{E,r}(4 \times 10^7)$ as a function of r. This elliptic

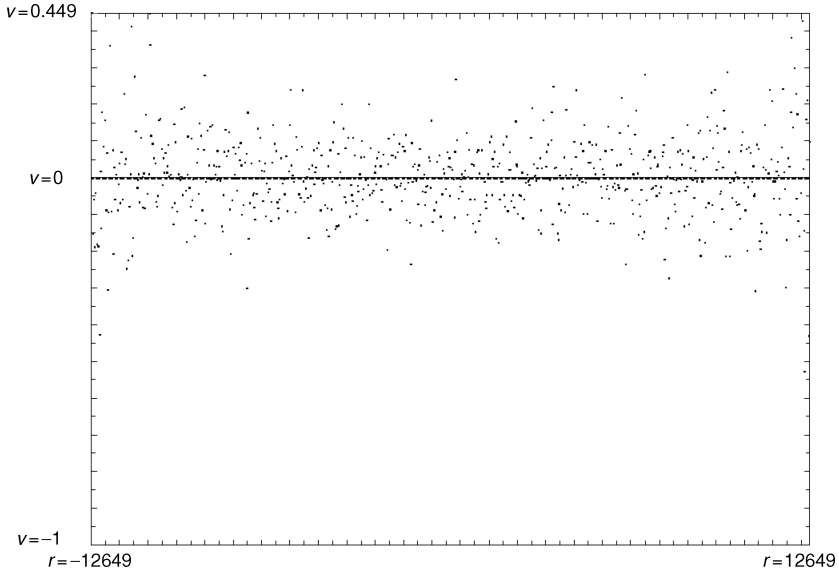

Fig. 9. The relative error $v = \frac{\pi_{E,r}(4\times 10^7) - F_{E,r}(4\times 10^7)}{F_{E,r}(4\times 10^7)}$.

curve has $m_E = 6$, and the "main factor"

$$\frac{m_E |\mathrm{Gal}\,(\mathbb{Q}(E[m_E])/\mathbb{Q})_r|}{|\mathrm{Gal}\,(\mathbb{Q}(E[m_E])/\mathbb{Q})|}$$

of the constant $C_{E,r}$ takes on four distinct values $\{1/2, 3/4, 9/8, 7/4\}$ as r ranges over the integers, which accounts for the four distinct bands visible in Figures 1 and 2.

We then plot various forms of the error in the approximation. In Figure 3, we plot the absolute error

$$v = \pi_{E,r}(4 \cdot 10^7) - F_{E,r}(4 \times 10^7),$$

while in Figure 4, we plot the relative error

$$v = \frac{\pi_{E,r}(4 \times 10^7) - F_{E,r}(4 \times 10^7)}{F_{E,r}(4 \times 10^7)}.$$

Note that the absolute (resp. relative) error is significantly smaller (resp. larger) at the ends of the graph than in the middle. This comes from the fact that we are approximating an integer valued function with a continuous one.

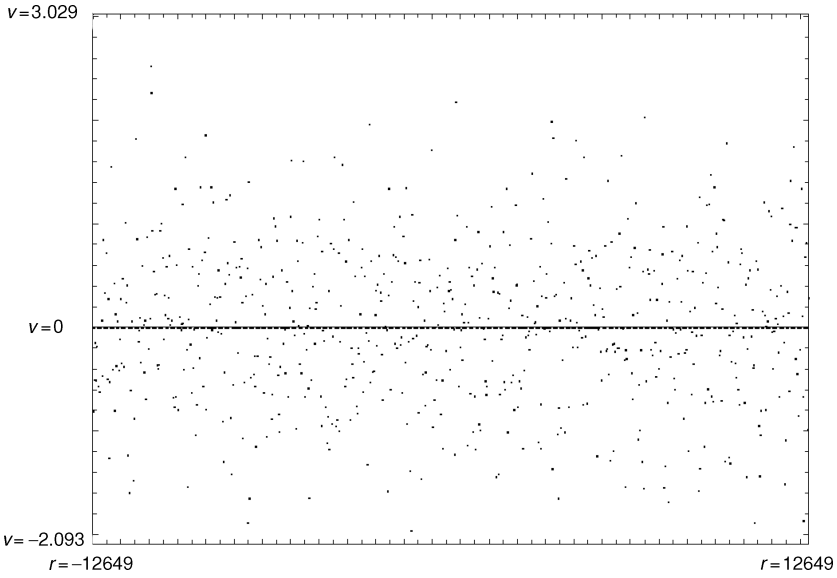

Fig. 10. $v = \frac{\text{Error}}{\sqrt{\text{Main term}}} = \frac{\pi_{E,r}(4\times10^7) - F_{E,r}(4\times10^7)}{\sqrt{F_{E,r}(4\times10^7)}}$.

We remark that in practice, the main difficulty in obtaining numerical data on these error terms lies in the constants $C_{E,r}$, which are difficult to compute in general. However, the elliptic curve we are considering is a Serre curve (see [8, p. 318] and also [6, p. 51]), so we may use Proposition 11 of [4], which computes $C_{E,r}$ explicitly for any Serre curve.

In Figure 5, we plot the error relative to square root of the main term, which looks remarkably like random noise.

Finally, in Figures 6–10, we plot the corresponding data for the elliptic curve E given by the Weierstrass equation

$$Y^2 = X^3 - 768108000X + 8194304162000,$$

which has CM by the complex order of discriminant -27 (i.e. by the unique order of index 3 in $\mathbb{Z}[1/2 + \sqrt{-3}/2]$).

Acknowledgments

We would like to thank A. Granville for helpful comments on an earlier version and J. Fearnley for advice regarding the numerical computations. Moreover, we wish to thank the referee for many valuable comments.

References

[1] Baier, S., and L. Zhao. "The Sato-Tate conjecture on average for small angles." *Transactions of the American Mathematical Society* (forthcoming).

[2] David, C., and F. Pappalardi. "Average Frobenius distributions of elliptic curves." *International Mathematics Research Notices* 4 (1999): 165–83.

[3] Deuring, M. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper." *Abhandlungen aus dem Mathematischen Seminer der Hansischen Universität* 14 (1941): 197–272.

[4] Jones, N. "Averages of elliptic curve constants." Preprint.

[5] Jones, N. "A bound for the 'torsion conductor' of a non-CM elliptic curve." *Proceedings of the American Mathematical Society* (forthcoming).

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

[7] Ram Murty, M. "On Artin's conjecture." *Journal of Number Theory* 16 (1983): 147–68.

[8] Serre, J.-P. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." *Inventiones Mathematicae* 15 (1972): 259–331.

[9] Silverman, J. *Advanced Topics in the Arithmetic of Elliptic Curves*. New York: Springer, 1994.

[10] Tate, J. T. "Algebraic Cycles and Poles of Zeta Functions." In *Arithmetical and Algebraic Geometry*, 93–110. Proceedings of a Conference at Purdue, Dec. 5–7, 1963. New York: Harper & Row, 1965.

[11] Taylor, R. "Automorphy for some l-adic lifts of automorphic mod l representations 2." (2008): preprint www.math.harvard.edu/∼rtaylor.