PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 6, June 2008, Pages 1977–1986
S 0002-9939(08)09324-6
Article electronically published on February 15, 2008

DISTRIBUTION OF FAREY FRACTIONS IN RESIDUE CLASSES AND LANG–TROTTER CONJECTURES ON AVERAGE

ALINA CARMEN COJOCARU AND IGOR E. SHPARLINSKI

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. We prove that the set of Farey fractions of order T, that is, the set $\{\alpha/\beta \in \mathbb{Q} \ : \ \gcd(\alpha,\beta)=1, \ 1 \le \alpha,\beta \le T\}$, is uniformly distributed in residue classes modulo a prime p provided $T \ge p^{1/2+\varepsilon}$ for any fixed $\varepsilon > 0$. We apply this to obtain upper bounds for the Lang–Trotter conjectures on Frobenius traces and Frobenius fields "on average" over a one-parametric family of elliptic curves.

1. INTRODUCTION

For a real positive T, we consider the set of Farey fractions

$$\mathcal{F}(T) = \{\alpha/\beta \in \mathbb{Q} \ : \ \gcd(\alpha,\beta)=1, \ 1 \le \alpha,\beta \le T\},$$

for which we know that

$$\#\mathcal{F}(T) = \left(\frac{6}{\pi^2} + o(1)\right) T^2$$

(hereafter we use $o(1)$ to denote a quantity which tends to zero as $T \to \infty$). We use some results of [20] to show that the elements of this set are uniformly distributed in residue classes modulo a prime p. More precisely, we prove:

Theorem 1. *Let p be a fixed prime. For an integer v, we denote by $R_{T,p}(v)$ the number of fractions $\alpha/\beta \in \mathcal{F}(T)$ with $\gcd(\beta,p)=1$ and $\alpha/\beta \equiv v \pmod p$. Then*

$$\sum_{1 \le v \le p-1} \left| R_{T,p}(v) - \frac{6}{\pi^2} \cdot \frac{T^2}{p} \right| = O\left(T^2 p^{-1} + T p^{1/2+o(1)}\right).$$

We apply this result to study Lang–Trotter conjectures "on average" for specialization at elements of $\mathcal{F}(T)$ of the elliptic curve

$$E(t): \quad Y^2 = X^3 + A(t)X + B(t) \tag{1}$$

over $\mathbb{Q}(t)$, where $A(t), B(t) \in \mathbb{Z}[t]$. For a general background on elliptic curves, we refer the reader to [21]. To state our results for elliptic curves, let us first recall some standard notation.

Given an elliptic curve E over $\mathbb{Q}$ and $a \in \mathbb{Z}$, we denote by $\Pi_E(a,x)$ the number of primes $p \le x$ which do not divide the conductor N_E of E and such that

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

Received by the editors May 14, 2007.
2000 *Mathematics Subject Classification.* Primary 11B57, 11G07, 14H52.

where E_p denotes the reduction E_p of E modulo p.

For a fixed imaginary quadratic field $\mathbb{K}$, we denote by $\Pi_E(\mathbb{K}, x)$ the number of primes $p \le x$ which do not divide N_E and such that

$$a_p(E) \neq 0 \qquad \text{and} \qquad \mathbb{Q}\left(\sqrt{a_p(E)^2 - 4p}\right) = \mathbb{K}.$$

Two celebrated Lang–Trotter conjectures assert that: if $a \neq 0$, or $a = 0$ and E is without complex multiplication (CM), then

$$\Pi_E(a, x) = (c(E, a) + o(1)) \frac{\sqrt{x}}{\log x}$$

for some constant $c(E, a) \ge 0$ depending only on E and a; if E is without complex multiplication, then

$$\Pi_E(\mathbb{K}, x) = (C(E, \mathbb{K}) + o(1)) \frac{\sqrt{x}}{\log x}$$

for some constant $C(E, \mathbb{K}) > 0$ depending only on E and $\mathbb{K}$.

Despite a series of interesting (conditional and unconditional) results, these conjectures are widely open; even the Generalized Riemann Hypothesis (GRH) only allows one to obtain upper bounds on $\Pi_E(a, x)$ and $\Pi_E(\mathbb{K}, x)$, and those are not of the conjectured order of magnitude. Indeed, if E is without CM and $a \neq 0$, then M. R. Murty, V. K. Murty and N. Saradha [17] have proved, under GRH, that $\Pi_E(a, x) \ll x^{4/5}/(\log x)^{1/5}$, while A. C. Cojocaru and C. David [5] have proved, under GRH, that $\Pi_E(\mathbb{K}, x) \ll x^{4/5}/(\log x)^{1/5}$. These results improve upon earlier work of J.-P. Serre [19] and A. C. Cojocaru, É. Fouvry and M. R. Murty [6]. In the case of $a = 0$, better bounds are known: unconditionally, N. Elkies [10, 11] has shown that, if E is without CM, there are infinitely primes p such that $a_p = 0$ (for explicit lower bounds, see [11] and [13]). Also unconditionally, N. Elkies and M. R. Murty have noted that $\Pi_E(0, x) \ll x^{3/4}$ (see [10, pp. 25–26] and [12]). No lower bound is known for $\Pi_E(a, x)$ if $a \neq 0$ and $\Pi_E(\mathbb{K}, x)$. Moreover, the existing unconditional upper bounds for these quantities are quite weak. More precisely, J.-P. Serre [19] has shown that if E is without CM and $a \neq 0, \pm 2$, then

$$\Pi_E(a, x) \ll \frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}},$$

and if $a = \pm 2$, then

$$\Pi_E(a, x) \ll \frac{x(\log\log x)^{1/2}(\log\log\log x)^{1/4}}{(\log x)^{5/4}}.$$

Also unconditionally, A. C. Cojocaru, É. Fouvry and M. R. Murty [6] have given the bound

$$\Pi_E(\mathbb{K}, x) \ll \frac{x(\log\log x)^{13/12}}{(\log x)^{25/24}}.$$

Thus we see that, if E is without CM and $a \neq 0$, then, unconditionally, only logarithmic improvements of the trivial estimates $\Pi_E(a, x) \le \pi(x)$ and $\Pi_E(\mathbb{K}, x) \le \pi(x)$ are known (where, as usual, $\pi(x)$ is the number of primes $p \le x$). If E is with CM and $a \neq 0$, then, unconditionally, one has that $\Pi_E(a, x) \ll x^{1/2}/\log x$, while $\mathbb{Q}(\sqrt{a_p(E)^2 - 4p})$ is isomorphic to the CM field of E for all primes p of ordinary reduction.

Due to the lack of strong unconditional results in the non-CM case, it makes sense to study $\Pi_E(a,x)$ and $\Pi_E(\mathbb{K},x)$ on average over some natural families of curves. For example, É. Fouvry and R. M. Murty [13], and C. David and F. Pappalardi [8], have considered the average of $\Pi_E(a,x)$ for the family of curves $Y^2 = X^3 + uX + v$ where the integers u and v satisfy the inequalities $|u| \le U$, $|v| \le V$; they have shown that if $UV \ge x^{3/2+\varepsilon}$ and $\min\{U,V\} \ge x^{1/2+\varepsilon}$ for some fixed positive $\varepsilon > 0$, then, "on average", the Lang–Trotter conjecture holds for such curves. This result has been extended in various directions [1, 2, 3, 4, 9, 14, 15, 16]. A. C. Cojocaru and C. Hall [7] have recently considered the one parametric family of curves of the form (1) and established an improved upper bound on the average value of $\Pi_E(a,x)$ over curves of such families when the parameter t runs through the elements of $\mathcal{F}(T)$ with T of the same order of magnitude as x.

Since obtaining tight "individual" estimates is an ultimate goal, it also makes sense to reduce the amount of "averaging". In this direction, we show that one can obtain the bound of [7, Theorem 4] (established for $T \gg x$) starting with $T \ge x^{3/4+\varepsilon}$ for some fixed $\varepsilon > 0$. We also obtain a similar result for $\Pi_E(\mathbb{K},x)$.

We recall that the notation $U \ll V$ and $U = O(V)$ are both equivalent to the statement that $|U| \le cV$ holds with some constant $c > 0$, which throughout the paper may depend on the polynomials $A(t)$ and $B(t)$ in (1).

Theorem 2. *Let $A(t), B(t) \in \mathbb{Z}[t]$ be fixed polynomials such that $E(t)$ given by (1) is an elliptic curve over $\mathbb{Q}(t)$ with non-constant j-invariant, that is,*

$$\Delta(t) = -16(4A(t)^3 + 27B(t)^2) \ne 0$$

and

$$j(t) = -\frac{6912A(t)^3}{4A(t)^3 + 27B(t)^2} \notin \mathbb{Q}.$$

Then for arbitrary real positive x and T,

1. *for any integer $a \ne 0$,*

$$\sum_{\substack{\tau \in \mathcal{F}(T) \\ \Delta(\tau) \ne 0}} \Pi_{E(\tau)}(a,x) \ll T^2 x^{3/4} + T x^{3/2+o(1)};$$

2. *for $a = 0$,*

$$\sum_{\substack{\tau \in \mathcal{F}(T) \\ \Delta(\tau) \ne 0}} \Pi_{E(\tau)}(0,x) \ll T^2 x^{2/3} + T x^{3/2+o(1)};$$

3. *for any imaginary quadratic field $\mathbb{K}$,*

$$\sum_{\substack{\tau \in \mathcal{F}(T) \\ \Delta(\tau) \ne 0}} \Pi_{E(\tau)}(\mathbb{K},x) \ll T^2 x^{2/3} + T x^{3/2+o(1)}.$$

It is easy to see that, for $T \ge x^{3/4+\varepsilon}$ for any fixed $\varepsilon > 0$, the bound of part 1 of Theorem 2 becomes

$$\frac{1}{\#\mathcal{F}(T)} \sum_{\substack{\tau \in \mathcal{F}(T) \\ \Delta(\tau) \ne 0}} \Pi_{E(\tau)}(a,x) \ll x^{3/4};$$

this is exactly the same as the bound of [7, Theorem 4], which, however, had been established only for $T \gg x$. Similarly, for $T \ge x^{5/6+\varepsilon}$ for any fixed $\varepsilon > 0$, the bounds of parts 2 and 3 become

$$\frac{1}{\#\mathcal{F}(T)} \sum_{\substack{\tau \in \mathcal{F}(T) \\ \Delta(\tau) \neq 0}} \Pi_{E(\tau)}(0, x) \ll x^{2/3};$$

$$\frac{1}{\#\mathcal{F}(T)} \sum_{\substack{\tau \in \mathcal{F}(T) \\ \Delta(\tau) \neq 0}} \Pi_{E(\tau)}(\mathbb{K}, x) \ll x^{2/3}.$$

We also see that Theorem 2 is non-trivial for $T \ge x^{1/2+\varepsilon}$.

2. Proof of Theorem 1

First, we note that $R_{T,p}(0) = O(T^2/p)$, which is within the total error term of Theorem 1. Thus it is enough to concentrate on $R_{T,p}(v)$ with $v = 1, \ldots, p-1$.

For an integer d we let

$$M_{W,p,d}(v) = \#\{(\alpha, \beta) \in \mathbb{Z}^2 \ : \ 1 \le \alpha, \beta \le W, \ d \mid \gcd(\alpha, \beta), \ \gcd(p, \beta) = 1, \\ \alpha/\beta \equiv v \pmod p\}.$$

Clearly, $M_{W,p,d}(t) = 0$ if $p|d$ and $M_{W,p,d}(t) = M_{W/d,p,1}(t)$.

Now let $\mu(d)$ denote the Möbius function. Using the inclusion-exclusion principle, we obtain that

$$\begin{aligned} R_{T,p}(v) &= \sum_{d=1}^{\infty} \mu(d) M_{T,p,d}(v) = \sum_{\substack{d=1 \\ p \nmid d}}^{\infty} \mu(d) M_{T/d,p,1}(v) \\ &= \sum_{1 \le d < p} \mu(d) M_{T/d,p,1}(v) + \sum_{\substack{d \ge p \\ p \nmid d}} \mu(d) M_{T/d,p,1}(v) \\ &= \sum_{1 \le d < p} \mu(d) \frac{(T/d)^2}{p} \\ &\qquad + O\left(\sum_{1 \le d < p} \left| M_{T/d,p,1}(v) - \frac{(T/d)^2}{p} \right| + \sum_{d \ge p} M_{T/d,p,1}(v) \right). \end{aligned}$$

We see that

$$\sum_{1 \le d < p} \mu(d) \frac{(T/d)^2}{p} = \frac{T^2}{p} \left(\zeta(2)^{-1} + O(p^{-1}) \right) = \frac{T^2}{p} \left(\frac{6}{\pi^2} + O(p^{-1}) \right),$$

where $\zeta(s)$ is the Riemann zeta function. Therefore

$$\sum_{1 \le v \le p-1} \left| R_{T,p}(v) - \frac{6}{\pi^2} \cdot \frac{T^2}{p} \right| = O(T^2 p^{-1} + \Delta_1 + \Delta_2), \tag{2}$$

where

$$\begin{aligned}\Delta_1 &= \sum_{1\le d<p}\sum_{1\le v\le p-1}\left|M_{T/d,p,1}(v)-\frac{(T/d)^2}{p}\right|,\\ \Delta_2 &= \sum_{d\ge p}\sum_{1\le v\le p-1}M_{T/d,p,1}(v).\end{aligned}$$

Using the Cauchy inequality, we deduce that

$$\left(\sum_{1\le v\le p-1}\left|M_{T/d,p,1}(v)-\frac{(T/d)^2}{p}\right|\right)^2 \le p\sum_{1\le v\le p-1}\left|M_{T/d,p,1}(v)-\frac{(T/d)^2}{p}\right|^2. \tag{3}$$

We now recall the bound

$$\sum_{1\le v\le p-1}\left|M_{W,p,1}(v)-\frac{W^2}{p}\right|^2 \le W^2p^{o(1)}, \tag{4}$$

which is a special case of more general results of [20] (note that the results of [20] apply to the congruence $\alpha\equiv v\beta \pmod p$ where β is not necessarily relatively prime to p, but the difference of $O\left(W^2/p^2\right)$ for each v does not affect the total error term). We now derive from (3) and (4) that

$$\Delta_1 \le \sum_{1\le d<p}\sqrt{p^{1+o(1)}(T/d)^2} = p^{1/2+o(1)}T\sum_{1\le d<p}\frac{1}{d} = p^{1/2+o(1)}T. \tag{5}$$

The trivial bound

$$\sum_{1\le v\le p-1}M_{W,p,1}(v)\le W^2$$

implies that

$$\Delta_2 \le \sum_{d>p}(T/d)^2 = O(T^2p^{-1}). \tag{6}$$

Substituting (5) and (6) in (2), we derive the desired result.

3. Proof of Theorem 2

3.1. **Preliminaries.** For a fixed $\tau\in\mathbb{Q}$, let $E(\tau)$ denote the elliptic curve over $\mathbb{Q}$ obtained by specializing $E(t)$ at $t=\tau$. Let $\Delta(\tau)$ and $N(\tau)$ denote its discriminant and conductor, respectively. For a prime $p\nmid N(\tau)$, let $E_p(\tau)$ denote the reduction of $E(\tau)$ modulo p, and let $a_p(\tau)=p+1-\#E_p(\tau)$. Without loss of generality, we assume that $p\ge 5$.

Now let $\ell\ne p$ be primes such that $\ell\ge 17$ and $j(t)$ is non-constant in $\mathbb{F}_p(t)$. Let $\mathbb{L}=\mathbb{F}_p(t)$ and let $[\mathbb{L}]$ be its set of places. Let $\mathcal{B}\subseteq[\mathbb{L}]$ be the set of places of bad reduction of $E(t)/\mathbb{L}$, which is finite and has the property that $\deg\mathcal{B}$ is bounded by a constant independent of p. Let $\mathbb{L}(E(t)[\ell])/\mathbb{L}$ be the extension of ℓ-division points of $E(t)$. Since $p\ge 5$, this is a tamely ramified Galois extension, whose Galois group we denote G_ℓ.

Since $\ell \geq 17$, we know from [7, Theorem 1] that the geometric Galois group of $\mathbb{L}(E[\ell])/\mathbb{L}$ is $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Equivalently, the Galois group G_ℓ is the unique subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ containing $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and satisfying $\det(G_\ell) = \langle p \rangle$.

We set

$$G_\ell^p = \{g \in G_\ell : \det(g) = p\}$$

and

$$C^p = C \cap G_\ell^p$$

for a finite union C of conjugacy classes of G_ℓ. We have the following particular case of V. K. Murty and J. Scherk [18, Theorem 2] (see also Section 3 of [7]).

Lemma 3. *Let $U \subseteq [\mathbb{L}]$ be the open complement of the ramification locus $Z \subseteq [\mathbb{L}]$ of $\mathbb{L}(E(t)[\ell])/\mathbb{L}$. For $v \in U(\mathbb{F}_p)$, let Frob_v denote the Frobenius at v in $\mathbb{L}(E(t)[\ell])/\mathbb{L}$. Then*

$$\#\{v \in U(\mathbb{F}_p) : \mathrm{Frob}_v \subseteq C^p\} = \frac{|C^p|}{\ell\,(\ell^2-1)}|U(\mathbb{F}_p)| + O_{g,d}\left(|C^p|^{1/2}p^{1/2}\right),$$

where the implied $O_{g,d}$-constant depends only on the genus g of $\mathbb{L}$ and the degree d of Z.

We use this result to prove Theorem 2.

For part 3 we also need the following elementary result (see [5, Lemma 14], for example).

Lemma 4. *Let a, b be independent variables and $k \geq 1$ an integer. Then there exists a polynomial $P(X) \in \mathbb{Z}[X]$ such that*

$$\frac{(a^k+b^k)^2}{(ab)^k} = P\left(\frac{(a+b)^2}{ab}\right).$$

3.2. **Parts 1 and 2: Frobenius traces.** To prove part 1, we follow the same lines as in the proof of [7, Theorem 4]. In particular, for any prime ℓ we have that

$$\sum_{\substack{\tau \in \mathcal{F}(T)\\ \Delta(\tau)\neq 0}} \Pi_{E(\tau)}(a,x) = \sum_{\substack{\tau \in \mathcal{F}(T)\\ \Delta(\tau)\neq 0}} \sum_{\substack{p\leq x,\\ p\nmid N(\tau)\\ a_p(\tau)=a}} 1 \leq \sum_{\substack{\tau \in \mathcal{F}(T)\\ \Delta(\tau)\neq 0}} \sum_{\substack{p\leq x,\\ p\nmid N(\tau)\\ a_p(\tau)\equiv a \pmod{\ell}}} 1$$

$$\leq \sum_{p\leq x} \sum_{\substack{\tau \in \mathcal{F}(T)\\ \Delta(\tau)\neq 0\\ N(\tau)\not\equiv 0 \pmod{p}\\ a_p(\tau)\equiv a \pmod{\ell}}} 1 = \sum_{p\leq x} \sum_{\substack{v=1\\ \Delta(v)N(v)\not\equiv 0 \pmod{p}\\ a_p(v)\equiv a \pmod{\ell}}}^{p-1} R_{T,p}(v).$$

Now, applying Theorem 1, we obtain

$$\begin{aligned}
&\sum_{\substack{v=1\\ \Delta(v)N(v)\not\equiv 0 \pmod p\\ a_p(v)\equiv a \pmod \ell}}^{p-1} R_{T,p}(v)\\
&\quad\le \sum_{\substack{v=1\\ \Delta(v)N(v)\not\equiv 0 \pmod p\\ a_p(v)\equiv a \pmod \ell}}^{p-1} \frac{6}{\pi^2}\cdot\frac{T^2}{p} + \sum_{\substack{v=1\\ \Delta(v)N(v)\not\equiv 0 \pmod p\\ a_p(v)\equiv a \pmod \ell}}^{p-1} \left|R_{T,p}(v) - \frac{6}{\pi^2}\cdot\frac{T^2}{p}\right|\\
&\quad\le \frac{6}{\pi^2}\cdot\frac{T^2}{p} \sum_{\substack{v=1\\ \Delta(v)N(v)\not\equiv 0 \pmod p\\ a_p(v)\equiv a \pmod \ell}}^{p-1} 1 + \sum_{v=1}^{p-1}\left|R_{T,p}(v) - \frac{6}{\pi^2}\cdot\frac{T^2}{p}\right|\\
&\quad\le \frac{6}{\pi^2}\cdot\frac{T^2}{p} \sum_{\substack{v=1\\ \Delta(v)N(v)\not\equiv 0 \pmod p\\ a_p(v)\equiv a \pmod \ell}}^{p-1} 1 + O\left(T^2p^{-1} + Tp^{1/2+o(1)}\right).
\end{aligned}$$

Hence,

$$\begin{aligned}
&\sum_{\substack{\tau\in\mathcal{F}(T)\\ \Delta(\tau)\ne 0}} \Pi_{E(\tau)}(a,x)\\
&\qquad\le \frac{6T^2}{\pi}\sum_{p\le x}\frac{1}{p} \sum_{\substack{1\le v\le p-1\\ \Delta(v)N(v)\not\equiv 0 \pmod p\\ a_p(v)\equiv a \pmod \ell}} 1 + O\left(\sum_{p\le x}\left(T^2p^{-1} + Tp^{1/2+o(1)}\right)\right).
\end{aligned}$$

Using Lemma 3 as in [7, Theorem 2] with C equal to

$$C_\ell = \{g \in G_\ell \ :\ \mathrm{tr}(g) = a\},$$

we obtain that the inner sum over v is $p/\ell + O(\ell p^{1/2})$ (provided that $\ell \ge 17$). Therefore

$$\sum_{\substack{\tau\in\mathcal{F}(T)\\ \Delta(\tau)\ne 0}} \Pi_{E(\tau)}(a,x) \ll T^2x\ell^{-1} + \ell T^2x^{1/2} + Tx^{3/2+o(1)}.$$

Finally, by choosing ℓ as the smallest prime with $\ell \ge \max\{17, x^{1/4}\}$, we conclude the proof of part 1 of Theorem 2.

To prove part 2, we remark that the condition $\mathrm{tr}(g) = 0$ defining C_ℓ makes sense not only in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, but also in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Therefore we apply Lemma 3 to the field extension corresponding to the projection of G_ℓ in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Then

$$\sum_{\substack{1\le v\le p-1\\ \Delta(v)N(v)\not\equiv 0 \pmod p\\ a_p(v)\equiv 0 \pmod \ell}} 1 = p/\ell + O(\ell^{1/2}p^{1/2})$$

(provided that $\ell \ge 17$), and so

$$\sum_{\substack{\tau\in\mathcal{F}(T)\\ \Delta(\tau)\ne 0}} \Pi_{E(\tau)}(0,x) \ll T^2x\ell^{-1} + \ell^{1/2}T^2x^{1/2} + Tx^{3/2+o(1)}.$$

By choosing ℓ as the smallest prime with $\ell \geq \max\{17, x^{1/3}\}$, we conclude the proof of part 2 of Theorem 2.

3.3. **Part 3: Frobenius fields.** As in part 1, we have that

$$\sum_{\substack{\tau \in \mathcal{F}(T) \\ \Delta(\tau) \neq 0}} \Pi_{E(\tau)}(\mathbb{K}, x) = \sum_{p \leq x} \sum_{\substack{1 \leq v \leq p-1 \\ \Delta(v)N(v) \not\equiv 0 \pmod p \\ a_p(v) \not\equiv 0 \pmod p \\ \mathbb{Q}\left(\sqrt{a_p(v)^2 - 4p}\right) = \mathbb{K}}} R_{T,p}(v)$$

$$= \frac{6T^2}{\pi} \sum_{p \leq x} \frac{1}{p} \sum_{\substack{0 \leq v \leq p-1 \\ \Delta(v)N(v) \not\equiv 0 \pmod p \\ a_p(v) \not\equiv 0 \pmod p \\ \mathbb{Q}\left(\sqrt{a_p(v)^2 - 4p}\right) = \mathbb{K}}} 1 + O\left(\sum_{p \leq x} \left(T^2 p^{-1} + T p^{1/2 + o(1)}\right)\right).$$

It remains to estimate the inner sum in the first term.

Let $0 \leq v \leq p-1$ be such that $p \nmid \Delta(v), p \nmid N(v)$, $a_p(v) \not\equiv 0 \pmod p$ and $\mathbb{Q}\left(\sqrt{a_p(v)^2 - 4p}\right) = \mathbb{K}$. Let $\pi_p(v)$ be defined by

$$X^2 - a_p(v)X + p = (X - \pi_p(v))\left(X - \overline{\pi_p(v)}\right).$$

Then $\mathbb{K} = \mathbb{Q}\left(\sqrt{a_p(v)^2 - 4p}\right) = \mathbb{Q}(\pi_p(v))$, and so p splits completely in $\mathbb{K}$. We write $p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}\overline{\mathfrak{p}}$ for some conjugate prime ideals $\mathfrak{p}, \overline{\mathfrak{p}}$ of $\mathcal{O}_{\mathbb{K}}$. In particular, $\mathfrak{p} = (\pi_p(v))$.

Let h and w be the class number and the number of units of $\mathcal{O}_{\mathbb{K}}$. We define

$$\pi_p(\mathbb{K}) \in \mathcal{O}_{\mathbb{K}}$$

by

$$\pi_p(\mathbb{K}) = \alpha^w, \quad \text{where } \mathfrak{p}^h = \alpha\mathcal{O}_{\mathbb{K}}.$$

(Note that we have two choices for $\pi_p(\mathbb{K})$, and we simply make one.) By combining the above observations, we obtain that

$$\pi_p(v)^{hw} = \pi_p(\mathbb{K}). \tag{7}$$

We reinterpret (7) as a Chebotarev condition in some extension of $\mathbb{F}_p(t)$ (note that here p and $\mathbb{K}$ are fixed, and v is a specialization of t). To do this, let us choose a rational prime $\ell \geq 17$, $\ell \neq p$, and consider the Galois extension $\mathbb{L}(E[\ell])/\mathbb{L}$. From classical theory we know that the Frobenius at v in this extension, viewed as an element of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, has the property that its trace $\operatorname{tr}\mathrm{Frob}_v$ satisfies

$$\operatorname{tr}\mathrm{Frob}_v \equiv \pi_p(v) + \overline{\pi_p(v)} \pmod \ell.$$

Thus $\pi_p(v)$ has a "Chebotarev interpretation" in this extension.

Now we combine (7) with Lemma 4, getting

$$\frac{\left(\pi_p(\mathbb{K}) + \overline{\pi_p(\mathbb{K})}\right)^2}{\pi_p(\mathbb{K})\overline{\pi_p(\mathbb{K})}} = \frac{\left(\pi_p(v)^{hw} + \overline{\pi_p(v)}^{hw}\right)^2}{\pi_p(v)^{hw}\overline{\pi_p(v)}^{hw}} = P\left(\frac{(\pi_p(v) + \overline{\pi_p(v)})^2}{\pi_p(v)\overline{\pi_p(v)}}\right).$$

Let us define

$$C_\ell = \left\{ g \in G_\ell \ : \ P\left(\frac{\operatorname{Tr}(g)^2}{\det g}\right) = \frac{\left(\pi_p(\mathbb{K}) + \overline{\pi_p(\mathbb{K})}\right)^2}{\pi_p(\mathbb{K})\overline{\pi_p(\mathbb{K})}} \right\},$$

where $\mathrm{Tr}(g)$ and $\det g$ denote the trace and determinant of g, respectively. Then

$$\sum_{\substack{0\le v\le p-1\\ \Delta(v)N(v)\not\equiv 0 \pmod p\\ a_p(v)\not\equiv 0 \pmod p\\ \mathbb{Q}\left(\sqrt{a_p(v)^2-4p}\right)=\mathbb{K}}} 1 \le \#\left\{1\le v\le p-1 \ : \ p\nmid \Delta(v)N(v),\ \mathrm{Frob}_v\subseteq C_\ell\right\}. \tag{8}$$

To estimate (8) we can now invoke Lemma 3. Again, as in the proof of part 2, we remark that the condition defining C_ℓ makes sense not only in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, but also in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Thus we apply Lemma 3 to the field extension corresponding to the projection of G_ℓ in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. It is an easy calculation to show that $\#C_\ell^p = O(\ell^2)$ and $\#\overline{C}_\ell^p = O(\ell)$, where $\overline{C}_\ell^p$ is the union of conjugacy classes in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ of the elements in C_ℓ^p. After putting everything together and continuing as in part 2, we conclude the proof.

Acknowledgments

The authors are very grateful to Chris Hall for valuable comments.

The first author would like to thank the Fields Institute for an excellent working environment. This work was supported in part by NSF grant DMS 0636750 (for the first author) and by ARC grant DP0556431 (for the second author).

References

[1] A. Akbary, C. David and R. Juricevic, 'Average distributions and product of L-series', *Acta Arith.*, **111** (2004), 239–268. MR2039225 (2004k:11086)

[2] S. Baier, 'The Lang–Trotter conjecture on average', J. Ramanujan Math. Soc., to appear.

[3] W. D. Banks, and I. E. Shparlinski, 'Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height', *Preprint*, 2006 (available at `http://arxiv.org/abs/math.NT/0609144`).

[4] J. Battista, J. Bayless, D. Ivanov and K. James, 'Average Frobenius distributions for elliptic curves with nontrivial rational torsion' *Acta Arith.*, **119** (2005), 81–91. MR2163519 (2006g:11106)

[5] A. C. Cojocaru and C. David, 'Frobenius fields for elliptic curves', *Amer. J. Math.* (to appear).

[6] A. C. Cojocaru, É. Fouvry and M. R. Murty, 'The square sieve and the Lang–Trotter conjecture', *Canadian J. Math.*, **57** (2005), 1155–1177. MR2178556 (2006e:11074)

[7] A. C. Cojocaru and C. Hall, 'Uniform results for Serre's theorem for elliptic curves', *Internat. Math. Res. Notices*, **2005** (2005), 3065–3080. MR2189500 (2006g:11107)

[8] C. David and F. Pappalardi, 'Average Frobenius distribution of elliptic curves', *Internat. Math. Res. Notices*, **4** (1999), 165–183. MR1677267 (2000g:11045)

[9] C. David and F. Pappalardi, 'Average Frobenius distribution for inerts in $\mathbb{Q}(i)$', *J. Ramanujan Math. Soc.*, **19** (2004), 1–21. MR2139503 (2006i:11059)

[10] N.D. Elkies, 'Supersingular primes of a given elliptic curve over a number field', Ph.D. thesis, Harvard University, Cambridge, MA, 1987.

[11] N. D. Elkies, 'The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$', *Invent. Math.*, **89** (1987), 561–567. MR903384 (88i:11034)

[12] N. Elkies, 'Distribution of supersingular primes', *Astérisque, J. Arithmétiques de Luminy, 1989*, **198–200** (1991), 127–132. MR1144318 (93b:11070)

[13] É. Fouvry and M. R. Murty, 'On the distribution of supersingular primes', *Canad. J. Math.*, **48** (1996), 81–104. MR1382477 (97a:11084)

[14] E.-U. Gekeler, 'Frobenius distributions of elliptic curves over finite prime fields', *Int. Math. Res. Notes*, **2003** (2003), 1999–2018. MR1995144 (2004d:11048)

[15] K. James, 'Average Frobenius distributions for elliptic curves with 3-torsion', *J. Number Theory*, **109** (2004), 278–298. MR2106483 (2005k:11110)

[16] K. James and G. Yu, 'Average Frobenius distribution of elliptic curves', *Acta Arith.*, **124** (2006), 79–100. MR2262142

[17] M. R. Murty, V. K. Murty and N. Saradha, 'Modular forms and the Chebotarev density theorem', *Amer. J. Math.*, **110** (1998), 253–281. MR935007 (89d:11036)
[18] V. K. Murty and J. Scherk, 'Effective versions of the Chebotarev density theorem for function fields', *C.R. Acad. Sci. Paris, Série I*, **319** (1994), 523–528. MR1298275 (95j:11104)
[19] J-P. Serre, 'Queques applications du théorème de densité de Chebotarev', *Publ. Math. I.H.E.S.*, no. 54 (1981), 123–201. MR644559 (83k:12011)
[20] I. E. Shparlinski, 'Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average', *Michigan Math. J.* (to appear).
[21] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995. MR817210 (87g:11070)

Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, Chicago, Illinois 60607; and Institute of Mathematics of the Romanian Academy, Calea Grivitei 21, 010702, Bucharest, Romania
E-mail address: cojocaru@math.uic.edu

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au