ACTA ARITHMETICA
119.1 (2005)

Average Frobenius distributions for elliptic curves with nontrivial rational torsion

by

Jonathan Battista (East Lansing, MI),
Jonathan Bayless (Hanover, NH),
Dmitriy Ivanov (Stanford, CA) and
Kevin James (Clemson, SC)

1. Introduction. In this paper we consider the Lang–Trotter conjecture (Conjecture 1 below) for various families of elliptic curves with prescribed torsion structure. We prove that the Lang–Trotter conjecture holds in an average sense for these families of curves (see Theorem 3).

Let $E/\mathbb{Q}$ denote an elliptic curve and let Δ_E denote its discriminant. As usual, let $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$. Then we have the following conjecture of Lang and Trotter [10].

Conjecture 1 (Lang–Trotter). *Let $E/\mathbb{Q}$ be any elliptic curve and let $r \in \mathbb{Z}$ ($r \neq 0$ if E has complex multiplication). Then*

$$\pi_E^r(X) := \#\{p \leq X : a_p(E) = r\} \sim C_{E,r} \frac{\sqrt{X}}{\log X},$$

where $C_{E,r}$ is an explicit constant depending only on E and r.

More precisely, let $\varrho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ denote the Galois representation on the full torsion subgroup of $E(\overline{\mathbb{Q}})$ where $\widehat{\mathbb{Z}} = \prod \mathbb{Z}_p$. Let $\widetilde{\varrho}_{E,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ denote its reduction modulo m which yields the usual Galois representation on the m-torsion points of $E(\overline{\mathbb{Q}})$. Then there is an integer m_E guaranteed by [14] such that for all $p \nmid m_E$, $\widetilde{\varrho}_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and such that $\varrho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the full inverse image through the reduction modulo m_E map of $\widetilde{\varrho}_{E,m_E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ (see Section 2 of [2] for a more detailed explanation). Lang and Trotter define

2000 *Mathematics Subject Classification*: Primary 11G05; Secondary 11F80.
All authors were partially supported by NSF grant DMS-0139569. The fourth author was also partially supported by NSF grant DMS-0090117.

$$(1)\quad C_{E,r} := \frac{2}{\pi}\cdot\frac{m_E\cdot\#(\widetilde{\varrho}_{E,m_E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))_r)}{\#(\widetilde{\varrho}_{E,m_E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})))}\prod_{\substack{q\nmid m_E\\ q\nmid r}}\frac{q(q^2-q-1)}{(q+1)(q-1)^2}\prod_{\substack{q\nmid m_E\\ q\mid r}}\frac{q^2}{q^2-1},$$

where for any subgroup G of $\mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z})$, G_r denotes the subset of elements of trace r. Note that the ratios of polynomials in q in the previous expression are

$$\frac{q|(\mathrm{GL}_2(\mathbb{F}_q))_r|}{|\mathrm{GL}_2(\mathbb{F}_q)|}.$$

In [4] and [2], this conjecture is proved to hold in an average sense, if one averages over all elliptic curves. As in [10], let

$$\pi_{1/2}(X) = \int_2^X \frac{dt}{2\sqrt{t}\log t} \sim \frac{\sqrt{X}}{\log X}.$$

Then from [2], we have the following result:

THEOREM 1 (David–Pappalardi). *Let $E(a,b): y^2 = x^3 + ax + b$ and let $\varepsilon > 0$. If $A, B > X^{1+\varepsilon}$, then we have, as $X \to \infty$,*

$$\frac{1}{4AB}\sum_{\substack{|a|\le A\\ |b|\le B}}\pi^r_{E(a,b)}(X) \sim D_r\pi_{1/2}(X),$$

where

$$D_r := \frac{2}{\pi}\prod_{q\nmid r}\frac{q(q^2-q-1)}{(q+1)(q-1)^2}\prod_{q\mid r}\frac{q^2}{q^2-1}.$$

In fact, David and Pappalardi [2] prove the following stronger result.

THEOREM 2 (David–Pappalardi). *Let $\varepsilon > 0$ and fix $c > 0$. If $A, B > X^{2+\varepsilon}$, then for all $d > 2c$ and for all elliptic curves $E(a,b)$ with $|a| \le A$ and $|b| \le B$, with at most $\mathrm{O}(AB/\log^d X)$ exceptions, we have the inequality*

$$|\pi^r_{E(a,b)} - D_r\pi_{1/2}(X)| \ll \frac{\sqrt{X}}{\log^c X}.$$

One immediately notices the similarities between $C_{E,r}$ and D_r. From Theorem 1 we see, when one averages over all elliptic curves, that the constant obtained is similar to the conjectured constant $C_{E,r}$. In fact if we set $m_E = 1$ in (1) then we obtain D_r. One should note, though, that m_E is never 1 (see [14]). However, Duke [3] has shown that for almost all elliptic curves, $\widetilde{\varrho}_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for all primes p. It is still not known if the constants obtained in [2, 4] are consistent with the ones conjectured by Lang and Trotter, that is, we do not know if the average of the $C_{E,r}$'s above is D_r.

Since the set of elliptic curves having nontrivial rational torsion subgroups has density zero in the set of all elliptic curves, the results mentioned above ignore curves with nontrivial rational torsion subgroups. From (1), we see that the presence of nontrivial rational torsion points has a substantial effect on the constant $C_{E,r}$ conjectured by Lang and Trotter. In particular, if E has a rational point of order m, then $m \mid m_E$ and $\widetilde{\varrho}_{E,m}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Thus, it seems quite natural to investigate the behavior of $\pi_E^r(X)$ for elliptic curves with a nontrivial rational point of order m. We note that by Mazur's Theorem, [13], $m \in \{2,3,4,5,6,7,8,9,10,12\}$. In [6], the fourth author has computed the average value of $\pi_E^r(X)$ for $r \not\equiv 2 \pmod 3$ as E varies over elliptic curves having a rational point of order 3. We will concentrate on extending those results to all $m \in \{3,5,7,9\}$. In the course of proving our main result for these values of m (see Section 3), we will rely on the main result of [7]. In order to obtain similar results for $m \in \{2,4,6,8,10,12\}$, one would require a generalization of the work in [7] since one would need to distinguish curves with cyclic 2-torsion from those with full 2-torsion. This will be the focus of future work.

The families of elliptic curves defined over $\mathbb{Q}$ with prescribed torsion subgroups have been parameterized by Kubert [9]. We list in Table 1 the parameterizations of elliptic curves having a rational point of order m.

Table 1

m	Parameterization	Discriminant
3	$E(a_1,a_3): y^2+a_1xy+a_3y=x^3$	$a_1^3a_3^3-27a_3^4$
5	$E(s): y^2+(1-s)xy-sy=x^3-sx^2$	$s^5(s^2-11s-1)$
7	$E(s): y^2+(1-s^2+s)xy-(s^3-s^2)y$ $=x^3-(s^3-s^2)x^2$	$s^7(s-1)^7(s^3-8s^2+5s+1)$
9	$E(s): y^2+((1-s)(s^2+1))xy-s(s^2-s+1)^2y$ $=x^3-s(s^2-s+1)^2x^2$	$\Delta_9(s)$ (see below)

For all curves we will assume that the discriminant is nonzero. Note that for $m=9$, the discriminant of $E(s)$ is given by

$$\Delta_9(s) = s^5(-2-21s+70s^2-132s^3+144s^4-106s^5+46s^6-11s^7+s^8) \times (s^2-s+1)^7.$$

Also, for any prime p one can follow the argument given in [8, pp. 145–146], to see that any elliptic curve over $\mathbb{F}_p$ with an $\mathbb{F}_p$-point of order m can be written in the corresponding form in our Table 1. Thus, the reductions of the curves in the above table modulo a prime p cover all m-torsion elliptic curves over $\mathbb{F}_p$. We shall make use of this fact in Section 2.

Let us consider the families of curves $E(s)$ having an m-torsion point with m odd. Suppose that we have $r \not\equiv 2 \pmod m$. Then all of the curves

with $a_p(E) = r$ have cyclic m-torsion (see the discussion on page 85 for an explanation of this fact). In this case, we see that $m \mid m_E$ for each curve E in the family and in fact, for the obvious choice of generators for $E[m]$, we have

$$G := \varrho_{E,m}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} : b \in \mathbb{Z}/m\mathbb{Z},\ d \in (\mathbb{Z}/m\mathbb{Z})^* \right\}.$$

Thus one expects that when one averages over curves with rational m-torsion, the contribution to the constant from the primes dividing m is

$$C_r(m) = \frac{m|G_r|}{|G|} = \begin{cases} 0 & \text{when } (r-1, m) > 1, \\ m/\phi(m) & \text{otherwise.} \end{cases}$$

That is to say, one might expect that C_r should be

$$\frac{2}{\pi} \cdot \frac{m}{\phi(m)} \cdot \prod_{\substack{q \nmid m \\ q \nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q \nmid m \\ q \mid r}} \frac{q^2}{q^2-1}.$$

In this paper, we prove the following theorem.

THEOREM 3. *Let $E(s)$ be the parameterization of elliptic curves having a point of order $m \in \{5, 7, 9\}$. Then, for any $c > 0$, we have*

$$\frac{1}{\mu(N)} \sideset{}{'}\sum_{|s| \le N} \pi^r_{E(s)}(X) = \frac{2}{\pi} C_{r,m} \pi_{1/2}(X) + \mathrm{O}\left(\frac{X^{3/2}}{N} + \frac{\sqrt{X}}{\log^c X} \right),$$

where $\sum'$ represents the sum over non-singular curves, $\mu(N)$ represents the number of curves in the sum,

$$C_{r,m} = C_r(m) \prod_{\substack{q \nmid m \\ q \nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q \nmid m \\ q \mid r}} \frac{q^2}{q^2-1},$$

and

$$C_r(m) = \begin{cases} 5/4 & \text{if } m = 5 \text{ and } r \equiv 0, 3, 4 \pmod 5, \\ 7/6 & \text{if } m = 7 \text{ and } r \equiv 0, 3, 4, 5, 6 \pmod 7, \\ 3/2 & \text{if } m = 9 \text{ and } r \equiv 0, 3, 6 \pmod 9. \end{cases}$$

This leads us to the immediate corollary:

COROLLARY 1. *For any $\varepsilon > 0$, select $N > X^{1+\varepsilon}$. Assuming the notation from Theorem 3, for any $c > 0$ we have*

$$\frac{1}{\mu(N)} \sideset{}{'}\sum_{|s| \le N} \pi^r_{E(s)}(X) \sim \frac{2}{\pi} C_{r,m} \frac{\sqrt{X}}{\log X}.$$

In fact, we can prove the following stronger result.

THEOREM 4. *Suppose that $m \in \{5,7,9\}$ and $E(s)$ is the parameterization of elliptic curves having a rational point of order m. Let $\varepsilon > 0$ and fix $c > 0$. If $N > X^{1+\varepsilon}$, then for all $d > 2c$ and for all elliptic curves $E(s)$ with $|s| \le N$, with at most $\mathrm{O}(N/\log^d X)$ exceptions, we have the inequality*

$$|\pi^r_{E(s)} - C_{r,m}\pi_{1/2}(X)| \ll \frac{\sqrt{X}}{\log^c X}.$$

Given Theorem 3, the proof of Theorem 4 is analogous to the proof of Theorem 2. We refer the reader to [2] for the details of this proof and concentrate our efforts on proving Theorem 3.

2. Isomorphisms of m-torsion curves. Suppose for $p > 3$ that $\widetilde{E}$ is an isomorphism class of curves over $\mathbb{F}_p$ having m-torsion. Then there is a model of $\widetilde{E}$ of the form $E : y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{F}_p$. Using an argument analogous to the one given in [8, pp. 145–146], we can select a point (x_0, y_0) of order m on E and make several changes of variables to obtain a model for $\widetilde{E}$ of the appropriate form $E(s)$ from Table 1.

For $m \in \{5,7,9\}$, we note that the value of s depends only on the x-coordinate of our chosen m-torsion point and not on the particular values of A and B chosen. If we replace $E : y^2 = x^3 + Ax + B$ and (x_0, y_0) by an isomorphic curve $E' : y^2 = x^3 + Au^4x + Bu^6$ and the corresponding point (u^2x_0, u^3y_0) of order m then we obtain the same value for s. Thus the number of values of s which yield a model for $\widetilde{E}$ is simply the number of distinct x-coordinates among the points of order m on $\widetilde{E}$. Thus, if $E(s)$ has full m-torsion, there are $m\phi(m) - \phi^2(m)/2$ curves $E(S)$ with $E(S) \cong E(s)$, whereas if $E(s)$ has cyclic m-torsion, there are $\phi(m)/2$ such models.

We note that if $E(\mathbb{F}_p)$ has full m-torsion then the action of Frobenius on $E[m]$ is trivial and thus the trace r of the Frobenius must be 2 modulo m. We will only consider the case $r \not\equiv 2 \pmod m$. Thus, the curves under consideration will have cyclic m-torsion.

We recall that Deuring's theorem (see [1, 11]) tells us that the number of isomorphism classes of curves $\widetilde{E}/\mathbb{F}_p$ with $p+1-r$ points is $H(4p-r^2)+\mathrm{O}(1)$. For the remainder of this section, we will assume that $r \not\equiv 2 \pmod m$ and that $m \mid (p+1-r)$ and thus any curve with $p+1-r$ points will have cyclic m-torsion. If $m \in \{5,7\}$, for $r^2 < 4p$ we have

$$\sum_{\substack{1 \le s \le p \\ \#E(s)(\mathbb{F}_p) = p+1-r}} 1 = \begin{cases} \frac{1}{2}\phi(m)H(4p-r^2) + \mathrm{O}(1) \\ \quad \text{if } (r-1,m) = 1 \text{ and } r \not\equiv 2 \pmod m, \\ \quad \text{and } p \not\equiv r-1 \pmod{m^2}, \\ 0 \quad \text{if } (r-1,m) > 1. \end{cases} \tag{2}$$

In the case of $m = 9$, we assume that $r \not\equiv 2 \pmod 3$. Then, any curve with $p+1-r$ points will have cyclic 9-torsion. Thus for $r^2 < 4p$, we have

$$\sum_{\substack{1\le s\le p\\ \#E(s)(\mathbb{F}_p)=p+1-r}} 1 = \begin{cases} 3H(4p-r^2)+\mathrm{O}(1) \\ \quad \text{if } \mathrm{ord}_3(p+1-r)=2 \text{ and } r\not\equiv 2 \pmod 3, \\ 0 \quad \text{if } (r-1,9)>1. \end{cases}$$

3. Estimates for weighted sums of class numbers. First we fix some notation. We will let

$$B(r) := \max\{r^2/4, 5\} \quad \text{and} \quad d_p(f) := \frac{r^2-4p}{f^2}.$$

Also, let

$$S_f^r(X) := \{B(r) < p \le X : p \equiv r-1 \pmod m,\ 4p \equiv r^2, r^2-f^2 \pmod{4f^2}\}.$$

We recall the following definition of the Hurwitz class number (in what follows, we will assume that $\Delta \equiv 0, 1 \pmod 4$ is negative):

$$H(-\Delta) = 2 \sum_{\substack{f^2\mid\Delta\\ \Delta/f^2\equiv 0,1 \pmod 4}} \frac{h(\Delta/f^2)}{\omega(\Delta/f^2)},$$

where $h(\Delta)$ is the usual class number. We recall the class number formula

$$h(\Delta) = \frac{\omega(\Delta)\sqrt{-\Delta}}{2\pi} L(1, \chi_\Delta).$$

Combining these we have

$$H(-\Delta) = \frac{1}{\pi} \sum_{\substack{f^2\mid\Delta\\ \Delta/f^2\equiv 0,1 \pmod 4}} \frac{\sqrt{-\Delta}}{f} L(1, \chi_{\Delta/f^2}). \tag{3}$$

Next we prove the following useful lemmas.

Lemma 1. *We have*

$$\sum_{\substack{B(r)<p<X\\ p\equiv r-1 \pmod m}} H(4p-r^2) = \mathrm{O}(X^{3/2}).$$

Proof. Using (3), we rewrite the first sum above as

$$\frac{1}{\pi} \sum_{\substack{B(r)<p<X\\ p\equiv r-1 \pmod m}} \sum_{\substack{f^2\mid(4p-r^2)\\ d_p(f)\equiv 0,1 \pmod 4}} \frac{\sqrt{4p-r^2}}{f} L(1, \chi_{d_p(f)}).$$

By the main result of [12], $L(1,\chi_{d_p(f)}) \ll \log p$. Thus for X sufficiently large, the above sum is bounded above by a constant multiple of

$$(4)\quad \frac{2}{\pi}\sqrt{X}\log X\Bigg(\sum_{f\le X^{1/4}/\sqrt{m}}\frac{1}{f}\sum_{p\in S_f^r(X)}1+\sum_{X^{1/4}/\sqrt{m}\le f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(X)}1\Bigg).$$

Recall that the Brun–Titchmarsh inequality [5] states that for any a,

$$\pi(X,a,mf^2) := \#\{p<X : p\equiv a \pmod{mf^2}\} < \frac{3X}{\phi(mf^2)\log(X/mf^2)}.$$

For $f\le X^{1/4}/\sqrt{m}$, we have $\log(X/mf^2)\ge \frac{1}{2}\log X$. Thus, for such f,

$$\pi(X,a,mf^2) < \frac{6X}{f\phi(f)\log X}.$$

For $f\ge X^{1/4}/\sqrt{m}$,

$$\pi(X,a,mf^2) < \#\{n\le X : n\equiv a \pmod{\operatorname{lcm}[m,f^2]}\} \le \sqrt{X}.$$

Note that $\#S_f^r(X) = \mathrm{O}(\pi(X,1,mf^2))$. Thus, substituting the above estimates on $\pi(X,a,mf^2)$ into (4), we have

$$\frac{2}{\pi}\sqrt{X}\log X\Bigg(\sum_{f\le X^{1/4}/m}\frac{6X}{f^2\phi(f)\log X}+\sum_{X^{1/4}/m\le f\le 2\sqrt{X}/m}\frac{\sqrt{X}}{f}\Bigg)=\mathrm{O}(X^{3/2}).\ \blacksquare$$

Lemma 2.

$$(5)\quad \sum_{\substack{B(r)\le p\le X\\ p\equiv r-1\,(\mathrm{mod}\,m)}}\frac{H(4p-r^2)}{p}=\frac{2}{\pi\sqrt{X}\log X}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(X)}L(1,\chi_d)\log p$$
$$-\frac{2}{\pi}\int_2^X\sum_{f\le 2\sqrt{y}}\frac{1}{f}\sum_{p\in S_f^r(y)}L(1,\chi_d)\log p\,\frac{d}{dy}\left[\frac{1}{\sqrt{y}\log y}\right]dy+\mathrm{O}(\log X).$$

Proof. Using (3), we have

$$(6)\quad \sum_{\substack{B(r)\le p\le X\\ p\equiv r-1\,(\mathrm{mod}\,m)}}\frac{H(4p-r^2)}{p}=\frac{1}{\pi}\sum_{f\le 2\sqrt{X}}\sum_{p\in S_f^r(X)}\frac{\sqrt{4p-r^2}}{pf}L(1,\chi_{d_p(f)}).$$

If we observe that $\sqrt{4p-r^2}=2\sqrt{p}+\mathrm{O}(1/\sqrt{p})$, the right hand side becomes

$$(7)\quad \frac{2}{\pi}\sum_{f\le 2\sqrt{X}}\sum_{p\in S_f^r(X)}\frac{L(1,\chi_d)}{\sqrt{p}f}+\mathrm{O}\Bigg(\sum_{f\le 2\sqrt{X}}\sum_{p\in S_f^r(X)}\frac{L(1,\chi_d)}{p^{3/2}f}\Bigg)$$
$$=\frac{2}{\pi}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(X)}\frac{L(1,\chi_d)}{\sqrt{p}}+\mathrm{O}(\log X).$$

Now, using partial summation, we can write

$$\sum_{p\in S_f^r(X)} L(1,\chi_d)\log p\cdot\frac{1}{\sqrt{p}\log p} \tag{8}$$

$$=\frac{1}{\sqrt{X}\log X}\sum_{p\in S_f^r(X)} L(1,\chi_d)\log p-\int_2^X\sum_{p\in S_f^r(y)} L(1,\chi_d)\log p\,\frac{d}{dy}\left[\frac{1}{\sqrt{y}\log y}\right]dy.$$

Thus combining (6), (7) and (8) and observing that if $f>2\sqrt{y}$ then $S_f^r(y)=\emptyset$, we arive at (5). ∎

The following theorem is an immediate consequence of the main result in [7]:

THEOREM 5. *Suppose that $m\in\{5,7,9\}$ and $(r-1,m)=1$. Then for any $c>0$,*

$$\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(X)} L(1,\chi_{d_p(f)})\log p=\frac{C_{r,m}}{\phi(m)}\,X+\mathrm{O}\left(\frac{X}{\log^c X}\right),$$

where

$$C_{r,m}=C_r(m)\prod_{\substack{q\nmid m\\ q\nmid r}}\frac{q(q^2-q-1)}{(q+1)(q-1)^2}\prod_{\substack{q\nmid m\\ q\mid r}}\frac{q^2}{q^2-1},$$

and

$$C_r(m)=\begin{cases}5/4 & \text{if } m=5 \text{ and } r\equiv 0,3,4 \pmod 5,\\ 7/6 & \text{if } m=7 \text{ and } r\equiv 0,3,4,5,6 \pmod 7,\\ 3/2 & \text{if } m=9 \text{ and } r\equiv 0,3,6 \pmod 9.\end{cases}$$

COROLLARY 2. *Suppose that $m\in\{5,7,9\}$ and $(r-1,m)=1$ and let $C_{r,m}$ be as above. Then for any $c>0$,*

$$\sum_{\substack{B(r)\le p\le X\\ p\equiv r-1\,(\mathrm{mod}\,m)}}\frac{H(4p-r^2)}{p}=\frac{4C_{r,m}}{\pi\phi(m)}\,\pi_{1/2}(X)+\mathrm{O}\left(\frac{\sqrt{X}}{\log^c X}\right).$$

Proof. Combining Lemma 2 with Theorem 5, we have

$$\sum_{\substack{B(r)\le p\le X\\ p\equiv r-1\,(\mathrm{mod}\,m)}}\frac{H(4p-r^2)}{p} \tag{9}$$

$$=\frac{2C_{r,m}}{\pi\phi(m)}\left(\frac{\sqrt{X}}{\log X}-\int_2^X\left[y+\mathrm{O}\left(\frac{y}{\log^c y}\right)\right]\frac{d}{dy}\left[\frac{1}{\sqrt{y}\log y}\right]dy\right)$$

$$+\mathrm{O}\left(\frac{\sqrt{X}}{\log^c X}\right).$$

We make the following observations:

(1) $\dfrac{d}{dy}\left(\dfrac{1}{\sqrt{y}\log y}\right) = -\left(\dfrac{1}{2y^{3/2}\log y} + \dfrac{1}{y^{3/2}\log^2 y}\right)$.

(2) The O-term inside the integral contributes $\mathrm{O}(\sqrt{X}/\log^c X)$.

(3) $$\frac{\sqrt{X}}{\log X} = \int_2^X \frac{d}{dy}\left[\frac{\sqrt{y}}{\log y}\right] dy = \int_2^X \frac{dy}{2\sqrt{y}\log y} - \int_2^X \frac{dy}{\sqrt{y}\log^2 y}$$
$$= \pi_{1/2}(X) + \int_2^X \frac{dy}{\sqrt{y}\log^2 y},$$

hence

$$\pi_{1/2}(X) = \frac{\sqrt{X}}{\log X} + \int_2^X \frac{dy}{\sqrt{y}\log^2 y}.$$

So equation (9) becomes

$$\sum_{\substack{B(r)\le p\le X\\ p\equiv r-1 \,(\mathrm{mod}\, m)}} \frac{H(4p-r^2)}{p}$$
$$= \frac{2C_{r,m}}{\pi\phi(m)}\left(\frac{\sqrt{X}}{\log X} + \int_2^X \frac{dy}{2\sqrt{y}\log y} + \int_2^X \frac{dy}{\sqrt{y}\log^2 y}\right) + \mathrm{O}\left(\frac{\sqrt{X}}{\log^c X}\right)$$
$$= \frac{4C_{r,m}}{\pi\phi(m)}\,\pi_{1/2}(X) + \mathrm{O}\left(\frac{\sqrt{X}}{\log^c X}\right). \ \blacksquare$$

4. Proof of Theorem 3. Let $E(s)$ be the parameterization of elliptic curves having a point of order $m \in \{5,7\}$. Suppose that $(r-1,m) = 1$ and that $r \not\equiv 2 \,(\mathrm{mod}\, m)$. For the curves that we are interested in counting, $a_p(E(s)) = r$. Thus, we have $p + 1 - r = \#E(\mathbb{F}_p)$. Also, since the group of points on $E(s)$ has a subgroup of order m, we see that $p \equiv r - 1 \,(\mathrm{mod}\, m)$. By the definition of $\pi^r_{E(s)}(X)$, we can write

(10) $$\frac{1}{\mu(N)} \sideset{}{'}\sum_{|s|\le N} \pi^r_{E(s)}(X)$$
$$= \frac{1}{\mu(N)} \sum_{\substack{B(r)\le p\le X\\ p\equiv r-1 \,(\mathrm{mod}\, m)}} \Big(\sum_{\substack{|s|\le N\\ a_p(E(s))=r}} 1\Big) + \mathrm{O}\left(\frac{X}{N\log X}\right),$$

where the error term comes from no longer excluding singular curves in our sum.

Using (2), we can write

$$\sum_{\substack{|s|\le N\\ a_p(E(s))=r}} 1 = \left(\frac{\phi(m)}{2}\cdot H(4p-r^2)+\mathrm{O}(1)\right)\left(\frac{2N}{p}+\mathrm{O}(1)\right)$$
$$= \frac{N\phi(m)}{p}\cdot H(4p-r^2)+\mathrm{O}\left(H(4p-r^2)+\frac{2N}{p}\right).$$

If we now substitute this into equation (10) and note that $N/\mu(N)=\mathrm{O}(1)$, we obtain

$$\frac{1}{\mu(N)}\sum_{|s|\le N}{}' \pi^r_{E(s)}(X)$$
$$= \frac{\phi(m)}{\mu(N)}\sum_{\substack{B(r)\le p\le X\\ p\equiv r-1\,(\mathrm{mod}\,m)}}\left(\frac{N}{p}\,H(4p-r^2)+\mathrm{O}\left(H(4p-r^2)+\frac{2N}{p}\right)\right)$$
$$+\mathrm{O}\left(\frac{X}{N\log X}\right)$$
$$= \frac{\phi(m)}{2}\sum_{\substack{B(r)\le p\le X\\ p\equiv r-1\,(\mathrm{mod}\,m)}}\frac{H(4p-r^2)}{p}+\mathrm{O}\left(\frac{1}{N}\sum_{\substack{B(r)\le p\le X\\ p\equiv r-1\,(\mathrm{mod}\,m)}}H(4p-r^2)\right)$$
$$+\mathrm{O}\left(\frac{X}{N\log X}+\log\log X\right).$$

Applying Lemmas 2 and 1, we have

$$\frac{1}{\mu(N)}\sum_{|s|\le N}{}' \pi^r_{E(s)}(X) = \frac{2}{\pi}\,C_{r,m}\pi_{1/2}(X)+\mathrm{O}\left(\frac{X^{3/2}}{N}+\frac{\sqrt{X}}{\log^c X}\right).\ \blacksquare$$

References

[1] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. 43 (1968), 57–60.

[2] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices 1999, no. 4, 165–183.

[3] W. Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. 325 (1997), 813–818.

[4] E. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. 48 (1996), 31–104.

[5] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[6] K. James, *Average Frobenius distributions for elliptic curves with* 3*-torsion*, J. Number Theory 109 (2004), 278–298.

[7] —, *Averaging special values of Dirichlet L series*, The Ramanujan J., to appear.

[8] A. W. Knapp, *Ellipcit Curves*, Math. Notes 40, Princeton Univ. Press, Princeton, NJ, 1992.

[9] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) 33 (1976), 193–237.

[10] S. Lang and H. Trotter, *Frobenius Distributions in* GL_2*-extensions*, Lecture Notes in Math. 504, Springer, Berlin, 1976.

[11] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) 126 (1987), 649–673.

[12] S. Louboutin, *Explicit upper bounds on* $|L(1,\chi)|$, C. R. Acad. Sci. Paris Sér. I Math. 323 (1996), 443–446.

[13] B. Mazur, *Rational isogenies of prime degree* (with an appendix by D. Goldfeld), Invent. Math. 44 (1978), 129–162.

[14] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.

Department of Mathematics
Michigan State University
East Lansing, MI 48824, U.S.A.
E-mail: battist5@msu.edu

Department of Mathematics
Dartmouth College
6188 Bradley Hall
Hanover, NH 03755-3551, U.S.A.
E-mail: Jonathan.Bayless@dartmouth.edu

Stanford University
Mathematics, Bldg. 380
450 Serra Mall
Stanford, CA 94305-2125, U.S.A.
E-mail: ivanov@math.stanford.edu

Department of Mathematical Sciences
Clemson University
P.O. Box 340975
Clemson, SC 29634-0975, U.S.A.
E-mail: kevja@clemson.edu

Received on 13.12.2004
and in revised form on 10.3.2005 (4908)