IMRN International Mathematics Research Notices
1999, No. 4

Average Frobenius Distributions of Elliptic Curves

Chantal David and Francesco Pappalardi

1 Introduction

Let E be an elliptic curve defined over the rationals. For any prime p of good reduction, let E_p be the elliptic curve over $\mathbb{F}_p$ obtained by reducing E mod p. Let $a_p(E)$ be the trace of the Frobenius morphism of $E/\mathbb{F}_p$. Then, $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$, and $|a_p(E)| \le 2\sqrt{p}$. The case where $a_p(E) = 0$ corresponds to supersingular reduction mod p.

For a fixed $r \in \mathbb{Z}$, what can be said about the number of primes p such that $a_p(E) = r$? If E has complex multiplication, Deuring showed that half of the primes are primes of supersingular reduction (see [3]). More precisely, let

$$\pi_E^r(x) = \#\left\{p \le x:\ a_p\left(E\right) = r\right\}.$$

Then, if E has complex multiplication, $\pi_E^0(x) \sim 1/2\ \pi(x)$ as $x \to \infty$. If E has complex multiplication and $r \ne 0$, then the primes with a fixed trace of the Frobenius morphism are primes in quadratic progressions. For example, consider the elliptic curve $E\colon\ Y^2 = X^3 - X$ with complex multiplication by $\mathbb{Z}[i]$. It is easy to see that $a_p(E) = \pm 2$ if and only if $p = 1 + n^2$ for some integer n. If $q(n)$ is a quadratic progression, and

$$Q(x) = \#\{p \le x:\ p = q(n) \text{ for some } n\},$$

it was conjectured by Hardy and Littlewood [9] that $Q(x) \sim C\,(\sqrt{x}/\log x)$ as $x \to \infty$.

This conjecture is part of a more general conjecture of Lang and Trotter [11].

Conjecture 1.1 (Lang-Trotter conjecture). Let E be an elliptic curve defined over $\mathbb{Q}$, and let r be an integer. Except for the case where $r = 0$ and E has complex multiplication,

Received 25 June 1998.
Communicated by Peter Sarnak.

there is a constant $C_{E,r}$ such that

$$\pi_E^r(x) \sim C_{E,r}\,\frac{\sqrt{x}}{\log x} \qquad \text{as } x \to \infty. \tag{1}$$

Using their probabilistic model, Lang and Trotter gave an explicit description of the conjectural constant $C_{E,r}$ (see Section 2). The constant $C_{E,r}$ can be 0, and the asymptotic relation is then interpreted to mean that there is only a finite number of primes such that $a_p(E) = r$. It was shown by Elkies that this cannot happen when $r = 0$; i.e., for any $E/\mathbb{Q}$, there are infinitely many primes of supersingular reduction [5]. However, if $r \neq 0$, there could be only finitely many primes p such that $a_p(E) = r$. For example, if $E/\mathbb{Q}$ has a rational torsion point of order t, then t divides $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$ for all primes of good reduction, which imposes conditions on the values of $a_p(E)$.

We prove in this paper average estimates related to the Lang-Trotter conjecture. The average distribution fits the one predicted by the conjecture, and the conjectural constant $C_{E,r}$ of Lang and Trotter is confirmed by our results, as seen in Section 2. Average estimates for the case $r = 0$ were already obtained by Fouvry and Murty [6], and we obtain a generalization of their results for any $r \in \mathbb{Z}$. The techniques of Fouvry and Murty do not seem to extend to the general case $r \in \mathbb{Z}$. Our proof then differs significantly from theirs.

In the following, we fix $r \in \mathbb{Z}$, and we denote by $E(a,b)$ the elliptic curve $Y^2 = X^3 + aX + b$ with $a, b \in \mathbb{Z}$. Then

$$\pi^r_{E(a,b)}(x) = \#\left\{p \le x\colon\ a_p\left(E(a,b)\right) = r\right\}.$$

Following [11], we define

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

Theorem 1.2. Let r be an integer, $A, B \ge 1$. For every $c > 0$, we have

$$\frac{1}{4AB}\sum_{|a|\le A,\,|b|\le B} \pi^r_{E(a,b)}(x) = C_r\,\pi_{1/2}(x) + O\left(\left(\frac{1}{A}+\frac{1}{B}\right)x^{3/2} + \frac{x^{5/2}}{AB} + \frac{\sqrt{x}}{\log^c x}\right), \tag{2}$$

where

$$C_r = \frac{2}{\pi}\prod_{l\mid r}\left(1-\frac{1}{l^2}\right)^{-1}\prod_{l\nmid r}\frac{l(l^2-l-1)}{(l-1)(l^2-1)}. \tag{3}$$

The constants in the O-symbol depend only on c and r.

As the infinite product of (3) converges to a positive number, the constant C_r is nonzero, even if some $C_{E,r}$ can be zero, as mentioned above.

From the last theorem, we immediately obtain that the Lang-Trotter conjecture is true "on average."

Corollary 1.3. Let $\epsilon > 0$. If $A, B > x^{1+\epsilon}$, we have as $x \to \infty$,

$$\frac{1}{4AB} \sum_{|a| \le A,\, |b| \le B} \pi^r_{E(a,b)}(x) \sim C_r \frac{\sqrt{x}}{\log x}.$$

In analogy with the classical terminology, we can say that the *average order* of $\pi^r_{E(a,b)}(x)$ is $C_r(\sqrt{x}/\log x)$. Using the same techniques, we can also prove that the *normal order* of $\pi^r_{E(a,b)}(x)$ is $C_r(\sqrt{x}/\log x)$. Then, $\pi^r_{E(a,b)}(x) \sim C_r(\sqrt{x}/\log x)$ for "almost all" $E(a,b)$ rather than on average (see Corollary 1.5). We are grateful to A. Granville for suggesting this application of our techniques.

Theorem 1.4. Let $\epsilon > 0$. If $A, B > x^{1+\epsilon}$, then for every $c > 0$, we have

$$\frac{1}{4AB} \sum_{|a| \le A,\, |b| \le B} \left|\pi^r_{E(a,b)}(x) - C_r \pi_{1/2}(x)\right|^2 = O\left(\frac{x}{\log^c x} + \left(\frac{1}{A} + \frac{1}{B}\right) x^3 + \frac{1}{AB} x^5\right), \tag{4}$$

where the constant in the O-symbol depends only on c and r.

The following corollary is a standard application of the Turán normal order method.

Corollary 1.5. Let $\epsilon > 0$ and fix $c > 0$. If $A,\ B > x^{2+\epsilon}$, then for all $d > 2c$ and for all elliptic curves $E(a,b)$ with $|a| \le A$ and $|b| \le B$ with at most $O(AB/\log^d x)$ exceptions, we have the inequality

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

In Section 2, we compare the constant C_r with the constants $C_{E,r}$ predicted by Lang and Trotter. Sections 3 and 4 contain the proof of Theorem 1.2, and Section 5 contains the proof of Theorem 1.4.

2 The Lang-Trotter constant $C_{E,r}$

To formulate their conjecture, Lang and Trotter considered a probabilistic model compatible with the Cebotarev density theorem and with the Sato-Tate conjecture. From the model, they obtained an explicit description of the constant $C_{E,r}$ in terms of Galois representations, as described below. We compare in this section the conjectural constants $C_{E,r}$ of Lang and Trotter with the constant C_r of Theorem 1.2.

Let $\rho_{E,m}$ be the Galois representation

$$\rho_{E,m}\colon \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Aut}(E[m]),$$

where $E[m]$ is the subgroup of m-torsion points of $E(\overline{\mathbb{Q}})$. Since $E[m] \simeq \left(\mathbb{Z}/m\mathbb{Z}\right)^2$, after choosing a basis for $E[m]$, we can identify $\mathrm{Aut}(E[m])$ with $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Let $G(m)$ be the image of $\rho_{E,m}$ in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, and, for any subgroup G of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, let G_r be the subset of elements of G of trace r modulo m.

Let E be an elliptic curve without complex multiplication. Serre proved in [13] that the image of the Galois representation on the full torsion subgroup of $E(\overline{\mathbb{Q}})$ is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. It follows that there exists an integer m_E such that $\rho_{E,l}$ is surjective for all primes l not dividing m_E, and such that the image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of the Galois representation on the torsion subgroup of $E(\overline{\mathbb{Q}})$ is the full inverse image of $G(m_E)$. The Lang-Trotter constant $C_{E,r}$ is then defined as [see 11, p. 36]

$$\begin{aligned} C_{E,r} &= \frac{2}{\pi}\,\frac{m_E\,|G(m_E)_r|}{|G(m_E)|}\prod_{l \nmid m_E}\frac{l\,|G(l)_r|}{|G(l)|} \\ &= \frac{2}{\pi}\,\frac{m_E\,|G(m_E)_r|}{|G(m_E)|}\prod_{\substack{l \nmid m_E \\ l \mid r}}\left(1-\frac{1}{l^2}\right)^{-1}\prod_{\substack{l \nmid m_E \\ l \nmid r}}\frac{l(l^2-l-1)}{(l-1)(l^2-1)}. \end{aligned} \tag{5}$$

The second equality follows from the easy estimates

$$\frac{l\,|\,\mathrm{GL}_2(\mathbb{F}_l)_r|}{|\,\mathrm{GL}_2(\mathbb{F}_l)|} = \begin{cases} \dfrac{l^3(l-1)}{l(l-1)^2(l+1)} & \text{when } r \equiv 0 \ (l); \\[2ex] \dfrac{l^2(l^2-l-1)}{l(l-1)^2(l+1)} & \text{when } r \not\equiv 0 \ (l). \end{cases}$$

Comparing (3) and (5), we see that the local factors are exactly the same for the primes $l \nmid m_E$. More precisely, is it true that

$$\frac{1}{4AB}\sum_{|a|\le A,\,|b|\le B} C_{E(a,b),r} \sim C_r \qquad \text{as} \qquad A, B \to \infty?$$

There are partial results for the case $r = 0$ due to Fouvry and Ullmo [7]. The recent estimates of Duke [4], who showed that for "most" elliptic curves $E/\mathbb{Q}$, $\rho_{E,l}(G) = \mathrm{GL}_2(\mathbb{F}_l)$ for all primes l, are also relevant to this problem. But this does not imply that $m_E = 1$ (and then $C_{E,r} = C_r$) for those curves. In fact, we never have $m_E = 1$ as shown in [13, Proposition 22].

3 An average of special values of L-series

We show in Section 4 how the average

$$\frac{1}{4AB} \sum_{|a|\le A\ |b|\le B} \pi^r_{E(a,b)}(x)$$

can be rewritten as an average of special values of Dirichlet L-series by counting the number of curves over the finite fields $\mathbb{F}_p$ with $a_p = r$. The proof of Theorem 1.2 is then obtained by studying this average of L-series, which we evaluate in this section.

Let $B(r) = \max\left(3,\ r,\ r^2/4\right)$. In particular, $p > B(r)$ ensures $|r| \le 2\sqrt{p}$, a necessary condition for $a_p(E) = r$.

For $d \equiv 0, 1 (4)$, d not a perfect square, and $n \neq 0$, let $\chi_d(n) = (d/n)$ be the Kronecker symbol (see, for example, [10, p. 304]). The Kronecker symbol is a real character modulo $|d|$, and for $n > 0$,

$$\begin{aligned} d_1 \equiv d_2\ (n) &\Rightarrow \left(\frac{d_1}{n}\right) = \left(\frac{d_2}{n}\right) \qquad \text{for } n \text{ odd} \\ d_1 \equiv d_2\ (4n) &\Rightarrow \left(\frac{d_1}{n}\right) = \left(\frac{d_2}{n}\right) \qquad \text{for } n \in \mathbb{N}. \end{aligned} \tag{6}$$

We give the proof of Theorem 1.2 for r odd. The proof is similar when r is even; therefore, we omit it.

The main result of this section is the following theorem.

Theorem 3.1. Let r be an odd integer, and let

$$K_r = \sum_{\substack{f=1\\(2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{c_f^r(n)}{nf\varphi\left(nf^2\right)} \quad \text{with} \quad c_f^r(n) = \sum_{\substack{a(4n)^*\\(r^2-af^2,4n)=4}} \left(\frac{a}{n}\right), \tag{7}$$

where $\sum_{a(4n)^*}$ is the sum over a complete set of invertible residues mod $4n$.

Furthermore, let

$$\mathcal{S}_f(x) = \left\{ B(r) < p \le x \;\middle|\; 4p \equiv r^2\ (f^2),\ \text{and } d = \frac{r^2-4p}{f^2} \equiv 0, 1\ (4) \right\}.$$

Then for any $c > 0$,

$$\sum_{f\le 2\sqrt{x}} \frac{1}{f} \sum_{p\in\mathcal{S}_f(x)} L(1,\chi_d)\log p = K_r x + O\left(\frac{x}{\log^c x}\right). \tag{8}$$

Proof of Theorem 3.1. As r is odd, if $f^2 \mid r^2 - 4p$, then f is odd, and $d = (r^2-4p)/f^2 \equiv 1$ (4). Furthermore, since $(r, f) \mid p$, and $p > B(r)$, we have $(r, f) = 1$.

For a fixed parameter $U > 0$ to be chosen later, we have

$$L(1,\chi_d) = \sum_{n\geq 1}\left(\frac{d}{n}\right)\frac{1}{n} = \sum_{n\leq U}\left(\frac{d}{n}\right)\frac{1}{n} + O\left(\frac{\sqrt{|d|}\log|d|}{U}\right)$$
$$= \sum_{n\leq U}\left(\frac{d}{n}\right)\frac{1}{n} + O\left(\frac{\sqrt{p}\log p}{fU}\right) \tag{9}$$

using the Polya-Vinogradov inequality (see [2, p. 135]). Using (9), we can rewrite the left-hand side of (8) as

$$\sum_{\substack{f\leq 2\sqrt{x}\\(2r,f)=1}}\frac{1}{f}\sum_{n\leq U}\frac{1}{n}\sum_{p\in\mathcal{S}_f(x)}\left(\frac{d}{n}\right)\log p + O\left(\frac{x^{3/2}\log x}{U}\right). \tag{10}$$

For a fixed parameter V with $1 \leq V \leq 2\sqrt{x}$ to be chosen later, the first part of (10) is

$$\sum_{\substack{f\leq V\\(2r,f)=1}}\frac{1}{f}\sum_{n\leq U}\frac{1}{n}\sum_{p\in\mathcal{S}_f(x)}\left(\frac{d}{n}\right)\log p + \sum_{\substack{V<f\leq 2\sqrt{x}\\(2r,f)=1}}\frac{1}{f}\sum_{n\leq U}\frac{1}{n}\sum_{p\in\mathcal{S}_f(x)}\left(\frac{d}{n}\right)\log p.$$

The summation for large values of f is easily evaluated as

$$\left|\sum_{\substack{V<f\ll 2\sqrt{x}\\(2r,f)=1}}\frac{1}{f}\sum_{n\leq U}\frac{1}{n}\sum_{p\in\mathcal{S}_f(x)}\left(\frac{d}{n}\right)\log p\right| \leq \log x\ \log U\sum_{V<f\leq 2\sqrt{x}}\frac{1}{f}\sum_{\substack{n\leq x\\ n\equiv 4^* r^2 (f^2)}} 1$$
$$\ll x\log x\log U\sum_{V<f\leq 2\sqrt{x}}\frac{1}{f^3} \ll \frac{x\log x\log U}{V^2},$$

where 4^* is an integer such that $4^*\cdot 4 \equiv 1\ (f^2)$.

Therefore, we can rewrite the left-hand side of (8) as

$$\sum_{\substack{f\leq V\\(2r,f)=1}}\frac{1}{f}\sum_{n\leq U}\frac{1}{n}\sum_{p\in\mathcal{S}_f(x)}\left(\frac{d}{n}\right)\log p + O\left(\frac{x^{3/2}\log x}{U} + \frac{x\log x\log U}{V^2}\right). \tag{11}$$

The sum over "small values" of f and n leads to the main term. It is evaluated by splitting the sum according to the residue of d mod $4n$. Since $d = (r^2-4p)/f^2$ is odd, and $\left(\frac{d}{n}\right) = 0$

when $(d,n) > 1$, using (6), we get

$$\sum_{\substack{f\le V\\(2r,f)=1}} \frac{1}{f}\sum_{n\le U}\frac{1}{n}\sum_{p\in\mathcal{S}_f(x)}\left(\frac{d}{n}\right)\log p = \sum_{\substack{n\le U, f\le V\\(2r,f)=1}}\frac{1}{fn}\sum_{a(4n)^*}\left(\frac{a}{n}\right)\sum_{\substack{p\in\mathcal{S}_f(x)\\ d\equiv a(4n)}}\log p. \tag{12}$$

In the above sum, the two conditions $p \in \mathcal{S}_f(x)$ and $d = (r^2-4p)/f^2 \equiv a\ (4n)$ are equivalent to $B(r) < p \le x$ and $p \equiv (r^2-af^2)/4\ (nf^2)$. Furthermore, as $(2r,f)=1$, $\left((r^2-af^2)/4, nf^2\right) = 1 \iff (r^2-af^2, 4n) = 4$.

We use the standard notation

$$\psi_1(x;n,a) = \sum_{\substack{p\le x\\ p\equiv a\ (n)}} \log p,$$

$$E_1(x;n,a) = \psi_1(x;n,a) - \frac{x}{\varphi(n)} \quad \text{for } (a,n)=1.$$

Lemma 3.2 (Theorem of Barban, Davenport, and Halberstam). With the notation above, for any $K > 0$ and $x/\log^K x \le Q \le x$, we have

$$\sum_{n\le Q}\sum_{a(n)^*} E_1^2(x;n,a) \ll Qx\log x.$$

This classical result can be found, for example, in Davenport [2, p. 169].

We rewrite (12) as

$$\sum_{\substack{n\le U, f\le V\\(2r,f)=1}}\frac{1}{fn}\sum_{a(4n)^*}\left(\frac{a}{n}\right)\psi_1\left(x; nf^2, \frac{r^2-af^2}{4}\right) + O\left(U\log V\right),$$

where the term $O(U\log V)$ comes from the primes less than $B(r)$, and the O-constant depends on r only. Using the notation defined above, we rewrite the last equation as

$$x\sum_{\substack{n\le U, f\le V\\(2r,f)=1}}\frac{c_f^r(n)}{fn\varphi(nf^2)} + O(U\log V) + \sum_{\substack{n\le U, f\le V\\(2r,f)=1}}\frac{1}{fn}\sum_{\substack{a(4n)^*\\(r^2-af^2,4n)=4}}\left(\frac{a}{n}\right)E_1\left(x;nf^2,\frac{r^2-af^2}{4}\right). \tag{13}$$

The second sum of (13) is dominated by the error term. Indeed, using the Cauchy-Schwartz inequality, we bound it by

$$\sum_{\substack{f\le V\\(2r,f)=1}} \frac{1}{f}\left(\sum_{n\le U}\frac{\varphi(4n)}{n^2}\right)^{1/2}\left(\sum_{n\le U}\sum_{\substack{a(4n)^*\\(r^2-af^2,4n)=4}} E_1^2\left(x;nf^2,\frac{r^2-af^2}{4}\right)\right)^{1/2}$$

$$\le (\log U)^{1/2}\sum_{\substack{f\le V\\(2r,f)=1}} \frac{1}{f}\left(\sum_{n\le U}\sum_{\substack{a(4n)^*\\(r^2-af^2,4n)=4}} E_1^2\left(x;nf^2,\frac{r^2-af^2}{4}\right)\right)^{1/2}$$

$$\le (\log U)^{1/2}\sum_{\substack{f\le V\\(2r,f)=1}} \frac{1}{f}\left(\sum_{n\le U}\sum_{b(nf^2)^*} E_1^2(x;nf^2,b)\right)^{1/2},$$

as $a_1 \not\equiv a_2\ (4n)$ ensures that $b_1 = (r^2-a_1f^2)/4 \not\equiv b_2 = (r^2-a_2f^2)/4\ (nf^2)$.

Fix any $c > 0$. Then the last sum is bounded by

$$\le \log V\,(\log U)^{1/2}\left(\sum_{n\le UV^2}\sum_{a(n)^*} E_1^2(x;n,a)\right)^{1/2},$$

which is

$$\le \log V\,(\log U)^{1/2}\ \frac{x}{\log^{c+2} x} \tag{14}$$

when

$$UV^2 \le \frac{x}{\log^{B(c)} x} \tag{15}$$

from Lemma 3.2, with $B(c) = 2c+6$.

Finally, using (11), (13), and (14), we obtain

$$\sum_{f\le 2\sqrt{x}} \frac{1}{f}\sum_{p\in\mathcal{S}_f(x)} L(1,\chi_d)\ \log p$$

$$= x\sum_{\substack{n\le U,f\le V\\(2r,f)=1}} \frac{c_f^r(n)}{fn\varphi(nf^2)}$$

$$+ O\left(U\log V + \frac{x\log V\log^{1/2}U}{\log^{c+2}x} + \frac{x^{3/2}\log x}{U} + \frac{x\log x\log U}{V^2}\right) \tag{16}$$

for any U, V satisfying (15).

In order to find the asymptotic behavior of the main term, we have to estimate the growth of

$$c_f^r(n) = \sum_{\substack{a(4n)^* \\ (r^2-af^2,4n)=4}} \left(\frac{a}{n}\right).$$

Let $\kappa(n)$ be the multiplicative arithmetic function generated by the identity

$$\kappa(l^\alpha) = \begin{cases} l & \alpha \text{ odd}, \\ 1 & \alpha \text{ even}, \end{cases}$$

for any prime l and any positive integer α. Then for a positive integer n, $\kappa(n)$ is the smallest integer dividing n such that $n/\kappa(n)$ is a square.

Lemma 3.3. The following hold.

(1) If n is odd, then

$$c_f^r(n) = \sum_{\substack{a(n)^* \\ (r^2-af^2,n)=1}} \left(\frac{a}{n}\right).$$

(2) $c_f^r(n)$ is a multiplicative function of n.

(3) For any prime l, $c_f^r(l^\alpha) = c_{(f,l)}^r(l^\alpha)$.

(4) If $\alpha \geq 1$, then $c_1^r(2^\alpha) = (-2)^\alpha/2$.

(5) If l is an odd prime, then

$$\frac{c_1^r(l^\alpha)}{l^{\alpha-1}} = \begin{cases} l-1-\left(\frac{r^2}{l}\right) & \text{if } \alpha \text{ is even}, \\ -\left(\frac{r^2}{l}\right) & \text{if } \alpha \text{ is odd}. \end{cases}$$

(6) If l is an odd prime ($l \nmid r$), then

$$\frac{c_l^r(l^\alpha)}{l^{\alpha-1}} = \begin{cases} 0 & \text{if } \alpha \text{ is odd}, \\ l-1 & \text{if } \alpha \text{ is even}. \end{cases}$$

(7) For all n, $\left|c_f^r(n)\right| \leq n/\kappa(n)$.

Proof. (1) By definition,

$$c_f^r(n) = \sum_{\substack{a(4n)^*,a\equiv 1(4) \\ (r^2-af^2,4n)=4}} \left(\frac{a}{n}\right) + \sum_{\substack{a(4n)^*,a\equiv 3(4) \\ (r^2-af^2,4n)=4}} \left(\frac{a}{n}\right).$$

The second sum is empty since $r^2 + f^2 \equiv 2$ (4). If $a \equiv 1$ (4), then $(r^2 - af^2, 4n) = 4$ if and only if $(r^2 - af^2, n) = 1$. This gives

$$c_f^r(n) = \sum_{\substack{a(4n)^*,a\equiv 1(4) \\ (r^2-af^2,n)=1}} \left(\frac{a}{n}\right).$$

As n is odd, there is a bijection between the invertible residues modulo $4n$ which are congruent to 1 modulo 4 and the residues modulo n. We then use property (6) of the Kronecker symbols to deduce the claim.

(2) Clearly, $c_f^r(1) = 1$. Let $n = n_1 n_2$ with $(n_1, n_2) = 1$. We can suppose, without loss of generality, that $2 \nmid n_1$. By (1), we have

$$c_f^r(n_1)\, c_f^r(n_2) = \sum_{\substack{a_1 (n_1)^* \\ (r^2 - a_1 f^2, n_1) = 1}} \sum_{\substack{a_2 (4n_2)^* \\ (r^2 - a_2 f^2, 4n_2) = 4}} \left(\frac{a_1}{n_1}\right)\left(\frac{a_2}{n_2}\right). \tag{17}$$

Now for any a_1 and a_2 in the above sums, let a be the unique integer such that $1 \le a \le 4n$, $(a, 4n) = 1$, $a = a_1 + k_1 n_1 = a_2 + k_2 4n_2$ for some integers k_1 and k_2.

It is easy to see that $(r^2 - a_1 f^2, n_1) = 1$ and $(r^2 - a_2 f^2, 4n_2) = 4$ if and only if $(r^2 - af^2, 4n) = 4$. Therefore, we can write the right-hand side of (17) as

$$\sum_{\substack{a_1 (n_1)^*,\ a_2 (4n_2)^* \\ (r^2 - af^2, 4n) = 4}} \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right) = \sum_{\substack{a_1 (n_1)^*,\ a_2 (4n_2)^* \\ (r^2 - af^2, 4n) = 4}} \left(\frac{a}{n}\right).$$

The statement now follows by the Chinese remainder theorem.

(3) If $(f, l) = 1$, then the two sets $\{a \mid a (\mathrm{mod}\, 4l^\alpha),\ (a, 4l^\alpha) = 1\}$ and $\{af^2 \mid a (\mathrm{mod}\ 4l^\alpha),\ (a, 4l^\alpha) = 1\}$ are equal. So, if l is odd,

$$c_f^r(l^\alpha) = \sum_{\substack{a (l^\alpha)^* \\ (r^2 - af^2, l) = 1}} \left(\frac{a}{l}\right)^\alpha = \sum_{\substack{b (l^\alpha)^* \\ (r^2 - b, l) = 1}} \left(\frac{b}{l}\right)^\alpha \left(\frac{f^*}{l}\right)^{2\alpha} = c_1^r(l^\alpha), \tag{18}$$

where $f^* f \equiv 1\ (l)$. The proof is similar for $l = 2$. If $(f, l) = l$, then l is odd and, since $(r, f) = 1$, we have that $(r^2 - af^2, l) = 1$ for all a invertible residues modulo l^α. Therefore,

$$c_f^r(l^\alpha) = \sum_{a (l^\alpha)^*} \left(\frac{a}{l}\right)^\alpha = c_l^r(l^\alpha). \tag{19}$$

(4) Since $(\frac{a_1}{2}) = (\frac{a_2}{2})$ when $a_1 \equiv a_2\ (8)$, we have

$$c_1^r(2^\alpha) = 2^{\alpha - 1} \sum_{\substack{a (8)^* \\ (r^2 - a, 8) = 4}} \left(\frac{a}{2}\right)^\alpha.$$

Now $r^2 \equiv 1\ (8)$, so $(r^2 - a, 8) = 4$ if and only if $a \equiv 5\ (8)$. Therefore,

$$c_1^r(2^\alpha) = 2^{\alpha - 1} \left(\frac{5}{2}\right)^\alpha = (-2)^\alpha / 2.$$

(5) Using (18), we write

$$c_1^r(l^\alpha) = l^{\alpha - 1} \sum_{\substack{a (l)^* \\ (r^2 - a, l) = 1}} \left(\frac{a}{l}\right)^\alpha = l^{\alpha - 1} \sum_{a (l)^*} \left(\frac{a}{l}\right)^\alpha - l^{\alpha - 1} \left(\frac{r^2}{l}\right),$$

and the claim is deduced from the orthogonality relations of the Legendre symbols.

(6) This is a consequence of (19), by the orthogonality relations of the Legendre symbols.

(7) is a consequence of (2), (4), (5), and (6). ■

Lemma 3.4. Let

$$c = \prod_{l \text{ prime}} \left(1 + \frac{1}{l(\sqrt{l} - 1)}\right).$$

Then

$$\sum_{n>U} \frac{1}{\kappa(n)\varphi(n)} \sim \frac{c}{\sqrt{U}}.$$

In particular, $\sum_{n=1}^{\infty}(1/\kappa(n)\varphi(n))$ converges.

Proof. Let

$$C(t) = \sum_{n \le t} \frac{n^{3/2}}{\kappa(n)\varphi(n)}.$$

Using the partial summation formula (see [12, Exercise 1.1]), we immediately deduce that

$$\sum_{n>U} \frac{1}{\kappa(n)\varphi(n)} = \frac{3}{2}\int_U^{\infty} \frac{C(t)}{t^{5/2}} + \lim_{N\to\infty} \frac{C(N)}{N^{3/2}} - \frac{C(U)}{U^{3/2}}. \tag{20}$$

We claim that the following asymptotic formula holds:

$$C(t) \sim \frac{c}{2}\, t. \tag{21}$$

The lemma then follows easily by substituting (21) in (20).

To prove (21), we consider the Dirichlet series

$$K(s) = \sum_{n=1}^{\infty} \frac{n^{3/2}}{\kappa(n)\varphi(n)}\, n^{-s},$$

which clearly converges for $\Re(s) > 5/2$. Since both κ and φ are multiplicative functions, a straightforward computation gives the Euler product expansion

$$K(s) = \prod_{l \text{ prime}} \left(1 + \frac{l(l^{s-3/2} + 1)}{(l-1)(l^{2s-1} - 1)}\right).$$

This shows that $K(s)$ converges for $\Re(s) > 1$.

By computing the product

$$K(s) \cdot \frac{1}{\zeta(2s-1)} = \prod_{l \text{ prime}} \left(1 + \frac{1 + l^{s-1/2}}{l^{2s-1}(l-1)}\right),$$

which converges for $\Re(s) > 1/2$, we deduce that $K(s)$ admits a meromorphic continuation in the half plane $\Re(s) > 1/2$, with only a simple pole at $s = 1$ and residue

$$\frac{1}{2}\prod_{l \text{ prime}}\left(1+\frac{1}{l(\sqrt{l}-1)}\right).$$

Since $K(s)$ is regular on the vertical line $\Re(s) = 1$ ($s \neq 1$), we apply the Wiener-Ikehara Tauberian theorem (see, for example, [12, Theorem 1.1]) to $K(s)$ to deduce (21). This proves the lemma. ■

Theorem 3.1 now follows easily from Lemmas 3.3 and 3.4, as

$$x\sum_{\substack{n\le U, f\le V\\(2r,f)=1}}\frac{c_f^r(n)}{fn\varphi(nf^2)} = x\sum_{\substack{f\le V\\(2r,f)=1}}\sum_{n=1}^{\infty}\frac{c_f^r(n)}{fn\varphi(nf^2)} + O\left(x\sum_{f\le V}\frac{1}{f}\sum_{n>U}\frac{1}{\kappa(n)\varphi(nf^2)}\right)$$

from Lemma 3.3(7). But $\varphi(nf^2) \ge \varphi(n)\varphi(f^2)$, which gives

$$O\left(x\sum_{f\le V}\frac{1}{f}\sum_{n>U}\frac{1}{\kappa(n)\varphi(nf^2)}\right) = O\left(\frac{x}{U^{1/2}}\right)$$

from Lemma 3.4. Finally,

$$\begin{aligned} x\sum_{\substack{n\le U, f\le V\\(2r,f)=1}}\frac{c_f^r(n)}{fn\varphi(nf^2)} &= x\sum_{\substack{f=1\\(2r,f)=1}}^{\infty}\sum_{n=1}^{\infty}\frac{c_f^r(n)}{fn\varphi(nf^2)} \\ &\quad + O\left(x\sum_{f>V}\frac{1}{f\varphi(f^2)}\sum_{n=1}^{\infty}\frac{1}{\kappa(n)\varphi(n)}\right) + O\left(\frac{x}{U^{1/2}}\right) \\ &= K_r x + O\left(\frac{x}{V^2}\right) + O\left(\frac{x}{U^{1/2}}\right). \end{aligned} \tag{22}$$

This completes the proof of the theorem. Indeed, from (16) and (22),

$$\begin{aligned} &\sum_{f\le 2\sqrt{x}}\frac{1}{f}\sum_{p\le x}{}^{*}L(1,\chi_d)\log p \\ &\quad = K_r x + O\left(\frac{x}{V^2}+\frac{x}{U^{1/2}}\right) \\ &\qquad + O\left(U\log V + \frac{x\log V(\log U)^{1/2}}{\log^{c+2}x} + \frac{x^{3/2}\log x}{U} + \frac{x\log x\log U}{V^2}\right) \end{aligned}$$

for any U, V satisfying (15). Choosing

$$U = \sqrt{x}\log^{c+1}x,$$

$$V = (\log x)^{1/2(c+2)},$$

we deduce the result. ■

4 Proof of Theorem 1.2.

For $r \le 2\sqrt{p}$, the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ with $p+1-r$ points is the total number of ideal classes of the ring $\mathbb{Z}\left[\left(D+\sqrt{D}\right)/2\right]$, where $D = r^2-4p$ is a negative integer which is congruent to 0 or 1 modulo 4. This total number of ideal classes is the Kronecker class number

$$H(r^2-4p) = 2 \sum_{\substack{f^2 \mid r^2-4p \\ d \equiv 0,1(4)}} \frac{h(d)}{w(d)}, \tag{23}$$

where the sum ranges over positive integers f such that f^2 divides r^2-4p, and $d = (r^2-4p)/f^2$ is congruent to 0 or 1 modulo 4. As usual, $h(d)$ and $w(d)$ denote the class number and the number of units, respectively, of the order of discriminant d.

Suppose that $p \neq 2, 3$. Then, any elliptic curve over $\mathbb{F}_p$ has a model

$$E\colon\ Y^2 = X^3 + aX + b$$

with $a, b \in \mathbb{F}_p$. The elliptic curves $E'(a', b')$ over $\mathbb{F}_p$, which are $\mathbb{F}_p$-isomorphic to E, are given by all the choices

$$a' = \mu^4 a \quad\text{and}\quad b' = \mu^6 b$$

with $\mu \in \mathbb{F}_p^*$. The number of such E' is

$$\begin{aligned} &(p-1)/6 \quad \text{when } a = 0 \text{ and } p \equiv 1(3);\\ &(p-1)/4 \quad \text{when } b = 0 \text{ and } p \equiv 1(4);\\ &(p-1)/2 \quad \text{otherwise.} \end{aligned}$$

Then, the number of curves $E(a, b)$ with $a, b \in \mathbb{Z}$, $0 \le a, b < p$ and $a_p(E(a, b)) = r$ is

$$H(r^2-4p)\left(\frac{p-1}{2}\right) + O(p) = \frac{p\,H(r^2-4p)}{2} + O(p). \tag{24}$$

This result can be found in Birch [1].

We then write

$$\frac{1}{4AB} \sum_{|a| \le A,\, |b| \le B} \pi^r_{E(a,b)}(x) = \frac{1}{4AB} \sum_{p \le x} \#\left\{|a| \le A, |b| \le B\colon\ a_p\left(E(a,b)\right) = r\right\}$$

as

$$\frac{1}{4AB} \sum_{B(r) < p \le x} \left(\frac{2A}{p} + O(1)\right)\left(\frac{2B}{p} + O(1)\right)\left(\frac{p\,H(r^2-4p)}{2} + O(p)\right).$$

This last equation can be rewritten as

$$\frac{1}{2}\sum_{B(r)<p\le x}\frac{H(r^2-4p)}{p}+O\left(\sum_{B(r)<p\le x}H(r^2-4p)\left(\frac{1}{A}+\frac{1}{B}+\frac{p}{AB}\right)\right)+O\left(\log\log x\right). \quad (25)$$

Using

$$H(r^2-4p)\le\sum_{\substack{f^2\mid r^2-4p\\ d\equiv 0,1(4)}}h(d)\ll\sqrt{p}\log p\sum_{f^2\mid r^2-4p}\frac{1}{f},$$

and the Brun-Titchmarsh theorem (see, for example, [8]), we have the estimates

$$\begin{aligned}\sum_{p\le x}H(r^2-4p)&\ll\sqrt{x}\log x\sum_{p\le x}\sum_{f^2\mid r^2-4p}\frac{1}{f}\\ &\ll\sqrt{x}\log x\sum_{f\le 2\sqrt{x}}\frac{1}{f\varphi(f)}\frac{x}{\log x}\ll x^{3/2},\end{aligned} \quad (26)$$

$$\sum_{p\le x}pH(r^2-4p)\ll x^{5/2}. \quad (27)$$

Finally, replacing these estimates in (25), we have

$$\begin{aligned}\frac{1}{4AB}\sum_{|a|\le A,\,|b|\le B}\pi^{r}_{E(a,b)}(x)&=\frac{1}{2}\sum_{B(r)<p\le x}\frac{H(r^2-4p)}{p}\\ &\quad+O\left(\left(\frac{1}{A}+\frac{1}{B}\right)x^{3/2}+\frac{x^{5/2}}{AB}+\log\log x\right).\end{aligned} \quad (28)$$

We now use Theorem 3.1 to evaluate the main term of (28). Using (23), we write

$$\frac{1}{2}\sum_{B(r)<p\le x}\frac{H(r^2-4p)}{p}=\sum_{f\le 2\sqrt{x}}\sum_{p\in\mathcal{S}_f(x)}\frac{1}{p}\frac{h(d)}{w(d)}, \quad (29)$$

where

$$\mathcal{S}_f(x)=\{B(r)<p\le x\mid 4p-r^2\equiv 0\ (f^2),\ \text{and}\ d=\frac{r^2-4p}{f^2}\equiv 0,1\ (4)\}.$$

As $d=(r^2-4p)/f^2$ is a negative integer, the class number formula reads as

$$h(d)=\frac{w(d)|d|^{1/2}}{2\pi}L(1,\chi_d), \quad (30)$$

where χ_d is the Kronecker symbol defined in Section 3. Therefore, replacing (30) in (29), we have

$$\frac{1}{2}\sum_{B(r)<p\le x}\frac{H(r^2-4p)}{p}=\frac{1}{2\pi}\sum_{f\le 2\sqrt{x}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}\frac{\sqrt{4p-r^2}}{p}L(1,\chi_d)$$
$$=\frac{1}{\pi}\sum_{f\le 2\sqrt{x}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}\frac{L(1,\chi_d)}{\sqrt{p}}+O\left(\log^2 x\right).$$

With partial summation, we write

$$\sum_{f\le 2\sqrt{x}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}\frac{L(1,\chi_d)}{\sqrt{p}}=\frac{1}{\sqrt{x}\log x}\sum_{f\le 2\sqrt{x}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}L(1,\chi_d)\log p$$
$$-\int_2^x\sum_{f\le 2\sqrt{t}}\left(\frac{1}{f}\sum_{p\in\mathcal{S}_f(t)}L(1,\chi_d)\log p\right)\frac{d}{dt}\left(\frac{1}{\sqrt{t}\log t}\right)dt, \tag{31}$$

since $\mathcal{S}_f(t)=\emptyset$ for $f>2\sqrt{t}$. Using Theorem 3.1, (31) can be rewritten as

$$K_r\int_2^x\frac{dt}{2\sqrt{t}\log t}+K_r\left(\frac{\sqrt{x}}{\log x}+\int_2^x\frac{dt}{\sqrt{t}\log^2 t}\right)$$
$$+O\left(\frac{\sqrt{x}}{\log^{c+1}x}\right)+O\left(\int_2^x\frac{dt}{\sqrt{t}\log^{c+1}t}\right),$$

which gives

$$\frac{1}{2}\sum_{B(r)<p\le x}\frac{H(r^2-4p)}{p}=\frac{2K_r}{\pi}\,\pi_{1/2}(x)+O\left(\frac{\sqrt{x}}{\log^c x}\right). \tag{32}$$

Replacing (32) in (28), the only thing left to show is that $C_r=(2/\pi)K_r$ has the correct Euler product expansion.

Lemma 4.1. Suppose that r is an odd integer. Let

$$K_r=\sum_{\substack{f=1\\(2r,f)=1}}^{\infty}\sum_{n=1}^{\infty}\frac{c_f^r(n)}{nf\varphi\left(nf^2\right)}\quad\text{with}\quad c_f^r(n)=\sum_{\substack{a(4n)^*\\(r^2-af^2,4n)=4}}\left(\frac{a}{n}\right),$$

where $\sum_{a(n)^*}$ is the sum over a complete set of invertible residues mod n. Then

$$K_r=\prod_{l\mid r}\left(1-\frac{1}{l^2}\right)^{-1}\prod_{l\nmid r}\frac{l(l^2-l-1)}{(l-1)(l^2-1)}.$$

Proof of Lemma 4.1. Since $c_f^r(n)$ is a multiplicative function of n (Lemma 3.3(2)), we have that

$$K_r = \sum_{\substack{f=1 \\ (f,2r)=1}}^{\infty} \frac{1}{f\varphi(f^2)} \prod_{l} \left(\sum_{\alpha \geq 0} \frac{c_f^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \cdot \frac{\varphi((f^2, l^\alpha))}{(f^2, l^\alpha)} \right). \tag{33}$$

Using Lemma 3.3(3), we rewrite the above product as

$$\begin{aligned} \prod_{l} \left(\sum_{\alpha \geq 0} \frac{c_f^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \cdot \frac{\varphi((f^2, l^\alpha))}{(f^2, l^\alpha)} \right) &= \prod_{l \nmid f} \left(\sum_{\alpha \geq 0} \frac{c_1^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \right) \prod_{l \mid f} \left(\sum_{\alpha \geq 0} \frac{c_f^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \frac{\varphi((f^2, l^\alpha))}{(f^2, l^\alpha)} \right) \\ &= \prod_{l} \left(\sum_{\alpha \geq 0} \frac{c_1^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \right) \prod_{l \mid f} \left(\frac{\sum_{\alpha \geq 0} \frac{c_f^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \frac{\varphi((f^2, l^\alpha))}{(f^2, l^\alpha)}}{\sum_{\alpha \geq 0} \frac{c_1^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)}} \right). \end{aligned}$$

Replacing inside (33), and using the multiplicativity of the functions in the outer sum of (33), we obtain

$$\begin{aligned} K_r &= \prod_{l} \left(\sum_{\alpha \geq 0} \frac{c_1^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \right) \prod_{l \nmid 2r} \left(1 + \sum_{\beta \geq 1} \frac{1}{l^\beta \varphi(l^{2\beta})} \cdot \frac{\sum_{\alpha \geq 0} \frac{c_l^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \cdot \frac{\varphi((l^{2\beta}, l^\alpha))}{(l^{2\beta}, l^\alpha)}}{\sum_{\alpha \geq 0} \frac{c_1^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)}} \right) \\ &= \prod_{l \mid 2r} \left(\sum_{\alpha \geq 0} \frac{c_1^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \right) \prod_{l \nmid 2r} \left(1 + \sum_{\alpha \geq 1} \frac{c_1^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} + \frac{1}{l^3 - 1} \left(\frac{l}{l-1} + \sum_{\alpha \geq 1} \frac{c_l^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} \right) \right). \end{aligned}$$

With Lemma 3.3, we compute

$$\sum_{\alpha \geq 1} \frac{c_1^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} = \begin{cases} \dfrac{2}{3} & \text{if } l = 2, \\[2ex] \dfrac{1}{l^2 - 1} & \text{if } l \mid r, \\[2ex] \dfrac{-2}{(l-1)(l^2-1)} & \text{if } l \nmid 2r, \end{cases}$$

and for $l \nmid 2r$,

$$\sum_{\alpha \geq 1} \frac{c_l^r(l^\alpha)}{l^\alpha \varphi(l^\alpha)} = \frac{1}{l^2 - 1}.$$

Replacing in the expression for K_r above, this gives

$$\begin{aligned} K_r &= \frac{2}{3} \prod_{l \mid r} \left(1 - \frac{1}{l^2} \right)^{-1} \prod_{l \nmid 2r} \left(1 - \frac{2}{(l-1)(l^2-1)} + \frac{1}{(l-1)(l^2-1)} \right) \\ &= \prod_{l \mid r} \left(1 - \frac{1}{l^2} \right)^{-1} \prod_{l \nmid r} \frac{l(l^2 - l - 1)}{(l-1)(l^2-1)}. \end{aligned}$$

This completes the proof of Theorem 1.2 for r odd. ■

5 Proof of Theorem 1.4.

We prove Theorem 1.4 in this section. As in the proof of Theorem 1.2, the main ingredient is Theorem 3.1.

Let

$$\mu = \frac{1}{4AB} \sum_{|a|\le A,\, |b|\le B} \pi^r_{E(a,b)}(x).$$

Fix any $c > 0$. Then, for $A, B > x^{1+\epsilon}$, Theorem 1.2 gives

$$\mu = C_r \pi_{1/2}(x) + O\left(\frac{\sqrt{x}}{\log^c x}\right). \tag{34}$$

Thus, by the triangle inequality, the left-hand side of (4) is

$$\ll \frac{1}{4AB} \sum_{|a|\le A,\, |b|\le B} \left|\pi^r_{E(a,b)}(x) - \mu\right|^2 + O\left(\frac{x}{\log^{2c} x}\right). \tag{35}$$

Now in general, if $\mu = (1/N)\sum_{n=1}^N \lambda_n$, then $(1/N)\sum_{n=1}^N (\lambda_n - \mu)^2 = (1/N)\sum_{n=1}^N \lambda_n^2 - \mu^2$. Therefore, the left-hand side of (4) is

$$\ll \frac{1}{4AB} \sum_{|a|\le A,\, |b|\le B} \left(\pi^r_{E(a,b)}(x)\right)^2 - \mu^2 + O\left(\frac{x}{\log^{2c} x}\right). \tag{36}$$

We then write

$$\left(\pi^r_{E(a,b)}(x)\right)^2 = \pi^r_{E(a,b)}(x) + \#\left\{p, q \le x \mid p \ne q,\ a_p(E(a,b)) = a_q(E(a,b)) = r\right\},$$

where the pairs p, q and q, p are both counted.

Proceeding as in the proof of Theorem 1.2 and using the Chinese remainder theorem, we obtain from the last line that

$$\frac{1}{4AB} \sum_{|a|\le A,\, |b|\le B} \left(\pi^r_{E(a,b)}(x)\right)^2 = \mu + \frac{1}{4} \sum_{B(r)<p,q\le x,\ p\ne q} \frac{H(r^2-4p)}{p}\frac{H(r^2-4q)}{q} + E(x, A, B),$$

where

$$E(x, A, B) \ll \sum_{p,q\le x} \frac{H(r^2-4p) + H(r^2-4q)}{pq}$$
$$+ \sum_{p,q\le x} H(r^2-4p)\ H(r^2-4q)\ \left(\frac{1}{A} + \frac{1}{B} + \frac{pq}{AB}\right).$$

Therefore, using the estimates (26) and (27), we obtain

$$E(x, A, B) \ll \frac{\sqrt{x}\log\log x}{\log x} + \left(\frac{1}{A} + \frac{1}{B}\right)x^3 + \frac{x^5}{AB}. \tag{37}$$

Then

$$\frac{1}{4AB}\sum_{|a|\le A,\, |b|\le B}\left(\pi^r_{E(a,b)}(x)\right)^2 = \mu + \left(\frac{1}{2}\sum_{B(r)<p\le x}\frac{H(r^2-4p)}{p}\right)^2 - \frac{1}{4}\sum_{p\le x}\frac{H(r^2-4p)^2}{p^2} + E(x, A, B),$$

and using (32) and (37), this gives

$$\frac{1}{4AB}\sum_{|a|\le A,\, |b|\le B}\left(\pi^r_{E(a,b)}(x)\right)^2 = \left(C_r\pi_{1/2}(x)\right)^2 + O\left(\frac{x}{\log^c x} + \left(\frac{1}{A} + \frac{1}{B}\right)x^3 + \frac{x^5}{AB}\right).$$

Replacing in (36), and using (34), this completes the proof of Theorem 1.4 ∎

Acknowledgments

The first author's research was partially supported by the Centre Interuniversitaire en Calcul Mathématique Algébrique (CICMA); and by the National Sciences and Engineering Research Council (NSERC).

The second author's research was partially supported by CICMA and by Consiglio Nazionale delle Ricerche.

This work was done when the second author was visiting CICMA. He thanks the faculty and staff of CICMA for their hospitality and financial support. Both authors would like to thank A. Granville for helpful discussions and for mentioning to us the result of Theorem 1.4. We also thank W. D. Banks and H. Kisilevsky for helpful discussions.

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] H. Davenport, *Multiplicative Number Theory*, 2d ed., Springer-Verlag, New York, 1980.

[3] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

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

[5] N. D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* Q, Invent. Math. **89** (1987), 561–567.

[6] E. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. **48** (1996), 81–104.

[7] E. Fouvry and E. Ullmo, private communication.

[8] H. Halberstam and H.-E. Richert, *Sieve Methods*, London Math. Soc. Monogr. **4**, Academic Press, London, 1974.

[9] G. H. Hardy and J. E. Littlewood, *Some problems of partitio numenorum III*, Acta. Math. **44** (1923), 1–70.

[10] L.-K. Hua, *Introduction to Number Theory*, trans. P. Shiu, Springer-Verlag, Berlin, 1982.

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

[12] M. R. Murty and V. K. Murty, *Non-vanishing of L-functions and Applications*, Progr. Math. **157**, Birkhäuser, Basel, 1997.

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

David: Concordia University, Department of Mathematics,1455 de Maisonneuve Blvd. West, Montréal, Quebec H3G 1M8, Canada; chantal@cicma.concordia.ca

Pappalardi: Università degli Studi Roma Tre, Dipartimento di Matematica, Largo S. L. Murialdo, 1, 00146, Roma, Italia; pappa@mat.uniroma3.it