ACTA ARITHMETICA
124.1 (2006)

Average Frobenius distribution of elliptic curves

by

Kevin James (Clemson, SC) and Gang Yu (Columbia, SC)

1. Introduction. Given an elliptic curve $E/\mathbb{F}_p$, let $E(\mathbb{F}_p)$ denote the Mordell–Weil group, which consists of the $\mathbb{F}_p$-rational points on the curve along with an identity at infinity. A simple heuristic shows that the normal order of $E(\mathbb{F}_p)$ is $p+1$. If we let

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

Hasse's theorem asserts that

$$|a_E(p)| < 2\sqrt{p}. \tag{1.1}$$

It follows from Deuring's theorem (see [2] or [7]) that (1.1) is best possible in the sense that, given a prime p, and an integer $r \in (-2\sqrt{p}, 2\sqrt{p})$, there exists an elliptic curve $E/\mathbb{F}_p$ such that $a_E(p) = r$.

Let [1]

$$\frac{a_E(p)}{2\sqrt{p}} = \cos\theta_E(p), \qquad \theta_E(p) \in [0, \pi].$$

Then for a particular curve $E/\mathbb{Q}$, it is quite natural to ask how $\theta_E(p)$ varies with p.

When E has complex multiplication, the answer turns out to be easy. In this case, asymptotically, half of primes p satisfy $a_E(p) = 0$. Apart from these *supersingular* primes, the primes p with $\theta_E(p)$ in a fixed range are those given by $p = f(u, v)$, where $f(u, v)$ is a certain positive definite binary quadratic form, with $|u|/p$ in the corresponding range. The distribution of such primes, with a certain uniformity, is known and can be traced back to Hecke's famous work [5, 6].

2000 *Mathematics Subject Classification*: Primary 11G05; Secondary 11N05.

The first author wishes to thank the University of South Carolina for their kind hospitality. The research described in this paper began while he was their guest.

The first author's research is partially supported by the National Science Foundation through DMS-0244001.

[1] We remark that, in some references, it is defined that $-a_E(p)/2\sqrt{p} = \cos\theta_E(p)$. This however does not change the statement of the Sato–Tate conjecture.

When E does not have complex multiplication, the problem is much more difficult. With the experimental support of Sato, Tate [10] has given theoretical evidence for the following conjecture (for further discussion see [2, 8, 9]).

Sato–Tate Conjecture. *Suppose E is an elliptic curve over $\mathbb{Q}$ which does not admit complex multiplication. For any $0 \le \theta_1 \le \theta_2 \le \pi$ and $x > 1$, let*

$$\pi_E^{(\theta_1,\theta_2)}(x) := \#\{p \le x : \theta_1 \le \theta_E(p) \le \theta_2\}.$$

Then

$$\lim_{x\to\infty} \frac{\pi_E^{(\theta_1,\theta_2)}(x)}{\pi(x)} = \frac{2}{\pi} \int_{\theta_1}^{\theta_2} \sin^2\theta \, d\theta,$$

where $\pi(x)$ is the number of primes up to x.

For $-1 \le \alpha \le \beta \le 1$ and $x > 1$, let

$$\pi_E(\alpha, \beta; x) := \#\left\{p \le x : \alpha \le \frac{a_E(p)}{2\sqrt{p}} \le \beta\right\}.$$

Then by a simple change of variables, we see that the Sato–Tate conjecture is equivalent to

$$\lim_{x\to\infty} \frac{\pi_E(\alpha, \beta; x)}{\pi(x)} = \frac{2}{\pi} \int_{\alpha}^{\beta} \sqrt{1 - t^2} \, dt.$$

In [2], using the Selberg trace formula, Birch proved that, for any positive integer k, one has

$$\text{mean } |a_E(p)|^{2k} \sim \frac{2k! p^k}{k!(k+1)!}$$

as $p \to \infty$. Here the mean is taken subject to E varying over all elliptic curves over $\mathbb{F}_p$. Birch's result essentially implies that the Sato–Tate conjecture for elliptic curves is true on average.

Suppose $\mathcal{S}$ is a subset of $\mathbb{Z}$ which is not too sparse. For $-1 \le \alpha \le \beta \le 1$ and $x > 1$, let $\pi_E(\alpha, \beta, \mathcal{S}; x)$ be the number of primes $p \le x$ satisfying

$$\alpha \le \frac{a_E(p)}{2\sqrt{p}} \le \beta, \qquad a_E(p) \in \mathcal{S}.$$

From the probabilistic point of view, there should be an asymptotic formula for $\pi_E(\alpha, \beta, \mathcal{S}; x)$ as $x \to \infty$ if $\mathcal{S}$ is not too sparse and is uniformly distributed. It is then natural to ask how $\pi_E(\alpha, \beta, \mathcal{S}; x)$ may depend on $\mathcal{S}$.

We can show that, when $\mathcal{S}$ is nice enough, $\pi_{E(a,b)}(\alpha, \beta, \mathcal{S}; x)$ has an asymptotic formula for almost all elliptic curves $E(a, b)$ with a, b varying in certain ranges depending on x, where $E(a, b)$ is given by the equation

$$E(a, b): \quad y^2 = x^3 + ax + b.$$

This gives a heuristic for the relation of $\pi_E(\alpha, \beta, \mathcal{S}; x)$ and $\mathcal{S}$.

Due to symmetry, we may consider only the average behavior of

$$\pi_E(\alpha, \mathcal{S}; x) := \pi_E(0, \alpha, \mathcal{S}; x)$$

for a given $\mathcal{S}$ and $\alpha \in [0, 1]$. Without loss of generality, $\mathcal{S}$ may be taken as a subset of $\mathbb{Z}_{\geq 0}$.

It will be clear from our treatment that $\mathcal{S}$ is *nice* for our purposes provided that, for large N, the exponential sum

$$\sum_{n \in \mathcal{S} \cap [1,N]} e(n^2 \lambda)$$

can be well approximated when λ is on major arcs (which are reasonably large in terms of N) in applying the Hardy–Littlewood circle method. From this, experts who are familiar with the Hardy–Littlewood method may have noted that $\mathcal{S}$ can be chosen, for example, to be an arithmetic progression, the set of kth powers, smooth numbers, values of an integer-valued polynomial at primes, or even the set of integers which are sums of a fixed number of exponentials (powers of 2, for instance).

In this paper, we shall only consider the case that $\mathcal{S}$ is the set of all kth powers. The results for the various cases listed above follow from similar proofs. Henceforth, $\mathcal{K}$ will denote the set of all kth powers for a fixed $k \in \mathbb{N}$.

For $0 < \alpha < 1$ and positive real numbers U, V, A, B, X, let

$$S_\alpha(U, V, A, B; \mathcal{K}; X) = \frac{1}{AB} \sum_{\substack{U < a \leq U + A \\ V < b \leq V + B}} \pi_{E(a,b)}(\alpha, \mathcal{K}; X).$$

The function $S_\alpha(U, V, A, B; \mathcal{K}; X)$ measures, in a certain range, the average number of primes up to X with $a_E(p) \in \mathcal{K}$ and $\theta_E(p)$ belonging to a given interval $[\arccos \alpha, \pi/2)$. We will investigate the asymptotic behavior of $S_\alpha(U, V, A, B; \mathcal{K}; X)$ when A and B are large enough in comparison with X, as $X \to \infty$.

THEOREM 1. *Let $0 < \alpha < 1$ be fixed and let U and V be any real numbers. For any given $\varepsilon > 0$ and X sufficiently large, if $A, B > X \log X$, then*

$$S_\alpha(U, V, A, B; \mathcal{K}; X) \sim c_k(\alpha) \pi_k(X),$$

where

$$\pi_k(X) = \int_2^X \frac{t^{1/2k - 1/2}}{\log t}\, dt = (1 + O((\log X)^{-1})) \frac{2k}{k+1} \frac{X^{1/2 + 1/2k}}{\log X},$$

$$c_k(\alpha) = \left(\frac{1}{3} + \frac{2}{3}\,\delta(k)\right) \frac{2^{1/k}}{k\pi} \int_0^\alpha |t|^{1/k - 1} \sqrt{1 - t^2}\, dt,$$

and $\delta(k)$ *is given by*

$$\delta(k) = \begin{cases} 1 & \text{if } k = 1, \\ 0 & \text{if } k > 1. \end{cases} \tag{1.2}$$

Note that, taking $k = 1$, Theorem 1 implies that the Sato–Tate conjecture holds on average. With a little extra effort, we can show that $c_k(\alpha)\pi_k(X)$ is actually the normal order of $\pi_E(\alpha, \mathcal{K}; X)$.

THEOREM 2. *Let* $0 < \alpha < 1$ *be fixed, and let* $U, V \in \mathbb{R}$. *Suppose that* A, B *and* X *are sufficiently large real numbers and that* $A, B > (X \log X)^2$. *Then*

$$\frac{1}{AB} \sum_{\substack{U<a\le U+A \\ V<b\le V+B}} |\pi_{E(a,b)}(\alpha, \mathcal{K}; X) - c_k(\alpha)\pi_k(X)|^2 = o((\pi_k(X))^2).$$

We also note that under our assumptions on A and B, the contribution to $S_\alpha(U, V, A, B; \mathcal{K}; X)$ by curves $E(a, b)$ with complex multiplication is negligible. (There are only 13 j-invariants associated with CM curves, hence, the total number of CM curves encountered is $O(A + B)$ and therefore the contribution of CM curves to $S_\alpha(U, V, A, B; \mathcal{K}; X)$ is easily seen to be $O(\pi_k(X)(1/A+1/B))$, which under our assumptions on A and B is $o(1)$.) In view of this and Theorem 2, it seems reasonable for us to make the following conjecture.

CONJECTURE 1. *For a given elliptic curve* $E/\mathbb{Q}$ *without complex multiplication, and* $-1 < \alpha < \beta < 1$, *we have*

$$\pi_E(\alpha, \beta, \mathcal{K}; X) \sim (c_k(\beta) - c_k(\alpha))\pi_k(X). \tag{1.3}$$

We have not pursued uniformity in α in Theorems 1 and 2. Nevertheless, it is clear from our proof that α can be related to X and the asymptotic formulas still hold as long as α is bounded away from 0 and 1 by $(\log X)^{-c}$ for any $c > 0$. This is essentially equivalent to the normal order of $\pi_E(\alpha, \beta; X)$ being $(c_k(\beta) - c_k(\alpha))\pi_k(X)$ provided $\beta - \alpha > (\log X)^{-c}$ for any $c > 0$. The $(\log X)^{-c}$ can be further improved to $\exp(-c_1\sqrt{\log X})$ for some $c_1 > 0$ if, instead of directly using the approximation (2.6) on major arcs, one separately discusses the cases for those q and $\chi \pmod q$ with $L(s, \chi)$ having a possible Siegel zero. However, this will not be the focus of this paper.

The organization of this paper is as follows. We first employ the Hardy–Littlewood method in Section 2 to derive estimates on the number of representations of certain integers n as $n = r^2 - 4p$. We then derive an estimate for a weighted average of special values of truncated Dirichlet L-functions in Section 3. We employ these estimates to prove the main theorem in Sec-

tion 4. In Section 5 we prove Theorem 2. Finally, we make some closing remarks in Section 6.

2. A problem of representations. In this section we employ the Hardy–Littlewood method (see [11]) in order to give an asymptotic formula for the number of representations of a negative integer $n \equiv 0$ or $1 \pmod 4$ as

$$n = r^2 - 4p,$$

subject to $p \le X$ being a prime, and $r \in \mathcal{K} \cap [0, 2\alpha\sqrt{p}]$, where $0 < \alpha < 1$. We give an asymptotic main term for the number of representations which is large when some local conditions are satisfied, and an error term which is small on average.

For convenience, we consider the following weighted number of representations:

$$R(n) = \sum_{\substack{p \le X \\ r \le (2\alpha\sqrt{p})^{1/k} \\ r^{2k} - 4p = n}} \log p. \tag{2.1}$$

Let $P = (\log X)^{2^{2k+3}}$. For a positive integer m, let $\operatorname{ord}_2(m)$ be the non-negative integer such that $2^{\operatorname{ord}_2(m)} \parallel m$, and write $[m]_{\mathrm{o}} = 2^{-\operatorname{ord}_2(m)} m$ for the odd part of m.

THEOREM 3. *With $R(n)$ defined by* (2.1), *we have*

$$R(n) = \mathfrak{S}(n, P) J(n) + E(n) + O(X^{1/2k} (\log X)^{-3}), \tag{2.2}$$

where

$$\mathfrak{S}(n, P) = \sum_{m \le P} \frac{\mu([m]_{\mathrm{o}})}{\phi([m]_{\mathrm{o}})} F(2^{\operatorname{ord}_2(m)}, n) \sideset{}{^*}\sum_{\substack{\chi \,(\mathrm{mod}\, [m]_{\mathrm{o}}) \\ \chi^{2k} = \chi^0}} \chi(n),$$

the $*$ means that the summation is over the primitive characters modulo $[m]_{\mathrm{o}}$, $F(2^{\operatorname{ord}_2(m)}, n)$ is given by (2.13) *below*,

$$J(n) = \sum_{\substack{m \le X \\ s \le 4\alpha^2 m \\ s - 4m = n}} \frac{1}{2k} s^{1/2k - 1}$$

and $E(n)$ satisfies

$$\sum_{-n \le 4X} |E(n)|^2 \ll \frac{X^{1+1/k}}{(\log X)^{20}}. \tag{2.3}$$

In the following, we can suppose $X(\log X)^{-2^{k+2}} < -n \le 4X$, since it follows from considering the ranges for p and r that $R(n)$ is trivially bounded by the error term $O(X^{1/2k}(\log X)^{-3})$ in (2.2) when $-n \le X(\log X)^{-2^{k+2}}$.

Let $g = 1 + (\log X)^{-5}$. To remove the dependence of r on p, we split the range of p into subintervals $(Xg^{-(l+1)}, Xg^{-l}]$, $l = 0, 1, \dots, L$, where

$$L = \left[\frac{\log(4X/-n)}{\log g}\right] \ll (\log X)^5 \log\log X.$$

Then we have

$$R(n) = \sum_{l=0}^{L} R_l(n), \quad \text{where} \quad R_l(n) = \sum_{\substack{Xg^{-(l+1)} < p \le Xg^{-l} \\ r \le (2\alpha\sqrt{p})^{1/k} \\ r^{2k} - 4p = n}} \log p. \tag{2.4}$$

Let

$$R_l^*(n) = \sum_{\substack{Xg^{-(l+1)} < p \le Xg^{-l} \\ r \le (2\alpha\sqrt{Xg^{-l}})^{1/k} \\ r^{2k} - 4p = n}} \log p.$$

Then it is clear that

$$\begin{aligned} 0 &\le R_l^*(n) - R_l(n) \\ &\le \sum_{\substack{Xg^{-(l+1)} < p \le Xg^{-l} \\ (2\alpha\sqrt{p})^{1/k} < r \le (2\alpha\sqrt{Xg^{-l}})^{1/k} \\ r^{2k} - 4p = n}} \log p \ll \log X + \left(\frac{X}{g^l}\right)^{1/2k} (\log X)^{-4}. \end{aligned}$$

Note that, from the ranges of p and r in the above sum (and from the fact that $\alpha < 1$), it follows that there are at most $O_\alpha(1)$ values of l such that $R_l^*(n) - R_l(n)$ is non-zero, thus we have

$$R(n) = \sum_{l=0}^{L} R_l^*(n) + O(X^{1/2k}(\log X)^{-3}). \tag{2.5}$$

For a real number β, let

$$s_l(\beta) = \sum_{Xg^{-(l+1)} < p \le Xg^{-l}} e(p\beta)\log p, \qquad t_l(\beta) = \sum_{r \le (2\alpha\sqrt{Xg^{-l}})^{1/k}} e(r^{2k}\beta).$$

We first note that

$$R_l^*(n) = \int_{PX^{-1}}^{1+PX^{-1}} t_l(\beta) s_l(-4\beta) e(-n\beta)\, d\beta.$$

We divide the unit interval $[PX^{-1}, 1+PX^{-1}]$ into two parts: the major arcs

$$\mathfrak{M} = \bigcup_{q \le P} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a), \quad \text{where} \quad \mathfrak{M}(q,a) = \{\beta : |\beta - a/q| \le PX^{-1}\},$$

and the minor arcs $\mathfrak{m} = [PX^{-1}, 1 + PX^{-1}] \setminus \mathfrak{M}$. It is clear that, for our choice of P, the $\mathfrak{M}(q,a)$'s are disjoint.

Note that for $l \le L$, we have $X(\log X)^{-2^{k+2}} \ll Xg^{-(l+1)} \ll Xg^{-l} \ll X$. Thus from [11] (Lemma 3.1), we see that there exists a positive constant C such that whenever $1 \le a \le q \le P$, $(a,q) = 1$, $\beta \in \mathfrak{M}(q,a)$, we have

$$s_l(-4\beta) = \frac{\mu(q/(4,q))}{\phi(q/(4,q))}\, u_l(-4(\beta - a/q)) + O(X \exp(-C\sqrt{\log X})), \tag{2.6}$$

where

$$u_l(\lambda) = \sum_{Xg^{-(l+1)} < m \le Xg^{-l}} e(m\lambda).$$

For $\beta \in \mathfrak{M}(q,a)$, from Theorem 4.1 of [11], we trivially have

$$t_l(\beta) = q^{-1} S_{2k}(q,a) v_l(\beta - a/q) + O(P^{2/3}), \tag{2.7}$$

where

$$S_{2k}(q,a) = \sum_{m=1}^{q} e(am^{2k}/q), \qquad v_l(\lambda) = \sum_{s \le 4\alpha^2 X/g^l} \frac{1}{2k}\, s^{1/2k-1} e(s\lambda).$$

From [11, Lemma 2.8] we have

$$u_l(\lambda) \ll \min\{Xg^{-l}, \|\lambda\|^{-1}\}, \qquad v_l(\lambda) \ll \min\{(Xg^{-l})^{1/2k}, \|\lambda\|^{-1/2k}\}. \tag{2.8}$$

Thus from (2.6)–(2.8), we get

$$\begin{aligned} R_l^*(n) = {} & \sum_{q \le P} \frac{\mu(q/(4,q))}{q\phi(q/(4,q))} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S_{2k}(q,a) e(-an/q) \\ & \times \int_{-P/X}^{P/X} u_l(-4\lambda) v_l(\lambda) e(-n\lambda)\, d\lambda + E_l(n) \\ & + O\bigg(X^{1/2k} \exp\bigg(\frac{-C}{2} \sqrt{\log X} \bigg) \bigg), \end{aligned} \tag{2.9}$$

where

$$E_l(n) = \int_{\mathfrak{m}} s_l(-4\beta) t_l(\beta) e(-n\beta)\, d\beta.$$

Let

$$\begin{aligned} \mathfrak{S}(n,P) &= \sum_{q \le P} F(q,n), \quad \text{where} \\ F(q,n) &= \frac{\mu(q/(4,q))}{q\phi(q/(4,q))} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S_{2k}(q,a) e(-an/q). \end{aligned} \tag{2.10}$$

We note that $F(q,n)$ is multiplicative. (While it is well known that $F(q,n)$ is multiplicative if the $(4,q)$ is not present, it is straightforward to check that the presence of $(4,q)$ does not affect the multiplicativity.)

For an odd prime p, we see that $F(p^h,n)=0$ if $p\,|\,n$ or $h\geq 2$. If $p\nmid 2n$, we have

$$F(p,n)=\frac{-1}{p(p-1)}\sum_{a=1}^{p-1}e(-an/p)\sum_{m=1}^{p}e(am^{2k}/p) \tag{2.11}$$
$$=\frac{-1}{p(p-1)}\Big[p\Big(\sum_{\substack{m=1\\ m^{2k}\equiv n\,(\mathrm{mod}\,p)}}^{p}1\Big)-p\Big]=\frac{-1}{p-1}\sum_{\substack{\chi\,(\mathrm{mod}\,p)\\ \chi^{2k}=\chi^0\\ \chi\neq\chi^0}}\chi(n).$$

Thus

$$F(q,n)=F(2^{\mathrm{ord}_2(q)},n)\,\frac{\mu([q]_{\mathrm{o}})}{\phi([q]_{\mathrm{o}})}\sideset{}{^*}\sum_{\substack{\chi\,(\mathrm{mod}\,[q]_{\mathrm{o}})\\ \chi^{2k}=\chi^0}}\chi(n). \tag{2.12}$$

It is easy to check that

$$F(2^h,n)=\begin{cases}0 & \text{if } h=1 \text{ or } h\geq 4,\\ 1 & \text{if } h=0 \text{ or } h=2,\\ -2\chi_n(2) & \text{if } h=3 \text{ and } n\equiv 1\ (\mathrm{mod}\,4),\\ 0 & \text{if } h=3,\ k=1 \text{ and } n\equiv 0\ (\mathrm{mod}\,4),\\ -2 & \text{if } h=3,\ k>1 \text{ and } n\equiv 0\ (\mathrm{mod}\,4).\end{cases} \tag{2.13}$$

From the estimates (2.8), we now have

$$\Big(\int_{-1/2}^{-P/X}+\int_{P/X}^{1/2}\Big)u_l(-4\lambda)v_l(\lambda)e(-n\lambda)\,d\lambda\ll\int_{P/X}^{1/2}\lambda^{-1-1/2k}\,d\lambda\ll\Big(\frac{X}{P}\Big)^{1/2k}.$$

From this and (2.9), and the fact that $\mathfrak{S}(n,P)\ll(\log X)^{k-1}$, we have

$$R_l^*(n)=\mathfrak{S}(n,P)\int_{-1/2}^{1/2}u_l(-4\lambda)v_l(\lambda)e(-n\lambda)\,d\lambda+E_l(n) \tag{2.14}$$
$$+O(X^{1/2k}(\log X)^{k-1}P^{-1/2k}),$$

where it is clear that $X^{1/2k}(\log X)^{k-1}P^{-1/2k}\ll X^{1/2k}(\log X)^{-16}$.

Let

$$J_l^*(n)=\int_{-1/2}^{1/2}u_l(-4\lambda)v_l(\lambda)e(-n\lambda)\,d\lambda.$$

Then it is obvious that

$$J_l^*(n) = \sum_{\substack{Xg^{-(l+1)}<m\le Xg^{-l}\\ s\le 4\alpha^2 Xg^{-l}\\ s-4m=n}} \frac{1}{2k}\, s^{1/2k-1}.$$

Similar to (2.5), we have

$$\sum_{l=0}^{L} J_l^*(n) = J(n) + O(X^{1/2k}(\log X)^{-4}).$$

Let

$$E(n) = \sum_{l=0}^{L} E_l(n);$$

then we have proved (2.2). To prove (2.3), we first recall $L \le (\log X)^6$ and observe that

$$\sum_n |E(n)|^2 \ll (\log X)^{12} \max_{0\le l\le L} \sum_{-n\le 4X} |E_l(n)|^2. \tag{2.15}$$

By Bessel's inequality, we have

$$\sum_{-n\le 4X} |E_l(n)|^2 \ll \int_{\mathfrak{m}} |s_l(4\beta)t_l(\beta)|^2\, d\beta. \tag{2.16}$$

By Weyl's inequality, we have

$$t_l(\beta) \ll X^{1/2k}P^{-2^{1-2k}} \log X \ll X^{1/2k}(\log X)^{-15}, \qquad \beta \in \mathfrak{m}.$$

Thus

$$\begin{aligned}\int_{\mathfrak{m}} |s_l(4\beta)t_l(\beta)|^2\, d\beta &\ll X^{1/k}(\log X)^{-30}\int_0^1 |s_l(\beta)|^2\, d\beta\\ &\ll X^{1/k}(\log X)^{-28}\left(\frac{X}{g^l} - \frac{X}{g^{l+1}}\right) \ll \frac{X^{1+1/k}}{(\log X)^{33}},\end{aligned}$$

which, along with (2.15) and (2.16), implies (2.3).

3. A weighted sum. In this section we derive an estimate for a weighted sum of special values of truncated Dirichlet L-functions. More precisely, letting $L_0(d) = \sum_{n\le X^{2/3}} \chi_d(n)/n$ and

$$K_0(X) = \frac{1}{2\pi}\sum_{p\le X} \log p \sum_{0<r\le (2\alpha\sqrt{p})^{1/k}} \sum_{\substack{r^{2k}-4p=df^2\\ f\le(\log X)^2\\ d\equiv 0,1 \,(\mathrm{mod}\, 4)}} \sqrt{|d|}\, L_0(d), \tag{3.1}$$

we prove

THEOREM 4. *We have*

$$K_0(X) = \left(\frac{2k}{3k+1}\, c_k(\alpha) + O((\log X)^{-2})\right) X^{3/2+1/2k}. \tag{3.2}$$

From Theorem 3, we deduce

$$K_0(X) = \frac{1}{2\pi} \sum_{\substack{f \le (\log X)^2 \\ 0 < -df^2 \le 4X \\ d \equiv 0,1 \,(\mathrm{mod}\, 4)}} \sqrt{|d|}\, L_0(d)(\mathfrak{S}(df^2, P) J(df^2) + E(df^2) + O(X^{1/2k}(\log X)^{-3})). \tag{3.3}$$

Next, we note that

$$\begin{aligned} \sum_{f,d} \sqrt{|d|}\, |L_0(d) E(df^2)| &\ll \log X \sqrt{\sum_{-n \le 4X} |n| \tau^2(|n|)} \sqrt{\sum_{-n \le 4X} |E(n)|^2} \\ &\ll X (\log X)^{5/2} \left(\frac{X^{1+1/k}}{(\log X)^{20}}\right)^{1/2} \\ &\ll \frac{X^{3/2+1/2k}}{(\log X)^7}, \end{aligned} \tag{3.4}$$

and the contribution of $O(X^{1/2k}(\log X)^{-3})$ to (3.3) is $O(X^{3/2+1/2k}(\log X)^{-2})$. Thus, we have

$$K_0(X) = \frac{1}{2\pi} \sum_{\substack{f \le (\log X)^2 \\ 0 < -df^2 \le 4X \\ d \equiv 0,1 \,(\mathrm{mod}\, 4)}} \sqrt{|d|}\, L_0(d) \mathfrak{S}(df^2, P) J(df^2) + O(X^{3/2+1/2k}(\log X)^{-2}). \tag{3.5}$$

Now, if $-df^2 \le 4(1-\alpha^2)X$, then for each $s \le -\alpha^2 df^2/(1-\alpha^2)$ satisfying $s \equiv df^2 \pmod 4$ we have a unique $m = (s - df^2)/4 \in [s/4\alpha^2, X]$. If $4(1-\alpha^2)X < -df^2 \le 4X$, then each $s \le 4X + df^2$ congruent to df^2 modulo 4 gives a unique $m = (s - df^2)/4 \in [s/4\alpha^2, X]$. Note that for any $N > 0$, $h \in \mathbb{Z}$, we have

$$\sum_{\substack{s \le N \\ s \equiv h \,(\mathrm{mod}\, 4)}} \frac{1}{2k}\, s^{1/2k-1} = \frac{1}{8k} \sum_{s \le N} s^{1/2k-1} + O(1) = \frac{1}{4}\, N^{1/2k} + O(1).$$

Thus,

$$J(df^2) = \begin{cases} \dfrac{1}{4}\left(\dfrac{-\alpha^2 df^2}{1-\alpha^2}\right)^{1/2k} + O(1) & \text{if } -df^2 \le 4(1-\alpha^2)X, \\ \dfrac{1}{4}(4X + df^2)^{1/2k} + O(1) & \text{if } 4(1-\alpha^2)X < -df^2 \le 4X. \end{cases} \tag{3.6}$$

Let

$$K_0^a(X) = \frac{1}{8\pi}\left(\frac{\alpha^2}{1-\alpha^2}\right)^{1/2k} \sum_{\substack{f\le(\log X)^2\\ 0<-df^2\le 4(1-\alpha^2)X\\ d\equiv 0,1 \,(\mathrm{mod}\, 4)}} |d|^{1/2+1/2k} f^{1/k}$$
$$\times \sum_{n\le X^{2/3}} \frac{\chi_d(n)}{n} \sum_{2^j m\le P} \frac{\mu(m)}{\phi(m)} F(2^j, df^2) \sideset{}{^*}\sum_{\substack{\chi \,(\mathrm{mod}\, m)\\ \chi^{2k}=\chi^0}} \chi(df^2),$$

$$K_0^b(X) = \frac{1}{8\pi} \sum_{\substack{f\le(\log X)^2\\ 4(1-\alpha^2)X<-df^2\le 4X\\ d\equiv 0,1 \,(\mathrm{mod}\, 4)}} \sqrt{|d|}\,(4X+df^2)^{1/2k}$$
$$\times \sum_{n\le X^{2/3}} \frac{\chi_d(n)}{n} \sum_{2^j m\le P} \frac{\mu(m)}{\phi(m)} F(2^j, df^2) \sideset{}{^*}\sum_{\substack{\chi \,(\mathrm{mod}\, m)\\ \chi^{2k}=\chi^0}} \chi(df^2),$$

where in both expressions, the second to last summation is subject to m being odd, $j = 0, 2, 3$ and $F(2^j, df^2)$ being given by (2.13). Then we have

$$K_0(X) = K_0^a(X) + K_0^b(X) + O(X^{3/2+1/2k}(\log X)^{-2}). \tag{3.7}$$

Note that

$$\frac{2^{1+1/k}k\alpha^{1/k}(1-\alpha^2)^{3/2}}{(3k+1)\pi} + \frac{2^{1/k}}{\pi}\int_0^{\alpha^2} t^{1/2k}\sqrt{1-t}\,dt$$
$$= \frac{2^{1+1/k}}{(3k+1)\pi}\int_0^{\alpha} t^{1/k-1}\sqrt{1-t^2}\,dt.$$

(Both sides are equal to 0 at $\alpha = 0$ and have the same derivatives with respect to α.) Then Theorem 4 follows from the following lemma.

Lemma 3.1. *We have*

$$K_0^a(X) = \left(\frac{1}{3} + \frac{2}{3}\,\delta(k)\right)\frac{2^{1+1/k}k\alpha^{1/k}(1-\alpha^2)^{3/2}}{(3k+1)\pi}\,X^{3/2+1/2k} + O\left(\frac{X^{3/2+1/2k}}{(\log X)^4}\right), \tag{3.8}$$

$$K_0^b(X) = \left(\frac{1}{3} + \frac{2}{3}\,\delta(k)\right)\frac{2^{1/k}X^{3/2+1/2k}}{\pi}\int_0^{\alpha^2} t^{1/2k}\sqrt{1-t}\,dt + O\left(\frac{X^{3/2+1/2k}}{(\log X)^4}\right). \tag{3.9}$$

Proof. The proofs of (3.8) and (3.9) are almost identical, so we only give a proof for (3.9). We first note that

$$K_0^b(X) = \frac{1}{8\pi} \sum_{j,f,m,n} \frac{\mu(m)}{n\phi(m)} \times \sideset{}{^*}\sum_{\substack{\chi \,(\mathrm{mod}\, m)\\ \chi^{2k}=\chi^0}} \sum_{\substack{4(1-\alpha^2)X/f^2 < -d \le 4X/f^2\\ d\equiv 0,1 \,(\mathrm{mod}\, 4)}} \sqrt{|d|}\,(4X+df^2)^{1/2k} \chi_d(n) F(2^j, df^2)\chi(df^2),$$

where the summation over j, f, m, n is also subject to $f \le (\log X)^2$, $2^j m \le P = (\log X)^{2^{2k+3}}$, $j = 0, 2, 3$, $n \le X^{2/3}$.

We split the sum into two parts: K_0^{be} subject to $d \equiv 0 \pmod 4$ and K_0^{bo} subject to $d \equiv 1 \pmod 4$. Write $d = 4D$ in K_0^{be}; then

$$K_0^{\mathrm{be}} = \frac{2^{1/k}}{4\pi} \sum_{\substack{j,f,m,n\\ 2\nmid mn}} \frac{\mu(m)F(2^j,4)}{n\phi(m)} \times \sideset{}{^*}\sum_{\substack{\chi \,(\mathrm{mod}\, m)\\ \chi^{2k}=\chi^0}} \chi(4f^2) \sum_{(1-\alpha^2)X/f^2 < -D \le X/f^2} \sqrt{|D|}\,(X+Df^2)^{1/2k} \chi_D(n)\chi(D),$$

where we have replaced $F(2^j, 4Df^2)$ by $F(2^j, 4)$ in view of (2.13). If $\psi = \chi\big(\frac{\cdot}{n}\big) \ne \chi^0$, then from the Pólya–Vinogradov estimate, the innermost sum of K_0^{be} equals

$$\psi(-1) \int_{(1-\alpha^2)X/f^2}^{X/f^2} \sqrt{t}\,(X - f^2t)^{1/2k} \cdot \frac{d}{dt}\Big[\sum_{s\le t} \psi(s)\Big]\,dt \ll \frac{X^{1/2+1/2k}\sqrt{mn}\log(mn+1)}{f} \ll \frac{X^{5/6+1/2k}P}{f}. \tag{3.10}$$

It is then easy to see that the terms of K_0^{be} with $\chi\big(\frac{\cdot}{n}\big) \ne \chi^0$ contribute at most $O(X^{1+1/2k})$. Now, we notice that $\chi\big(\frac{\cdot}{n}\big) = \chi^0$ only when $\chi = \big(\frac{\cdot}{m}\big)$ (since $\chi \pmod m$ is primitive) and $n = mw^2$ for some $w \in \mathbb{N}$. Thus, we have

$$K_0^{\mathrm{be}} = \frac{2^{1/k}}{4\pi} \sum_{\substack{j,f,m,w\\ (m,f)=1\\ 2\nmid mw}} \frac{\mu(m)F(2^j,4)}{m\phi(m)w^2} \times \sum_{\substack{(1-\alpha^2)X/f^2 < -D \le X/f^2\\ (D,mw)=1}} \sqrt{|D|}\,(X+Df^2)^{1/2k} + O(X^{1+1/2k}), \tag{3.11}$$

where the summation over j, f, m, w is also subject to $f \le (\log X)^2$, $2^j m \le P = (\log X)^{2^{2k+3}}$, $j = 0, 2, 3$, and $w \le X^{1/3}/\sqrt{m}$. Note that the inner sum

equals

$$\int_{(1-\alpha^2)X/f^2}^{X/f^2} \sqrt{t}\,(X-f^2t)^{1/2k}\,d \sum_{\substack{u\le t\\(u,mw)=1}} 1 \tag{3.12}$$

$$= \int_{(1-\alpha^2)X/f^2}^{X/f^2} \sqrt{t}\,(X-f^2t)^{1/2k}\,d\Big\{\frac{\phi(mw)}{mw}\,t + O(mw)\Big\}$$

$$= \frac{\phi(mw)X^{3/2+1/2k}}{mwf^3}\int_0^{\alpha^2} t^{1/2k}\sqrt{1-t}\,dt + O\Big(\frac{mwX^{1/2+1/2k}}{f}\Big).$$

From this and (3.11), we have

$$K_0^{\mathrm{be}} = \Big(\frac{2^{1/k}X^{3/2+1/2k}}{4\pi}\int_0^{\alpha^2} t^{1/2k}\sqrt{1-t}\,dt\Big) \tag{3.13}$$

$$\times \sum_{\substack{j,f,m,w\\(m,f)=1\\2\nmid mw}} \frac{\mu(m)\phi(mw)F(2^j,4)}{m^2\phi(m)w^3f^3} + O(X^{1+1/2k}).$$

Now we note that the sum over j,f,m,w is equal to

$$\sum_{\substack{2^jm\le P\\2\nmid m}} \frac{\mu(m)F(2^j,4)}{m^2\phi(m)} \tag{3.14}$$

$$\times\Big(\sum_{\substack{f=1\\(f,m)=1}}^{\infty}\frac{1}{f^3} + O\Big(\frac{1}{(\log X)^4}\Big)\Big)\Big(\sum_{\substack{w=1\\2\nmid w}}^{\infty}\frac{\phi(mw)}{w^3} + O\Big(\frac{m^{3/2}}{X^{1/3}}\Big)\Big)$$

$$= \sum_{\substack{2^jm\le P\\2\nmid m}} \frac{\mu(m)F(2^j,4)}{m^2\phi(m)} \sum_{\substack{f=1\\(f,m)=1}}^{\infty}\frac{1}{f^3}\sum_{\substack{w=1\\2\nmid w}}^{\infty}\frac{\phi(mw)}{w^3} + O\Big(\frac{1}{(\log X)^4}\Big)$$

$$= \frac{16}{7}\,\delta(k) \sum_{\substack{f,m,w\\2\nmid mwf\\(f,m)=1}} \frac{\mu(m)\phi(mw)}{m^2\phi(m)w^3f^3} + O\Big(\frac{1}{(\log X)^4}\Big),$$

where in the last sum, the variables f,m,k range over the odd positive integers. Here we have factored out the powers of 2 in f, which yields the constant factor $1+2^{-3}+2^{-6}+\cdots = 8/7$, and it is easy to see that a factor $2\delta(k)$ arises from summing up $F(2^0,4)$, $F(2^2,4)$ and $F(2^3,4)$ according to (2.13).

LEMMA 3.2. *We have*

$$C := \sum_{\substack{f,m,w\\ 2\nmid mwf\\ (f,m)=1}} \frac{\mu(m)\phi(mw)}{m^2\phi(m)w^3f^3} = 1.$$

Proof. We first note that

$$\begin{aligned} C &= \sum_{\substack{m,w\\ 2\nmid mw}} \frac{\mu(m)\phi(mw)}{m^2\phi(m)w^3}\,\zeta(3)\prod_{l\mid 2m}\left(1-\frac{1}{l^3}\right)\\ &= \frac{7}{8}\,\zeta(3)\sum_{\substack{m,w\\ 2\nmid mw}} \frac{\mu(m)\phi(mw)}{m^2\phi(m)w^3}\sum_{v\mid m}\frac{\mu(v)}{v^3}\\ &= \frac{7}{8}\,\zeta(3)\sum_{\substack{K=1\\ 2\nmid K}}^{\infty}\frac{\phi(K)a(K)}{K^3}, \end{aligned}$$

where

$$a(K) = \sum_{m\mid K}\frac{\mu(m)m}{\phi(m)}\sum_{v\mid m}\frac{\mu(v)}{v^3},$$

which is obviously a multiplicative function. Note that, for a prime l, $a(l) = a(l^2) = a(l^3) = \cdots$. Thus

$$\begin{aligned} C &= \frac{7}{8}\,\zeta(3)\prod_{l>2}\left(1+a(l)\left(\frac{\phi(l)}{l^3}+\frac{\phi(l^2)}{l^6}+\cdots\right)\right)\\ &= \frac{7}{8}\,\zeta(3)\prod_{l>2}\left(1+\frac{a(l)}{l(l+1)}\right). \end{aligned} \tag{3.15}$$

It is easy to see that

$$a(l) = 1+\frac{-l}{l-1}\left(1-\frac{1}{l^3}\right) = -\frac{l+1}{l^2}.$$

Thus, from this and (3.15), we have

$$C = \frac{7}{8}\,\zeta(3)\prod_{l>2}\left(1-\frac{1}{l^3}\right) = 1,$$

which proves the lemma. ∎

From (3.13), (3.14) and Lemma 3.2, we have

$$K_0^{be} = \frac{2^{2+1/k}X^{3/2+1/2k}}{7\pi}\,\delta(k)\int_0^{\alpha^2} t^{1/2k}\sqrt{1-t}\,dt + O\left(\frac{X^{3/2+1/2k}}{(\log X)^4}\right). \tag{3.16}$$

Now we try to find an asymptotic formula for K_0^{bo}. We first note that

$$K_0^{bo} = \frac{1}{8\pi} \sum_{j,f,m,n} \frac{\mu(m)}{n\phi(m)} \sideset{}{^*}\sum_{\substack{\chi \,(\mathrm{mod}\, m) \\ \chi^{2k}=\chi^0}} \chi(f^2)$$
$$\times \sum_{\substack{4(1-\alpha^2)X/f^2 < -d \le 4X/f^2 \\ d \equiv 1 \,(\mathrm{mod}\, 4)}} \sqrt{|d|}\,(4X + df^2)^{1/2k} F(2^j, df^2)\chi_d(n)\chi(d).$$

We replace the restriction $d \equiv 1 \pmod 4$ by introducing a characteristic function $\frac{1}{2}(\chi_4(d) + \chi_{-4}(d))$.

When $j = 0$ or 2, we have $F(2^j, df^2) = 1$. We note that $\chi_{-4}(d)\chi_d(n)\chi(d)$ and, if $\chi\big(\frac{\cdot}{n}\big) \neq \chi^0$, $\chi_4(d)\chi_d(n)\chi(d)$ are both non-principal characters modulo $4mn$. Thus, with the same estimate as (3.10), we see that the total contribution from the terms containing $\chi_{-4}(d)$ and the terms containing $\chi_4(d)$ but with $\chi\big(\frac{\cdot}{n}\big) \neq \chi^0$ is $O(X^{1+1/2k})$. We remark that $\chi\big(\frac{\cdot}{n}\big) = \chi^0$ if and only if $\chi = \big(\frac{\cdot}{m}\big)$ and $n = mw^2$ for some $w \in \mathbb{N}$.

When $j = 3$ and f is odd, we have $F(2^j, df^2) = -2\big(\frac{2}{d}\big)$. Note that then

$$\frac{1}{2}\,(\chi_4(d) + \chi_{-4}(d))\chi_d(n)\chi(d)F(2^3, df^2) = -\left(\left(\frac{2}{d}\right) + \left(\frac{-2}{d}\right)\right)\chi(d)\left(\frac{d}{n}\right). \tag{3.17}$$

While the terms associated with non-principal characters contribute at most $O(X^{1+1/2k})$ from the Pólya–Vinogradov estimate, the only possible principal characters arise from $\chi = \big(\frac{\cdot}{m}\big)$. When $\chi = \big(\frac{\cdot}{m}\big)$, apart from the factor -1, (3.17) is the sum of two non-principal characters modulo $8mn$ if mn is not twice a square. These terms again give a contribution $O(X^{1+1/2k})$ to K_0^{bo} with the same estimate as (3.10). When $n = 2mw^2$ for some integer w, (3.17) is simply equal to $-(1 + \chi_{-4}(d))$. The terms containing $\chi_{-4}(d)$ again contribute at most $O(X^{1+1/2k})$ to K_0^{bo}.

When $j = 3$ and f is even, we have $F(2^j, df^2) = -2(1 - \delta(k))$. Thus

$$\frac{1}{2}\,(\chi_4(d) + \chi_{-4}(d))\chi_d(n)\chi(d)F(2^3, df^2) = -(1-\delta(k))\left(\left(\frac{4}{d}\right) + \left(\frac{-4}{d}\right)\right)\chi(d)\left(\frac{d}{n}\right). \tag{3.18}$$

It is clear that the only principal character arises from $\chi = \big(\frac{\cdot}{m}\big)$ and $n = mw^2$ for some $w \in \mathbb{N}$, in which case the term in (3.18) contributing to the main term is equal to $-(1 - \delta(k))$.

From the above discussion, we have

$$K_0^{bo} = \frac{1}{16\pi} \sum_{\substack{j,f,m,w \\ j=0,2 \\ (m,2f)=1}} \frac{\mu(m)}{m\phi(m)w^2} \times \sum_{\substack{4(1-\alpha^2)X/f^2<-d\le 4X/f^2 \\ (d,2mw)=1}} \sqrt{|d|}\,(4X+df^2)^{1/2k} - \frac{1}{16\pi} \sum_{\substack{f,m,w \\ (m,f)=1 \\ 2\nmid mf}} \frac{\mu(m)}{m\phi(m)w^2} \sum_{\substack{4(1-\alpha^2)X/f^2<-d\le 4X/f^2 \\ (d,2mw)=1}} \sqrt{|d|}\,(4X+df^2)^{1/2k} - \frac{1-\delta(k)}{8\pi} \sum_{\substack{f,m,w \\ (m,2f)=1 \\ 2|f}} \frac{\mu(m)}{m\phi(m)w^2} \sum_{\substack{4(1-\alpha^2)X/f^2<-d\le 4X/f^2 \\ (d,2mw)=1}} \sqrt{|d|}\,(4X+df^2)^{1/2k} + O(X^{1+1/2k}), \tag{3.19}$$

where in the first sum the summation over f, m, w is also subject to $f \le (\log X)^2$, $2^j m \le P$ and $w \le X^{1/3}/\sqrt{2^j m}$, and in the second and the third sums the summation over f, m, w is also subject to $f \le (\log X)^2$, $m \le P/8$, $w \le X^{1/3}/\sqrt{2m}$ and $w \le X^{1/3}/\sqrt{m}$, respectively. Similar to (3.12), we see that the innermost sums of the three sums in (3.19) are equal to

$$\frac{2^{2+1/k}\phi(2mw)X^{3/2+1/2k}}{mwf^3} \int_0^{\alpha^2} t^{1/2k}\sqrt{1-t}\,dt + O\bigg(\frac{mwX^{1/2+1/2k}}{f}\bigg). \tag{3.20}$$

From (3.19) and (3.20), and by an argument similar to (3.14), we get

$$K_0^{bo} = \frac{2^{1/k}c^{bo}X^{3/2+1/2k}}{4\pi} \int_0^{\alpha^2} t^{1/2k}\sqrt{1-t}\,dt + O\bigg(\frac{X^{3/2+1/2k}}{(\log X)^4}\bigg), \tag{3.21}$$

where

$$c^{bo} = 2 \sum_{\substack{f,m,w=1 \\ (m,2f)=1}}^{\infty} \frac{\mu(m)\phi(2mw)}{m^2\phi(m)w^3f^3} - \sum_{\substack{f,m,w=1 \\ (m,f)=1 \\ 2\nmid mf}}^{\infty} \frac{\mu(m)\phi(2mw)}{m^2\phi(m)w^3f^3} - 2(1-\delta(k)) \sum_{\substack{f,m,w=1 \\ (m,2f)=1 \\ 2|f}}^{\infty} \frac{\mu(m)\phi(2mw)}{m^2\phi(m)w^3f^3}.$$

From Lemma 3.2, we see that

$$\sum_{\substack{f,m,w=1\\(m,2f)=1}}^{\infty} \frac{\mu(m)\phi(2mw)}{m^2\phi(m)w^3f^3}$$

$$= \frac{8}{7} \sum_{\substack{2\nmid mf\\(m,f)=1}} \frac{\mu(m)}{m^2\phi(m)f^3} \sum_{2\nmid h} \frac{\phi(mh)}{h^3} \left(1+\frac{2}{2^3}+\frac{4}{4^3}+\frac{8}{8^3}+\cdots\right) = \frac{32}{21}\,C = \frac{32}{21}.$$

Similarly,

$$\sum_{\substack{f,m,w=1\\(m,f)=1\\2\nmid mf}}^{\infty} \frac{\mu(m)\phi(2mw)}{m^2\phi(m)w^3f^3} = \frac{4}{3}, \qquad \sum_{\substack{f,m,w=1\\(m,2f)=1\\2\mid f}}^{\infty} \frac{\mu(m)\phi(2mw)}{m^2\phi(m)w^3f^3} = \frac{4}{21}.$$

Combining these with (3.21), we get

$$K_0^{bo} = \left(\frac{1}{3}+\frac{2}{21}\delta(k)\right)\frac{2^{1/k}X^{3/2+1/2k}}{\pi} \int_0^{\alpha^2} t^{1/2k}\sqrt{1-t}\,dt + O\left(\frac{X^{3/2+1/2k}}{(\log X)^4}\right). \tag{3.22}$$

Now, from (3.16) and (3.22), we have proved (3.9).

4. Proof of Theorem 1. By Deuring's theorem (see [2], [7]), we know that for a given prime p and an integer $r \in (-2\sqrt{p}, 2\sqrt{p})$, the number $N(p,r)$ of elliptic curves $E(a,b): y^2 = x^3+ax+b$ with $a,b \in \mathbb{F}_p$ and $a_p(E(a,b)) = r$ is given by

$$N(p,r) = \frac{pH(r^2-4p)}{2} + O(p), \tag{4.1}$$

where $H(r^2-4p)$ denotes the Kronecker class number:

$$H(r^2-4p) = 2 \sum_{\substack{r^2-4p=df^2\\d\equiv 0,1 \pmod 4}} \frac{h(d)}{w(d)}. \tag{4.2}$$

Here $w(d)$ and $h(d)$ respectively denote the number of units and the class number of the order of discriminant d.

Proof of Theorem 1. Observe that changing the order of summation in $S_\alpha(U,V,A,B;\mathcal{K};X)$ and recalling (4.1), we deduce that

$$\begin{aligned} S_\alpha(U,V,A,B;\mathcal{K};X) &= \frac{1}{AB} \sum_{p\le X} \sum_{\substack{0<r\le 2\alpha\sqrt{p}\\ r\in\mathcal{K}}} \left(\frac{A}{p}+O(1)\right)\left(\frac{B}{p}+O(1)\right)N(p,r) \\ &= (1+O((\log X)^{-1}))M(X) + O(X^{1/2k}), \end{aligned} \tag{4.3}$$

where

$$M(X) = \frac{1}{2} \sum_{\substack{p \le X \\ 0 < r \le 2\alpha\sqrt{p} \\ r \in \mathcal{K}}} \frac{H(r^2 - 4p)}{p}. \tag{4.4}$$

Theorem 1 now follows from our next result.

THEOREM 5. *For fixed $0 < \alpha < 1$ and sufficiently large X, we have*

$$M(X) \sim c_k(\alpha)\pi_k(X).$$

Proof. Using (4.2), we have

$$M(X) = \sum_{p \le X} \frac{1}{p} \sum_{0 < r \le (2\alpha\sqrt{p})^{1/k}} \sum_{\substack{r^{2k} - 4p = df^2 \\ d \equiv 0,1 \pmod 4}} \frac{h(d)}{w(d)}. \tag{4.5}$$

We note that in the sum we have $d < 0$, thus using Dirichlet's class number formula and well known estimates on L-functions, we get

$$\frac{h(d)}{w(d)} = \frac{\sqrt{|d|}}{2\pi} L(1, \chi_d) \ll \sqrt{|d|} \log(|d| + 1), \tag{4.6}$$

where χ_d is the Kronecker symbol. We see that the terms in the sum of (4.5) subject to $f > (\log X)^2$ contribute at most

$$\begin{aligned} &\ll \sum_{p \le X} \frac{1}{p} \sum_{r \le (2\alpha\sqrt{p})^{1/k}} \sum_{\substack{r^{2k} - 4p = df^2 \\ f > (\log X)^2}} \frac{\sqrt{p} \log p}{f} \\ &\ll \log X \sum_{(\log X)^2 < f \le 2\sqrt{X}} \frac{1}{f} \sum_{r \le (2\alpha\sqrt{X})^{1/k}} \sum_{\substack{r^{2k}/4 < p \le X \\ 4p \equiv r^2 \pmod{f^2}}} \frac{1}{\sqrt{p}} \\ &\ll \log X \sum_{(\log X)^2 < f \le 2\sqrt{X}} \frac{1}{f} \sum_{r \le (2\alpha\sqrt{X})^{1/k}} \left(\frac{\sqrt{X}}{f^2} + \frac{1}{r^{2k}} \right) \ll \frac{X^{1/2+1/2k}}{(\log X)^3}. \end{aligned} \tag{4.7}$$

This, together with (4.5), gives

$$M(X) = \sum_{p \le X} \frac{1}{p} \sum_{0 < r \le (2\alpha\sqrt{p})^{1/k}} \sum_{\substack{r^{2k} - 4p = df^2 \\ f \le (\log X)^2 \\ d \equiv 0,1 \pmod 4}} \frac{h(d)}{w(d)} + O\left(\frac{X^{1/2+1/2k}}{(\log X)^3} \right). \tag{4.8}$$

Since χ_d is non-principal, from the Pólya–Vinogradov theorem, we have

$$\begin{aligned} L(1, \chi_d) &= \sum_{n \le X^{2/3}} \frac{\chi_d(n)}{n} + O\left(\frac{\sqrt{|d|} \log |d|}{X^{2/3}} \right) \\ &= L_0(d) + O(|d|^{1/2} X^{-2/3} \log X), \quad \text{say.} \end{aligned} \tag{4.9}$$

Combining (4.6), (4.8) and (4.9), we get

$$M(X) = M_0(X) + O\left(\frac{X^{1/2+1/2k}}{(\log X)^3}\right), \tag{4.10}$$

where

$$M_0(X) = \frac{1}{2\pi}\sum_{p\le X}\frac{1}{p}\sum_{r\le(2\alpha\sqrt{p})^{1/k}}\sum_{\substack{r^{2k}-4p=df^2\\ f\le(\log X)^2\\ d\equiv 0,1 \pmod 4}}\sqrt{|d|}\,L_0(d). \tag{4.11}$$

Using Theorem 4 and partial summation, we have

$$M_0(X) = \int_2^X \frac{1}{t\log t}\,dK_0(t) = c_k(\alpha)\pi_k(X) + O\left(\frac{X^{1/2+1/2k}}{(\log X)^3}\right).$$

Combining this with (4.10) proves Theorem 5.

5. Proof of Theorem 2. By Theorem 1, it is clear that Theorem 2 follows from

$$\begin{aligned} F_\alpha(U,V,A,B;\mathcal{K};X) &:= \frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\pi_{E(a,b)}(\alpha;\mathcal{K};X)^2 \\ &= (1+o(1))(c_k(\alpha)\pi_k(X))^2. \end{aligned} \tag{5.1}$$

Note that the left side of (5.1) is equal to

$$\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p,q\le X\\ a_{E(a,b)}(p)\le 2\alpha\sqrt{p}\\ a_{E(a,b)}(q)\le 2\alpha\sqrt{q}\\ a_{E(a,b)}(p),a_{E(a,b)}(q)\in\mathcal{K}}} 1. \tag{5.2}$$

From Theorem 1, the terms with $p=q$ in (5.2) contribute $O(\pi_k(X))$. Thus we have

$$\begin{aligned} &F_\alpha(U,V,A,B;\mathcal{K};X) \\ &\quad = \frac{1}{AB}\sum_{p\ne q\le X}\sum_{\substack{r\le(2\alpha\sqrt{p})^{1/k}\\ s\le(2\alpha\sqrt{q})^{1/k}}}\sum_{\substack{U<a\le U+A\\ V<b\le V+B\\ a_{E(a,b)}(p)=r^k\\ a_{E(a,b)}(q)=s^k}} 1 + O(\pi_k(X)). \end{aligned} \tag{5.3}$$

From the Chinese Remainder Theorem, the inner sum of (5.3) is equal to

$$\left(\frac{A}{pq}+O(1)\right)\left(\frac{B}{pq}+O(1)\right)N(p,r^k)N(q,s^k). \tag{5.4}$$

When $A, B > (X \log X)^2$, the main term $ABN(p, r^k)N(q, s^k)/p^2q^2$ in (5.4) dominates the error term by at least a factor $(\log X)^2$. Thus, from (5.3) and (5.4), we have

$$
\begin{aligned}
(5.5)\quad & F_\alpha(U, V, A, B; \mathcal{K}; X) \\
&= \left(1 + O\left(\frac{1}{(\log X)^2}\right)\right) \sum_{p \neq q \le X} \sum_{\substack{r \le (2\alpha\sqrt{p})^{1/k} \\ s \le (2\alpha\sqrt{q})^{1/k}}} \frac{N(p, r^k)}{p^2} \frac{N(q, s^k)}{q^2} + O(\pi_k(X)) \\
&= \frac{1}{4}\left(1 + O\left(\frac{1}{(\log X)^2}\right)\right) \sum_{p \neq q \le X} \sum_{\substack{r \le (2\alpha\sqrt{p})^{1/k} \\ s \le (2\alpha\sqrt{q})^{1/k}}} \frac{H(r^{2k} - 4p)}{p} \frac{H(s^{2k} - 4q)}{q} \\
&\quad + O(\pi_k(X)) \\
&= \left(1 + O\left(\frac{1}{(\log X)^2}\right)\right) M(X)^2 + O(\pi_k(X)).
\end{aligned}
$$

Theorem 2 then follows from Theorem 5.

6. Further remarks. Following the work of Fouvry and Murty [4], David and Pappalardi [3] have considered average Frobenius distributions of elliptic curves. More precisely, they showed

THEOREM 6. *Let r be an odd integer, $A, B \ge 1$. Let*

$$
\pi_E^r(X) := \#\{p \le X : a_E(p) = r\}, \qquad \pi_{1/2}(X) = \int_2^X \frac{dt}{2\sqrt{t}\log t} \sim \frac{\sqrt{X}}{\log X}.
$$

For every $c > 0$, we have

$$
\begin{aligned}
(6.1)\quad & \frac{1}{4AB} \sum_{\substack{|a| \le A \\ |b| \le B}} \pi^r_{E(a,b)}(X) \\
&\qquad = C_r \pi_{1/2}(X) + O\left(\left(\frac{1}{A} + \frac{1}{B}\right) X^{3/2} + \frac{X^{5/2}}{AB} + \frac{\sqrt{X}}{(\log X)^c}\right)
\end{aligned}
$$

where

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

The O-constant depends on c and r.

Theorem 1 cannot be deduced from this since the result of Theorem 6 is not uniform in r. In fact, (6.1) does not hold for large r. It is quite easy to

show that, for $t \geq 1$, one has

$$\sum_{\substack{r \leq t \\ 2 \nmid r}} C_r = \frac{1}{\pi}\, t + O(1).$$

Let $\mathcal{S}$ be the set of all odd integers. If we assume that (6.1) is uniform, then for $0 < \alpha < 1$, by partial summation, we have

$$\text{avg. } \pi_E(\alpha, \mathcal{S}; X) \sim \sum_{\substack{r \leq 2\alpha\sqrt{X} \\ 2 \nmid r}} C_r(\pi_{1/2}(X) - \pi_{1/2}(r^2/(2\alpha)^2)) \sim \frac{1}{\pi}\, \alpha\pi(X).$$

This cannot be true because, following our argument, it is easy to derive that

$$\text{avg. } \pi_E(\alpha, \mathcal{S}; X) \sim \left(\frac{2}{3\pi} \int_0^{\alpha} \sqrt{1 - t^2}\, dt\right)\pi(X).$$

We would also like to point out that in Theorem 1, and in the main theorems of [1] and [3], the minimal ranges of A and B can be reduced a little by estimating some exponential sums. This is of independent interest but not our focus in this paper. So we have not done so.

The authors are very grateful to the anonymous referee for his/her careful reading of the manuscript and helpful suggestions.

References

[1] A. Akbary, C. David and R. Juricevic, *Average distributions and products of special values of L-series*, Acta Arith. 111 (2004), 239–268.

[2] 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.

[3] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Int. Math. Res. Not. 1999, no. 4, 165–183.

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

[5] M. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, I*, Math. Z. 1 (1918), 357–376.

[6] —, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, II*, ibid. 6 (1920), 11–51.

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

[8] A. P. Ogg, *A remark on the Sato–Tate Conjecture*, Invent. Math. 9 (1970), 198–200.

[9] F. Shahidi, *Symmetric power L-functions for* GL(2), in: Elliptic Curves and Related Topics, H. Kisilevsky and M. R. Murty (eds.), CRM Proc. Lecture Notes 4, Amer. Math. Soc., Providence, RI, 1994, 159–182.

[10] J. Tate, *Algebraic cycles and poles of zeta functions*, in: Arithmetical Algebraic Geometry, O. F. G. Schilling (ed.), Harper & Row, New York, 1965, 93–110.

[11] R. C. Vaughan, *The Hardy–Littlewood Method*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

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

Department of Mathematics
University of South Carolina
1523 Greene Street
Columbia, SC 29208, U.S.A.
E-mail: yu@math.sc.edu

Received on 12.8.2005
and in revised form on 28.4.2006 (5053)