Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height

William D. Banks
Department of Mathematics, University of Missouri
Columbia, MO 65211 USA
bbanks@math.missouri.edu

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

September 6, 2006

Abstract

We obtain asymptotic formulae for the number of primes $p \leqslant x$ for which the reduction modulo p of the elliptic curve

$$\mathbf{E}_{a,b} \ : \ Y^2 = X^3 + aX + b$$

satisfies certain "natural" properties, on average over integers a and b with $|a| \leqslant A$ and $|b| \leqslant B$, where A and B are small relative to x. Specifically, we investigate behavior with respect to the Sato–Tate conjecture, cyclicity, and divisibility of the number of points by a fixed integer m.

1 Introduction

1.1 Motivation

For integers a and b such that $4a^3 + 27b^2 \neq 0$, we denote by $\mathbf{E}_{a,b}$ the elliptic curve defined by the *affine Weierstraß equation*:

$$\mathbf{E}_{a,b} \ : \ Y^2 = X^3 + aX + b.$$

For a basic background on elliptic curves, we refer the reader to the book [36] by Silverman.

For a prime $p > 3$, we denote by $\mathbb{F}_p$ the finite field with p elements, which we identify with the set of integers $\{0, \pm 1, \ldots, \pm(p-1)/2\}$.

When $p \nmid 4a^3 + 27b^2$, the set $\mathbf{E}_{a,b}(\mathbb{F}_p)$ consisting of the $\mathbb{F}_p$-rational points of $\mathbf{E}_{a,b}$ together with a point at infinity forms an *abelian group* under an appropriate composition rule called *addition*, and the number of elements in the group $\mathbf{E}_{a,b}(\mathbb{F}_p)$ satisfies the *Hasse bound*:

$$\left|\#\mathbf{E}_{a,b}(\mathbb{F}_p) - p - 1\right| \leqslant 2\sqrt{p}$$

(see, for example, [36, Chapter V, Theorem 1.1]).

A well known conjecture in the theory of elliptic curves, known as the *Lang–Trotter conjecture* (see [27]), asserts that for any elliptic curve $\mathbf{E}_{a,b}$ and any fixed integer t, the number $\pi_{a,b}(t; x)$ of primes $p \leqslant x$ (with $p \nmid 4a^3 + 27b^2$) such that

$$\#\mathbf{E}_{a,b}(\mathbb{F}_p) = p + 1 - t$$

satisfies the asymptotic formula

$$\pi_{a,b}(t; x) \sim c_{a,b,t} \cdot \frac{\sqrt{x}}{\log x} \qquad (x \to \infty)$$

for some constant $c_{a,b,t}$ that depends only on a, b, and t, provided that $\mathbf{E}_{a,b}$ does not have *complex multiplication* (see [36, Section III.4]) or t is nonzero. The Lang–Trotter conjecture remains open, although some progress has been made (see the survey [32]).

Fouvry and Murty [17] have studied the problem of estimating $\pi_{a,b}(0; x)$ *on average* over integers a, b with $|a| \leqslant A$ and $|b| \leqslant B$, and they have shown (see [17, Theorem 6]) that the asymptotic formula

$$\frac{1}{4AB} \sum_{|a| \leqslant A} \sum_{|b| \leqslant B} \pi_{a,b}(0; x) \sim \frac{\pi}{3} \cdot \frac{\sqrt{x}}{\log x} \qquad (x \to \infty)$$

holds uniformly in the range

$$AB \geqslant x^{3/2+\varepsilon} \qquad \text{and} \qquad \min\{A, B\} \geqslant x^{1/2+\varepsilon}, \tag{1}$$

where $\varepsilon > 0$ is fixed. For the case $t \neq 0$, David and Pappalardi [14] have established the following asymptotic formula:

$$\frac{1}{4AB} \sum_{|a| \leqslant A} \sum_{|b| \leqslant B} \pi_{a,b}(t; x) \sim C_t \cdot \frac{\sqrt{x}}{\log x} \qquad (x \to \infty),$$

where

$$C_t = \frac{2}{\pi} \prod_{p \,|\, t} \left(1 - \frac{1}{p^2}\right)^{-1} \prod_{p \nmid t} \frac{p(p^2 - p - 1)}{(p-1)(p^2-1)}\,.$$

for a shorter range of A and B, and this result has been extended by Baier [2] to the full range (1). Other results along these lines have been obtained in [1, 5, 15, 19, 24, 25].

Here, we investigate the average behavior of the family of curves $\mathbf{E}_{a,b}$ with $|a| \leqslant A$ and $|b| \leqslant B$ with respect to other natural statistical properties of their reductions modulo p. Although these properties are expected to hold for individual curves, such results remain inaccessible.

1.2 Our Results

In the present paper, we study how the family of curves $\mathbf{E}_{a,b}$ with $|a| \leqslant A$ and $|b| \leqslant B$ behaves with respect to:

- the *Sato–Tate conjecture* about the distribution of the cardinalities $\#\mathbf{E}_{a,b}(\mathbb{F}_p)$ (see [26]);
- *cyclicity* of the group $\mathbf{E}_{a,b}(\mathbb{F}_p)$, a notion which essentially dates back to the work of Borosh, Moreno and Porta [7] and of Serre [35];
- *divisibility* of $\#\mathbf{E}_{a,b}(\mathbb{F}_p)$ by a given integer m.

Accordingly, for real $0 \leqslant \alpha < \beta \leqslant \pi$, we define the *Sato–Tate density*

$$\mu_{\mathtt{ST}}(\alpha, \beta) = \frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 \theta \, d\theta,$$

and we define $\psi_{a,b}(p) \in [0, \pi]$ via the identity

$$p + 1 - \#\mathbf{E}_{a,b}(\mathbb{F}_p) = 2\sqrt{p}\,\cos\psi_{a,b}(p).$$

For real $0 \leqslant \alpha < \beta \leqslant \pi$, we denote by $\Pi^{\mathtt{ST}}_{a,b}(\alpha, \beta; x)$ the number of primes $p \leqslant x$ (with $p \nmid 4a^3 + 27b^2$) for which $\alpha \leqslant \psi_{a,b}(p) \leqslant \beta$. The *Sato–Tate conjecture* asserts that if $\mathbf{E}_{a,b}$ does not have complex multiplication (see [36]), then the asymptotic formula

$$\Pi^{\mathtt{ST}}_{a,b}(\alpha, \beta; x) \sim \mu_{\mathtt{ST}}(\alpha, \beta) \cdot \frac{x}{\log x} \qquad (x \to \infty) \tag{2}$$

holds (see [6, 26, 33]).

It is well known that $\mathbf{E}_{a,b}(\mathbb{F}_p)$ is an abelian group of rank at most two. We denote by $\Pi^{\mathtt{C}}_{a,b}(x)$ the number of primes $p \leqslant x$ (with $p \nmid 4a^3 + 27b^2$) for which $\mathbf{E}_{a,b}(\mathbb{F}_p)$ is *cyclic*. The conjectured asymptotic formula

$$\Pi^{\mathtt{C}}_{a,b}(x) \sim C_{a,b} \cdot \frac{x}{\log x} \qquad (x \to \infty),$$

where $C_{a,b}$ is a constant that depends only on a and b, has been established conditionally (under the *Extended Riemann Hypothesis*) in some cases, and there are several unconditional lower bounds on $\Pi^{\mathtt{C}}_{a,b}(x)$; see the original papers [8, 9, 12, 13, 20, 31, 35] as well as the recent surveys [10, 32].

Finally, for a fixed integer $m \geqslant 1$, we denote by $\Pi^{\mathtt{D}}_{a,b}(m; x)$ the number of primes $p \leqslant x$ (with $p \nmid 4a^3 + 27b^2$) for which $m \mid \#\mathbf{E}_{a,b}(\mathbb{F}_p)$.

We remark that the *Chebotarev density theorem* can be used to study $\Pi^{\mathtt{D}}_{a,b}(m; x)$ for individual curves (see [10]); by averaging over a and b, we obtain sharper results which are also uniform in m up to any fixed power of $\log x$.

We also remark that Taylor [37] has recently announced a complete proof of the Sato–Tate conjecture, which implies (2) in particular. Nevertheless, this work on individual curves does not imply any results on average due to the lack of uniformity with respect to the coefficients a and b of the Weierstraß equation.

Here, we obtain an asymptotic formula for the number of pairs (a, b) with $|a| \leqslant A$, $|b| \leqslant B$ and $p \nmid 4a^3 + 27b^2$ such that $\mathbf{E}_{a,b}(\mathbb{F}_p)$ belongs to a certain sufficiently "massive" collection of isomorphism classes of elliptic

curves. Using this result, we derive an asymptotic formulae for the sums

$$N^{\mathtt{ST}}_{\alpha,\beta}(A,B;x) = \sum_{|a|\leqslant A}\sum_{|b|\leqslant B} \Pi^{\mathtt{ST}}_{a,b}(\alpha,\beta;x),$$
$$N^{\mathtt{C}}(A,B;x) = \sum_{|a|\leqslant A}\sum_{|b|\leqslant B} \Pi^{\mathtt{C}}_{a,b}(x),$$
$$N^{\mathtt{D}}_{m}(A,B;x) = \sum_{|a|\leqslant A}\sum_{|b|\leqslant B} \Pi^{\mathtt{D}}_{a,b}(m;x).$$

The main terms in our expansions of $N^{\mathtt{ST}}_{\alpha,\beta}(A,B;x)$, $N^{\mathtt{C}}(A,B;x)$ and $N^{\mathtt{D}}_{m}(A,B;x)$ are derived from asymptotic formulae of Birch [6], Vlăduţ [39] and Howe [21], respectively. The asymptotic formula of Birch [6] is not quite sufficient for our purposes, however, so we give an explicit bound for the error term, which is obtained using the method of Niederreiter [34].

In the case of the Sato–Tate distribution, the computation of the error term is almost trivial. The other cases require a more specialized treatment, which is done using now standard techniques; for example, we apply a result of Indlekofer, Wehmeier and Lucht [22].

In the last section, we give an outline of several other questions about reductions of elliptic curves that can be approached with our method.

1.3 Our Method

The functions $N^{\mathtt{ST}}_{\alpha,\beta}(A,B;x)$, $N^{\mathtt{C}}(A,B;x)$ and $N^{\mathtt{D}}_{m}(A,B;x)$ can also be studied using the method of Fouvry and Murty [17], which makes essential use of the *Weil bound*; see [29, Chapter 5]. Here, however, we obtain sharper results by applying bounds on multiplicative character sums rather than estimating exponential sums as in [17]. Using the *Polya–Vinogradov* and *Burgess bounds* (see [23, Theorems 12.5 and 12.6]) one already obtains stronger results for individual primes than with exponential sums. Moreover, the use of multiplicative character sums allows for additional savings on average over primes $p \leqslant x$. In the present paper, we use a result of Garaev [18] on multiplicative character sums, which is derived from a variant of the large sieve inequality (see [23, Section 7.4]).

We also use a modification of the method of [4], which is based on bounds for double exponential sums and dates back to the early works of Vinogradov; see [38, Exercise 14a, Chapter VI], for example.

As a result, we obtain nontrivial bounds in a region that is significantly wider than (1). In fact, our bounds are nontrivial whenever A and B satisfy the inequalities

$$x^{\varepsilon} \leqslant A, B \leqslant x^{1-\varepsilon} \qquad \text{and} \qquad AB \geqslant x^{1+\varepsilon}\sqrt{\min\{A, B\}}\,. \tag{3}$$

Since $\sqrt{\min\{A, B\}} \leqslant (AB)^{1/4}$, our bounds are nontrivial whenever

$$A, B \leqslant x^{1-\varepsilon} \qquad \text{and} \qquad AB \geqslant x^{4/3+\varepsilon}.$$

It is not difficult to obtain a version of our results without any upper bound restriction on $\max\{A, B\}$. This is not too surprising since the underlying problem is easier for larger values of A and B. We have not done this in the present paper, however, since this leads to more cluttered expressions for the error term, and the case of small A and B seems to be of the most interest.

One of the main ingredients of the method of Fouvry and Murty is the use of the Weil bound to prove the asymptotic formula $2AB/p + O(p^{1/2+o(1)})$ for the number of curves $\mathbf{E}_{a,b}$, with $|a| \leqslant A \leqslant (p-1)/2$ and $|b| \leqslant B \leqslant (p-1)/2$, that are isomorphic to a given curve $\mathbf{E}_{r,s}$; see [17, Section 7]. Here, we show that, on average over r and s, the error term can be improved substantially, and this suffices for the problems that we consider below. On the other hand, our method does not directly apply to the question considered in [17] since a set of elliptic curves over $\mathbb{F}_p$ with a prescribed number of $\mathbb{F}_p$-rational points (that is, a set of isogenous curves) is much "thinner" than the sets of curves that we consider. Of course, there is some possibility that both approaches might be combined to improve the threshold (1) for the original problem.

We remark that Baier and Zhao [3] have also studied the distribution of $N^{\mathsf{ST}}_{\alpha,\beta}(A, B; x)$ by a very different method. Their results are quite different from ours (but there is partial overlap) and in many cases are weaker with respect to the range of A and B as well as the uniformity in α and β. In particular, among other restrictions, the inequalities

$$A, B \geqslant x^{1/2+\varepsilon}$$

are required in [3, Theorem 1]. In some cases, however, the results of [3] are stronger than ours. It is worth mentioning that Baier and Zhao [3] have estimated the average deviation of $\Pi^{\mathsf{ST}}_{a,b}(\alpha, \beta; x)$ from the value predicted by the Sato–Tate conjecture.

1.4 Notation

Throughout the paper, any implied constants in symbols O and $\ll$ may occasionally depend, where obvious, on the real positive parameters ε and K but are absolute otherwise. We recall that the notations $U \ll V$ and $U = O(V)$ are both equivalent to the statement that $|U| \leqslant cV$ holds with some constant $c > 0$.

The letters p and q always denote prime numbers, while m and n always denote integer numbers.

As usual, we denote by $\pi(x)$ the number of primes $p \leqslant x$.

1.5 Acknowledgements

The authors would like to thank Nick Katz for several comments concerning the Sato–Tate conjecture and in particular for his suggestion of Lemma 6. This work began during a pleasant visit by W. B. to Macquarie University; the support and hospitality of this institution are gratefully acknowledged. During the preparation of this paper, I. S. was supported in part by ARC grant DP0556431.

2 Preliminaries

2.1 Exponential and character sums

For a prime p, we write $\mathbf{e}_p(u) = \exp(2\pi i u/p)$ for all $u \in \mathbb{F}_p$. Then,

$$p^{-1} \sum_{v \in \mathbb{F}_p} \mathbf{e}_p(uv) = \begin{cases} 1 & \text{if } u = 0; \\ 0 & \text{if } u \in \mathbb{F}_p^*. \end{cases} \tag{4}$$

The following statement is elementary and well known; see, for example, [38, Chapter III, Exercise 11c]:

Lemma 1. *Uniformly for all primes p and positive integers L, M, we have*

$$\sum_{v \in \mathbb{F}_p^*} \left| \sum_{n=L+1}^{L+M} \mathbf{e}_p(nv) \right| \ll p \log p.$$

The next result combines the Polya–Vinogradov bound (for $\nu = 1$) with the Burgess bounds (for $\nu \geqslant 2$); see [23, Theorems 12.5 and 12.6].

Lemma 2. *For all primes p, positive integers L, M, ν, and non-principal multiplicative characters χ modulo p, we have*

$$\left|\sum_{n=L+1}^{L+M} \chi(n)\right| \leqslant M^{1-1/\nu} p^{(\nu+1)/(4\nu^2)+o(1)} \qquad (p \to \infty),$$

where the function implied by $o(1)$ depends only on ν.

Finally, we use the following statement, which is contained in the more general result [18, Theorem 11] of Garaev (which also applies to character sums with composite moduli and allows significantly more flexibility in the choice of M):

Lemma 3. *Fix $\varepsilon > 0$ and $\eta \in (0, 1/4)$. If $x > 0$ is sufficiently large, then for all $M \geqslant x^{\varepsilon}$, all primes $p \leqslant x$ with at most $x^{4\eta+o(1)}$ exceptions, and all non-principal multiplicative characters χ modulo p, we have*

$$\left|\sum_{n=1}^{M} \chi(n)\right| \leqslant M^{1-\eta},$$

where the function implied by $o(1)$ depends only on ε and η.

2.2 Distribution of powers

Let $d_p = \gcd(p-1, 6)$ and put

$$\sigma_p(M) = \max_{\substack{\chi^{d_p}=\chi_0 \\ \chi \neq \chi_0}} \left\{1, \left|\sum_{n=1}^{M} \chi(n)\right|\right\}, \tag{5}$$

where the maximum is taken over all non-principal multiplicative characters χ modulo p such that χ^{d_p} is the principal character χ_0.

For any integers B, s we define

$$\mathcal{Z}_s(B, p) = \{u \in \mathbb{F}_p^* \ : \ su^6 \equiv b \pmod p \text{ where } |b| \leqslant B\}.$$

We have the following bound on the cardinality of $\mathcal{Z}_s(B; p)$:

Lemma 4. *For all primes p and positive integers B, s such that $p \nmid s$, we have*

$$\left|\#\mathcal{Z}_s(B; p) - 2B\right| \leqslant 11\, \sigma_p(B).$$

Proof. For all $n \in \mathbb{Z}$ we have

$$\#\{u \in \mathbb{F}_p^* \ : \ u^6 \equiv n \pmod p\} = \sum_{\chi^{d_p}=\chi_0} \chi(n),$$

where the sum is taken over all multiplicative characters χ modulo p such that $\chi^{d_p} = \chi_0$. If $\overline{s}$ is an integer such that $s\overline{s} \equiv 1 \pmod p$, it follows that

$$\#\mathcal{Z}_s(B;p) = \sum_{|b|\leqslant B} \sum_{\chi^{d_p}=\chi_0} \chi(b\overline{s}) = (2B+1) + \sum_{\substack{\chi^{d_p}=\chi_0 \\ \chi\neq\chi_0}} \overline{\chi}(s) \sum_{|b|\leqslant B} \chi(b).$$

Since each inner sum is bounded by

$$\left| \sum_{|b|\leqslant B} \chi(b) \right| \leqslant 2\,\sigma_p(B),$$

and

$$\#\{\chi \ : \ \chi^{d_p} = \chi_0,\ \chi \neq \chi_0\} = d_p - 1 \leqslant 5,$$

the result follows. □

For any integers A, B, r, s we define

$$\mathcal{Z}_{r,s}(A,B;p) = \{u \in \mathcal{Z}_s(B;p) \ : \ ru^4 \equiv a \pmod p \text{ where } |a| \leqslant A\}.$$

Lemma 5. *For all primes p and positive integers A, B, r, s such that $p \nmid rs$, we have*

$$\sum_{r\in\mathbb{F}_p} \left| \#\mathcal{Z}_{r,s}(A,B;p) - \frac{4AB}{p} \right| \ll A\,\sigma_p(B) + B^{1/2}p.$$

Proof. Using (4), it follows that

$$\begin{aligned}\#\mathcal{Z}_{r,s}(A,B;p) &= \sum_{u\in\mathcal{Z}_s(B;p)} \sum_{|a|\leqslant A} p^{-1} \sum_{v\in\mathbb{F}_p} \mathbf{e}_p\big((ru^4-a)v\big) \\ &= \frac{2A\cdot\#\mathcal{Z}_s(B;p)}{p} + O(1) + p^{-1} \sum_{v\in\mathbb{F}_p^*} \sum_{u\in\mathcal{Z}_s(B;p)} \mathbf{e}_p(ru^4v) \sum_{|a|\leqslant A} \mathbf{e}_p(-av).\end{aligned}$$

Therefore, by Lemma 4 we obtain the bound

$$\begin{aligned}\sum_{r\in\mathbb{F}_p}\left|\#\mathcal{Z}_{r,s}(A,B;p)-\frac{4AB}{p}\right| \\ \ll A\,\sigma_p(B)+p^{-1}\sum_{v\in\mathbb{F}_p^*}\sum_{r\in\mathbb{F}_p}\left|\sum_{u\in\mathcal{Z}_s(B;p)}\mathbf{e}_p(ru^4v)\right|\left|\sum_{|a|\leqslant A}\mathbf{e}_p(av)\right|.\end{aligned} \tag{6}$$

By the Cauchy inequality, we see that

$$\begin{aligned}\left(\sum_{r\in\mathbb{F}_p}\left|\sum_{u\in\mathcal{Z}_s(B;p)}\mathbf{e}_p(ru^4v)\right|\right)^2 &\leqslant p\sum_{r\in\mathbb{F}_p}\left|\sum_{u\in\mathcal{Z}_s(B;p)}\mathbf{e}_p(ru^4v)\right|^2\\ &= p\sum_{u_1,u_2\in\mathcal{Z}_s(B;p)}\sum_{r\in\mathbb{F}_p}\mathbf{e}_p(r(u_1^4-u_2^4)v)\\ &\leqslant 4p^2\cdot\#\mathcal{Z}_s(B;p).\end{aligned}$$

For the last inequality, we have used the fact that each inner sum over r vanishes unless $u_1^4\equiv u_2^4 \pmod p$ (since $v\in\mathbb{F}_p^*$), in which case the sum is equal to p, and for every $u_1\in\mathcal{Z}_s(B;p)$ there are at most four values of $u_2\in\mathcal{Z}_s(B;p)$ which satisfy this congruence.

Applying the previous bound to (6) along with Lemma 1, it follows that

$$\begin{aligned}\sum_{r\in\mathbb{F}_p}\left|\#\mathcal{Z}_{r,s}(A,B;p)-\frac{4AB}{p}\right| \\ \ll A\,\sigma_p(B)+\sqrt{\#\mathcal{Z}_s(B;p)}\sum_{v\in\mathbb{F}_p^*}\left|\sum_{|a|\leqslant A}\mathbf{e}_p(av)\right| \\ \ll A\,\sigma_p(B)+\sqrt{\#\mathcal{Z}_s(B;p)}\;p\log p.\end{aligned}$$

Since $\mathcal{Z}_s(B;p)\ll B$ (see Lemma 4), the result follows. □

2.3 Statistics of elliptic curves

It is well known that if $a,b,r,s\in\mathbb{F}_p$, then the two curves $\mathbf{E}_{a,b}$ and $\mathbf{E}_{r,s}$ are *isomorphic over* $\mathbb{F}_p$ if and only if $a=ru^4$ and $b=su^6$ for some $u\in\mathbb{F}_p^*$. In particular, each curve $\mathbf{E}_{a,b}$ with $a,b\in\mathbb{F}_p^*$ is isomorphic to $(p-1)/2$ elliptic

curves $\mathbf{E}_{r,s}$, and there are $2p + O(1)$ distinct isomorphism classes of elliptic curves over $\mathbb{F}_p$; see [28]. Thus, our results can be conveniently formulated in terms of counting functions for individual curves $\mathbf{E}_{a,b}$ rather than in terms of isomorphism classes of curves, as in the papers [6, 21, 39].

Let $\mathcal{T}_p(\alpha, \beta)$ be the set of set of pairs $(a, b) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ such that the inequalities $\alpha \leqslant \psi_{a,b}(p) \leqslant \beta$ hold. Thanks to Birch [6], one knows that

$$\#\mathcal{T}_p(\alpha, \beta) \sim \mu_{\mathtt{ST}}(\alpha, \beta)p^2 \qquad (p \to \infty),$$

however we require a stronger result. What is needed is a full analogue for the Sato–Tate density of the bound of Niederreiter [34] on the discrepancy in the distribution of values of (normalized) Kloosterman sums. Fortunately, such a result can be obtained using the same methods since all of the underlying tools, namely [34, Lemma 3] and [26, Theorem 13.5.3], apply to $\psi_{a,b}(p)$ as well as to values of Kloosterman sums. In particular, from [26, Theorem 13.5.3] it follows that

$$\left| \frac{1}{(q-1)^2} \sum_{\substack{a,b \in \mathbb{F}_p^* \\ 4a^3+27b^2 \neq 0}} \frac{\sin\left((n+1)\psi_{a,b}(p)\right)}{\sin\left(\psi_{a,b}(p)\right)} \right| = O(nq^{-1/2}) \qquad (n = 1, 2, \dots)$$

(see also the work of Fisher [16, Section 5]). Thus, as in [34], we have:

Lemma 6. *Uniformly for all primes p, we have*

$$\max_{0 \leqslant \alpha < \beta \leqslant \pi} \left| \#\mathcal{T}_p(\alpha, \beta) - \mu_{\mathtt{ST}}(\alpha, \beta)p^2 \right| \ll p^{7/4}.$$

Next, for any prime p we denote

$$\vartheta_p = \prod_{q \,|\, p-1} \left(1 - \frac{1}{q\left(q^2 - 1\right)}\right),$$

where the product is taken over all prime divisors q of $p - 1$.

Let $\mathcal{C}_p$ be the set of pairs $(a, b) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ such that $\mathbf{E}_{a,b}(\mathbb{F}_p)$ is cyclic. The cardinality of $\mathcal{C}_p$ has been estimated by Vlăduţ [39] as follows:

Lemma 7. *For all primes p, we have*

$$\left| \#\mathcal{C}_p - \vartheta_p p^2 \right| \leqslant p^{3/2 + o(1)} \qquad (p \to \infty).$$

Finally, for any integer k, let $\omega_k(m)$ denote the completely multiplicative function which is defined on prime powers q^j as follows:

$$\omega_k(q^j) = \begin{cases} \dfrac{1}{q^{j-1}(q-1)} & \text{if } k \not\equiv 1 \pmod{q^{\lceil j/2 \rceil}}; \\ \dfrac{q^{\lfloor j/2 \rfloor + 1} + q^{\lfloor j/2 \rfloor} - 1}{q^{j + \lfloor j/2 \rfloor - 1}(q^2-1)} & \text{if } k \equiv 1 \pmod{q^{\lceil j/2 \rceil}}. \end{cases} \tag{7}$$

For an integer m, let $\mathcal{D}_p(m)$ be the set of pairs $(a,b) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ such that $m \mid \#\mathbf{E}_{a,b}(\mathbb{F}_p)$. Then, by the result of Howe [21] we have the following asymptotic formula for $\#\mathcal{D}_p(m)$:

Lemma 8. *For all primes p and integers m, we have*

$$\left|\#\mathcal{D}_p(m) - \omega_p(m)p^2\right| \leqslant m^{1+o(1)}p^{3/2} \qquad (m \to \infty).$$

3 Main Results

3.1 Distribution of curves over finite fields

For an arbitrary subset $\mathcal{S} \subseteq \mathbb{F}_p \times \mathbb{F}_p$, we denote by $M_p(\mathcal{S}, A, B)$ the number of curves $\mathbf{E}_{a,b}$ such that $(a,b) \in \mathcal{S}$, $|a| \leqslant A$ and $|b| \leqslant B$. Here, we obtain an asymptotic formula for $M_p(\mathcal{S}, A, B)$.

Similar to (5), we now define $e_p = \gcd(p-1, 4)$ and put

$$\rho_p(M) = \max_{\substack{\chi^{e_p} = \chi_0 \\ \chi \neq \chi_0}} \left\{1, \left|\sum_{n=1}^{M} \chi(n)\right|\right\},$$

where the maximum is taken over all non-principal multiplicative characters χ modulo p such that χ^{e_p} is the principal character χ_0. We also denote

$$\mathcal{E}(A, B; p) = \min\left\{A\,\sigma_p(B) + B^{1/2}p,\ B\,\rho_p(A) + A^{1/2}p\right\}.$$

Theorem 9. *For all primes $p > 3$, integers $1 \leqslant A, B \leqslant (p-1)/2$, and subsets $\mathcal{S} \subseteq \mathbb{F}_p \times \mathbb{F}_p$ such that whenever $(r,s) \in \mathcal{S}$ and $\mathbf{E}_{a,b}(\mathbb{F}_p) \cong \mathbf{E}_{r,s}(\mathbb{F}_p)$ one has $(a,b) \in \mathcal{S}$, the following bound holds uniformly:*

$$\left|M_p(\mathcal{S}, A, B) - \frac{4AB}{p^2}\,\#\mathcal{S}\right| \ll \mathcal{E}(A, B; p).$$

Proof. It follows from the properties of isomorphic curves given in Section 2.3 that

$$M_p(\mathcal{S}, A, B) = \frac{1}{p-1} \sum_{(r,s)\in\mathcal{S}} \#\mathcal{Z}_{r,s}(A, B; p) + O(A + B),$$

where we have estimated the contribution from curves with $ab = 0$ trivially as $O(A + B)$; note that if $a = ru^4$ and $b = su^6$ then the same relations also hold with $-u$ instead of u, so each group $\mathbf{E}_{a,b}(\mathbb{F}_p)$ with $|a| \leqslant A$ and $|b| \leqslant B$ is counted exactly $p - 1$ times in the sum on the right-hand side. Next, we apply Lemma 5, which yields the estimate

$$M_p(\mathcal{S}, A, B) = \frac{4AB}{p(p-1)} \#\mathcal{S} + O\left(A\,\sigma_p(B) + B^{1/2}p\right).$$

Therefore,

$$\left| M_p(\mathcal{S}, A, B) - \frac{4AB}{p^2} \#\mathcal{S} \right| \ll A\,\sigma_p(B) + B^{1/2}p + ABp^{-1}.$$

Since $B^{1/2}p \geqslant ABp^{-1}$, the last term can be dropped, and we have

$$\left| M_p(\mathcal{S}, A, B) - \frac{4AB}{p^2} \#\mathcal{S} \right| \ll A\,\sigma_p(B) + B^{1/2}p.$$

Examining our arguments closely, in particular those of Section 2, we see that the roles of A and B are fully interchangeable, hence we also have

$$\left| M_p(\mathcal{S}, A, B) - \frac{4AB}{p^2} \#\mathcal{S} \right| \ll B\,\rho_p(A) + A^{1/2}p,$$

which concludes the proof. □

Combining Theorem 9 with Lemma 2 we obtain

Corollary 10. *Under the hypotheses of Theorem 9, the bound*

$$\left| M_p(\mathcal{S}, A, B) - \frac{4AB}{p^2} \#\mathcal{S} \right| \leqslant \min\left\{ AB^{1-1/\nu}p^{(\nu+1)/(4\nu^2)} + B^{1/2}p,\ A^{1-1/\nu}Bp^{(\nu+1)/(4\nu^2)} + A^{1/2}p \right\} p^{o(1)}$$

holds with any fixed integer $\nu \geqslant 1$, where the function implied by $o(1)$ depends only on ν.

Applying Corollary 10 with $\nu = 3$, we obtain:

Corollary 11. *Under the hypotheses of Theorem 9, for any fixed $\varepsilon > 0$ there exists $\delta > 0$ such that if $AB \geqslant p^{4/3+\varepsilon}$, then*

$$\left| M_p(\mathcal{S}, A, B) - \frac{4AB}{p^2} \#\mathcal{S} \right| \ll ABp^{-\delta},$$

where the constant implied by $\ll$ depends only on ε.

Finally, taking ν large enough in Corollary 10, we obtain the following:

Corollary 12. *Under the hypotheses of Theorem 9, for any fixed $\varepsilon > 0$ there exists $\delta > 0$ such that if $\max\{A, B\} \geqslant p^{7/8-\varepsilon/3}$ and $\min\{A, B\} \geqslant p^{1/4+\varepsilon}$, then*

$$\left| M_p(\mathcal{S}, A, B) - \frac{4AB}{p^2} \#\mathcal{S} \right| \ll ABp^{-\delta},$$

where the constant implied by $\ll$ depends only on ε.

3.2 Sato–Tate conjecture on average

Theorem 13. *For any fixed $\varepsilon > 0$ there exists $\delta > 0$ such that for all integers A and B satisfying the inequalities (3) and all real numbers $0 \leqslant \alpha < \beta \leqslant \pi$, we have*

$$N^{\mathtt{ST}}_{\alpha,\beta}(A, B; x) = \big(4\mu_{\mathtt{ST}}(\alpha, \beta) + O\big(x^{-\delta}\big)\big)\, AB\, \pi(x),$$

where the constant implied by O depends only on ε.

Proof. Let us assume that $A \geqslant B$ since the case $A < B$ is similar. Using the trivial bounds $M_p(\mathcal{T}_p(\alpha, \beta), A, B) \leqslant AB$ and $\mu_{\mathtt{ST}}(\alpha, \beta) \ll 1$ for primes $p \leqslant 2A + 1$, we have

$$N^{\mathtt{ST}}_{\alpha,\beta}(A, B; x) = \sum_{2A+1 < p \leqslant x} M_p(\mathcal{T}_p(\alpha, \beta), A, B) + O(A^2 B).$$

Applying Lemma 6 and Theorem 9, we derive that

$$\big| M_p(\mathcal{T}_p(\alpha, \beta), A, B) - 4\mu_{\mathtt{ST}}(\alpha, \beta) AB \big| \ll \mathcal{E}(A, B; p) + ABp^{-1/4}.$$

Therefore,

$$\big| N^{\mathtt{ST}}_{\alpha,\beta}(A, B; x) - 4\mu_{\mathtt{ST}}(\alpha, \beta) AB\, \pi(x) \big| \ll A^2 B + ABx^{3/4} + \sum_{p \leqslant x} \mathcal{E}(A, B; p).$$

Applying Lemma 3 with $\eta = 1/8$, we get

$$\sum_{p \leqslant x} \sigma_p(B) \leqslant Bx^{1/2+o(1)} + B^{7/8}x \qquad (x \to \infty),$$

and it follows that

$$\sum_{p \leqslant x} \mathcal{E}(A, B; p) \ll ABx^{1/2+o(1)} + AB^{7/8}x + B^{1/2}x^2 \qquad (x \to \infty). \tag{8}$$

After simple calculations, we obtain the stated result. □

3.3 Cyclicity on average

Let Θ denote the following constant:

$$\Theta = \prod_q \left(1 - \frac{1}{q(q-1)\,(q^2-1)}\right),$$

where the product runs over all primes q.

Theorem 14. *Let $\varepsilon > 0$ and $K > 0$ be fixed. Then, for all integers A and B satisfying the inequalities* (3)*, we have*

$$N^{\mathtt{c}}(A, B; x) = \left(4\Theta + O\left((\log x)^{-K}\right)\right) AB\,\pi(x),$$

where the constant implied by O depends only on ε and K.

Proof. Let us assume that $A \geqslant B$ since the case $A < B$ is similar. Using the trivial bounds $M_p(\mathcal{C}_p, A, B) \leqslant AB$ and $\vartheta_p \ll 1$ for primes $p \leqslant 2A + 1$, we have

$$N^{\mathtt{c}}(A, B; x) = \sum_{2A+1 < p \leqslant x} M_p(\mathcal{C}_p, A, B) + O(A^2B).$$

Applying Lemma 7 and Theorem 9, we derive that

$$\left|M_p(\mathcal{C}_p, A, B) - 4\vartheta_p AB\right| \leqslant \left(\mathcal{E}(A, B; p) + ABp^{-1/2}\right) p^{o(1)}.$$

Since $A^{1/2}p \geqslant B^{1/2}p \geqslant ABp^{-1/2}$ for $B \leqslant A \leqslant (p-1)/2$, the second term can be dropped, and we have

$$\left|M_p(\mathcal{C}_p, A, B) - 4\vartheta_p AB\right| \leqslant \mathcal{E}(A, B; p)p^{o(1)}.$$

Hence, using (8) and the inequality $A^2B \leqslant ABx/(\log x)^{K+1}$, after simple calculations we see that

$$N^{\mathsf{c}}(A,B;x) = 4AB\sum_{p\leqslant x}\vartheta_p + O\left(\frac{ABx}{(\log x)^{K+1}}\right). \tag{9}$$

Now write

$$\sum_{p\leqslant x}\vartheta_p = \sum_{p\leqslant x} f(p-1),$$

where

$$f(n) = \prod_{q\,|\,n}\left(1-\frac{1}{q\,(q^2-1)}\right),$$

the product being taken over all prime divisors q of n; note that $f(n)$ is a multiplicative function. Let $g(n)$ be the multiplicative function that is defined on prime powers q^k as follows:

$$g(q^k) = \begin{cases} \dfrac{-1}{q\,(q^2-1)} & \text{if } k=1;\\ 0 & \text{if } k\geqslant 2.\end{cases}$$

Then,

$$f(n) = \sum_{d\,|\,n} g(d).$$

It is easy to check that the functions $f(n)$ and $g(n)$ satisfy the conditions of [22, Theorem 3], hence it follows that

$$\sum_{p\leqslant x}\vartheta_p = \sum_{p\leqslant x} f(p-1) = \Theta\,\pi(x) + O\left(\frac{x}{(\log x)^{K+1}}\right) \tag{10}$$

with

$$\Theta = \sum_{n=1}^{\infty}\frac{g(d)}{\varphi(d)} = \prod_{q}\left(1-\frac{1}{q(q-1)\,(q^2-1)}\right).$$

Inserting the estimate (10) into (9), we conclude the proof. □

3.4 Divisibility on average

Put

$$\mu = \prod_{q^j \parallel m} q^{\lceil j/2 \rceil}, \tag{11}$$

and set

$$\Omega_m = \frac{1}{\varphi(\mu)} \sum_{\substack{1 \leqslant k \leqslant \mu \\ \gcd(k,\mu)=1}} \omega_k(m),$$

where $\varphi(\mu)$ is the Euler function, and $\omega_k(m)$ is the completely multiplicative function which is defined on prime powers q^j by (7). For example, if $m = q$ is prime, then we have

$$\Omega_q = \frac{1}{q-1}\left(\frac{q}{q^2-1} + \sum_{k=2}^{q-1} \frac{1}{q-1}\right) = \frac{q^2-2}{(q-1)(q^2-1)}.$$

Theorem 15. *Let $\varepsilon > 0$ and $K > 0$ be fixed. Then, for all integers A and B satisfying the inequalities* (3) *and all integers $m \leqslant (\log x)^K$, we have*

$$N_m^{\mathtt{D}}(A, B; x) = \left(4\Omega_m + O\left((\log x)^{-K}\right)\right) AB\,\pi(x),$$

where the constant implied by O depends only on K and ε.

Proof. Let us assume that $A \geqslant B$ since the case $A < B$ is similar. Using the trivial bounds $M_p(\mathcal{D}_p(m), A, B) \leqslant AB$ and $\vartheta_p \ll 1$ for primes $p \leqslant 2A+1$, we have

$$N_m^{\mathtt{D}}(A, B; x) = \sum_{2A+1 < p \leqslant x} M_p(\mathcal{D}_p(m), A, B) + O(A^2 B).$$

Applying Lemma 8 and Theorem 9, we see that for $p \leqslant x$ and $x \to \infty$:

$$\begin{aligned} \left|M_p(\mathcal{D}_p(m), A, B) - 4\omega_p(m)AB\right| &\leqslant \left(\mathcal{E}(A, B; p) + ABp^{-1/2}\right) p^{o(1)} \\ &\leqslant \mathcal{E}(A, B; p) p^{o(1)}, \end{aligned}$$

where the second inequality follows from the fact that the term $ABp^{-1/2}$ never dominates $\mathcal{E}(A, B; p)$ (see the proof of Theorem 14). Hence, using (8) we conclude that

$$\begin{aligned} N_m^{\mathtt{D}}(A, B; x) = 4AB \sum_{p \leqslant x} \omega_p(m) \\ + O\left(ABx^{1/2+o(1)} + AB^{7/8}x + B^{1/2}x^2 + A^2B\right). \end{aligned}$$

As the value of $\omega_p(m)$ depends only on the residue class of p modulo μ, where μ is given by (11), using the *Siegel–Walfisz theorem* (see [23, Corollary 5.29]) we immediately obtain the desired result. $\square$

4 Further Applications

For specific ranges of the parameters A and B, one can use Lemma 2 instead of (or in conjunction with) Lemma 3 to obtain stronger and more explicit bounds for the error term in Theorem 13. On the other hand, for Theorems 14 and 15 the main contribution to the error comes from the imprecision involved in estimating sums with ϑ_p and $\omega_p(m)$, respectively.

Using Lemma 2 in place of Lemma 3 also allows one to study averages in which the parameters a and b vary over the shifted intervals $[H+1, H+K]$ and $[L+1, L+M]$, respectively.

Here, we have not used the full strength of the results of Garaev [18]. Doing so, one can actually replace the lower bound $A, B \geqslant x^{\varepsilon}$ in (3) with the bound $A, B \geqslant \exp\left(c\sqrt{\log x}\right)$ for an appropriate constant $c > 0$.

For fixed integers $m > k \geqslant 0$, one can also study the counting functions $\varpi_{a,b}^{(E)}(m, k; x)$ and $\varpi_{a,b}^{(t)}(m, k; x)$ of primes $p \leqslant x$ (with $p \nmid 4a^3 + 27b^2$) such that

$$\#\mathbf{E}_{a,b}(\mathbb{F}_p) \equiv k \pmod m \qquad \text{and} \qquad p + 1 - \#\mathbf{E}_{a,b}(\mathbb{F}_p) \equiv k \pmod m,$$

respectively. Our method can be adapted to obtain asymptotic formulae for the average values

$$\frac{m}{8AB} \sum_{|a| \leqslant A} \sum_{|b| \leqslant B} \varpi_{a,b}^{(E)}(m, k; x) \qquad \text{and} \qquad \frac{m}{8AB} \sum_{|a| \leqslant A} \sum_{|b| \leqslant B} \varpi_{a,b}^{(t)}(m, k; x)$$

over a wide range of values in the parameters A, B and m.

In principle, one can combine our approach with the results of [30] to study the distribution of the discriminants of complex multiplication fields of the curves $\mathbf{E}_{a,b}(\mathbb{F}_p)$, on average over a and b. Such discriminants are related to the size of the *Tate–Shafarevich group* of $\mathbf{E}_{a,b}(\mathbb{F}_p)$; thus, our approach can likely be used to improve some of the estimates of [11] on average.

We remark that the distribution of prime values of $\#\mathbf{E}_{a,b}(\mathbb{F}_p)$ is of great interest in the theory of cryptography. Hopefully, our method can be adapted to study this question as a and b vary over short intervals.

For the questions described above, the corresponding sets of curves are "massive" enough to allow for an application of Theorem 9; however, the primary obstacle in each case is the evaluation of the main term, which may require a significant effort even if the work is feasible.

It is natural to try to combine our approach with recent work of James and Yu [25] which studies, on average over $|a| \leqslant A$ and $|b| \leqslant B$, the number of primes $p \leqslant x$ for which $p + 1 - \mathbf{E}_{a,b}(\mathbb{F}_p)$ is a perfect k-th power. In some cases, it may be possible to lower the threshold on A and B. For $k \geqslant 3$ the corresponding set of curves appears to be too sparse, but perhaps for $k = 2$ there is a chance for our method to yield an improvement.

References

[1] A. Akbary, C. David and R. Juricevic, 'Average distributions and products of special values of L-series', *Acta Arith.* **111** (2004), no. 3, 239-268.

[2] S. Baier, 'The Lang–Trotter conjecture on average', *Preprint*, 2006.

[3] S. Baier and L. Zhao, 'The Sato–Tate conjecture on average for small angles', *Preprint*, 2006.

[4] W. D. Banks and I. E. Shparlinski, 'Average normalisations of elliptic curves', *Bull. Austral. Math. Soc.* **66** (2002), no. 3, 353-358.

[5] J. Battista, J. Bayless, D. Ivanov and K. James, 'Average Frobenius distributions for elliptic curves with nontrivial rational torsion', *Acta Arith.* **119** (2005), no. 1, 81-91.

[6] B. J. Birch, 'How the number of points of an elliptic curve over a fixed prime field varies', *J. Lond. Math. Soc.* **43** (1968), no. 1, 57-60.

[7] I. Borosh, C. J. Moreno and H. Porta, 'Elliptic curves over finite fields. II', *Math. Comput.* **29** (1975), 951-964.

[8] A. Cojocaru, 'On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves', *J. Number Theory* **96** (2002), no. 2, 335-350.

[9] A. Cojocaru, 'Cyclicity of CM elliptic curves modulo p', *Trans. Amer. Math. Soc.* **355** (2003), no. 7, 2651-2662 (electronic).

[10] A. Cojocaru, 'Questions about the reductions modulo primes of an elliptic curve', in *Number theory*, 61-79, *CRM Proc. Lecture Notes*, **36**, Amer. Math. Soc., Providence, RI, 2004.

[11] A. Cojocaru and W. Duke, 'Reductions of an elliptic curve and their Tate-Shafarevich groups', *Math. Ann.* **329** (2004), no. 3, 513-534.

[12] A. Cojocaru and M. R. Murty, 'Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem', *Math. Ann.* **330** (2004), no. 3, 601-625.

[13] A. Cojocaru, É. Fouvry and M. R. Murty, 'The square sieve and the Lang–Trotter conjecture', *Canad. J. Math.* **57** (2005), no. 6, 1155-1177.

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

[15] C. David and F. Pappalardi, 'Average Frobenius distribution for inerts in $\mathbb{Q}(i)$', *J. Ramanujan Math. Soc.* **19** (2004), no. 3, 181-201.

[16] B. Fisher, 'Equdistribution theorems (d'après P. Deligne amd N. Katz)', in *Columbia University Number Theory Seminar (New York, 1992)*, Astérisque, vol. 228, Soc. Math. France, 1995, 69-79.

[17] É. Fouvry and M. R. Murty, 'On the distribution of supersingular primes', *Canad. J. Math.* **48** (1996), no. 1, 81-104.

[18] M. Z. Garaev, 'Character sums in short intervals and the multiplication table modulo a large prime', *Monat. Math.* **148** (2006), no. 2, 127-138.

[19] E.-U. Gekeler, 'Frobenius distributions of elliptic curves over finite prime fields', *Int. Math. Res. Not.* **2003**, no. 37, 1999-2018.

[20] R. Gupta and M. R. Murty, 'Cyclicity and generation of points mod p on elliptic curves', *Invent. Math.* **101** (1990), no. 1, 225-235.

[21] E. W. Howe, 'On the group orders of elliptic curves over finite fields, *Compositio Math.* **85** (1993), no. 2, 229-247.

[22] K.-H. Indlekofer, S. Wehmeier and L. G. Lucht, 'Mean behaviour and distribution properties of multiplicative functions', *Comput. Math. Appl.* **48** (2004), no. 12, 1947-1971.

[23] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, RI, 2004.

[24] K. James, 'Average Frobenius distributions for elliptic curves with 3-torsion', *J. Number Theory* **109** (2004), no. 2, 278-298.

[25] K. James and G. Yu, 'Average Frobenius distribution of elliptic curves', *Acta Arith.* **124** (2006), no. 1, 79-100.

[26] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Princeton Univ. Press, Princeton, NJ, 1988.

[27] S. Lang and H. Trotter, 'Frobenius distributions in GL_2-extensions', in *Lecture Notes in Mathematics*, Vol. 504. Springer-Verlag, Berlin-New York, 1976.

[28] H. W. Lenstra, 'Factoring integers with elliptic curves', *Ann. of Math. (2)* **126** (1987), no. 3, 649-673.

[29] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[30] F. Luca and I. E. Shparlinski, 'Discriminants of complex multiplication fields of elliptic curves over finite fields', *Canad. Math. Bull.* (to appear).

[31] M. R. Murty, 'On Artin's conjecture', *J. Number Theory* **16** (1983), no. 2, 147-168.

[32] M. R. Murty and I. E. Shparlinski, 'Group structure of elliptic curves over finite fields and applications', in *Topics in Geometry, Coding Theory and Cryptography*, Springer-Verlag, 2006 (to appear).

[33] V. K. Murty, 'On the Sato–Tate conjecture', in *Number Theory Related to Fermat's Last Theorem (Cambridge, Mass., 1981)*, Birkhäuser, Boston, Mass., 1982, 195-205.

[34] H. Niederreiter, 'The distribution of values of Kloosterman sums', *Arch. Math.* **56** (1991), no. 3, 270-277.

[35] J.-P. Serre, 'Résumé des cours de 1977-1978', in *Collected Papers, Vol. III*, 465-468, Springer Verlag, Berlin, 1986.

[36] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.

[37] R. Taylor, 'Automorphy for some l-adic lifts of automorphic mod l representations, II', *Preprint*, 2006.

[38] I. M. Vinogradov, *Elements of number theory*, Dover Publications, New York, 1954.

[39] S. G. Vlăduţ, 'Cyclicity statistics for elliptic curves over finite fields', *Finite Fields Appl.* **5** (1999), no. 1, 13-25.