Michigan Math. J. 62 (2013), 491–505

On the Lang–Trotter and Sato–Tate Conjectures on Average for Polynomial Families of Elliptic Curves

IGOR E. SHPARLINSKI

1. Introduction

1.1. BACKGROUND. For a prime p, we denote by $\mathbb{F}_p$ the finite field with p elements.

Given an elliptic curve $\mathbf{E}$ over $\mathbb{Q}$ and a prime p we use $\mathbf{E}(\mathbb{F}_p)$ to denote the set of the $\mathbb{F}_p$-rational points of the reduction of $\mathbf{E}$ modulo p, provided that p does not divide the discriminant $\Delta(\mathbf{E})$ of $\mathbf{E}$, together with a point at infinity. This set forms an *abelian group* under an appropriate composition rule and satisfies the *Hasse bound*:

$$|\#\mathbf{E}(\mathbb{F}_p) - p - 1| \le 2\sqrt{p}; \tag{1}$$

see [35] for background on elliptic curves.

Accordingly, we denote by $\Pi^{\mathrm{LT}}(\mathbf{E}, t; x)$ the number of primes $3 < p \le x$ (with $p \nmid \Delta(\mathbf{E})$) for which $\#\mathbf{E}(\mathbb{F}_p) = p + 1 - t$. The *Lang–Trotter conjecture* asserts that if $\mathbf{E}$ does not have complex multiplication then the asymptotic formula

$$\Pi^{\mathrm{LT}}(\mathbf{E}, t; x) \sim c(\mathbf{E}, t)\frac{\sqrt{x}}{\log x}, \quad x \to \infty, \tag{2}$$

holds for some explicitly given constant $c(\mathbf{E}, t) \ge 0$ depending only on $\mathbf{E}$ and t. Furthermore, the usual interpretation of the value $c(\mathbf{E}, t) = 0$ is $\Pi^{\mathrm{LT}}(\mathbf{E}, t; x) = O(1)$.

Since the Lang–Trotter conjecture (2) remains widely open (see [13; 14; 15; 26; 28; 29; 30; 32; 37]), it is natural to obtain its analogues "on average" over various interesting families of curves. As one example, for integers a and b such that $4a^3 + 27b^2 \ne 0$, we denote by $\mathbf{E}_{a,b}$ the elliptic curve defined by the *affine Weierstraß equation,*

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

and put

$$\Pi^{\mathrm{LT}}_{a,b}(t; x) = \Pi^{\mathrm{LT}}(\mathbf{E}_{a,b}, t; x).$$

Fouvry and Murty [17] initiated the study of $\Pi^{\mathrm{LT}}_{a,b}(t; x)$ and similar quantities on average, and they showed that the asymptotic formula

Received April 30, 2012. Revision received October 10, 2012.
This work was supported in part by ARC Grant no. DP1092835.

$$\frac{1}{4AB}\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{LT}}_{a,b}(t;x)\sim C(t)\frac{\sqrt{x}}{\log x},\quad x\to\infty, \tag{3}$$

holds for $t=0$ (with $C(0)=\pi/3$) in the range

$$AB\ge x^{3/2+\varepsilon}\quad\text{and}\quad \min\{A,B\}\ge x^{1/2+\varepsilon} \tag{4}$$

for arbitrary fixed $\varepsilon>0$ (for $4a^3+27b^2=0$ we define $\Pi^{\mathrm{LT}}_{a,b}(t;x)=0$). David and Pappalardi [11] proved that (3) holds for any fixed t, with some explicit constant $C(t)>0$ depending only on t, but in a smaller range than (4). This range has been expanded to the original level described in (4) by Baier [2]. Finally, Baier [3] obtained (3) in an even wider range:

$$AB\ge x^{3/2+\varepsilon}\quad\text{and}\quad \min\{A,B\}\ge x^{\varepsilon}$$

(in this range, the term with $ab=0$ must be eliminated from the summation in (3) because its contribution may exceed the main term).

In addition, for an elliptic curve $\mathbf{E}$ over $\mathbb{Q}$ and a prime $p>3$ we recall (1) and define the angle $\psi(\mathbf{E};p)\in[0,\pi]$ via the identity

$$+1-\#\mathbf{E}(\mathbb{F}_p)=2\sqrt{p}\cos\psi(\mathbf{E};p). \tag{5}$$

(We may also define $\psi(\mathbf{E};p)$ arbitrarily—say, as $\psi(\mathbf{E};p)=0$ if p divides $4a^3+27b^2$.) For $0\le\alpha<\beta\le\pi$, we denote by $\Pi^{\mathrm{ST}}(\mathbf{E},\alpha,\beta;x)$ the number of primes $p\le x$ (where p does not divide $4a^3+27b^2$) for which $\alpha\le\psi(\mathbf{E};p)\le\beta$. In this case, the *Sato–Tate conjecture* asserts that if $\mathbf{E}$ does not have complex multiplication then the asymptotic formula

$$\Pi^{\mathrm{ST}}(\mathbf{E},\alpha,\beta;x)\sim\mu_{\mathrm{ST}}(\alpha,\beta)\frac{x}{\log x},\quad x\to\infty, \tag{6}$$

holds, where

$$\mu_{\mathrm{ST}}(\alpha,\beta)=\frac{2}{\pi}\int_\alpha^\beta\sin^2\gamma\,d\gamma \tag{7}$$

is the *Sato–Tate density*; see [8; 22; 27].

The method of Fouvry and Murty [17] is based on bounds of exponential sums; it is quite universal and has been applied to a number of related questions (see [1; 4; 5; 7; 11; 12; 20; 21; 33; 34]). In particular, by using this method it is easy to show that

$$\frac{1}{4AB}\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{ST}}_{a,b}(t;x)\sim\mu_{\mathrm{ST}}(\alpha,\beta)\frac{x}{\log x},\quad x\to\infty, \tag{8}$$

in the same range (4); as before, we define

$$\Pi^{\mathrm{ST}}_{a,b}(t;x)=\Pi^{\mathrm{ST}}(\mathbf{E}_{a,b},t;x).$$

Although Taylor [36] gave a complete proof of (6) (except for the curves $\mathbf{E}$ with integral j-invariant), this does not imply any results *on average* owing to the lack of uniformity with respect to the coefficients a and b in the Weierstraß equation.

A different approach was also suggested in [6], one based on bounds of multiplicative character sums (see [5; 34] for further applications of this approach).

We remark that the original purpose of [6] was to improve some results on the Sato–Tate conjecture for the curves $\mathbf{E}_{a,b}$ on average and also to obtain (8) for a wider range than (4)—namely, under the conditions

$$AB \ge x^{1+\varepsilon} \quad \text{and} \quad \min\{A, B\} \ge x^{\varepsilon}. \tag{9}$$

See [3; 4] for some other approaches.

1.2. Results. Here we show that the ideas of [6] can also be used for extending (3) and (8) to more general families of curves.

Let us fix two polynomials $f(T), g(T) \in \mathbb{Z}[T]$ that are not powers of another polynomial over $\mathbb{Q}$. Here we consider the family of curves $\mathbf{E}_{f(a),g(b)}$ and obtain analogues of the asymptotic formulas (3) and (8) for these curves—that is, we obtain asymptotic formulas for the average values

$$\frac{1}{4AB}\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{LT}}_{f(a),g(b)}(t;x), \qquad \frac{1}{4AB}\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{ST}}_{f(a),g(b)}(\alpha,\beta;x).$$

As is usual with questions of this kind, our main concern is to minimize the extent of averaging and thereby obtain these asymptotic formulas in ranges comparable to those given by (4) and (9). (Note that the approach of Fouvry and Murty [17] does not seem to work for the families of curves $\mathbf{E}_{f(a),g(b)}$.)

We also study a 1-parametric family of curves $\mathbf{E}_{f(a),g(a)}$ with two polynomials f and g over $\mathbb{F}_p$ (satisfying some natural condition). We use a result of Michel [24] to show that, for a fixed $\varepsilon > 0$ and a sufficiently large prime p, the corresponding angles $\psi(\mathbf{E}_{f(a),g(a)}, p)$ are distributed with the Sato–Tate density when a runs through consecutive integers of an interval of length at least $p^{3/4+\varepsilon}$.

Finally, we recall that upper bounds for $\Pi^{\mathrm{LT}}_{f(\rho),g(\rho)}(t;x)$, on average when ρ runs through the set of Farey fractions of order Q, are given in [9; 10].

1.3. Notation. Throughout the paper, any constants implied by our use of the symbols O and $\ll$ may occasionally depend (in obvious instances) on the polynomials f and g and on the real parameters ε, but otherwise such constants are absolute. We recall that the expressions $U \ll V$ and $U = O(V)$ are both equivalent to stating that the inequality $|U| \le cV$ holds with some constant $c > 0$.

The letters p and q always denote prime numbers, while m and n always denote integers. As usual, we use $\pi(x)$ to denote the number of primes $p \le x$.

2. Character Sums and Distribution of Power Residues

2.1. Character Sums

For a prime p, we denote by $\mathcal{X}_p$ the set of multiplicative characters of $\mathbb{F}_p$, by χ_0 the principal character of $\mathbb{F}_p$, and by $\mathcal{X}_p^* = \mathcal{X}_p \setminus \{\chi_0\}$ the set of nonprincipal characters; we refer the reader to [19, Chap. 3] for the necessary background on multiplicative characters. We recall the following orthogonality relations. For any integer $f \mid p-1$ and $v \in \mathbb{F}_p$,

$$\frac{1}{f}\sum_{\substack{\chi\in\mathcal{X}_p\\ \chi^f=\chi_0}}\chi(v)=\begin{cases}1 & \text{if } v=w^f \text{ for some } w\in\mathbb{F}_p^*,\\ 0 & \text{otherwise.}\end{cases} \tag{10}$$

Also, we have

$$\frac{1}{p-1}\sum_{u\in\mathbb{F}_p^*}\chi_1(u)\bar{\chi}_2(u)=\begin{cases}1 & \text{if } \chi_1=\chi_2,\\ 0 & \text{otherwise}\end{cases} \tag{11}$$

for all $\chi_1,\chi_2\in\mathcal{X}_p$ (here, $\bar{\chi}_2$ is the character obtained from χ_2 by complex conjugation).

The following result is a special case of the Weil bound (see [19, eq. (12.23)]).

LEMMA 1. *For any prime p and polynomial $h(T)\in\mathbb{Z}[T]$ that is not a power of another polynomial in the algebraic closure of $\mathbb{F}_p$, uniformly over all integers m and nontrivial multiplicative characters χ modulo p we have*

$$\sum_{u=1}^{p}\chi(h(u))\exp\left(2\pi i\frac{mu}{p}\right)\ll p^{1/2}.$$

Combining Lemma 1 with the standard reduction between complete and incomplete sums (see [19, Sec. 12.2]), we obtain the following result.

LEMMA 2. *For any prime p and polynomial $h(T)\in\mathbb{Z}[T]$ that is not a power of another polynomial in the algebraic closure of $\mathbb{F}_p$, uniformly over all positive integers L, M and nontrivial multiplicative characters χ modulo p we have*

$$\sum_{n=L+1}^{L+M}\chi(h(n))\ll\left(\frac{M}{p}+1\right)p^{1/2}\log p.$$

2.2. *Distribution of Powers*

Adapting the idea of Fouvry and Murty [17], we study the distribution of the pairs

$$\{(ru^4,su^6):u\in\mathbb{F}_p\},\quad r,s\in\mathbb{F}_p^*, \tag{12}$$

among the residues modulo p of the polynomial values $(f(a),g(b))$ with $|a|\le A$ and $|b|\le B$. However, we forgo the exponential sums used in [17]; instead, we follow the approach of [6] and study the distribution of the pairs (12) using multiplicative character sums.

We also note that, since the polynomials $f(T),g(T)\in\mathbb{Z}[T]$ are not powers of another polynomial over $\mathbb{Q}$, for any sufficiently large prime p they are not powers of a polynomial in the algebraic closure of $\mathbb{F}_p$. Thus Lemma 2 applies to character sums with $f(T)$ and $g(T)$.

We begin by investigating the distribution of the second component su^6 of the pairs (12). Accordingly, we define

$$\mathcal{Z}_s(B;p)=\{(u,b)\in\mathbb{F}_p^*\times[-B,B]:su^6\equiv g(b)\pmod p,\ |b|\le B\}.$$

Although we are usually interested in only the first component u, here we define $\mathcal{Z}_s(B;\, p)$ as a set of pairs (u, b). In essence this means that each u is taken with the mulitplicity of the residue class su^6 among the elements of $[-B, B]$.

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

LEMMA 3. *For any prime p, integer $B \geq 1$, and $s \in \mathbb{F}_p^*$, we have*

$$\#\mathcal{Z}_s(B;\, p) = 2B + O\left(\left(\frac{B}{p} + 1\right) p^{1/2+o(1)}\right)$$

as $p \to \infty$.

Proof. Define

$$d_p = \gcd(p - 1, 6).$$

By the orthogonality relation (10), for all $n \in \mathbb{Z}$ we have

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

If $\bar{s}$ is an integer such that $s\bar{s} \equiv 1 \pmod p$, then

$$\#\mathcal{Z}_s(B;\, p) = \sum_{|b| \leq B} \sum_{\substack{\chi \in \mathcal{X}_p \\ \chi^{d_p} = \chi_0}} \chi(\bar{s} g(b)) = 2B + O(1) + \sum_{\substack{\chi \in \mathcal{X}_p^* \\ \chi^{d_p} = \chi_0}} \bar{\chi}(s) \sum_{|b| \leq B} \chi(g(b)).$$

An application of Lemma 2 now concludes the proof. □

Next we account for the distribution of the first component ru^4 of the pairs (12). For any integers $A, B \geq 1$ and $r, s \in \mathbb{F}_p$, define the set of triples

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

LEMMA 4. *For any prime p, integers $A, B \geq 1$, and $s \in \mathbb{F}_p^*$, we have*

$$\sum_{r \in \mathbb{F}_p^*} \left| \#\mathcal{Z}_{r,s}(A, B;\, p) - \frac{2A\mathcal{Z}_s(B;\, p)}{p - 1} \right|^2 \leq \left(\frac{A}{p} + 1\right)^2 \left(\frac{B}{p} + 1\right) B p^{1+o(1)}$$

as $p \to \infty$.

Proof. From (10) it follows that

$$\begin{aligned} &\#\mathcal{Z}_{r,s}(A, B;\, p) \\ &\quad = \sum_{(u,b) \in \mathcal{Z}_s(B;p)} \sum_{|a| \leq A} \frac{1}{p - 1} \sum_{\chi \in \mathcal{X}_p} \chi(ru^4) \overline{\chi(f(a))} \\ &\quad = \frac{2A\#\mathcal{Z}_s(B;\, p)}{p - 1} + \frac{1}{p - 1} \sum_{\chi \in \mathcal{X}_p^*} \chi(r) \sum_{(u,b) \in \mathcal{Z}_s(B;p)} \chi(u^4) \sum_{|a| \leq A} \bar{\chi}(f(a)). \end{aligned}$$

Therefore,

$$\#\mathcal{Z}_{r,s}(A,B;\,p) - \frac{2A\#\mathcal{Z}_s(B;\,p)}{p-1} \ll \frac{1}{p-1}\left|\sum_{\chi\in\mathcal{X}_p^*}\chi(r)\sum_{(u,b)\in\mathcal{Z}_s(B;p)}\chi(u^4)\sum_{|a|\le A}\bar\chi(f(a))\right|.$$

Hence

$$\sum_{r\in\mathbb{F}_p^*}\left|\#\mathcal{Z}_{r,s}(A,B;\,p) - \frac{4AB}{p-1}\right|^2 \ll W, \tag{13}$$

where

$$W = \frac{1}{(p-1)^2}\sum_{r\in\mathbb{F}_p^*}\left|\sum_{\chi\in\mathcal{X}_p^*}\chi(r)\sum_{(u,b)\in\mathcal{Z}_s(B;p)}\chi(u^4)\sum_{|a|\le A}\bar\chi(f(a))\right|^2.$$

Squaring out and changing the order of summation now yields

$$W = \frac{1}{(p-1)^2}\sum_{\chi_1,\chi_2\in\mathcal{X}_p^*}\sum_{(u_1,b_1),(u_2,b_2)\in\mathcal{Z}_s(B;p)}\chi_1(u_1^4)\bar\chi_2(u_2^4)\sum_{|a_1|,|a_2|\le A}\bar\chi_1(f(a_1))\chi_2(f(a_2))\sum_{r\in\mathbb{F}_p}\chi_1(r)\bar\chi_2(r).$$

From the orthogonality relation (11) we deduce that

$$W = \frac{1}{p-1}\sum_{\chi\in\mathcal{X}_p^*}\left|\sum_{(u,b)\in\mathcal{Z}_s(B;p)}\chi(u^4)\right|^2\left|\sum_{|a|\le A}\chi(f(a))\right|^2;$$

by Lemma 2, it follows that

$$W \le \left(\frac{A}{p}+1\right)^2 p^{o(1)}\sum_{\chi\in\mathcal{X}_p^*}\left|\sum_{(u,b)\in\mathcal{Z}_s(B;p)}\chi(u^4)\right|^2. \tag{14}$$

Next we extend the summation in (14) to include the trivial character $\chi = \chi_0$. Then, by the orthogonality relation (10), we have

$$\sum_{\chi\in\mathcal{X}_p^*}\left|\sum_{(u,b)\in\mathcal{Z}_s(B;p)}\chi(u^4)\right|^2 \le \sum_{\chi\in\mathcal{X}_p}\left|\sum_{(u,b)\in\mathcal{Z}_s(B;p)}\chi(u^4)\right|^2 = (p-1)T; \tag{15}$$

here T is the number of solutions to the congruence

$$u_1^4 \equiv u_2^4 \pmod p, \quad (u_1,b_1),(u_2,b_2)\in\mathcal{Z}_s(B;\,p).$$

Clearly, T does not exceed

$$u_1^{12} \equiv u_2^{12} \pmod p, \quad (u_1,b_1),(u_2,b_2)\in\mathcal{Z}_s(B;\,p). \tag{16}$$

Since $su_j^6 \equiv g(b_j) \pmod p$ for some b_j with $|b_j| \le B$ $(j = 1,2)$, it follows that each solution to (16) results in a congruence

$$g(b_1)^2 \equiv g(b_2)^2 \pmod p, \quad |b_1|,|b_2| \le B.$$

Hence $T \ll B(B/p+1)$, because each b_j corresponds to at most six values of u_j. Recalling (14) and (15) now concludes the proof. □

3. Elliptic Curves

3.1. Isomorphic Elliptic Curves

It is well known that if $a, b, r, s \in \mathbb{F}_p$ then $\mathbf{E}_{a,b}(\mathbb{F}_p) \cong \mathbf{E}_{r,s}(\mathbb{F}_p)$; that is, the curves $\mathbf{E}_{a,b}$ and $\mathbf{E}_{r,s}$ are *isomorphic over* $\mathbb{F}_p$ if and only if

$$a = ru^4 \quad \text{and} \quad b = su^6 \tag{17}$$

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 [23].

Thus we see that a link between the distribution of elliptic curves of various types and the sets $\mathcal{Z}_{r,s}(A, B; p)$ is given by Lemma 5.

For an arbitrary set $\mathcal{S} \subseteq \mathbb{F}_p \times \mathbb{F}_p$, denote by $M_p(\mathcal{S}, A, B)$ the number of curves $\mathbf{E}_{f(a),g(b)}$ such that the reduction modulo p of the pair $(f(a), g(b))$ belongs to $\mathcal{S}$ for $a \in [-A, A]$ and $b \in [-B, B]$.

LEMMA 5. *Suppose $f(T), g(T) \in \mathbb{Z}[T]$ are not powers of another polynomial over $\mathbb{Q}$. Assume that for a prime $p > 3$ we are given a set $\mathcal{S} \subseteq \mathbb{F}_p^* \times \mathbb{F}_p^*$ such that, whenever $(r, s) \in \mathcal{S}$ and $\mathbf{E}_{a,b}(\mathbb{F}_p) \cong \mathbf{E}_{r,s}(\mathbb{F}_p)$, it follows that $(a, b) \in \mathcal{S}$. Then the bound*

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

holds for any integers $A, B \geq 1$.

Proof. We estimate the contribution from the curves with

$$f(a)g(b)(4f(a)^3 + 27g(b)^2) \equiv 0 \pmod{p}$$

trivially as

$$O\left(\left(\frac{A}{p}+1\right)B + A\left(\frac{B}{p}+1\right)\right) = O\left(\frac{AB}{p} + A + B\right).$$

We also note that if $a \equiv ru^4 \pmod{p}$ and $b \equiv su^6 \pmod{p}$, then each group $\mathbf{E}_{f(a),g(b)}(\mathbb{F}_p)$ with $|a| \leq A$ and $|b| \leq B$ is counted precisely $p-1$ times in the sum on the right-hand side. □

3.2. Statistics of Elliptic Curves

Let $\mathcal{R}_p(t)$ be the set of pairs $(r, s) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ such that

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

We recall the following well-known estimate (see e.g. [23, Prop. 1.9]).

LEMMA 6. *For any fixed t,*

$$\mathcal{R}_p(t) \ll p^{3/2+o(1)}.$$

We define

$$\mathrm{li}_{1/2}(x) = \int_2^x \frac{dz}{2z^{1/2}\log z} = (1+o(1))\frac{x^{1/2}}{\log x}.$$

By a result of David and Pappalardi [11, eqs. (24), (29)] (see also [2, eq. (2.1), Lemma 3]), we have the following statement.

LEMMA 7. *For any fixed integer t there exists a constant $C(t) > 0$ such that, for any fixed $C > 0$,*

$$\sum_{p \le x} \frac{1}{p^2} \#\mathcal{R}_p(t) = C(t)\,\mathrm{li}_{1/2}(x) + O(x^{1/2}(\log x)^{-C}).$$

Let $\mathcal{T}_p(\alpha,\beta)$ be the set of pairs $(r,s) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ such that the inequalities $\alpha \le \psi_{r,s}(p) \le \beta$ hold, where the angles

$$\psi_{r,s}(p) = \psi(\mathbf{E}_{r,s};\, p)$$

are given by (5). It is natural to expect that

$$\#\mathcal{T}_p(\alpha,\beta) \sim \mu_{\mathrm{ST}}(\alpha,\beta)p^2$$

as $p \to \infty$, where $\mu_{\mathrm{ST}}(\alpha,\beta)$ is given by (7); this is known as the Sato–Tate conjecture *in the vertical aspect*. It has been established by Birch [8] (see also [25]), but here we require a stronger result. What is needed is a full analogue for the Sato–Tate density of the bound of Niederreiter [31] on the discrepancy in the distribution of values of Kloosterman sums. Fortunately, such a result can be obtained by using the same methods because all of the underlying tools (namely, [31, Lemma 3] and [22, Thm. 13.5.3]) apply to $\psi_{r,s}(p)$ as well as to values of Kloosterman sums. In particular, from [22, Thm. 13.5.3] it follows that

$$\frac{1}{(p-1)^2} \sum_{\substack{r,s \in \mathbb{F}_p^* \\ 4r^3+27s^2 \ne 0}} \frac{\sin((n+1)\psi_{r,s}(p))}{\sin(\psi_{r,s}(p))} \ll np^{-1/2}, \quad n = 1,2,\ldots \tag{18}$$

(see also the work of Fisher [16, Sec. 5]). Thus, as in [31], we have the following lemma.

LEMMA 8. *For any prime p,*

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

Michel [24, Prop. 1.1] gives a version of (18) for 1-parametric polynomial families of curves in which the sum is also twisted by additive characters.

LEMMA 9. *For any prime p and uniformly over all integers m, for any polynomials $f(T), g(T) \in \mathbb{Z}[T]$ we have*

$$\frac{1}{p} \sum_{\substack{a \in \mathbb{F}_p \\ 4f(a)^3+27g^2(a) \not\equiv 0 \pmod p}} \frac{\sin((n+1)\psi_{f(a),g(a)}(p))}{\sin(\psi_{f(a),g(a)}(p))} \exp\left(2\pi i \frac{ma}{p}\right) \ll np^{-1/2}$$

for $n = 1, 2, \ldots$.

Again, using the standard reduction between complete and incomplete sums (see [19, Sec. 12.2]) reveals that Lemma 9 implies the following result.

LEMMA 10. *For any prime* p, *integer* $A \geq 1$, *and polynomials* $f(T), g(T) \in \mathbb{Z}[T]$, *we have*

$$\frac{1}{p} \sum_{\substack{|a| \leq A \\ 4f(a)^3+27g^2(a) \not\equiv 0 \pmod p}} \frac{\sin((n+1)\psi_{f(a),g(a)}(p))}{\sin(\psi_{f(a),g(a)}(p))} \ll np^{-1/2+o(1)}$$

for $n = 1, 2, \ldots$.

Let $\mathcal{T}_{f,g,p}(A; \alpha, \beta)$ be the set of integers a with $|a| \leq A$ and such that the inequalities $\alpha \leq \psi_{f(a),g(a)}(p) \leq \beta$ hold; as before, the angles

$$\psi_{f(a),g(a)}(p) = \psi(\mathbf{E}_{f(a),g(a)}; p)$$

are given by (5). Applying the technique of Niederreiter [31], we immediately obtain the following analogue of Lemma 8.

LEMMA 11. *For any prime* p, *positive integer* $A < p/2$, *and polynomials* $f(T), g(T) \in Z[T]$ *such that* $4f(T)^3 + 27g(T)^2$ *is not identical to zero, we have*

$$\max_{0 \leq \alpha < \beta \leq \pi} |\#\mathcal{T}_{f,g,p}(A; \alpha, \beta) - 2\mu_{\mathrm{ST}}(\alpha, \beta)A| \ll A^{1/2}p^{1/4+o(1)}.$$

Proof. By [31, Lemma 3] we see that, for any integer k,

$$\max_{0 \leq \alpha < \beta \leq \pi} |\#\mathcal{T}_{f,g,p}(A; \alpha, \beta) - 2\mu_{\mathrm{ST}}(\alpha, \beta)A| \ll \frac{A}{k} + \sum_{n=1}^{k} \frac{1}{n} \left| \sum_{\substack{|a| \leq A \\ 4f(a)^3+27g^2(a) \not\equiv 0 \pmod p}} \frac{\sin((n+1)\psi_{f(a),g(a)}(p))}{\sin(\psi_{f(a),g(a)}(p))} \right|.$$

Applying Lemma 10 and choosing $k = \lceil A^{1/2}p^{-1/4} \rceil$ now yields the desired bound. □

Lemma 11 is a generalization of [25, Thm. 1.4] corresponding to the case of $A = (p-1)/2$ that follows directly from Lemma 9 applied with $m = 0$.

4. Main Results

4.1. General Estimate

We now have the following general result that can be applied to various families of elliptic curves. We formulate it in a general way so that it can be applied to the Lang–Trotter or Sato–Tate conjecture.

Let us define

$$E_\vartheta(U,V;z) = UVz^{-1/2-\vartheta/2} + UV^{1/2}z^{-\vartheta/2} + UVz^{-1} + Uz^{1/2-\vartheta} + U + Vz^{1/2-\vartheta/2} + V^{1/2}z^{1-\vartheta/2}.$$

THEOREM 12. *Suppose $f(T), g(T) \in \mathbb{Z}[T]$ are not powers of another polynomial over $\mathbb{Q}$. Assume that for a prime $p > 3$ we are given a set $\mathcal{S} \subseteq \mathbb{F}_p^* \times \mathbb{F}_p^*$ of cardinality*

$$\#\mathcal{S} \le p^{2-\vartheta+o(1)}$$

as $p \to \infty$ for some absolute constant $\vartheta \ge 0$ and such that, if $(r,s) \in \mathcal{S}$ and $\mathbf{E}_{a,b}(\mathbb{F}_p) \cong \mathbf{E}_{r,s}(\mathbb{F}_p)$, then $(a,b) \in \mathcal{S}$. Under these conditions, it follows that the bound

$$\left| M_p(\mathcal{S},A,B) - \frac{4AB\#\mathcal{S}}{(p-1)^2} \right| \le E_\vartheta(U,V;p)p^{o(1)}$$

holds for any integers $A, B \ge 1$, where

$$U = \max\{A,B\} \quad \textit{and} \quad V = \min\{A,B\}.$$

Proof. Assume that $A \ge B$. We can use Lemma 5 to derive

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

Furthermore, by Lemma 3 (and since $A \ge B$) we see that

$$M_p(\mathcal{S},A,B) - \frac{4AB\#\mathcal{S}}{(p-1)^2} \ll \Delta + ABp^{-1/2-\vartheta+o(1)} + Ap^{1/2-\vartheta+o(1)} + ABp^{-1} + A, \quad (19)$$

where

$$\Delta = \frac{1}{p-1}\sum_{(r,s)\in\mathcal{S}} \left| \#\mathcal{Z}_{r,s}(A,B;p) - \frac{2A\#\mathcal{Z}_s(B,p)}{p-1} \right|.$$

By the Cauchy inequality, it follows that

$$\begin{aligned}\Delta^2 &\ll \frac{\#\mathcal{S}}{p^2}\sum_{(r,s)\in\mathcal{S}} \left| \#\mathcal{Z}_{r,s}(A,B;p) - \frac{2A\#\mathcal{Z}_s(B,p)}{p-1} \right|^2 \\ &\le p^{-\vartheta+o(1)}\sum_{(r,s)\in\mathcal{S}} \left| \#\mathcal{Z}_{r,s}(A,B;p) - \frac{2A\#\mathcal{Z}_s(B,p)}{p-1} \right|^2 \\ &\le p^{-\vartheta+o(1)}\sum_{r,s\in\mathbb{F}_p^*} \left| \#\mathcal{Z}_{r,s}(A,B;p) - \frac{2A\#\mathcal{Z}_s(B,p)}{p-1} \right|^2.\end{aligned}$$

Now using Lemma 4 for each $s \in \mathbb{F}_p^*$, we obtain

$$\Delta^2 \ll \left(\frac{A}{p}+1\right)^2\left(\frac{B}{p}+1\right)Bp^{2-\vartheta+o(1)}.$$

Therefore,

$$\Delta \le ABp^{-1/2-\vartheta/2+o(1)} + AB^{1/2}p^{-\vartheta/2+o(1)} + Bp^{1/2-\vartheta/2+o(1)} + B^{1/2}p^{1-\vartheta/2+o(1)}.$$

Recalling (19) and using that

$$ABp^{-1/2-\vartheta/2} > ABp^{-1/2-\vartheta},$$

we obtain

$$\left|M_p(\mathcal{S}, A, B) - \frac{4AB\#\mathcal{S}}{(p-1)^2}\right| \le E_\vartheta(A, B; p)p^{o(1)}.$$

It is easy to see that the roles of A and B can be interchanged in all previous arguments, which concludes the proof. □

In all of this paper's applications we have $\vartheta \le 1/2$, in which case $UVz^{-1/2-\vartheta/2} \ge UVz^{-1}$ and $Uz^{1/2-\vartheta} \ge U$. As a result,

$$\begin{aligned} E_\vartheta(U, V; z) \ll{}& UVz^{-1/2-\vartheta/2} + UV^{1/2}z^{-\vartheta/2} + Uz^{1/2-\vartheta} \\ &+ Vz^{1/2-\vartheta/2} + V^{1/2}z^{1-\vartheta/2}. \end{aligned} \tag{20}$$

4.2. The Lang–Trotter Conjecture on Average

We now derive the following generalizations of (3).

THEOREM 13. *Suppose $f(T), g(T) \in \mathbb{Z}[T]$ are not powers of another polynomial over $\mathbb{Q}$. Assume that positive integers A and B are such that, for some $\varepsilon > 0$,*

$$\max\{AB^{1/2}, A^{1/2}B\} \ge x^{5/4+\varepsilon} \quad \text{and} \quad \min\{A, B\} \ge x^{1/2+\varepsilon}.$$

Then

$$\frac{1}{4AB}\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{LT}}_{f(a),g(b)}(t; x) = (C(t) + o(1))\frac{\sqrt{x}}{\log x}$$

for some constant $C(t) > 0$ depending only on t.

Proof. In the notation of Sections 3.1 and 3.2, we have

$$\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{LT}}_{f(a),g(b)}(t; x) = \sum_{p\le x} M_p(\mathcal{R}_p(t), A, B).$$

Assume that $A \ge B$. Now from Theorem 12 applied with $\mathcal{S} = \mathcal{R}_p(t)$ (thus $\vartheta = 1/2$ by Lemma 6, so we can also use (20)), we derive

$$\begin{aligned} &\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{LT}}_{f(a),g(b)}(t; x) - 4AB\sum_{p\le x}\frac{\mathcal{R}_p(t)}{(p-1)^2} \\ &\qquad \le (ABx^{1/4} + AB^{1/2}x^{3/4} + Ax + Bx^{5/4} + B^{1/2}x^{7/4})x^{o(1)} \end{aligned}$$

as $x \to \infty$.

By Lemma 6 and Lemma 7 (taken with, say, $C = 2$) we see that

$$\begin{aligned}\sum_{p\le x}\frac{\#\mathcal{R}_p(t)}{(p-1)^2} &= \sum_{p\le x}\#\mathcal{R}_p(t)\left(\frac{1}{p^2}+O(p^{-3})\right)\\ &= \sum_{p\le x}\frac{1}{p^2}\#\mathcal{R}_p(t)+O(1)\\ &= C(t)\,\mathrm{li}_{1/2}(x)+O(x^{1/2}(\log x)^{-2}).\end{aligned}$$

Disregarding the term $ABx^{1/4}$ (which is obviously smaller than the contribution from the error term in the previous formula), we therefore obtain

$$\begin{aligned}&\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{LT}}_{f(a),g(b)}(t;x)-4ABC(t)\,\mathrm{li}_{1/2}(x)\\ &\quad\ll (AB^{1/2}x^{3/4}+Ax+Bx^{5/4}+B^{1/2}x^{7/4})x^{o(1)}+ABx^{1/2}(\log x)^{-2}\\ &\quad\ll ABx^{1/2+o(1)}(B^{-1/2}x^{1/4}+B^{-1}x^{1/2}+A^{-1}x^{3/4}+A^{-1}B^{-1/2}x^{5/4})\\ &\qquad+ABx^{1/2}(\log x)^{-2}.\end{aligned}$$

Since $A \ge B$, it follows that $A^{3/2} \ge AB^{1/2} \ge x^{5/4+\varepsilon}$. Thus $A \ge x^{5/6+2\varepsilon/3}$ and, after simple calculations, we obtain the desired result in the case $A \ge B$.

The proof is completely analogous in the case $A < B$. □

Since $\max\{AB^{1/2}, A^{1/2}B\} \ge (AB)^{3/4}$, we can replace the first condition of Theorem 13 with $AB \ge x^{5/3+\varepsilon}$.

4.3. The Sato–Tate Conjecture on Average

We now use Theorem 12 to obtain a generalization of (8) and (9). Recall that the Sato–Tate density $\mu_{\mathrm{ST}}(\alpha,\beta)$ is given by (7).

THEOREM 14. *Suppose $f(T), g(T) \in \mathbb{Z}[T]$ are not powers of another polynomial over $\mathbb{Q}$. Assume that positive integers A and B are such that, for some $\varepsilon > 0$,*

$$\max\{AB^{1/2}, A^{1/2}B\} \ge x^{1+\varepsilon} \quad \textit{and} \quad \min\{A,B\} \ge x^{1/2+\varepsilon}.$$

Then, for all real numbers $0 \le \alpha < \beta \le \pi$, we have

$$\frac{1}{4AB}\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{ST}}_{f(a),g(b)}(\alpha,\beta;x) = (\mu_{\mathrm{ST}}(\alpha,\beta)+O(x^{-\delta}))\pi(x),$$

where $\delta > 0$ depends only on ε.

Proof. In the notation of Sections 3.1 and 3.2, we have

$$\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{ST}}_{f(a),g(b)}(\alpha,\beta;x) = \sum_{p\le x}M_p(\mathcal{T}_p(\alpha,\beta),A,B).$$

Assume that $A \ge B$. Now from Theorem 12 applied with $\mathcal{S} = \mathcal{T}_p(\alpha,\beta)$ (thus $\vartheta = 0$, so we can also use (20)), we derive

$$\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{ST}}_{f(a),g(b)}(\alpha,\beta;x) - 4AB\sum_{p\le x}\frac{\mathcal{T}_p(\alpha,\beta)}{(p-1)^2} \le (ABx^{1/2} + AB^{1/2}x + Ax^{3/2} + Bx^{3/2} + B^{1/2}x^2)x^{o(1)}$$

as $x \to \infty$. Since $A \ge B$, this expression can be simplified to read

$$\sum_{|a|\le A}\sum_{|b|\le B}\Pi^{\mathrm{ST}}_{f(a),g(b)}(\alpha,\beta;x) - 4AB\sum_{p\le x}\frac{\mathcal{T}_p(\alpha,\beta)}{(p-1)^2} \le (ABx^{1/2} + AB^{1/2}x + Ax^{3/2} + B^{1/2}x^2)x^{o(1)}.$$

Now using Lemma 8 (which contributes $ABx^{3/4+o(1)}$ to the error term and thus dominates the term $ABx^{1/2+o(1)}$), we obtain

$$\begin{aligned}\sum_{|a|\le A}\sum_{|b|\le B}&\Pi^{\mathrm{ST}}_{f(a),g(b)}(\alpha,\beta;x) - 4\mu_{\mathrm{ST}}(\alpha,\beta)AB\pi(x)\\ &\le (ABx^{3/4} + AB^{1/2}x + Ax^{3/2} + B^{1/2}x^2)x^{o(1)}\\ &= ABx^{1+o(1)}(x^{-1/4} + B^{-1/2} + B^{-1}x^{1/2} + A^{-1}B^{-1/2}x).\end{aligned}$$

Some simple calculations now yield the desired result in the case $A \ge B$.

In the case $A < B$, the proof is completely analogous. □

Since $\max\{AB^{1/2}, A^{1/2}B\} \ge (AB)^{3/4}$, we can replace the first condition of Theorem 14 with $AB \ge x^{4/3+\varepsilon}$.

Finally, from Lemma 11 we immediately obtain the following result for 1-parametric families of elliptic curves.

THEOREM 15. *Suppose $f(T), g(T) \in \mathbb{Z}[T]$ are such that $4f(T)^3 + 27g(T)^2$ is not identical to zero. Assume that a positive integer A is such that, for some $\varepsilon > 0$,*

$$A \ge x^{1/2+\varepsilon}.$$

Then, for all real numbers $0 \le \alpha < \beta \le \pi$ we have

$$\frac{1}{2A}\sum_{|a|\le A}\Pi^{\mathrm{ST}}_{f(a),g(a)}(\alpha,\beta;x) = (\mu_{\mathrm{ST}}(\alpha,\beta) + O(x^{-\delta}))\pi(x),$$

where $\delta > 0$ depends only on ε.

5. Comments

We remark that Theorem 15 may seem to imply Theorem 14 (i.e., for every b with $|b| \le B$ one could attempt to apply Theorem 15 to the corresponding family of curves). However, this is not the case because of the uniformity issue with respect to b. Note that Theorem 14 is just an example of several similar results that hold under the same conditions on A and B and describe the distribution of curves with special properties. As in [5; 6], these properties may include cyclicity, primality, or divisibility of $\#E_{f(a),g(b)}(\mathbb{F}_p)$ by a given integer. That being said, it is not clear how to obtain analogues of Theorem 15 for such questions.

ACKNOWLEDGMENTS. The author would like to thank Stephan Baier for very interesting discussions and for the observation that the argument of his work [3] may allow us to obtain a version of Theorem 13 in a wide range of uniformity with respect to the parameter t.

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] S. Baier, *The Lang–Trotter conjecture on average,* J. Ramanujan Math. Soc. 22 (2007), 299–314.

[3] ———, *A remark on the Lang–Trotter conjecture,* New directions in the theory of universal zeta- and L-functions (Würzburg, 2008), Ber. Math., pp. 11–18, Shaker, Aachen, 2009.

[4] S. Baier and L. Zhao, *The Sato–Tate conjecture on average for small angles,* Trans. Amer. Math. Soc. 361 (2009), 1811–1832.

[5] A. Balog, A. Cojocaru, and C. David, *Average twin prime conjecture for elliptic curves,* Amer. J. Math. 133 (2011), 1179–1229.

[6] W. D. Banks and I. E. Shparlinski, *Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height,* Israel J. Math. 173 (2009), 253–277.

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

[8] 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.

[9] A. Cojocaru and C. Hall, *Uniform results for Serre's theorem for elliptic curves,* Int. Math. Res. Not. 50 (2005), 3065–3080.

[10] A. Cojocaru and I. E. Shparlinski, *Distribution of Farey fractions in residue classes and Lang–Trotter conjectures on average,* Proc. Amer. Math. Soc. 136 (2008), 1977–1986.

[11] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves,* Internat. Math. Res. Notices 1999 (1999), 165–183.

[12] ———, *Average Frobenius distribution for inerts in* $\mathbb{Q}(i)$, J. Ramanujan Math. Soc. 19 (2004), 181–201.

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

[14] ———, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. 89 (1987), 561–567.

[15] ———, *Distribution of supersingular primes,* Journées arithmétiques (Luminy, 1989), Astérisque (1992), 127–132.

[16] B. Fisher, *Equidistribution theorems (d'après P. Deligne et N. Katz),* Columbia University number theory seminar (New York, 1992), Astérisque 228 (1995), 69–79.

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

[18] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers,* Oxford Univ. Press, Oxford, 1979.

[19] H. Iwaniec and E. Kowalski, *Analytic number theory,* Amer. Math. Soc. Colloq. Publ., 53, Amer. Math. Soc., Providence, RI, 2004.

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

[21] K. James and G. Yu, *Average Frobenius distribution of elliptic curves,* Acta Arith. 124 (2006), 79–100.
[22] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups,* Ann. of Math. Stud., 116, Princeton Univ. Press, Princeton, NJ, 1988.
[23] H. W. Lenstra, *Factoring integers with elliptic curves,* Ann. of Math. (2) 126 (1987), 649–673.
[24] P. Michel, *Le rang de familles de variétés abéliennes,* J. Algebraic Geom. 6 (1997), 201–234.
[25] S. J. Miller and M. R. Murty, *Effective equidistribution and the Sato–Tate law for families of elliptic curves,* J. Number Theory 131 (2011), 25–44.
[26] M. R. Murty, V. K. Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem,* Amer. J. Math. 110 (1998), 253–281.
[27] V. K. Murty, *On the Sato–Tate conjecture,* Number theory related to Fermat's last theorem (Cambridge, MA, 1981), Progr. Math., 26, pp. 195–205, Birkhäuser, Boston, 1982.
[28] ———, *Explicit formulae and the Lang–Trotter conjecture,* Rocky Mountain J. Math. 15 (1985), 535–551.
[29] ———, *Modular forms and the Chebotarev density theorem, II,* Analytic number theory (Kyoto, 1996), London Math. Soc. Lecture Note Ser., 247, pp. 287–308, Cambridge Univ. Press, Cambridge, 1997.
[30] V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields,* C. R. Acad. Sci. Paris Sér. I Math. 319 (1994), 523–528.
[31] H. Niederreiter, *The distribution of values of Kloosterman sums,* Arch. Math. (Basel) 56 (1991), 270–277.
[32] J.-P. Serre, *Queques applications du théorème de densité de Chebotarev,* Inst. Hautes Études Sci. Publ. Math. 54 (1981), 123–201.
[33] I. E. Shparlinski, *Exponents of modular reductions of families of elliptic curves,* Rev. Un. Mat. Argentina 50 (2009), 69–74.
[34] ———, *On the Sato–Tate conjecture on average for some families of elliptic curves,* Forum Math. 25 (2013), 647–664.
[35] J. H. Silverman, *The arithmetic of elliptic curves,* Springer-Verlag, Berlin, 1995.
[36] R. Taylor, *Automorphy for some l-adic lifts of automorphic* mod l *Galois representations, II,* Publ. Math. Inst. Hautes Études Sci. 108 (2008), 183–239.
[37] D. Q. Wan, *On the Lang–Trotter conjecture,* J. Number Theory 35 (1990), 247–268.

Department of Computing
Macquarie University
Sydney, NSW 2109
Australia

igor.shparlinski@mq.edu.au