LANG–TROTTER AND SATO–TATE DISTRIBUTIONS IN SINGLE AND DOUBLE PARAMETRIC FAMILIES OF ELLIPTIC CURVES

MIN SHA AND IGOR E. SHPARLINSKI

Abstract. We obtain new results concerning the Lang–Trotter conjectures on Frobenius traces and Frobenius fields over single and double parametric families of elliptic curves. We also obtain similar results with respect to the Sato–Tate conjecture. In particular, we improve a result of A. C. Cojocaru and the second author (2008) towards the Lang–Trotter conjecture on average for polynomially parameterized families of elliptic curves when the parameter runs through a set of rational numbers of bounded height. Some of the families we consider are much thinner than the ones previously studied.

1. Introduction

1.1. **Background and motivation.** For polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfying

$$\Delta(Z) \neq 0 \qquad \text{and} \qquad j(Z) \notin \mathbb{Q}, \tag{1}$$

where

$$\Delta(Z) = -16(4f(Z)^3 + 27g(Z)^2) \quad \text{and} \quad j(Z) = \frac{-1728(4f(Z))^3}{\Delta(Z)}$$

are the *discriminant* and *j-invariant* respectively, we consider the elliptic curve

$$E(Z): \quad Y^2 = X^3 + f(Z)X + g(Z) \tag{2}$$

over the function field $\mathbb{Q}(Z)$. For a general background on elliptic curves we refer to [31].

Here we are interested in studying the specialisations $E(t)$ of these curves on average over the parameter t running through some interesting sets of integers or rational numbers. More precisely, motivated by the Lang–Trotter and Sato–Tate conjectures we study the distributions of Frobenius traces, Frobenius fields and Frobenius angles of

2010 *Mathematics Subject Classification.* 11B57, 11G05, 11G20, 14H52.

Key words and phrases. Lang–Trotter conjecture, Sato–Tate conjecture, parametric families of elliptic curves.

the reductions of $E(t)$ modulo consecutive primes $p \le x$ for a growing parameter x, respectively.

Let us first introduce some standard notation.

Given an elliptic curve E over $\mathbb{Q}$ we denote by E_p the reduction of E modulo p. In particular, we use $E_p(\mathbb{F}_p)$ to denote the group of $\mathbb{F}_p$-rational points on E_p, where $\mathbb{F}_p$ is the finite field of p elements. We always assume that the elements of $\mathbb{F}_p$ are represented by the set $\{0, \ldots, p-1\}$ and thus we switch freely between the equations in $\mathbb{F}_p$ and congruences modulo p.

For $a \in \mathbb{Z}$, we use $\pi_E(a; x)$ to denote the number of primes $p \le x$ which do not divide the conductor N_E of E and such that

$$a_p(E) = a,$$

where

$$a_p(E) = p + 1 - \#E_p(\mathbb{F}_p)$$

is the so-called *Frobenius trace* of E_p. We also set $a_p(E) = 0$ for $p \mid N_E$.

For a fixed imaginary quadratic field $\mathbb{K}$, we denote by $\pi_E(\mathbb{K}; x)$ the number of primes $p \le x$ with $p \nmid N_E$ and such that

$$a_p(E) \ne 0 \qquad \text{and} \qquad \mathbb{Q}\left(\sqrt{a_p(E)^2 - 4p}\right) = \mathbb{K},$$

where $\mathbb{Q}(\sqrt{a_p(E)^2 - 4p})$ is the so-called *Frobenius field* of E with respect to p.

Two celebrated Lang–Trotter conjectures [21] assert that if E is without complex multiplication (CM), then

$$\pi_E(a; x) \sim c(E, a)\frac{\sqrt{x}}{\log x}$$

as $x \to \infty$, for some constant $c(E, a) \ge 0$ depending only on E and a; if E is without complex multiplication, then

$$\pi_E(\mathbb{K}; x) \sim C(E, \mathbb{K})\frac{\sqrt{x}}{\log x}$$

as $x \to \infty$, for some constant $C(E, \mathbb{K}) \ge 0$ depending only on E and $\mathbb{K}$.

However, the situation is quite different when E has complex multiplication. For example, Deuring [16] has showed that if E has complex multiplication, then

$$\pi_E(0; x) \sim \frac{1}{2} \cdot \frac{x}{\log x}. \tag{3}$$

Besides, it is well-known that if E is with complex multiplication, for any prime $p \nmid N_E$, we have

$$\mathbb{Q}\left(\sqrt{a_p(E)^2 - 4p}\right) \simeq \mathrm{End}_{\bar{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q},$$

where $\mathrm{End}_{\bar{\mathbb{Q}}}(E)$ stands for the endomorphism ring of E; but if E is without complex multiplication, there are infinitely many distinct such Frobenius fields as prime $p \nmid N_E$ varies.

Despite a series of interesting (conditional and unconditional) recent achievements, see [9, 10, 12, 14, 27, 30] for surveys and some recent results, these conjectures are widely open.

In addition, by Hasse's bound, see [31], we can define the *Frobenius angle* $\psi_p(E) \in [0, \pi]$ via the identity

$$\cos \psi_p(E) = \frac{a_p(E)}{2\sqrt{p}}. \tag{4}$$

For real numbers $0 \le \alpha < \beta \le \pi$, we define the *Sato–Tate density*

$$\mu_{\mathrm{ST}}(\alpha, \beta) = \frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 \vartheta \, d\vartheta = \frac{2}{\pi} \int_{\cos \beta}^{\cos \alpha} (1 - z^2)^{1/2} \, dz. \tag{5}$$

We denote by $\pi_E(\alpha, \beta; x)$ the number of primes $p \le x$ (with $p \nmid N_E$) for which $\psi_p(E) \in [\alpha, \beta]$. The *Sato–Tate conjecture*, that has recently been settled in the series of works of Barnet-Lamb, Geraghty, Harris, and Taylor [7], Clozel, Harris and Taylor [8], Harris, Shepherd-Barron and Taylor [19], and Taylor [32], asserts that if E is not a CM curve, then

$$\pi_E(\alpha, \beta; x) \sim \mu_{\mathrm{ST}}(\alpha, \beta) \cdot \frac{x}{\log x} \tag{6}$$

as $x \to \infty$. However, if E is a CM curve, Deuring's result (3) says that for half of primes p, the Frobenius angle $\psi_p(E) = \pi$.

So, due to the lack of conclusive results towards the Lang–Trotter conjectures, and also the lack of an explicit error term in the asymptotic formula (6), it makes sense to study $\pi_E(a; x)$, $\pi_E(\mathbb{K}; x)$ and $\pi_E(\alpha, \beta; x)$ on average over some natural families of elliptic curves.

Here we continue this line of research and in particular introduce new natural families of curves, which are sometimes much *thinner* than the ones previously studied in the literature. We note that the thinner the family the better the corresponding result approximates the ultimate goal of obtaining precise estimates for individual curves.

1.2. **Previously known results.** The idea of studying the properties of reduction E_p for $p \le x$ on average over a family of curves E is due to Fouvry and Murty [17], who have considered the average value of $\pi_E(0;x)$ and proved the Lang–Trotter conjecture on average for the family of curves

$$E_{u,v}: \ Y^2 = X^3 + uX + v, \tag{7}$$

where the integers u and v satisfy the inequalities $|u| \le U$, $|v| \le V$. The results of [17] is nontrivial provided that

$$\min\{U, V\} > x^{1/2+\varepsilon} \qquad \text{and} \qquad UV > x^{3/2+\varepsilon} \tag{8}$$

for some fixed positive $\varepsilon > 0$, then, on average, the Lang–Trotter conjecture holds for such curves. Note that the case of $\pi_E(0;x)$ corresponds to the distribution of so-called *supersingular primes*. David and Pappalardi [13], have extended the result of [17] to $\pi_E(a;x)$ with an arbitrary $a \in \mathbb{Z}$, however under a more restrictive condition on U and V than that given by (8), namely for $\min\{U, V\} > x^{1+\varepsilon}$. Finally, Baier [2] gives a full analogue of the result of [17] for any $a \in \mathbb{Z}$ and under the same restriction (8); later Baier [3] also replaces (8) by the following condition

$$\min\{U, V\} > (\log x)^{60+\varepsilon} \quad \text{and} \quad x^{3/2}(\log x)^{10+\varepsilon} < UV < \exp(x^{1/8-\varepsilon})$$

when $a \ne 0$. See also [4] for a refined version of the Lang–Trotter conjecture related to Frobenius traces with a uniform error term.

The Sato–Tate conjecture on average has also been studied for the family (7), see [5, 6]. In particular, Banks and Shparlinski [6] have shown that using bounds of multiplicative character sums and the large sieve inequality (instead of the exponential sum technique employed in [17]), one can study the Sato–Tate conjecture in a much wider range of U and V than that given by (8). Namely, the results of [6] are nontrivial when

$$UV \ge x^{1+\varepsilon} \qquad \text{and} \qquad \min\{U, V\} \ge x^{\varepsilon} \tag{9}$$

for some fixed positive $\varepsilon > 0$, and the Sato–Tate conjecture is true on average for this family of elliptic curves. The technique of [6] has been used in several other problems such as primality or distribution of values of $\#E_{u,v}(\mathbb{F}_p)$ in the domain, which is similar to (9), see [10, 15, 28].

Results towards the Lang–Trotter and Sato–Tate conjectures for more general families of the form $Y^2 = X^3 + f(u)X + g(v)$ with polynomials f, g and integers $|u| \le U$, $|v| \le V$, are given in [29]. Particularly, the conjectures are valid on average for these polynomial families of elliptic curves with restrictions on U and V.

Furthermore, Cojocaru and Hall [11] have considered the family of curves (2) and obtained an upper bound on the average value of $\pi_{E(t)}(a;x)$ for the parameter t that runs through the set of rational numbers

$$\mathcal{F}(T) = \{u/v \in \mathbb{Q} \ : \ \gcd(u,v) = 1, \ 1 \le u, v \le T\},$$

of height at most T. For the size of $\mathcal{F}(T)$, it is well known that

$$\#\mathcal{F}(T) \sim \frac{6}{\pi^2} T^2. \tag{10}$$

as $T \to \infty$, see [18, Theorem 331]. We recall that the set $\mathcal{F}(T) \cap [0,1]$ is the well-known set of *Farey fractions*.

Cojocaru and Shparlinski [12] have improved [11, Theorem 1.4] and obtained a similar bound for the average value of $\pi_{E(t)}(a;x)$. Namely, by [12, Theorem 2], if the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then, for any integer a, we have

$$\sum_{\substack{t \in \mathcal{F}(T) \\ \Delta(t) \ne 0}} \pi_{E(t)}(a;x) \ll Tx^{3/2+o(1)} + \begin{cases} T^2 x^{3/4} & \text{if } a \ne 0, \\ T^2 x^{2/3} & \text{if } a = 0; \end{cases} \tag{11}$$

and moreover for any imaginary quadratic field $\mathbb{K}$,

$$\sum_{\substack{t \in \mathcal{F}(T) \\ \Delta(t) \ne 0}} \pi_{E(t)}(\mathbb{K};x) \ll Tx^{3/2+o(1)} + T^2 x^{2/3}. \tag{12}$$

Here we use the Landau symbols O and o and the Vinogradov symbol $\ll$. We recall that the assertions $A = O(B)$ and $A \ll B$ are both equivalent to the inequality $|A| \le cB$ with some absolute constant c, while $A = o(B)$ means that $A/B \to 0$. We also use the asymptotic notation $\sim$. Throughout the paper the implied constants may depend on the polynomials $f(Z)$ and $g(Z)$ in (2).

1.3. **General outline of our results.** In this paper, we consider the Lang–Trotter and Sato–Tate conjectures on average for the polynomial family (2) of elliptic curves when the variable Z runs through sets of several different types. More precisely, given a large positive parameter T, we consider the case when Z runs through $\mathcal{F}(T)$ or a much "thinner" set of T consecutive integers, that is,

$$\mathcal{I}(T) = \{1, \ldots, T\}.$$

We believe that these are the first known results that involve one parametric family of curves, precisely with a parameter running through an interval of consecutive integers (note that $\mathcal{F}(T)$ has the structure and properties of a two parametric set).

Furthermore, we also consider the case when Z runs through the sums $u+v$ (taken with multiplicities) over all pairs $(u,v) \in \mathcal{U} \times \mathcal{V}$ for two subsets $\mathcal{U}, \mathcal{V} \in \mathcal{I}(T)$; to the best of our knowledge, results in these settings, with arbitrary non-empty sets $\mathcal{U}$ and $\mathcal{V}$, are completely new as well.

To derive our results we introduce several new ideas, such as using a result of Michel [23, Proposition 1.1] in a combination with a technique of Niederreiter [25, Lemma 3]. We also obtain several other results of independent interest such as estimates of Section 2.3 for the number of solutions of some congruences and equations with elements of $\mathcal{F}(T)$.

We start with an improvement and generalisation of the bound (11), and in fact give a proof that is simpler than that of (11). More precisely, for an elliptic curve E over $\mathbb{Q}$ and a sequence of integers $\mathfrak{A} = \{a_p\}$, supported on primes p, we define $\pi_E(\mathfrak{A}; x)$ as the number of primes $p \le x$ which do not divide the conductor N_E of E and such that

$$a_p(E) = a_p.$$

We say that $\mathfrak{A}$ is the *zero sequence* if $a_p = 0$ for every p, and $\mathfrak{A}$ is a *constant sequence* if all a_p equal to the same integer. Note that if $a_p = a$ for all p, that is, $\mathfrak{A}$ is a constant sequence, then $\pi_E(\mathfrak{A}; x) = \pi_E(a; x)$. Here, one of the interesting choices of the sequence $\mathfrak{A}$ is with

$$a_p = -\left\lfloor 2p^{1/2} \right\rfloor,$$

corresponding to curves with the largest possible number of $\mathbb{F}_p$-rational points.

1.4. **Formulations of our results.** We are now able to give exact formulations of our results.

Theorem 1. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any sequence of integers $\mathfrak{A} = \{a_p\}$, we have*

$$\sum_{\substack{t \in \mathcal{F}(T) \\ \Delta(t) \ne 0}} \pi_{E(t)}(\mathfrak{A}; x) \ll \begin{cases} Tx^{11/8+o(1)} + T^2 x^{7/8} & \text{for any } \mathfrak{A}, \\ Tx^{4/3+o(1)} + T^2 x^{5/6} & \text{if } \mathfrak{A} \text{ is the zero sequence.} \end{cases}$$

The proof of Theorem 1 is based on a simple idea using the Cauchy inequality and then estimating the second moment of the quantity of $R_{T,p}(w)$ (see Section 2.1) via a result of Ayyad, Cochrane and Zheng [1, Theorem 1]. This gives a stronger result than the approach of [12] which is based on deriving an asymptotic formula for the average deviation of $R_{T,p}(w)$ from its expected value (which also requires to use the inclusion-exclusion formula).

Comparing this with (11), we can see that if $a \neq 0$ Theorem 1 improves (11) and remains nontrivial when $x^{3/8+\varepsilon} \leq T \leq x^{5/8-\varepsilon}$ for small $\varepsilon > 0$. If $a = 0$ the same holds for $x^{1/3+\varepsilon} \leq T \leq x^{2/3-\varepsilon}$. Furthermore, we note that (11) is nontrivial only when $T \geq x^{1/2+\varepsilon}$, because the trivial upper bound is $O(T^2x)$.

We then consider the very interesting and natural special case of polynomials

$$f(Z) = 3Z(1728 - Z) \qquad \text{and} \qquad g(Z) = 2Z(1728 - Z)^2 \tag{13}$$

for which one can verify that $j(Z) = Z$. Thus for each specialisation $t \neq 0, 1728$, the j-invariant of the curve $E(t)$ equals t. For this special case, we obtain a better bound than that of Theorem 1.

Theorem 2. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ are given by (13), then for any sequence of integers $\mathfrak{A} = \{a_p\}$, we have*

$$\sum_{\substack{t \in \mathcal{F}(T) \\ \Delta(t) \neq 0}} \pi_{E(t)}(\mathfrak{A}; x) \ll Tx^{5/4+o(1)} + T^2x^{3/4+o(1)}.$$

We also get a non-trivial upper bound for the sum of $\pi_{E(r+s)}(\mathfrak{A}; x)$, where r and s run over $\mathcal{F}(T)$ and $x^{1/4+\varepsilon} \leq T \leq x^{1-\varepsilon}$ for small $\varepsilon > 0$.

Theorem 3. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1). Then for any sequence of integers $\mathfrak{A} = \{a_p\}$, we have*

$$\sum_{\substack{r,s \in \mathcal{F}(T) \\ \Delta(r+s) \neq 0}} \pi_{E(r+s)}(\mathfrak{A}; x) \ll T^5 + T^3x^{5/4+o(1)} + T^4x^{3/4+o(1)}.$$

Now, we state a new result concerning the Lang-Trotter conjecture involving Frobenius fields.

Theorem 4. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any imaginary quadratic field $\mathbb{K}$, we have*

$$\sum_{\substack{t \in \mathcal{F}(T) \\ \Delta(t) \neq 0}} \pi_{E(t)}(\mathbb{K}; x) \ll Tx^{4/3+o(1)} + T^2x^{5/6}.$$

Comparing this with (12), we can see that Theorem 4 improves (12) and remains nontrivial when $x^{1/3+\varepsilon} \leq T \leq x^{2/3-\varepsilon}$ for small $\varepsilon > 0$.

The following result is the first study on the sum of $\pi_{E(r+s)}(\mathbb{K}; x)$ when r and s run over $\mathcal{F}(T)$. Since the trivial bound is T^4x, this result is nontrivial when $T \geq x^{1/6+\varepsilon}$ for any $\varepsilon > 0$.

Theorem 5. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1). Then for any imaginary quadratic field $\mathbb{K}$, we have*

$$\sum_{\substack{r,s \in \mathcal{F}(T) \\ \Delta(r+s) \neq 0}} \pi_{E(r+s)}(\mathbb{K}; x) \ll T^4 x^{5/6} + T^{2+o(1)} x^{4/3}.$$

Unfortunately, currently there are no asymptotic formulas for the average value of $\pi_{E(t)}(\alpha, \beta; x)$ (which is relevant to the Sato–Tate conjecture) when the parameter t runs through $\mathcal{F}(T)$. In particular the arguments in the proof of Lemma 19 are not strong enough for this.

Here, we consider this problem in another direction. As usual, we use $\pi(x)$ to denote the number of primes $p \le x$.

Theorem 6. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), and for some $\varepsilon > 0$,*

$$x^{1/4+\varepsilon} \le T \le x^{1-\varepsilon}.$$

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

$$\frac{1}{(\#\mathcal{F}(T))^2} \sum_{\substack{r,s \in \mathcal{F}(T) \\ \Delta(r+s) \neq 0}} \pi_{E(r+s)}(\alpha, \beta; x) = (\mu_{\mathtt{ST}}(\alpha, \beta) + O(x^{-\delta}))\pi(x),$$

with arbitrary real δ satisfying $0 < \delta < \min\{\varepsilon, 1/4\}$.

Note that in Theorem 6 it can be easy to drop the condition $T \le x^{1-\varepsilon}$ and obtain a version of Theorem 6 under just one natural restriction $T \ge x^{1/4+\varepsilon}$. Since small values of T are of our primal interest, we have not attempted to do this.

We now recall that the common feature of the approaches of both [6] and [17] is that they need two independently varying parameters u and v. This has been a part of the motivation for Cojocaru and Hall [11] and Cojocaru and Shparlinski [12] to consider the family of curves (2). However, even this family cannot be considered as a truly single parametric family of curves, because the simple exclusion-inclusion principle reduces a problem with the parameter $t \in \mathcal{F}(T)$ to a series of problems with $t = u/v$, where u and v run independently through some intervals of consecutive integers.

To overcome this drawback, in [29], the family of curves (2) has been studied for specialisations t from the set

$$\mathcal{I}(T) = \{1, \ldots, T\} \tag{14}$$

of T consecutive integers. In particular, in [29, Theorem 15], an asymptotic formula is given for the average value of $\pi_{E(t)}(\alpha, \beta; x)$ over $t \in \mathcal{I}(T)$, provided that $T \ge x^{1/2+\varepsilon}$, thus providing yet another form of

the Sato–Tate conjecture on average. This result is a first example of averaging over a single parametric family of curves. The proof of [29, Theorem 15], amongst other things, is based on a result of Michel [23]. We note that unfortunately in [29, Lemma 9] a wrong reference is given, a correct one is [23, Proposition 1.1]. Here we use a similar approach to estimate the average value of $\pi_{E(t)}(\mathfrak{A}; x)$ over $t \in \mathcal{I}(T)$, that is, also for a single parametric family of curves, which is related to the Lang–Trotter conjecture.

Theorem 7. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any sequence of integers $\mathfrak{A} = \{a_p\}$, we have*

$$\sum_{\substack{t \in \mathcal{I}(T) \\ \Delta(t) \neq 0}} \pi_{E(t)}(\mathfrak{A}; x) \ll T^2 + T^{1/2} x^{5/4+o(1)}.$$

In Theorem 7, since the trivial upper bound is Tx, when $x^{1/2+\varepsilon} < T < x^{1-\varepsilon}$ for small $\varepsilon > 0$ the result is nontrivial. We also have an analogue of Theorem 7 over sum-sets.

Theorem 8. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any sequence of integers $\mathfrak{A} = \{a_p\}$ and sets of integer $\mathcal{U}, \mathcal{V} \subseteq \mathcal{I}(T)$, we have*

$$\sum_{\substack{u \in \mathcal{U}, v \in \mathcal{V} \\ \Delta(u+v) \neq 0}} \pi_{E(u+v)}(\mathfrak{A}; x) \ll T \#\mathcal{U} \#\mathcal{V} + (\#\mathcal{U} \#\mathcal{V})^{3/4} x^{5/4}.$$

As the above, in Theorem 8 the trivial upper bound is $\#\mathcal{U}\#\mathcal{V}x$, so the result is nontrivial when $T < x^{1-\varepsilon}$ and $\#\mathcal{U}\#\mathcal{V} > x^{1+\varepsilon}$ for small $\varepsilon > 0$, which implies that $T > x^{(1+\varepsilon)/2}$.

For the Lang–Trotter conjecture related to Frobenius fields, we get the following result when the parameter runs through $\mathcal{I}(T)$. The result is nontrivial when $T > x^{2/3+\varepsilon}$ for any $\varepsilon > 0$.

Theorem 9. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any imaginary quadratic field $\mathbb{K}$, we have*

$$\sum_{\substack{t \in \mathcal{I}(T) \\ \Delta(t) \neq 0}} \pi_{E(t)}(\mathbb{K}; x) \ll T^{1/2} x^{4/3} + T x^{5/6}.$$

We want to remark that since for any non-negative valued function $h(X)$, we have

$$\sum_{r,s \in \mathcal{I}(T)} h(r+s) \leq T \sum_{t \in \mathcal{I}(2T)} h(t),$$

Theorem 9 implies the following upper bound

$$\sum_{\substack{r,s\in\mathcal{I}(T)\\ \Delta(r+s)\neq 0}} \pi_{E(r+s)}(\mathbb{K};x) \ll T^{3/2}x^{4/3} + T^2x^{5/6}.$$

As mentioned before, in [29, Theorem 15], an asymptotic formula is given for the average value of $\pi_{E(t)}(\alpha,\beta;x)$ over $t \in \mathcal{I}(T)$. Here, we derive an analogue for the average value of $\pi_{E(u+v)}(\alpha,\beta;x)$, where u, v run through two subsets $\mathcal{U}, \mathcal{V}$, respectively.

Theorem 10. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), and non-empty sets of integer $\mathcal{U}, \mathcal{V} \subseteq \mathcal{I}(T)$ are such that, for some $\varepsilon > 0$,*

$$\#\mathcal{U}\#\mathcal{V} \geq x^{1+\varepsilon} \qquad \text{and} \qquad T \leq x^{1-\varepsilon}.$$

Then for any real numbers $0 \leq \alpha < \beta \leq \pi$, we have

$$\frac{1}{\#\mathcal{U}\#\mathcal{V}} \sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\neq 0}} \pi_{E(u+v)}(\alpha,\beta;x) = \left(\mu_{\mathrm{ST}}(\alpha,\beta) + O\left(x^{-\varepsilon/4}\right)\right)\pi(x).$$

Note that in Theorem 10, since $T^2 \geq \#\mathcal{U}\#\mathcal{V} \geq x^{1+\varepsilon}$, we have $T \geq x^{(1+\varepsilon)/2}$.

We remark that in this paper we often replace summation over primes by summation over all integers. Thus some terms in the above bounds can be improved by a small power of $\log x$.

2. Preliminaries

2.1. **Notation and general remarks.** Throughout the paper, p always denotes a prime number. For $t \in \mathbb{Q}$, let $N(t)$ denote the conductor of the specialisation of $E(Z)$ at $Z = t$. We always consider rational numbers in the form of irreducible fractions.

Note that for $t \in \mathbb{Q}$, $\Delta(t)$ may be a rational number. However, we know that the elliptic curve $E(t)$ has good reduction at prime p if and only if p does not divide both the numerator and denominator of $\Delta(t)$; see [31, Chapter VII, Proposition 5.1 (a)]. So, we can say that for any prime p, $p \nmid N(t)$ (that is, $E(t)$ has good reduction at p) if and only if $\Delta(t) \not\equiv 0 \pmod p$ (certainly, it first requires that p does not divide the denominator of $\Delta(t)$).

We define

$$P_{\mathcal{F}} = \#\{p \text{ prime} : \exists\, u/v \in \mathbb{Q}, p \mid v, p \nmid N(u/v)\}. \tag{15}$$

Since $p \nmid N(u/v)$, we have $\Delta(u/v) \not\equiv 0 \pmod p$, which requires that p does not divide the denominator of $\Delta(u/v)$. Noticing the form of

$\Delta(u/v)$ and $p \mid v$, we can see that $P_{\mathcal{F}}$ is upper bounded by a constant which only depends on the polynomials $f(Z), g(Z)$. For example, if $\deg f > \deg g$, then $P_{\mathcal{F}}$ is not greater than the number of prime divisors of $2a_f$, where a_f is the leading coefficient of $f(Z)$, because such a prime p must divide $2a_f$.

For an integer w, we denote by $R_{T,p}(w)$ the number of fractions $u/v \in \mathcal{F}(T)$ with $\gcd(v,p) = 1$ and $u/v \equiv w \pmod p$. In particular, we immediately derive the inequality

$$\sum_{\substack{t \in \mathcal{F}(T) \\ \Delta(t) \neq 0}} \pi_{E(t)}(\mathfrak{A}; x) \le P_{\mathcal{F}} T^2 + \sum_{\substack{t = u/v \in \mathcal{F}(T) \\ \Delta(t) \neq 0}} \sum_{\substack{p \le x \\ p \nmid v, p \nmid N(t) \\ a_{t,p} = a_p}} 1 \le P_{\mathcal{F}} T^2 + \sum_{p \le x} \sum_{\substack{0 \le w \le p-1 \\ \Delta(w) \not\equiv 0 \pmod p \\ a_{w,p} = a_p}} R_{T,p}(w), \tag{16}$$

where to simplify the notation we denote

$$a_{w,p} = a_p(E(w)). \tag{17}$$

We want to indicate that the treatment in (16) is an improvement of the inequality used in [12, Section 3.2] (at the bottom of [12, Page 1982]), however this does not affect the final result of [12, Theorem 2].

2.2. **Some congruences with traces.** The following estimate follows immediately from (16).

Lemma 11. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any sequence of integers $\mathfrak{A} = \{a_p\}$ and prime ℓ, we have*

$$\sum_{\substack{t \in \mathcal{F}(T) \\ \Delta(t) \neq 0}} \pi_{E(t)}(\mathfrak{A}; x) \le P_{\mathcal{F}} T^2 + \sum_{p \le x} \sum_{\substack{0 \le w \le p-1 \\ \Delta(w) \not\equiv 0 \pmod p \\ a_{w,p} \equiv a_p \pmod \ell}} R_{T,p}(w).$$

Next we need the following two bounds that have been obtained in the proof of [12, Theorem 2] (see the middle and the bottom of [12, Page 1983], and [12, Equation (8)] respectively) from an effective version of the *Chebotarev theorem* given by Murty and Scherk [24, Theorem 2], see also [11, Theorem 1.2].

Lemma 12. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any integer a and prime $\ell \ge 17$ and $\ell \neq p$, we have*

$$\sum_{\substack{0 \le w \le p-1 \\ \Delta(w) \not\equiv 0 \pmod p \\ a_{w,p} \equiv a \pmod \ell}} 1 = \frac{p}{\ell} + \begin{cases} O(\ell p^{1/2}) & \text{if } a \neq 0, \\ O(\ell^{1/2} p^{1/2}) & \text{if } a = 0, \end{cases}$$

where the implied constants are independent of a, p and ℓ.

Lemma 13. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any prime $\ell \geq 17$ and $\ell \neq p$, and any imaginary quadratic field $\mathbb{K}$, we have*

$$\sum_{\substack{0 \leq w \leq p-1 \\ \Delta(w) \not\equiv 0 \pmod p \\ a_{w,p} \not\equiv 0 \pmod p \\ \mathbb{Q}(\sqrt{a_{w,p}^2 - 4p}) = \mathbb{K}}} 1 = \frac{p}{\ell} + O(\ell^{1/2} p^{1/2}),$$

where the implied constants are independent of $\mathbb{K}$, p and ℓ.

2.3. **Some congruences with elements of $\mathcal{F}(T)$.** We first prove the following estimate on the average multiplicity of values in the reduction of $\mathcal{F}(T)$ modulo p, which is used several times later on.

Lemma 14. *For any prime p, define*

$$Q_{T,p} = \#\{(u_1/v_1, u_2/v_2) \in \mathcal{F}(T) \times \mathcal{F}(T) : \gcd(v_1 v_2, p) = 1, \\ u_1/v_1 \equiv u_2/v_2 \pmod p\}.$$

Then, we have

$$Q_{T,p} \ll T^4/p + T^2 (\log p)^2 = T^4/p + T^2 p^{o(1)},$$

where the implied constant is independent of p and T.

Proof. Dropping the condition

$$\gcd(v_1 v_2, p) = \gcd(u_1, v_1) = \gcd(u_2, v_2) = 1,$$

we see that $Q_{T,p}$ does not exceed the number of solutions to the congruence

$$u_1 v_2 \equiv u_2 v_1 \pmod p, \qquad 1 \leq u_1, u_2, v_1, v_2 \leq T,$$

which has been estimated as $O(T^4/p + T^2 (\log p)^2)$ by Ayyad, Cochrane and Zheng [1, Theorem 1] when $T < p$. Obviously, by fixing three variables and varying the remaining variable, when $p \leq T$ the number of such solutions is at most $2T^4/p$. So, we have

$$Q_{T,p} \ll T^4/p + T^2 (\log p)^2 = T^4/p + T^2 p^{o(1)},$$

where the implied constant is independent of p and T. □

We now need an additive analogue of Lemma 14. Namely, we need an upper bound on the number $V_{T,p}$ of solutions to the congruence

$$u_1/v_1 + u_2/v_2 \equiv u_3/v_3 + u_4/v_4 \pmod p, \\ u_i/v_i \in \mathcal{F}(T), \ i = 1,2,3,4, \qquad \gcd(v_1 v_2 v_3 v_4, p) = 1. \tag{18}$$

Trivially we have $V_{T,p} \ll T^8/p + T^7$. Using bounds of exponential sums with Farey fractions from [26], one can get an essentially optimal bound. We also denote $\mathbf{e}_p(z) = \exp(2\pi i z/p)$.

Lemma 15. *For any prime p, we have*

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{u/v \in \mathcal{F}(T)} \mathbf{e}_p(au/v) \right| \le T(Tp)^{o(1)}.$$

Proof. The desired result looks similar to [26, Theorem 1] taken with $m = p$. However in [26] the set $\mathcal{F}(T)$ is defined in a more traditional way with the additional condition $u < v$ (that is, $\mathcal{F}(T) \subseteq [0,1]$ in the definition of [26]). So we give here a short proof which relies on the bound in [26, Lemma 3]. Namely, let $U, V \ge 1$ be arbitrary integers and let for each v we are given two integers $U_v > L_v$ with $0 \le L_v < p$ and $U_v \le U$. Then by [26, Lemma 3], taken with $m = p$, we have

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{\substack{v=1 \\ \gcd(v,p)=1}}^{V} \sum_{u=L_v+1}^{U_v} \mathbf{e}_p(au/v) \right| \le (U+V)(Vp)^{o(1)}. \tag{19}$$

Now, for an integer $d \ge 1$ we use $\mu(d)$ to denote the Möbius function. We recall that $\mu(1) = 1$, $\mu(d) = 0$ if $d \ge 2$ is not square-free, and $\mu(d) = (-1)^{\omega(d)}$ otherwise, where $\omega(d)$ is the number of prime divisors of d. Then by the inclusion-exclusion principle,

$$\begin{aligned} \sum_{u/v \in \mathcal{F}(T)} \mathbf{e}_p(au/v) &= \sum_{d=1}^{T} \mu(d) \sum_{\substack{v=1 \\ \gcd(v,p)=1 \\ d \mid v}}^{T} \sum_{\substack{u=1 \\ d \mid u}}^{T} \mathbf{e}_p\left(au/v\right) \\ &= \sum_{d=1}^{T} \mu(d) \sum_{\substack{v=1 \\ \gcd(v,p)=1}}^{\lfloor T/d \rfloor} \sum_{u=1}^{\lfloor T/d \rfloor} \mathbf{e}_p\left(au/v\right). \end{aligned}$$

Now, for each $d = 1, \ldots, T$ we apply (19) to see that each inner sum is at most $Td^{-1}(Tp)^{o(1)}$. The result now follows. □

We are now ready to estimate $V_{T,p}$.

Lemma 16. *For any prime p, we have*

$$V_{T,p} = \frac{\left(\#\mathcal{F}(T)\right)^4}{p} + O(T^4(Tp)^{o(1)}).$$

Proof. Using the orthogonality of the exponential function, we write

$$V_{T,p} = \sum_{\substack{u_i/v_i \in \mathcal{F}(T)\\ i=1,2,3,4}} \sum \frac{1}{p} \sum_{a=0}^{p-1} \mathbf{e}_p\left(a\left(u_1/v_1 + u_2/v_2 - u_3/v_3 - u_4/v_4\right)\right).$$

Changing the order of summation and also noticing that $|z|^2 = z\overline{z}$, we obtain

$$V_{T,p} = \frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{u/v \in \mathcal{F}(T)} \mathbf{e}_p(au/v) \right|^4.$$

Now, the contribution from $a = 0$ gives the main term $\left(\#\mathcal{F}(T)\right)^4/p$, while for other sums we apply Lemma 15, which concludes the proof. □

2.4. **Preparations for distribution of angles.** Now, we introduce a direct consequence of a result of Niederreiter [25, Lemma 3], which is one of our key tools. For m arbitrary elements $w_1, \ldots, w_m$ lying in the interval $[-1, 1]$ (not necessarily distinct) and an arbitrary subinterval J of $[-1, 1]$, let $A(J; m)$ be the number of integers i, $1 \le i \le m$, with $w_i \in J$. For any $-1 \le a < b \le 1$, define the function

$$G(a, b) = \frac{2}{\pi} \int_a^b (1 - z^2)^{1/2}\, dz.$$

We also recall the Chebyshev polynomials U_n of the second kind, on $[-1, 1]$ they are defined by

$$U_n(z) = \frac{\sin((n+1)\arccos z)}{(1-z^2)^{1/2}} \quad \text{for } z \in [-1, 1],$$

where n is a nonnegative integer. In particular, for $\vartheta \in [0, \pi]$, we have

$$U_n(\cos\vartheta) = \frac{\sin((n+1)\vartheta)}{\sin\vartheta}.$$

Lemma 17. *For any integer $k \ge 1$, we have*

$$\max_{-1 \le a < b \le 1} |A([a, b]; m) - mG(a, b)| \ll \frac{m}{k} + \sum_{n=1}^{k} \frac{1}{n} \left| \sum_{i=1}^{m} U_n(w_i) \right|.$$

Proof. Note that for any $-1 \le a < b \le 1$, we have

$$\begin{aligned} &A([a, b]; m) - mG(a, b)\\ &\quad = \left(A([-1, b]; m) - mG(-1, b)\right) - \left(A([-1, a); m) - mG(-1, a)\right). \end{aligned}$$

For any odd positive integer κ, it follows directly from [25, Lemma 3] that

$$|A([a,b];m) - mG(a,b)| < \frac{16m}{0.362\cdot\pi\kappa+4} + \frac{2(4\kappa-3)}{0.362\cdot\pi\kappa+2\pi}\sum_{n=1}^{2\kappa-1}\frac{n+1}{n(n+2)}\left|\sum_{i=1}^{m}U_n(w_i)\right|.$$

The desired result now follows by varying the value of κ according to k. Here, one ought to notice the symbol "$\ll$" we use in the result. □

2.5. **Distribution of angles over $\mathcal{F}(T)$.** We now consider the angles $\psi_p(E(t))$ that are given by (4).

Michel [23, Proposition 1.1] gives the following bound on the weighed sums with the angles $\psi_p(E(t))$ for single parametric polynomial families of curves, where the sums is also twisted by additive characters.

We recall the notation $\mathbf{e}_p(z) = \exp(2\pi iz/p)$ from Section 2.3.

Lemma 18. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), we have*

$$\sum_{\substack{w\in\mathbb{F}_p\\ \Delta(w)\not\equiv 0 \pmod p}} \frac{\sin\left((n+1)\psi_p(E(w))\right)}{\sin\left(\psi_p(E(w))\right)}\mathbf{e}_p\left(mw\right) \ll np^{1/2},$$

uniformly over all integers m and $n \geq 1$.

The following result is a direct application of Lemma 18.

Lemma 19. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any prime p, we have*

$$\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\not\equiv 0 \pmod p}} \frac{\sin((n+1)\psi_p(E(r+s)))}{\sin(\psi_p(E(r+s)))} \ll nT^2p^{1/2+o(1)} + nT^4p^{-1/2},$$

uniformly over all integers $n \geq 1$.

Proof. Using the orthogonality of the exponential function, we write

$$\begin{aligned}\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\not\equiv 0 \pmod p}} & \frac{\sin((n+1)\psi_p(E(r+s)))}{\sin(\psi_p(E(r+s)))}\\ &= \sum_{\substack{w\in\mathbb{F}_p\\ \Delta(w)\not\equiv 0 \pmod p}} \frac{\sin\left((n+1)\psi_p(E(w))\right)}{\sin\left(\psi_p(E(w))\right)}\\ &\qquad \sum_{\substack{u_1/v_1\in\mathcal{F}(T),\,\gcd(v_1,p)=1\\ u_2/v_2\in\mathcal{F}(T),\,\gcd(v_2,p)=1}} \frac{1}{p}\sum_{m=0}^{p-1}\mathbf{e}_p(m(w-u_1/v_1-u_2/v_2))\\ &\qquad + O(nT^3(T/p+1)),\end{aligned}$$

where the last term comes from the exceptional case with $p \mid v_1v_2$. So changing the order of summation we obtain:

$$\begin{aligned}\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\not\equiv 0 \pmod p}} & \frac{\sin((n+1)\psi_p(E(r+s)))}{\sin(\psi_p(E(r+s)))}\\ &= \frac{1}{p}\sum_{m=0}^{p-1} \sum_{\substack{w\in\mathbb{F}_p\\ \Delta(w)\not\equiv 0 \pmod p}} \frac{\sin\left((n+1)\psi_p(E(w))\right)}{\sin\left(\psi_p(E(w))\right)}\mathbf{e}_p(mw)\\ &\qquad \sum_{\substack{u_1/v_1\in\mathcal{F}(T)\\ \gcd(v_1,p)=1}} \mathbf{e}_p(-mu_1/v_1) \sum_{\substack{u_2/v_2\in\mathcal{F}(T)\\ \gcd(v_2,p)=1}} \mathbf{e}_p(-mu_2/v_2).\end{aligned}$$

Using Lemma 18, we have

$$\begin{aligned}\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\not\equiv 0 \pmod p}} & \frac{\sin((n+1)\psi_p(E(r+s)))}{\sin(\psi_p(E(r+s)))}\\ &\ll np^{-1/2}\sum_{m=0}^{p-1}\left|\sum_{\substack{u_1/v_1\in\mathcal{F}(T)\\ \gcd(v_1,p)=1}}\mathbf{e}_p(-mu_1/v_1)\right|\left|\sum_{\substack{u_2/v_2\in\mathcal{F}(T)\\ \gcd(v_2,p)=1}}\mathbf{e}_p(-mu_2/v_2)\right|.\end{aligned}$$

It now remains to apply the Cauchy inequality and note that

$$\begin{aligned}
&\sum_{m=0}^{p-1} \left| \sum_{\substack{u/v \in \mathcal{F}(T) \\ \gcd(v,p)=1}} \mathbf{e}_p(-mu/v) \right|^2 \\
&\quad = \sum_{m=0}^{p-1} \sum_{\substack{u_1/v_1 \in \mathcal{F}(T) \\ u_2/v_2 \in \mathcal{F}(T) \\ \gcd(v_1 v_2,p)=1}} \mathbf{e}_p\left(m(u_2/v_2 - u_1/v_1)\right) \\
&\quad = \sum_{\substack{u_1/v_1 \in \mathcal{F}(T) \\ u_2/v_2 \in \mathcal{F}(T) \\ \gcd(v_1 v_2,p)=1}} \sum_{m=0}^{p-1} \mathbf{e}_p\left(m(u_2/v_2 - u_1/v_1)\right) \ll T^2 p^{1+o(1)} + T^4,
\end{aligned}$$

which follows from the orthogonality of the exponential function and Lemma 14. □

Now, we define $\mathscr{B}_{f,g,p}(\mathcal{F}(T); \alpha, \beta)$ as the number of pairs $(r, s) \in \mathcal{F}(T) \times \mathcal{F}(T)$ with $\Delta(r+s) \not\equiv 0 \pmod p$ such that

$$\alpha \le \psi_p(E(r+s)) \le \beta.$$

Now, combining Lemma 17 with Lemma 19 we derive the following result. Note that here we assume that the prime p is greater than T. Since we prefer small values of T, this assumption is reasonable.

Lemma 20. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any prime $p > T$, we have*

$$\begin{aligned}
\max_{0 \le \alpha < \beta \le \pi} &\left| \mathscr{B}_{f,g,p}(\mathcal{F}(T); \alpha, \beta) - \mu_{\mathtt{ST}}(\alpha, \beta)(\#\mathcal{F}(T))^2 \right| \\
&\ll T^3 p^{1/4+o(1)} + T^4 p^{-1/4+o(1)}.
\end{aligned}$$

Proof. Obviously, since $p > T$, we have

$$\#\{(r, s) \in \mathcal{F}(T) \times \mathcal{F}(T) : \ \Delta(r+s) \equiv 0 \pmod p\} \ll T^3.$$

We now associate to each pair $(r, s) \in \mathscr{B}_{f,g,p}(\mathcal{F}(T); \alpha, \beta)$ a value $\cos \psi_p(E(r+s))$. This enables us to apply Lemma 17. So, by Lemma 17,

for any positive integer k, we have

$$\begin{aligned}\max_{0\le\alpha<\beta\le\pi} &\left|\mathscr{B}_{f,g,p}(\mathcal{F}(T);\alpha,\beta)-\mu_{\mathtt{ST}}(\alpha,\beta)(\#\mathcal{F}(T))^2\right| \\ &\ll T^3+\frac{(\#\mathcal{F}(T))^2}{k} \\ &\quad+\sum_{n=1}^{k}\frac{1}{n}\left|\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\not\equiv 0 \pmod p}}\frac{\sin\left((n+1)\psi_p(E(r+s))\right)}{\sin\left(\psi_p(E(r+s))\right)}\right|.\end{aligned}$$

Here, the reason why the term T^3 appears in the above inequality is that the pairs (r,s) satisfying $\Delta(r+s)\equiv 0 \pmod p$ are not counted in $\mathscr{B}_{f,g,p}(\mathcal{F}(T);\alpha,\beta)$.

Thus, by (10) and Lemma 19, we get

$$\begin{aligned}\max_{0\le\alpha<\beta\le\pi} &\left|\mathscr{B}_{f,g,p}(\mathcal{F}(T);\alpha,\beta)-\mu_{\mathtt{ST}}(\alpha,\beta)(\#\mathcal{F}(T))^2\right| \\ &\ll T^3+\frac{T^4}{k}+kT^2p^{1/2+o(1)}+kT^4p^{-1/2} \\ &\ll \frac{T^4}{k}+kT^2p^{1/2+o(1)}+kT^4p^{-1/2}.\end{aligned} \tag{20}$$

Clearly, we can assume that $T\ge p^{1/4}$ as otherwise the result is weaker than the trivial bound $O(T^4)$.

Now, for $p^{1/2}\ge T\ge p^{1/4}$ we take $k=\lceil p^{-1/4}T\rceil$ to balance the first two terms in (20) and derive

$$\begin{aligned}\max_{0\le\alpha<\beta\le\pi} &\left|\mathscr{B}_{f,g,p}(\mathcal{F}(T);\alpha,\beta)-\mu_{\mathtt{ST}}(\alpha,\beta)(\#\mathcal{F}(T))^2\right| \\ &\ll T^3p^{1/4+o(1)}+T^5p^{-3/4}\le T^3p^{1/4+o(1)},\end{aligned} \tag{21}$$

For $T\ge p^{1/2}$ we take $k=\lceil p^{1/4}\rceil$ to balance the first and the third terms in (20) and derive

$$\begin{aligned}\max_{0\le\alpha<\beta\le\pi} &\left|\mathscr{B}_{f,g,p}(\mathcal{F}(T);\alpha,\beta)-\mu_{\mathtt{ST}}(\alpha,\beta)(\#\mathcal{F}(T))^2\right| \\ &\ll T^2p^{3/4+o(1)}+T^4p^{-1/4}\le T^4p^{-1/4+o(1)}.\end{aligned} \tag{22}$$

Finally, noticing that $T^4p^{-1/4}\le T^3p^{1/4}$ is equivalent to $T\le p^{1/2}$, we see that in both cases the bounds (21) and (22) can be combined in one bound

$$\begin{aligned}\max_{0\le\alpha<\beta\le\pi} &\left|\mathscr{B}_{f,g,p}(\mathcal{F}(T);\alpha,\beta)-\mu_{\mathtt{ST}}(\alpha,\beta)(\#\mathcal{F}(T))^2\right| \\ &\le T^3p^{1/4+o(1)}+T^4p^{-1/4+o(1)},\end{aligned}$$

which concludes the proof. □

2.6. **Distribution of angles over $\mathcal{I}(T)$.** We start with recalling the bound from [29, Lemma 10], which is essentially based on Lemma 18 and the standard reduction between complete and incomplete sums (see [20, Section 12.2]).

Lemma 21. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any prime p, we have*

$$\sum_{\substack{t \in \mathcal{I}(T) \\ \Delta(t) \not\equiv 0 \pmod p}} \frac{\sin((n+1)\psi_p(E(t)))}{\sin(\psi_p(E(t)))} \ll np^{1/2+o(1)},$$

uniformly over all integers $n \geq 1$.

Let $\mathscr{C}_{f,g,p}(\mathcal{I}(T); \alpha, \beta)$ be the number of integers $t \in \mathcal{I}(T)$, where $\mathcal{I}(T)$ is given by (14), with $\Delta(t) \not\equiv 0 \pmod p$, such that

$$\alpha \leq \psi_p(E(t)) \leq \beta.$$

Here, we reproduce the asymptotic formula on $\mathscr{C}_{f,g,p}(\mathcal{I}(T); \alpha, \beta)$ given in [29, Lemma 11] with a minor change (here we use a different notation).

Lemma 22. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any prime $p > T$, we have*

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

Proof. Note that since $p > T$, the number of $t \in \mathcal{I}(T)$ satisfying $\Delta(t) \equiv 0 \pmod p$ is upper bounded by a constant, say c, which only depends on the degrees of $f(Z)$ and $g(Z)$.

As in the proof of Lemma 20, by Lemma 17 and Lemma 21, for any positive integer k, we have

$$\begin{aligned}
&\max_{0 \leq \alpha < \beta \leq \pi} |\mathscr{C}_{f,g,p}(\mathcal{I}(T); \alpha, \beta) - \mu_{\mathtt{ST}}(\alpha, \beta)T| \\
&\quad \ll 1 + \frac{T}{k} + \sum_{n=1}^{k} \frac{1}{n} \left| \sum_{\substack{t \in \mathcal{I}(T) \\ \Delta(t) \not\equiv 0 \pmod p}} \frac{\sin\left((n+1)\psi_p(E(t))\right)}{\sin\left(\psi_p(E(t))\right)} \right| \\
&\quad \ll 1 + T/k + kp^{1/2+o(1)}.
\end{aligned}$$

It is easy to see that for $T \leq p^{1/2}$ the result is weaker than the trivial bound $O(T)$.

For $T > p^{1/2}$, taking $k = \left\lceil p^{-1/4}T^{1/2} \right\rceil$, we complete the proof. □

We now give yet another application of Lemma 18.

Lemma 23. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any non-empty subsets $\mathcal{U}, \mathcal{V} \subseteq \mathcal{I}(T)$ and any prime $p > T$, we have*

$$\sum_{\substack{u \in \mathcal{U}, v \in \mathcal{V} \\ \Delta(u+v) \not\equiv 0 \pmod p}} \frac{\sin((n+1)\psi_p(E(u+v)))}{\sin(\psi_p(E(u+v)))} \ll n(p\#\mathcal{U}\#\mathcal{V})^{1/2},$$

uniformly over all integers $n \geq 1$.

Proof. Applying the same argument as in the proof of Lemma 19, we have

$$\sum_{\substack{u \in \mathcal{U}, v \in \mathcal{V} \\ \Delta(u+v) \not\equiv 0 \pmod p}} \frac{\sin\left((n+1)\psi_p(E(u+v))\right)}{\sin\left(\psi_p(E(u+v))\right)} \ll np^{-1/2} \sum_{m=0}^{p-1} \left| \sum_{u \in \mathcal{U}} \mathbf{e}_p(-mu) \right| \left| \sum_{v \in \mathcal{V}} \mathbf{e}_p(-mv) \right|.$$

It now remains to apply the Cauchy inequality and note the identities

$$\sum_{m=0}^{p-1} \left| \sum_{u \in \mathcal{U}} \mathbf{e}_p(-mu) \right|^2 = p\#\mathcal{U} \quad \text{and} \quad \sum_{m=0}^{p-1} \left| \sum_{v \in \mathcal{V}} \mathbf{e}_p(-mv) \right|^2 = p\#\mathcal{V},$$

which follow from the orthogonality of the exponential function and $p > T$. □

Now, for any two non-empty subsets $\mathcal{U}, \mathcal{V} \subseteq \mathcal{I}(T)$, let $\mathscr{D}_{f,g,p}(\mathcal{U}, \mathcal{V}; \alpha, \beta)$ be the number of pairs $(u, v) \in \mathcal{U} \times \mathcal{V}$ with $\Delta(u+v) \not\equiv 0 \pmod p$ such that

$$\alpha \leq \psi_p(E(u+v)) \leq \beta.$$

As before, combining Lemma 17 with Lemma 23 we derive:

Lemma 24. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any subsets $\mathcal{U}, \mathcal{V} \subseteq \mathcal{I}(T)$ and any prime $p > T$, we have*

$$\max_{0 \leq \alpha < \beta \leq \pi} |\mathscr{D}_{f,g,p}(\mathcal{U}, \mathcal{V}; \alpha, \beta) - \mu_{\mathtt{ST}}(\alpha, \beta)\#\mathcal{U}\#\mathcal{V}| \ll p^{1/4}(\#\mathcal{U}\#\mathcal{V})^{3/4}.$$

Proof. Clearly, since $p > T$, we have

$$\#\{(u, v) \in \mathcal{U} \times \mathcal{V} \ : \ \Delta(u+v) \equiv 0 \pmod p\} \ll \min\{\#\mathcal{U}, \#\mathcal{V}\} \ll (\#\mathcal{U}\#\mathcal{V})^{1/2}.$$

As in the proof of Lemma 20, by Lemma 17, for any positive integer k we have

$$\begin{aligned}\max_{0\le\alpha<\beta\le\pi} &|\mathscr{D}_{f,g,p}(\mathcal{U},\mathcal{V};\alpha,\beta) - \mu_{\mathtt{ST}}(\alpha,\beta)\#\mathcal{U}\#\mathcal{V}| \\ &\ll (\#\mathcal{U}\#\mathcal{V})^{1/2} + \frac{\#\mathcal{U}\#\mathcal{V}}{k} \\ &\quad + \sum_{n=1}^{k}\frac{1}{n}\left|\sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\not\equiv 0 \pmod p}} \frac{\sin\left((n+1)\psi_p(E(u+v))\right)}{\sin\left(\psi_p(E(u+v))\right)}\right|.\end{aligned}$$

Thus, by Lemma 23, we get

$$\begin{aligned}\max_{0\le\alpha<\beta\le\pi} &|\mathscr{D}_{f,g,p}(\mathcal{U},\mathcal{V};\alpha,\beta) - \mu_{\mathtt{ST}}(\alpha,\beta)\#\mathcal{U}\#\mathcal{V}| \\ &\ll (\#\mathcal{U}\#\mathcal{V})^{1/2} + \frac{\#\mathcal{U}\#\mathcal{V}}{k} + k(p\#\mathcal{U}\#\mathcal{V})^{1/2} \\ &\ll \frac{\#\mathcal{U}\#\mathcal{V}}{k} + k(p\#\mathcal{U}\#\mathcal{V})^{1/2}.\end{aligned}$$

We can assume that $\#\mathcal{U}\#\mathcal{V} \ge p$, as otherwise the result is weaker than the trivial bound $O\left(\#\mathcal{U}\#\mathcal{V}\right)$. Then, taking $k = \left\lceil (p^{-1}\#\mathcal{U}\#\mathcal{V})^{1/4}\right\rceil$ and noticing

$$(p^{-1}\#\mathcal{U}\#\mathcal{V})^{1/4} \le k \le (p^{-1}\#\mathcal{U}\#\mathcal{V})^{1/4} + 1 \le 2(p^{-1}\#\mathcal{U}\#\mathcal{V})^{1/4},$$

we conclude the proof. □

3. Proofs of Main Results

3.1. **Proof of Theorem 1.** From Lemma 11, first using the Cauchy inequality and then discarding the conditions $\Delta(w) \not\equiv 0 \pmod p$ and $a_{w,p} \equiv a_p \pmod \ell$, we derive

$$\sum_{\substack{t\in\mathcal{F}(T)\\ \Delta(t)\ne 0}} \pi_{E(t)}(\mathfrak{A};x) \le P_{\mathcal{F}}T^2 + \sum_{p\le x} L_{T,p}^{1/2}Q_{T,p}^{1/2}, \tag{23}$$

where

$$L_{T,p} = \sum_{\substack{0\le w\le p-1\\ \Delta(w)\not\equiv 0 \pmod p\\ a_{w,p}\equiv a_p \pmod \ell}} 1 \qquad \text{and} \qquad Q_{T,p} = \sum_{0\le w\le p-1} R_{T,p}(w)^2.$$

It is easy to see that $Q_{T,p}$ is exactly the quantity defined in Lemma 14.

Therefore, for an arbitrary sequence $\mathfrak{A}$, substituting the bound of Lemma 14 in (23) and applying the bound of Lemma 12 to $L_{T,p}$ with

$\ell \sim x^{1/4}$, we obtain

$$\begin{aligned}\sum_{\substack{t \in \mathcal{F}(T)\\ \Delta(t)\neq 0}} & \pi_{E(t)}(\mathfrak{A}; x)\\ &\ll P_{\mathcal{F}} T^2 + \sum_{p \le x} \left(x^{-1/8} p^{1/2} + x^{1/8} p^{1/4}\right) \left(T^2 p^{-1/2} + T p^{o(1)}\right)\\ &\ll T x^{11/8+o(1)} + T^2 x^{7/8}.\end{aligned}$$

While $\mathfrak{A}$ is the zero sequence, applying the bound of Lemma 12 to $L_{T,p}$ with $\ell \sim x^{1/3}$, after similar calculations we conclude the proof.

3.2. **Proof of Theorem 2.** By (16) and as in the proof of Theorem 1, we have

$$\sum_{\substack{t \in \mathcal{F}(T)\\ \Delta(t)\neq 0}} \pi_{E(t)}(\mathfrak{A}; x) \le P_{\mathcal{F}} T^2 + \sum_{p \le x} M_{T,p}^{1/2} Q_{T,p}^{1/2}, \tag{24}$$

where

$$M_{T,p} = \sum_{\substack{0 \le w \le p-1\\ \Delta(w) \not\equiv 0 \pmod p\\ a_{w,p} = a_p}} 1,$$

and $Q_{T,p}$ is as before.

For integer t, we define $H(t,p)$ as the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ with Frobenius trace t.

Notice that each elliptic curve $E(w)$ has j-invariant w, which implies that each $E(w)$ represents a distinct $\mathbb{F}_p$-isomorphism class of elliptic curves over $\mathbb{F}_p$. So, we have

$$M_{T,p} \le H(a_p, p).$$

By [22, Proposition 1.9 (a)], for $p \ge 5$ we know that

$$H(a_p, p) \ll p^{1/2+o(1)},$$

where the implied constant is independent of p and a_p. So, we obtain

$$M_{T,p} \ll p^{1/2+o(1)}.$$

Then, substituting this bound in (24) and using the bound of $Q_{T,p}$ from Lemma 14, we derive the desired result.

3.3. **Proof of Theorem 3.** Here, we use a method quite different from the above.

For each a_p, we define two angels $\alpha_p, \beta_p \in [0, \pi]$ such that

$$\cos\alpha_p = \min\left\{\frac{a_p}{2\sqrt{p}} + \frac{1}{p}, 1\right\} \quad \text{and} \quad \cos\beta_p = \max\left\{\frac{a_p}{2\sqrt{p}} - \frac{1}{p}, -1\right\}.$$

Then, we have

$$\begin{aligned}\mu_{\mathtt{ST}}(\alpha_p, \beta_p) = \frac{2}{\pi}\int_{\alpha_p}^{\beta_p} \sin^2\vartheta\, d\vartheta &= \frac{2}{\pi}\int_{\cos\beta_p}^{\cos\alpha_p} (1-z^2)^{1/2}\, dz \\ &\le \frac{2}{\pi}(\cos\alpha_p - \cos\beta_p) \le \frac{4}{\pi p}.\end{aligned} \tag{25}$$

We recall the definition (17) and observe that for each elliptic curve $E(t), t \in \mathcal{F}(T)$ and a prime p, the Frobenius trace $a_{t,p} = a_p$ if and only if

$$\cos\psi_p(E(t)) = \frac{a_p}{2\sqrt{p}}.$$

Thus, if $a_{t,p} = a_p$, we have

$$\alpha_p \le \psi_p(E(t)) \le \beta_p.$$

Applying the above discussions and noticing the discussion about $N(r+s)$ and $\Delta(r+s)$ in Section 2.1, we get

$$\begin{aligned}\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\neq 0}} \pi_{E(r+s)}(\mathfrak{A}; x) &= \sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\neq 0}} \sum_{\substack{p\le x\\ p\nmid N(r+s)\\ a_{r+s,p}=a_p}} 1 \\ &= \sum_{p\le x} \sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\not\equiv 0 \pmod p\\ a_{r+s,p}=a_p}} 1 \le \sum_{p\le x} \mathscr{B}_{f,g,p}(\mathcal{F}(T); \alpha_p, \beta_p),\end{aligned}$$

where $\mathscr{B}_{f,g,p}(\mathcal{F}(T);\alpha_p,\beta_p)$ has been defined in Section 2.5. Then, combining the above results with Lemma 20, we obtain

$$\begin{aligned}
&\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\neq 0}} \pi_{E(r+s)}(\mathfrak{A};x)\\
&\quad\ll \sum_{p\le T} T^4 + \sum_{T<p\le x}\left(\mu_{\mathtt{ST}}(\alpha_p,\beta_p)T^4 + T^3p^{1/4+o(1)} + T^4p^{-1/4+o(1)}\right)\\
&\quad\ll \sum_{p\le T} T^4 + \sum_{p\le x}\left(T^4/p + T^3p^{1/4+o(1)} + T^4p^{-1/4+o(1)}\right)\\
&\quad\ll T^5 + T^4\log x + T^3x^{5/4+o(1)} + T^4x^{3/4+o(1)}\\
&\quad\ll T^5 + T^3x^{5/4+o(1)} + T^4x^{3/4+o(1)},
\end{aligned}$$

which completes the proof.

3.4. **Proof of Theorem 4.** As Lemma 11 and using the Cauchy inequality, we obtain

$$\begin{aligned}
\sum_{\substack{t\in\mathcal{F}(T)\\ \Delta(t)\neq 0}} \pi_{E(t)}(\mathbb{K};x) &\le P_{\mathcal{F}}T^2 + \sum_{p\le x}\sum_{\substack{0\le w\le p-1\\ \Delta(w)\not\equiv 0 \pmod p\\ a_{w,p}\neq 0\\ \mathbb{Q}\left(\sqrt{a_{w,p}^2-4p}\right)=\mathbb{K}}} R_{T,p}(w)\\
&\le P_{\mathcal{F}}T^2 + \sum_{p\le x} N_{T,p}^{1/2}Q_{T,p}^{1/2},
\end{aligned}$$

where

$$N_{T,p} = \sum_{\substack{0\le w\le p-1\\ \Delta(w)\not\equiv 0 \pmod p\\ a_{w,p}\neq 0\\ \mathbb{Q}\left(\sqrt{a_{w,p}^2-4p}\right)=\mathbb{K}}} 1,$$

and $Q_{T,p}$ is as before.

Applying the bound of Lemma 13 to $N_{T,p}$ with $\ell\sim x^{1/3}$, we obtain

$$N_{T,p} \ll px^{-1/3} + x^{1/6}p^{1/2}. \tag{26}$$

Now, using the bound of $Q_{T,p}$ from Lemma 14, we obtain

$$\begin{aligned}
&\sum_{\substack{t\in\mathcal{F}(T)\\ \Delta(t)\neq 0}} \pi_{E(t)}(\mathbb{K};x)\\
&\qquad\ll T^2 + \sum_{p\le x}\left(p^{1/2}x^{-1/6} + x^{1/12}p^{1/4}\right)\left(T^2p^{-1/2} + Tp^{o(1)}\right),
\end{aligned}$$

and after simple calculations, we complete the proof.

3.5. **Proof of Theorem 5.** For an integer w, we denote by $U_{T,p}(w)$ the number of pairs $(u_1/v_1, u_2/v_2) \in \mathcal{F}(T) \times \mathcal{F}(T)$ with $\gcd(v_1v_2, p) = 1$ and $u_1/v_1 + u_2/v_2 \equiv w \pmod p$.

As in the proof of Theorem 4, we obtain

$$\begin{aligned}\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\neq 0}} \pi_{E(r+s)}(\mathbb{K}; x) &\le P_{\mathcal{F}}T^4 + \sum_{p\le x} \sum_{\substack{0\le w\le p-1\\ \Delta(w)\not\equiv 0 \pmod p\\ a_{w,p}\neq 0\\ \mathbb{Q}\left(\sqrt{a_{w,p}^2-4p}\right)=\mathbb{K}}} U_{T,p}(w)\\ &\le P_{\mathcal{F}}T^4 + \sum_{p\le x} N_{T,p}^{1/2} V_{T,p}^{1/2},\end{aligned}$$

where

$$N_{T,p} = \sum_{\substack{0\le w\le p-1\\ \Delta(w)\not\equiv 0 \pmod p\\ a_{w,p}\neq 0\\ \mathbb{Q}\left(\sqrt{a_{w,p}^2-4p}\right)=\mathbb{K}}} 1,$$

and $V_{T,p}$ is as in Section 2.3. Applying the bound of Lemma 13 to $N_{T,p}$ with $\ell \sim x^{1/3}$, we again obtain the bound (26) from which we conclude that $N_{T,p} \ll x^{2/3}$. Hence

$$\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\neq 0}} \pi_{E(r+s)}(\mathbb{K}; x) \ll T^4 + x^{1/3} \sum_{p\le x} V_{T,p}^{1/2}.$$

Using Lemma 16, we derive

$$\sum_{p\le x} V_{T,p}^{1/2} \ll T^4 x^{1/2} + T^{2+o(1)} x^{1+o(1)}.$$

Hence

$$\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\neq 0}} \pi_{E(r+s)}(\mathbb{K}; x) \ll T^4 x^{5/6} + T^{2+o(1)} x^{4/3+o(1)}.$$

Clearly we can assume that $T \ge x^{1/6}$ as otherwise the result is weaker than the trivial bound $O(T^4x)$. In this case replace $T^{2+o(1)}x^{4/3+o(1)}$ with $T^{2+o(1)}x^{4/3}$ and the result follows.

3.6. **Proof of Theorem 6.** Using the same notation as in Section 2.5 and noticing the discussion about $N(r+s)$ and $\Delta(r+s)$ in Section 2.1,

we have

$$\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\neq 0}} \pi_{E(r+s)}(\alpha,\beta;x) = \sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\neq 0}} \sum_{\substack{p\le x\\ p\nmid N(r+s)\\ \psi_p(E(r+s))\in[\alpha,\beta]}} 1$$
$$= \sum_{p\le x} \sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\not\equiv 0 \pmod p\\ \psi_p(E(r+s))\in[\alpha,\beta]}} 1 = \sum_{p\le x} \mathscr{B}_{f,g,p}(\mathcal{F}(T);\alpha,\beta).$$

By Lemma 20, we get

$$\sum_{\substack{r,s\in\mathcal{F}(T)\\ \Delta(r+s)\neq 0}} \pi_{E(r+s)}(\alpha,\beta;x) - \sum_{p\le x} \mu_{\mathtt{ST}}(\alpha,\beta)(\#\mathcal{F}(T))^2$$
$$\ll \sum_{p\le T} T^4 + \sum_{T<p\le x} \left(T^3 p^{1/4+o(1)} + T^4 p^{-1/4+o(1)}\right)$$
$$\ll T^5 + T^3 x^{5/4+o(1)} + T^4 x^{3/4+o(1)}.$$

Thus, the desired result follows from (10) and the assumption $x^{1/4+\varepsilon} \le T \le x^{1-\varepsilon}$.

3.7. **Proof of Theorem 7.** As in Section 3.3, we have

$$\sum_{\substack{t\in\mathcal{I}(T)\\ \Delta(t)\neq 0}} \pi_{E(t)}(\mathfrak{A};x) = \sum_{\substack{t\in\mathcal{I}(T)\\ \Delta(t)\neq 0}} \sum_{\substack{p\le x\\ p\nmid N(t)\\ a_{t,p}=a_p}} 1$$
$$= \sum_{p\le x} \sum_{\substack{t\in\mathcal{I}(T)\\ \Delta(t)\not\equiv 0 \pmod p\\ a_{t,p}=a_p}} 1 \le \sum_{p\le x} \mathscr{C}_{f,g,p}(\mathcal{I}(T);\alpha_p,\beta_p),$$

where α_p and β_p have been defined in Section 3.3, and $\mathscr{C}_{f,g,p}(\mathcal{I}(T);\alpha_p,\beta_p)$ has been defined in Section 2.6. Then, combining the above inequality with Lemma 22 and (25), we obtain

$$\sum_{\substack{t\in\mathcal{I}(T)\\ \Delta(t)\neq 0}} \pi_{E(t)}(\mathfrak{A};x)$$
$$\ll \sum_{p\le T} T + \sum_{T<p\le x} \left(\mu_{\mathtt{ST}}(\alpha_p,\beta_p)T + T^{1/2}p^{1/4+o(1)}\right)$$
$$\ll T^2 + \sum_{p\le x} \left(T/p + T^{1/2}p^{1/4+o(1)}\right)$$
$$\ll T^2 + T\log x + T^{1/2}x^{5/4+o(1)}.$$

Noticing that $T \log x \le \sqrt{T^2 \cdot T^{1/2} x^{5/4+o(1)}}$, we conclude the proof.

3.8. **Proof of Theorem 8.** As in Section 3.3, we obtain

$$\sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\neq 0}} \pi_{E(u+v)}(\mathfrak{A};x) = \sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\neq 0}} \sum_{\substack{p\le x\\ p\nmid N(u+v)\\ a_{u+v,p}=a_p}} 1$$

$$= \sum_{p\le x} \sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\not\equiv 0 \pmod p\\ a_{u+v,p}=a_p}} 1 \le \sum_{p\le x} \mathscr{D}_{f,g,p}(\mathcal{U},\mathcal{V};\alpha_p,\beta_p),$$

where α_p and β_p are as the above, and $\mathscr{D}_{f,g,p}(\mathcal{U},\mathcal{V};\alpha_p,\beta_p)$ has been defined in Section 2.6.

By Lemma 24 and the bound (25), we get

$$\sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\neq 0}} \pi_{E(u+v)}(\mathfrak{A};x)$$

$$\ll \sum_{p\le T} \#\mathcal{U}\#\mathcal{V} + \sum_{T<p\le x} (\mu_{\mathrm{ST}}(\alpha_p,\beta_p)\#\mathcal{U}\#\mathcal{V} + p^{1/4}(\#\mathcal{U}\#\mathcal{V})^{3/4})$$

$$\ll T\#\mathcal{U}\#\mathcal{V} + \sum_{p\le x} \left(\#\mathcal{U}\#\mathcal{V}/p + p^{1/4}(\#\mathcal{U}\#\mathcal{V})^{3/4}\right)$$

$$\ll T\#\mathcal{U}\#\mathcal{V} + \#\mathcal{U}\#\mathcal{V}\log x + (\#\mathcal{U}\#\mathcal{V})^{3/4}x^{5/4}.$$

We now note that the second term never dominates and can be removed. Indeed, since $\#\mathcal{U}\#\mathcal{V} \le T^2$, we have for the geometric mean of the first and the third terms:

$$\sqrt{T\#\mathcal{U}\#\mathcal{V}\cdot(\#\mathcal{U}\#\mathcal{V})^{3/4}x^{5/4}} \ge (\#\mathcal{U}\#\mathcal{V})^{9/8}x^{5/8} \gg \#\mathcal{U}\#\mathcal{V}\log x.$$

This completes the proof.

3.9. **Proof of Theorem 9.** The proof of Theorem 9 is almost the same as that of Theorem 4 in Section 3.4, and in fact, is simpler, because the parameter $t \in \mathcal{I}(T)$ is an integer.

We only need to note that the number of solutions to the congruence

$$t_1 \equiv t_2 \pmod p, \qquad t_1, t_2 \in \mathcal{I}(T),$$

is upper bounded by $O(T+T^2/p)$. Then, as in the proof of Theorem 4, we have

$$\sum_{\substack{t\in\mathcal{I}(T)\\ \Delta(t)\neq 0}} \pi_{E(t)}(\mathbb{K};x) \ll \sum_{p\le x} (x^{-1/6}p^{1/2} + x^{1/12}p^{1/4})(T^{1/2} + Tp^{-1/2})$$

$$\ll T^{1/2}x^{4/3} + Tx^{5/6},$$

which concludes the proof.

3.10. **Proof of Theorem 10.** Using the notation in Section 2.6 and noticing the discussion about $N(u+v)$ and $\Delta(u+v)$ in Section 2.1, we have

$$\sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\neq 0}} \pi_{E(u+v)}(\alpha,\beta;x) = \sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\neq 0}} \sum_{\substack{p\le x\\ p\nmid N(u+v)\\ \psi_p(E(u+v))\in[\alpha,\beta]}} 1$$
$$= \sum_{p\le x} \sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\not\equiv 0 \pmod p\\ \psi_p(E(u+v))\in[\alpha,\beta]}} 1 = \sum_{p\le x} \mathscr{D}_{f,g,p}(\mathcal{U},\mathcal{V};\alpha,\beta).$$

By Lemma 24, we get

$$\sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(u+v)\neq 0}} \pi_{E(u+v)}(\alpha,\beta;x) - \sum_{p\le x} \mu_{\mathrm{ST}}(\alpha,\beta)\#\mathcal{U}\#\mathcal{V}$$
$$\ll \sum_{p\le T} \#\mathcal{U}\#\mathcal{V} + \sum_{T<p\le x} p^{1/4}(\#\mathcal{U}\#\mathcal{V})^{3/4}$$
$$\ll \pi(T)\#\mathcal{U}\#\mathcal{V} + \pi(x)x^{1/4}(\#\mathcal{U}\#\mathcal{V})^{3/4}.$$

Then, the desired result follows from the assumptions $\#\mathcal{U}\#\mathcal{V} \ge x^{1+\varepsilon}$ and $T \le x^{1-\varepsilon}$.

Acknowledgements

The authors would like to thank the referee for careful reading and valuable comments. The research of the authors was supported by the Australian Research Council Grant DP130100237.

References

[1] A. Ayyad, T. Cochrane and Z. Zheng, *The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$, and mean values of character sums*, J. Number Theory 59 (1996), 398–413.

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

[3] S. Baier, *A remark on the Lang–Trotter conjecture*, in: New Directions in Value-Distribution Theory of Zeta and L-functions, R. Steuding and J. Steuding (eds.), Shaker Verlag, 2009, 11–18.

[4] S. Baier and N. Jones, *A refined version of the Lang–Trotter conjecture*, Int. Math. Res. Not. 3 (2009), 433–461.

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

[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] T. Barnet-Lamb, D. Geraghty, M. Harris and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, Publ. Res. Inst. Math. Sci. 47 (2011), 29–98.

[8] L. Clozel, M. Harris and R. Taylor, *Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations*, Pub. Math. IHES 108 (2008), 1–181.

[9] A. C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, in: Proc. 7th Meeting of the Canadian Number Theory Association (CRM Proceedings and Lecture Notes 36), E. Goren and H. Kisilevsky (ed.), Amer. Math. Soc., 2004, 61–79.

[10] A. C. Cojocaru and C. David, *Frobenius fields for elliptic curves*, Amer. J. Math. 130 (2008), 1535–1560.

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

[12] A. C. 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.

[13] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Int. Math. Res. Not. 1999 (1999), 165–183.

[14] C. David and E. Smith, *Elliptic curves with a given number of points over finite fields*, Compositio Math. 149 (2013), 175–203.

[15] C. David and J. J. Urroz, *Square-free discriminants of Frobenius rings*, Int. J. Number Theory 6 (2010), 1391–1412.

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

[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 University Press, Oxford, 1979.

[19] M. Harris, N. Shepherd-Barron and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Ann. Math. 171 (2010), 779–813.

[20] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.

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

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

[23] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Monatsh. Math. 120 (1995), 127–136.

[24] V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C.R. Acad. Sci. Paris, Série I 319 (1994), 523–528.

[25] H. Niederreiter, *The distribution of values of Kloosterman sums*, Arch. Math. 56 (1991), 270–277.

[26] I. E. Shparlinski, *Exponential sums with Farey fractions*, Bull. Polish Acad. Sci. Math. 57 (2009), 101–107.
[27] I. E. Shparlinski, *Tate–Shafarevich groups and Frobenius fields of reductions of elliptic curves*, Quart. J. Math. 61 (2010), 255–263.
[28] I. E. Shparlinski, *On the Sato–Tate conjecture on average for some families of elliptic curves*, Forum Math. 25 (2013), 647–664.
[29] I. E. Shparlinski, *On the Lang–Trotter and Sato–Tate conjectures on average for polynomial families of elliptic curves*, Michigan Math. J. 62 (2013), 491–505.
[30] I. E. Shparlinski, *Elliptic curves over finite fields: Number theoretic and cryptographic aspects*, in: Advances in Applied Mathematics, Modeling, and Computational Science, R. Melnik and I. Kotsireas (eds.), Springer, 2013, 65–90.
[31] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, 2009.
[32] R. Taylor, *Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations II*, Pub. Math. IHES 108 (2008), 183–239.

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: shamin2010@gmail.com

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: igor.shparlinski@unsw.edu.au