THE SATO–TATE DISTRIBUTION IN THIN PARAMETRIC FAMILIES OF ELLIPTIC CURVES

RÉGIS DE LA BRETÈCHE, MIN SHA, IGOR E. SHPARLINSKI, AND JOSÉ FELIPE VOLOCH

Abstract. We obtain new results concerning the Sato–Tate conjecture on the distribution of Frobenius traces over single and double parametric families of elliptic curves. We consider these curves for values of parameters having prescribed arithmetic structure: product sets, geometric progressions, and most significantly prime numbers. In particular, some families 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

$$\Delta(Z) \neq 0 \qquad \text{and} \qquad j(Z) \notin \mathbb{Q}, \tag{1.1}$$

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

$$E(Z): \quad Y^2 = X^3 + f(Z)X + g(Z) \tag{1.2}$$

over the function field $\mathbb{Q}(Z)$; see [36] for a general background on elliptic curves. In particular, we refer to [36] for the notions of the *conductor* N_E of an elliptic curve E and *CM-curves*.

There exists an extensive literature on investigating the properties of the specialisations $E(t)$ modulo consecutive primes $p \le x$ for a growing parameter x and for the parameter t that runs through some interesting sets $\mathcal{T}$ of integer or rational numbers, see [32] for a survey and some recent results; a short outline is also given in Section 1.2.

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

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

More precisely, 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 also define, as usual, the *Frobenius trace* $a_p(E) = p + 1 - \#E_p(\mathbb{F}_p)$.

There are several possible scenarios in the study of the curves from the family (1.2) (or similar family (1.5)) and their reductions:

- One can fix a curve and vary the prime p. This is usually called the *horizontal* aspect (and is typically very hard to study).
- One can fix a prime p and consider the curves $E_p(t)$ for all values of the parameter t from some "interesting" set $\mathcal{T}$. This is usually called the *vertical* aspect.
- One can vary both the prime p and the curves $E_p(t)$ for $t \in \mathcal{T}$, we call this the *mixed* aspect.

Clearly the mixed aspect combines both horizontal and vertical aspects and often leads to results which are not possible within either of them.

Recall that by the Hasse bound (see [36]), we can define the *Frobenius angle* $\psi_p(E) \in [0, \pi]$ via the identity

$$\cos \psi_p(E) = \frac{a_p(E)}{2\sqrt{p}}. \tag{1.3}$$

Then, in general terms, the *Sato–Tate conjecture* predicts that the distribution of the angles $\psi_p(E)$ is governed by the *Sato–Tate density*

$$\mu_{\mathtt{ST}}(\alpha, \beta) = \frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 \vartheta \, \mathrm{d}\vartheta = \frac{2}{\pi} \int_{\cos \beta}^{\cos \alpha} (1 - z^2)^{1/2} \, \mathrm{d}z, \tag{1.4}$$

where $[\alpha, \beta] \subseteq [0, \pi]$.

In the vertical aspect when p is fixed and E is chosen at random from the set of all elliptic curves over $\mathbb{F}_p$, this has been shown by Birch [9].

The horizontal aspects is much harder and the Sato–Tate conjecture has been settled only quite recently in the series of works of Barnet-Lamb, Geraghty, Harris and Taylor [7], Clozel, Harris and Taylor [10], Harris, Shepherd-Barron and Taylor [19], and Taylor [37]. In particular, given a non-CM elliptic curve E of conductor N_E, for the number $\pi_E(\alpha, \beta; x)$ of primes $p \le x$ (with $p \nmid N_E$) for which $\psi_p(E) \in [\alpha, \beta] \subseteq [0, \pi]$, we have

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

as $x \to \infty$. However, this asymptotic formula lacks an explicit error term.

Here, we are mostly interested in the vertical and mixed aspects however extended only to some families of curves, such as (1.2) specialised for parameters t from a sparse set $\mathcal{T}$, rather than for all curves over $\mathbb{F}_p$ as in [9]. We show for several such families of curves and sets $\mathcal{T}$ that the Frobenius angles are also distributed according to the Sato–Tate density. Several results of this type are already known, however mostly for sets $\mathcal{T}$ of integers having some *additive structure* such as intervals of consecutive integers or sumsets, see [32, 34]. Here, thanks to Lemma 3.4 we consider a new class of sets $\mathcal{T}$ which are defined by some *multiplicative conditions* such as primes or multiplicative subgroups of $\mathbb{F}_p^*$. In particular, such sets tend to be much sparser than the sets studied in previous works.

As an application of these results, we also consider the mixed situation when both the curve and the prime vary.

Similar questions have also been studied for some other families such as (1.5) below, with u and v in some subsets of $\mathbb{F}_p$, see Section 1.2 for more details.

1.2. **Previous results.** The idea of studying the properties of reduction E_p for $p \le x$ on average over a family of elliptic curves E is due to Fouvry and Murty [17], who have considered the frequency of vanishing $a_p(E_{u,v}) = 0$ for the family of curves

$$E_{u,v}: \ Y^2 = X^3 + uX + v, \tag{1.5}$$

where the integers u and v satisfy the inequalities $|u| \le U$, $|v| \le V$. The result of [17] has been extended to other values of $a_p(E_{u,v})$ by David and Pappalardi [14] and Baier [2], see also [3]. This corresponds to the *Lang–Trotter conjecture*, see [25], on average over a family of curves (1.5).

The above results and methods of [2, 3, 14, 17] can also be used to establish the Sato–Tate conjecture on average for the family (1.5), see also [4, 34]. However, Banks and Shparlinski [6] have shown that using a different approach, based on bounds of multiplicative character sums and the large sieve inequality (instead of the exponential sum technique employed in [17]), one can establish the Sato–Tate conjecture on average for the curves (1.5).

Furthermore, Shparlinski [34] has established the Sato–Tate conjecture on average for more general families of the form $E_{f(u),g(v)}$ with integers $|u| \le U$, $|v| \le V$. Recently, Sha and Shparlinski [32] have established the Sato–Tate conjecture on average for the families of curves $E(u + v)$, where u, v both run through some subsets of $\{1, 2, \dots, T\}$, or both run over the set $\mathcal{F}(T)$:

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

Finally, Cojocaru and Hall [11] have studied the family of curves (1.2) and obtained an upper bound on the frequency of the event $a_p(E(t)) = a$ for a fixed integer a, when the parameter t runs through the set $\mathcal{F}(T)$. Cojocaru and Shparlinski [12] have improved [11, Theorem 1.4], which then has been further improved by Sha and Shparlinski [32].

1.3. **Distribution of Frobenius traces and ranks.** Our motivation also comes from the so-called *explicit* formulas, which can be found in the works of Mestre [26, 27] that link the behaviour of Frobenius traces on consecutive primes (that is, the horizontal aspect) and the rank of the corresponding elliptic curve. This link has been used by Fouvry and Pomykala [18], Michel [28] and Silverman [35] to estimate the average rank in some families of elliptic curves. For example, Michel [28, Theorem 1.3] and, in a stronger form, Silverman [35, Theorem 0.1] give explicit bounds on the average rank of the curves $E(t)$ in the family (1.2) with t running through all integers of the interval $[-T, T]$ with $\Delta(t) \ne 0$ as $T \to \infty$. This direction is naturally related to the mixed aspect. The results here also can be compared to the recent result of Bhargava and Shankar [8] that the average rank of all elliptic curves over $\mathbb{Q}$ (when ordered by height) is bounded, see also [24, 31] for outlines of several other related results.

Combining our estimates with the approaches of [18, 28, 35], one may obtain upper bounds on average ranks of families of curves with parameters from sets of prescribed multiplicative structure, such as primes, geometric progressions, and product sets.

1.4. **General notation.** Here we use the Landau symbol 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 $c > 0$.

Throughout the paper the implied constants may, where obvious, depend on the polynomials f and g in (1.2) and the real positive parameter ε, and are absolute otherwise. Occasionally they also depend on the integer parameter λ which we indicate as O_λ and $\ll_\lambda$.

As usual, $A = o(B)$ means that $A/B \to 0$ and $A \sim B$ means that $A/B \to 1$.

Furthermore, the letters ℓ and p always denote a prime number, and as usual, we use $\pi(x)$ to denote the number of $p \le x$.

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 example, compare the definitions of $N_p(\alpha, \beta; \mathcal{G})$, $N_p(\alpha, \beta; \mathcal{U}, \mathcal{V})$ and $Q_p(\alpha, \beta; L)$ in Sections 2.2 and 2.3 below).

2. Main Results

2.1. **Our approach.** In this paper, we consider the Sato–Tate conjecture on average for the polynomial family (1.2) of elliptic curves when the variable Z is specialised to a parameter t from sets of prescribed multiplicative structure, such as subgroups of $\mathbb{F}_p^*$, prime numbers, and geometric progressions.

We believe that these are the first known results that involve such sets of parameters.

To derive our results we introduce several new ideas, such as a version of a result of Michel [28, Proposition 1.1] with multiplicative characters (see Lemma 3.4). This is combined with a technique of Niederreiter [30, Lemma 3]. To study the curves (1.2) for specialisations at consecutive primes, we also estimate some bilinear sums (which maybe of independent interest) and combine this bound with the Vaughan identity [38, 39].

We are now able to give exact formulations of our results. We always assume that the polynomials f and g in (1.2) are fixed and so we do not include them in our notation. We also often impose the following modulo p analogue of the condition (1.1):

$$\Delta(Z) \not\equiv 0 \pmod p \quad \text{and} \quad j(Z) \text{ is not constant modulo } p. \tag{2.1}$$

2.2. **Our results in the vertical aspect.** Here, we fix an interval $[\alpha, \beta] \subseteq [0, \pi]$, we also fix an arbitrary prime p for Theorems 2.1, 2.2, 2.3 and 2.4.

Given a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$, we denote by $N_p(\alpha, \beta; \mathcal{G})$ the number of $w \in \mathcal{G}$ for which $\Delta(w) \neq 0$ and $\psi_p(E(w)) \in [\alpha, \beta]$.

Theorem 2.1. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (2.1). Then for any subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order r, uniformly over $[\alpha, \beta] \subseteq [0, \pi]$, we have*

$$N_p(\alpha, \beta; \mathcal{G}) = \mu_{\mathtt{ST}}(\alpha, \beta) r + O\left(r^{1/2} p^{1/4}\right).$$

We remark that noticing the trivial bound $N_p(\alpha, \beta; \mathcal{G}) \le r$, the result in Theorem 2.1 is non-trivial when $r > r^{1/2} p^{1/4}$, namely $r > \sqrt{p}$.

Similarly, given two sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p^*$, we denote by $N_p(\alpha, \beta; \mathcal{U}, \mathcal{V})$ the number of $(u, v) \in \mathcal{U} \times \mathcal{V}$ for which $\Delta(uv) \neq 0$ and $\psi_p(E(uv)) \in [\alpha, \beta]$.

Theorem 2.2. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (2.1). Then for any non-empty subsets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p^*$, uniformly over $[\alpha, \beta] \subseteq [0, \pi]$, we have*

$$N_p(\alpha, \beta; \mathcal{U}, \mathcal{V}) = \mu_{\mathtt{ST}}(\alpha, \beta)\#\mathcal{U}\#\mathcal{V} + O\left((\#\mathcal{U}\#\mathcal{V})^{3/4} p^{1/4}\right).$$

Note that the result in Theorem 2.2 is non-trivial when $\#\mathcal{U}\#\mathcal{V} > p$.

Furthermore, given an integer L, we denote by $Q_p(\alpha, \beta; L)$ the number of primes $\ell \le L$ for which $\Delta(\ell) \not\equiv 0 \pmod p$ and $\psi_p(E(\ell)) \in [\alpha, \beta]$.

First we record the following result whose proof rests on the recent work of Fouvry, Kowalski and Michel [16].

Theorem 2.3. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (2.1). Then, for any $\varepsilon > 0$, there exists some $\rho > 0$ such that for any integer $L \ge p^{3/4+\varepsilon}$, uniformly over $[\alpha, \beta] \subseteq [0, \pi]$ we have*

$$Q_p(\alpha, \beta; L) = \left(\mu_{\mathtt{ST}}(\alpha, \beta) + O\left(p^{-\rho}\right)\right) \pi(L).$$

We remark that it is apparent from the proof of Theorem 2.3, given in Section 4.3, that we always have $\rho < 1/48$ within this approach (and perhaps much smaller depending on the constant A in Lemma 3.12). Hence, for large L, using different arguments we derive a stronger bound with an explicit saving.

Theorem 2.4. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (2.1). Then for any integer $L \ge 3$, uniformly over $[\alpha, \beta] \subseteq [0, \pi]$, we have*

$$\begin{aligned} Q_p(\alpha, \beta; L) = &\mu_{\mathtt{ST}}(\alpha, \beta)\pi(L) \\ &\qquad + O\left(\left(Lp^{-1/4} + L^{11/12} + L^{3/4}p^{1/4}\right) L^{c/\log\log L}\right), \end{aligned}$$

for some absolute constant $c > 0$.

One should note that the result in Theorem 2.4 is non-trivial only when $L > p$. We also remark that Theorem 2.4 is better than Theorem 2.3 when L is large but not too large compared with p (for example, polynomially lower and upper bounded in terms of p). Otherwise, Theorem 2.3 may be better, such as $L \ge \exp(p)$.

2.3. **Our results in the mixed aspect.** Here, we establish the Sato–Tate conjecture on average for some families of elliptic curves which have never been studied in the literature.

Recall that for any integer t with $\Delta(t) \neq 0$, we use $\pi_{E(t)}(\alpha, \beta; x)$ to denote the number of primes $p \le x$ with $p \nmid N_{E(t)}$ (or equivalently, $\Delta(t) \not\equiv 0 \pmod p$, see Section 3.1) and $\psi_p(E(t)) \in [\alpha, \beta]$. First, we get an analogue of [32, Theorems 10].

Theorem 2.5. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1), and non-empty sets of integer $\mathcal{U}, \mathcal{V} \subseteq [1, x]$, $x \geq 2$, are arbitrary. Then, uniformly over $[\alpha, \beta] \subseteq [0, \pi]$, we have*

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

In Theorem 2.5, if $x = o(\#\mathcal{U}\#\mathcal{V})$, then we indeed establish the Sato-Tate conjecture on average for the corresponding family of elliptic curves.

Now, we establish the Sato–Tate conjecture on average when the parameter runs through some new kinds of subsets which have not been studied before.

First, we establish the Sato–Tate conjecture on average with a parameter t from a geometric progression. Namely, given integers t, λ with $|\lambda| \geq 2$ and real $x \geq 2$, we use $\pi_\lambda(\alpha, \beta; t, x)$ to denote the number of $p \leq x$ with $\Delta(\lambda^t) \not\equiv 0 \pmod p$ and $\psi_p(E(\lambda^t)) \in [\alpha, \beta]$. We also define the *Erdős constant*

$$\delta = 1 - \frac{1 + \log\log 2}{\log 2} = 0.086071\ldots. \tag{2.2}$$

Then we have:

Theorem 2.6. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1). Then for any real $x \geq 3$ and integer*

$$T \geq x^{1/2}(\log x)^{1+3\delta/2}(\log\log x)^{9/4},$$

uniformly over $[\alpha, \beta] \subseteq [0, \pi]$, we have

$$\frac{1}{\pi(x)T} \sum_{\substack{1\leq t\leq T\\ \Delta(\lambda^t)\neq 0}} \pi_\lambda(\alpha, \beta; t, x) = \mu_{\mathtt{ST}}(\alpha, \beta) + O_\lambda\left((\log x)^{-3\delta/4}(\log\log x)^{-9/8}\right),$$

where δ is given by (2.2).

It is possible to get a better error term if one averages on λ, however we do not address this question here.

For families parametrised by primes, averaging the estimate in Theorem 2.3, we get the following result.

Theorem 2.7. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1). Then, for any $\varepsilon > 0$ with the constant $\rho > 0$ defined in Theorem 2.3, for any real $x \ge 2$ and integer L with $L \ge x^{3/4+\varepsilon}$, uniformly over $[\alpha, \beta] \subseteq [0, \pi]$ we have*

$$\frac{1}{\pi(x)\pi(L)} \sum_{\substack{\text{prime } \ell \le L \\ \Delta(\ell) \ne 0}} \pi_{E(\ell)}(\alpha, \beta; x) = \mu_{\mathtt{ST}}(\alpha, \beta) + O\left(x^{-\rho}\right).$$

Finally, for large values of L, averaging the estimate in Theorem 2.4, we derive the following explicit result.

Theorem 2.8. *Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1). Then, for any real $x \ge 2$ and any integer $L \ge 3$, uniformly over $[\alpha, \beta] \subseteq [0, \pi]$ we have*

$$\begin{aligned} \frac{1}{\pi(x)\pi(L)} & \sum_{\substack{\text{prime } \ell \le L \\ \Delta(\ell) \ne 0}} \pi_{E(\ell)}(\alpha, \beta; x) \\ & = \mu_{\mathtt{ST}}(\alpha, \beta) + O\left(\left(x^{-1/4} + L^{-1/12} + L^{-1/4}x^{1/4}\right) L^{c/\log\log L}\right), \end{aligned}$$

for some absolute constant $c > 0$.

Note that in Theorem 2.8, if $L \ge x^{1+\varepsilon}$ and L can be polynomially upper bounded in terms of x, then the error term tends to zero when x goes to infinity.

3. Preliminaries

3.1. Primes of good reduction.

We start with the observation that the condition (1.1) (over any field $\mathbb{K}$ of characteristic $p > 3$) implies that $\Delta(Z) \in \mathbb{K}[Z]$ is not a constant polynomial. Indeed, if $\Delta(Z) = c \ne 0$ for some $c \in \mathbb{K}$ then $f(Z)$ and $g(Z)$ have no common roots. Since $j(Z)$ is not constant, both f and g are also not constant. Now, considering the derivative $\Delta'(Z) = 0$, we easily see that f and g must have common roots, which leads to a contradiction.

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 fraction.

Note that for $t \in \mathbb{Q}$, the discriminant $\Delta(t)$ 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 [36, 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 $\Delta(t)$).

3.2. **Preparations for distribution of angles.** For m arbitrary elements $w_1, \ldots, w_m \in [-1,1]$ (not necessarily distinct) and an arbitrary subinterval $\mathcal{J} \subseteq [-1,1]$, let $A(\mathcal{J}; m)$ be the number of integers i, $1 \le i \le m$, with $w_i \in \mathcal{J}$. For any $-1 \le a < b \le 1$, define the function

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

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

$$U_n(\cos\vartheta) = \operatorname{sym}_n(\vartheta),$$

where

$$\operatorname{sym}_n(\vartheta) = \frac{\sin((n+1)\vartheta)}{\sin\vartheta}. \tag{3.1}$$

The following result is exactly from [32, Lemma 17], which is a direct consequence of a result of Niederreiter [30, Lemma 3].

Lemma 3.1. *For any integer $k \ge 1$, we have*

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

Corollary 3.2. *Given m arbitrary angles $\psi_1, \ldots, \psi_m \in [0,\pi]$ (not necessarily distinct), assume that for some constant $A > 0$ we have*

$$\left| \sum_{i=1}^{m} \operatorname{sym}_n(\psi_i) \right| \le n^A \sigma$$

for every integer $n \ge 1$. Then, uniformly over $[\alpha,\beta] \subseteq [0,\pi]$, we have

$$\#\{\psi_i \in [\alpha,\beta] : 1 \le i \le m\} = \mu_{\mathtt{ST}}(\alpha,\beta)m + O\left(m^{A/(A+1)}\sigma^{1/(A+1)}\right).$$

Proof. We apply Lemma 3.1 to the sequence $\cos\psi_1, \ldots, \cos\psi_m$ and obtain

$$\max_{[\alpha,\beta] \subseteq [0,\pi]} |\#\{\psi_i \in [\alpha,\beta] : 1 \le i \le m\} - \mu_{\mathtt{ST}}(\alpha,\beta)m| \ll \frac{m}{k} + k^A\sigma.$$

Now, assume that $\sigma < m$ as otherwise the result is trivial. Then, we conclude the proof by taking $k = \left\lceil (m/\sigma)^{1/(A+1)} \right\rceil$. $\square$

3.3. **Bounds on some single sums.** Michel [28, Proposition 1.1] gives a bound for the sum of the function $\mathrm{sym}_n(\vartheta)$, given by (3.1) twisted by additive characters.

We refer to [21] for background on characters. We use the notation $\mathbf{e}_p(z) = \exp(2\pi i z/p)$ and record here the following immediate consequence of [28, Proposition 1.1].

Lemma 3.3. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1), for any prime p we have*

$$\sum_{\substack{w \in \mathbb{F}_p \\ \Delta(w) \neq 0}} \mathrm{sym}_n\left(\psi_p(E(w))\right) \mathbf{e}_p\left(mw\right) \ll np^{1/2},$$

uniformly over all integers $m \geq 0$ and $n \geq 1$.

We need the following analogue of [28, Proposition 1.1] (in a more precise form than Lemma 3.3) for the sum of the function $\mathrm{sym}_n(\vartheta)$ twisted by multiplicative characters.

Lemma 3.4. *Given a prime p, if the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (2.1), then for any multiplicative character χ of $\mathbb{F}_p^*$ and any integer $n \geq 1$, we have*

$$\left| \sum_{\substack{w \in \mathbb{F}_p \\ \Delta(w) \neq 0}} \mathrm{sym}_n\left(\psi_p(E(w))\right) \chi\left(w\right) \right| \leq (n+1) \deg \Delta \sqrt{p}.$$

Proof. The proof is similar to that of [28, Proposition 1.1] and is a rather standard application of techniques of étale cohomology (see, for example, [29] for a general reference) and the work of Deligne and Katz (see [22, 23]). So, we only point out the changes that need to be made to the argument of the proof of [28, Proposition 1.1] and refer to [28] for more details and the main argument.

We work over $\mathbb{F}_p$. Let $U = \mathbb{A}^1 - \{Z\Delta(Z) = 0\}$ and $\mathcal{E}$ the total space of the family of elliptic curves given by (1.2) over U. Consider the map $\pi : \mathcal{E} \to U$ (given by Z).

Using the standard notation of $\pi_!$ as the direct image functor and $R^1\pi_!$ as the first derived functor of $\pi_!$ (see [29]), we now consider the sheaf $\mathcal{F} = R^1\pi_!\mathbb{Q}_\ell(1/2)$.

The desired result follows easily, for example, from [22, Key Lemma, Page 286], applied to $\mathrm{Sym}_n(\mathcal{F}) \otimes \mathcal{L}_\chi$, once the hypotheses are checked, where $\mathcal{L}_\chi$ is the Kummer sheaf associated to χ, as in [23] and that the needed facts about it are proved in [23, Section 7].

Michel [28] only needs to work in the larger open set $\mathbb{A}^1 - \{\Delta = 0\}$, but $\mathcal{L}_\chi$ is not well-behaved at $Z = 0$ unlike the sheaf corresponding to an additive character. On the other hand, $\mathcal{L}_\chi$ is tamely ramified. Just as in [28], using Sym_n the n-th symmetric power of a sheaf, we obtain the triviality of the following cohomology groups

$$H^i(U, \mathrm{Sym}_n(\mathcal{F}) \otimes \mathcal{L}_\chi) = 0, \qquad i \neq 1,$$

because of the monodromy of $\mathcal{F}$ computed there and the fact that $\mathcal{L}_\chi$ is a pure sheaf of rank one over U.

To complete the proof we need a formula for the dimension of the first cohomology group $H^1(U, \mathrm{Sym}_n(\mathcal{F}) \otimes \mathcal{L}_\chi)$. As both $\mathrm{Sym}_n(\mathcal{F})$ and $\mathcal{L}_\chi$ are lisse over U and $\mathcal{L}_\chi$ is tame of rank one, this dimension is the rank of $\mathrm{Sym}_n(\mathcal{F})$, namely $n+1$, times the Euler characteristic of U, that is

$$\#(\mathbb{P}^1 - U) + 2 \cdot 0 - 2 \leq \deg \Delta,$$

proving the desired estimate. □

Using characters to detect a multiplicative subgroup of $\mathbb{F}_p^*$, we immediately derive from Lemma 3.4 a more general result.

Lemma 3.5. *Given a prime p, if the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (2.1), then for any multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$, any multiplicative character χ of $\mathbb{F}_p^*$ and any integer $n \geq 1$, we have*

$$\left| \sum_{\substack{w \in \mathcal{G} \\ \Delta(w) \neq 0}} \mathrm{sym}_n \left(\psi_p(E(w))\right) \chi(w) \right| \leq (n+1) \deg \Delta \sqrt{p}.$$

Proof. Let $\mathcal{X}_p$ denote the set of all $p-1$ multiplicative characters of $\mathbb{F}_p$. Using the orthogonality of multiplicative characters, we obtain

$$\begin{aligned} &\sum_{\substack{w \in \mathcal{G} \\ \Delta(w) \neq 0}} \mathrm{sym}_n \left(\psi_p(E(w))\right) \chi(w) \\ &\qquad = \sum_{\substack{u \in \mathbb{F}_p^* \\ \Delta(u) \neq 0}} \mathrm{sym}_n \left(\psi_p(E(u))\right) \sum_{w \in \mathcal{G}} \frac{\chi(w)}{p-1} \sum_{\phi \in \mathcal{X}_p} \phi(wu^{-1}) \\ &\qquad = \frac{1}{p-1} \sum_{\phi \in \mathcal{X}_p} \sum_{\substack{u \in \mathbb{F}_p^* \\ \Delta(u) \neq 0}} \mathrm{sym}_n \left(\psi_p(E(u))\right) \bar{\phi}(u) \sum_{w \in \mathcal{G}} \chi(w)\phi(w), \end{aligned}$$

where $\bar{\phi}(u) = \phi(u^{-1})$. So, Lemma 3.4 yields that

$$\begin{aligned}\left|\sum_{\substack{w\in\mathcal{G}\\ \Delta(w)\neq 0}} \mathrm{sym}_n\left(\psi_p(E(w))\right)\right| &\le \frac{(n+1)\deg\Delta\sqrt{p}}{p-1}\sum_{\phi\in\mathcal{X}_p}\left|\sum_{w\in\mathcal{G}}\chi(w)\phi(w)\right|\\ &= (n+1)\deg\Delta\sqrt{p},\end{aligned}$$

where the identity follows from the fact that the sum $\sum_{w\in\mathcal{G}}\chi(w)\phi(w)$ is equal to $\#\mathcal{G}$ if the restriction of ϕ to $\mathcal{G}$ is the inverse of χ and zero otherwise. □

From Lemma 3.5, we see that for any polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfying (1.1), we have

$$\sum_{\substack{w\in\mathcal{G}\\ \Delta(w)\neq 0}} \mathrm{sym}_n\left(\psi_p(E(w))\right)\chi(w) \ll n\sqrt{p},$$

which is how we usually apply it.

Furthermore, we also have an analogue of Lemma 3.5 for incomplete sums which follows from the standard reduction between complete and incomplete sums (see [21, Section 12.2]).

Lemma 3.6. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1), then for any prime p, any integer λ with $\gcd(\lambda, p) = 1$ and of multiplicative order r modulo p, for any integer $T \le r$ and for any integer $n \ge 1$, we have*

$$\sum_{\substack{t=1\\ \Delta(\lambda^t)\not\equiv 0 \pmod p}}^{T} \mathrm{sym}_n\left(\psi_p(E(\lambda^t))\right) \ll n\sqrt{p}\log p.$$

Proof. The proof is based on the standard reduction between complete and incomplete sums (see [21, Section 12.2]). Indeed, let $\mathcal{G} \subseteq \mathbb{F}_p^*$ be the multiplicative subgroup of $\mathbb{F}_p^*$ generated by λ. Let $d = (p-1)/r$. Then, there exists a primitive element $\rho \in \mathbb{F}_p^*$ with $\lambda = \rho^d$. Now for $w \in \mathbb{F}_p^*$ we denote by $\operatorname{ind} w$ the unique integer $z \in [0, p-2]$ with $w = \rho^z$. Using the orthogonality of exponential function $\mathbf{e}(z) = \exp(2\pi i z)$, we write

$$\begin{aligned}&\sum_{\substack{t=1\\ \Delta(\lambda^t)\not\equiv 0 \pmod p}}^{T} \mathrm{sym}_n\left(\psi_p(E(\lambda^t))\right)\\ &\qquad = \sum_{\substack{w\in\mathbb{F}_p\\ \Delta(w)\neq 0}} \mathrm{sym}_n\left(\psi_p(E(w))\right)\sum_{t=1}^{T}\frac{1}{p-1}\sum_{s=0}^{p-2}\mathbf{e}\left(\frac{s(\operatorname{ind} w - dt)}{p-1}\right).\end{aligned}$$

Writing $\chi_s(w) = \mathbf{e}\left(s \operatorname{ind} w/(p-1)\right)$ and changing the order of summation we obtain

$$\sum_{\substack{t=1 \\ \Delta(\lambda^t)\not\equiv 0 \pmod p}}^{T} \operatorname{sym}_n\left(\psi_p(E(\lambda^t))\right) = \frac{1}{p-1}\sum_{s=0}^{p-2}\sum_{\substack{w\in\mathbb{F}_p \\ \Delta(w)\neq 0}} \operatorname{sym}_n\left(\psi_p(E(w))\right)\chi_s(w)\sum_{t=1}^{T}\mathbf{e}\left(-st/r\right).$$

It is easy to check that $\chi_s(w)$ is a multiplicative character of $\mathbb{F}_p^*$ for any $0 \le s \le p-2$. Thus by Lemma 3.4,

$$\sum_{\substack{t=1 \\ \Delta(\lambda^t)\not\equiv 0 \pmod p}}^{T} \operatorname{sym}_n\left(\psi_p(E(\lambda^t))\right) \ll np^{-1/2}\sum_{s=1}^{p-1}\left|\sum_{t=1}^{T}\mathbf{e}\left(st/r\right)\right|.$$

Using [21, Equation (8.6)], we know that if $r \nmid s$, we have

$$\left|\sum_{t=1}^{T}\mathbf{e}\left(st/r\right)\right| \le \frac{1}{2\|s/r\|},$$

where $\|s/r\|$ denotes the distance of s/r to the nearest integer. The result now follows. □

Finally we need the following slight generalisation of [34, Lemma 10], which is based on Lemma 3.3 and the same standard reduction between complete and incomplete sums (see [21, Section 12.2]) as we used in the proof of Lemma 3.6.

Lemma 3.7. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1), then for any prime p, any integers $M, N \ge 1$ and k with $\gcd(k,p) = 1$, we have*

$$\sum_{\substack{m=M+1 \\ \Delta(km)\not\equiv 0 \pmod p}}^{M+N} \operatorname{sym}_n\left(\psi_p(E(km))\right) \ll n\left(Np^{-1/2} + p^{1/2}\log p\right),$$

uniformly over all integers $n \ge 1$.

3.4. **Bounds on some bilinear sums.** The following bound of bilinear sums with "weights" is a direct application of Lemma 3.4.

Lemma 3.8. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1), then for any prime p, any $U, V \geq 1$ and non-empty sets of integers $\mathcal{U} \subseteq [1, U]$, $\mathcal{V} \subseteq [1, V]$ with $\gcd(uv, p) = 1$ for $u \in \mathcal{U}$, $v \in \mathcal{V}$, and two sequences of complex numbers $\{\alpha_u\}_{u\in\mathcal{U}}$ and $\{\beta_v\}_{v\in\mathcal{V}}$ with*

$$\max_{u\in\mathcal{U}} |\alpha_u| = A \qquad \text{and} \qquad \max_{v\in\mathcal{V}} |\beta_v| = B,$$

and for any integer $n \geq 1$, we have

$$\sum_{\substack{u\in\mathcal{U}, v\in\mathcal{V} \\ \Delta(uv)\not\equiv 0 \pmod p}} \alpha_u \beta_v \operatorname{sym}_n\left(\psi_p(E(uv))\right) \ll nAB\sqrt{\#\mathcal{U}(U/p+1)\#\mathcal{V}(V/p+1)p}.$$

Proof. Let $\mathcal{X}_p$ denote the set of all $p-1$ multiplicative characters of $\mathbb{F}_p$. We note S the sum to be bounded. Using the orthogonality of multiplicative characters and the fact that $\chi(w^{-1}) = \overline{\chi}(w)$ for the complex conjugated character $\overline{\chi}$, we write

$$S = \frac{1}{p-1} \sum_{\chi\in\mathcal{X}_p} \sum_{\substack{w\in\mathbb{F}_p \\ \Delta(w)\neq 0}} \operatorname{sym}_n\left(\psi_p(E(w))\right) \overline{\chi}(w) \sum_{u\in\mathcal{U}} \alpha_u \chi(u) \sum_{v\in\mathcal{V}} \beta_v \chi(v).$$

Using Lemma 3.4 and the Cauchy inequality, we have

$$\begin{aligned} S &\ll np^{-1/2} \sum_{\chi\in\mathcal{X}_p} \left|\sum_{u\in\mathcal{U}} \alpha_u \chi(u)\right| \left|\sum_{v\in\mathcal{V}} \beta_v \chi(v)\right|. \\ &\ll np^{-1/2} \left(\sum_{\chi\in\mathcal{X}_p} \left|\sum_{u\in\mathcal{U}} \alpha_u \chi(u)\right|^2 \sum_{\chi\in\mathcal{X}_p} \left|\sum_{v\in\mathcal{V}} \beta_v \chi(v)\right|^2 \right)^{1/2}. \end{aligned} \tag{3.2}$$

Applying the orthogonality of multiplicative characters again, we derive

$$\begin{aligned} \sum_{\chi\in\mathcal{X}_p} \left|\sum_{u\in\mathcal{U}} \alpha_u \chi(u)\right|^2 &= \sum_{\chi\in\mathcal{X}_p} \sum_{u_1,u_2\in\mathcal{U}} \alpha_{u_1} \overline{\alpha}_{u_2} \chi(u_1 u_2^{-1}) \\ &= (p-1) \sum_{\substack{u_1,u_2\in\mathcal{U} \\ u_1\equiv u_2 \pmod p}} \alpha_{u_1} \overline{\alpha}_{u_2}. \end{aligned}$$

Hence,

$$\sum_{\chi\in\mathcal{X}_p} \left|\sum_{u\in\mathcal{U}} \alpha_u \chi(u)\right|^2 \leq (p-1)A^2 \#\mathcal{U}(U/p+1). \tag{3.3}$$

Similarly, we have

$$\sum_{\chi \in \mathcal{X}_p} \left| \sum_{v \in \mathcal{V}} \beta_v \chi(v) \right|^2 \le (p-1) B^2 \# \mathcal{V} (V/p+1). \tag{3.4}$$

Substituting (3.3) and (3.4) in (3.2), and then recalling (3.2), we conclude the proof. ☐

Finally, we need the following modification of Lemma 3.8.

Lemma 3.9. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1), then for any prime p, any integers $U, V, W \ge 1$ with $U \ge W$ and $V \ge 2$, two sequences of integers $\{W_u\}_{u=W}^{U}$ and $\{V_u\}_{u=W}^{U}$ with $1 \le W_u \le V_u \le V$ for each u and two sequences of complex numbers $\{\alpha_u\}_{u=W}^{U}$ and $\{\beta_v\}_{v=1}^{V}$ with*

$$\max_{u=W,\ldots,U} |\alpha_u| = A \qquad \text{and} \qquad \max_{v=1,\ldots,V} |\beta_v| = B,$$

and for any integer $n \ge 1$, we have

$$\sum_{u=W}^{U} \alpha_u \sum_{\substack{v=W_u \\ \Delta(uv) \not\equiv 0 \pmod p}}^{V_u} \beta_v \operatorname{sym}_n(\psi_p(E(uv)))$$
$$\ll nAB\sqrt{V(U-W+1)(U/p+1)(V/p+1)p} \log V.$$

Proof. First note that for any $n \ge 1$, we have

$$|\operatorname{sym}_n(\vartheta)| \le n+1. \tag{3.5}$$

Hence the contribution from the terms with $p \mid uv$ is at most $nABV(U-W+1)/p$, which is not greater than the desired upper bound. Thus, we can assume that $\alpha_u = 0$ if $p \mid u$, and $\beta_v = 0$ if $p \mid v$.

We define $\mathbf{e}_V(z) = \exp(2\pi i z/V)$. Then, for each inner sum, using the orthogonality of exponential functions, we write

$$\begin{aligned}
&\sum_{\substack{v=W_u \\ \Delta(uv)\not\equiv 0 \pmod p}}^{V_u} \beta_v \operatorname{sym}_n\left(\psi_p(E(uv))\right) \\
&\qquad = \sum_{\substack{v=1 \\ \Delta(uv)\not\equiv 0 \pmod p}}^{V} \beta_v \operatorname{sym}_n\left(\psi_p(E(uv))\right) \\
&\qquad\qquad \sum_{w=W_u}^{V_u} \frac{1}{V} \sum_{-V/2<s\le V/2} \mathbf{e}_V(s(v-w)) \\
&\qquad = \frac{1}{V} \sum_{-V/2<s\le V/2} \sum_{w=W_u}^{V_u} \mathbf{e}_V(-sw) \\
&\qquad\qquad \sum_{\substack{v=1 \\ \Delta(uv)\not\equiv 0 \pmod p}}^{V} \beta_v \mathbf{e}_V(sv) \operatorname{sym}_n\left(\psi_p(E(uv))\right).
\end{aligned}$$

In view of [21, Bound (8.6)], for each $u = 1, \ldots, U$ and every integer s such that $|s| \le V/2$ we can write

$$\sum_{w=W_u}^{V_u} \mathbf{e}_V(-sw) = \sum_{w=1}^{V_u} \mathbf{e}_V(-sw) - \sum_{w=1}^{W_u-1} \mathbf{e}_V(-sw) = \eta_{s,u} \frac{V}{|s|+1}$$

for some complex number $\eta_{s,u} \ll 1$. Thus, if we put $\widetilde{\alpha}_{s,u} = \alpha_u \eta_{s,u}$ and $\widetilde{\beta}_{s,v} = \beta_v \mathbf{e}_V(sv)$, it follows that

$$\begin{aligned}
&\sum_{u=1}^{U} \alpha_u \sum_{\substack{v=W_u \\ \Delta(uv)\not\equiv 0 \pmod p}}^{V_u} \beta_v \operatorname{sym}_n\left(\psi_p(E(uv))\right) \\
&\qquad = \sum_{-V/2<s\le V/2} \frac{1}{|s|+1} \sum_{u=W}^{U} \sum_{\substack{v=1 \\ \Delta(uv)\not\equiv 0 \pmod p}}^{V} \widetilde{\alpha}_{s,u} \widetilde{\beta}_{s,v} \operatorname{sym}_n\left(\psi_p(E(uv))\right).
\end{aligned}$$

Applying Lemma 3.8 with the sequences $(\widetilde{\alpha}_{s,u})_{u=W}^{U}$ and $(\widetilde{\beta}_{s,v})_{v=1}^{V}$ for each s, and noting that

$$\sum_{-V/2<s\le V/2} \frac{1}{|s|+1} \ll \log V$$

we derive the desired upper bound. $\square$

We are now ready to establish our main technical tool, which gives a bound of bilinear sums over a certain "hyperbolic" region of summation.

Lemma 3.10. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1), then for any prime p, any integers $U, V, W \ge 1$, a sequence of integers $\{Z_u\}_{u=1}^{U}$ with*

$$1 \le W \le U, \quad U \ge 2 \qquad \text{and} \qquad 1 \le Z_u < V, \ u = W, \ldots, U,$$

and two sequences of complex numbers $\{\alpha_u\}_{u=W}^{U}$ and $\{\beta_v\}_{v=1}^{V}$ with

$$\max_{u=W,\ldots,U} |\alpha_u| = A \qquad \text{and} \qquad \max_{v=1,\ldots,V} |\beta_v| = B,$$

and for any integer $n \ge 1$, we have

$$\sum_{W \le u \le U} \alpha_u \sum_{\substack{Z_u \le v \le V/u \\ \Delta(uv) \not\equiv 0 \pmod p}} \beta_v \operatorname{sym}_n\left(\psi_p(E(uv))\right)$$
$$\ll nAB\left(Vp^{-1/2} + VW^{-1/2} + (UV)^{1/2} + (Vp)^{1/2}\right) \log U \log V.$$

Proof. Note that the desired upper bound is better than the direct consequence of Lemma 3.9.

Let $\alpha_u = 0$ if $u < W$ or $u > U$. We also set $I = \lfloor \log W \rfloor$ and $J = \lfloor \log U \rfloor$, and consider the half-open intervals

$$\mathcal{I}_j = [e^j, e^{j+1}), \qquad (I \le j \le J).$$

Then,

$$\sum_{W \le u \le U} \alpha_u \sum_{\substack{Z_u \le v \le V/u \\ \Delta(uv) \not\equiv 0 \pmod p}} \beta_v \operatorname{sym}_n\left(\psi_p(E(uv))\right)$$
$$= \sum_{j=I}^{J} \sum_{u \in \mathcal{I}_j} \sum_{\substack{Z_u \le v \le V/u \\ \Delta(uv) \not\equiv 0 \pmod p}} \alpha_u \beta_v \operatorname{sym}_n\left(\psi_p(E(uv))\right).$$

Using Lemma 3.9, each inner double sum satisfies the bound

$$\sum_{u \in \mathcal{I}_j} \sum_{\substack{Z_u \le v \le V/u \\ \Delta(uv) \not\equiv 0 \pmod p}} \alpha_u \beta_v \operatorname{sym}_n\left(\psi_p(E(uv))\right)$$
$$\ll nAB\sqrt{V(e^j/p+1)(Ve^{-j}/p+1)p} \log V$$
$$\ll nAB\sqrt{V^2p^{-1} + V^2e^{-j} + Ve^j + Vp} \log V.$$

Summing over $j \in [I, J]$ we conclude the proof. $\square$

3.5. **Vaughan's Identity.** As usual, we use $\mu(d)$ to denote the Möbius function and Λ to denote the von Mangoldt function given by

$$\Lambda(t) = \begin{cases} \log \ell & \text{if } t \text{ is a power of some prime } \ell, \\ 0 & \text{if } t \text{ is not a prime power.} \end{cases}$$

We need the following result of Vaughan [38, 39], which is stated here in the form given in [13, Chapter 24] (see also [21, Section 13.4]).

Lemma 3.11. *For any complex-valued function $\psi(t)$ and any real numbers $K, M \ge 1$ with $KM \le L$ and $L \ge 2$, we have*

$$\sum_{t=1}^{L} \Lambda(t)\psi(t) \ll \Sigma_1 + \Sigma_2 \log(KM) + \Sigma_3 \log L + \Sigma_4,$$

where

$$\Sigma_1 = \left| \sum_{t \le M} \Lambda(t)\psi(t) \right|,$$

$$\Sigma_2 = \sum_{k \le KM} \left| \sum_{m \le L/k} \psi(km) \right|,$$

$$\Sigma_3 = \sum_{k \le K} \max_{w \ge 1} \left| \sum_{w \le m \le L/k} \psi(km) \right|,$$

$$\Sigma_4 = \left| \sum_{M < m \le L/K} \Lambda(m) \sum_{K < k \le L/m} \left(\sum_{\substack{d \mid k \\ d \le K}} \mu(d) \right) \psi(km) \right|.$$

So, Lemma 3.11 reduces the problem of estimating the sums over primes to sums over consecutive integers and bilinear sums, which for the function sym_n are available from Sections 3.3 and 3.4.

3.6. **Bounds on some sums over primes.** We start with showing that [16, Theorem 1.5] applies to the functions $\mathrm{sym}_n(\psi_p(E(t)))$ for every $n \ge 1$ and leads to the following bound:

Lemma 3.12. *For any fixed prime p and $0 < \eta < 1/48$, and polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ that satisfy (2.1), we have*

$$\sum_{\substack{\text{prime } \ell \le L \\ \Delta(\ell) \not\equiv 0 \,(\mathrm{mod}\, p)}} \mathrm{sym}_n(\psi_p(E(\ell))) \ll n^A \pi(L) (1 + p/L)^{1/12} p^{-\eta}$$

for any integer $n \ge 1$, where the implied constant and the constant A depend only on $f(Z)$, $g(Z)$ and η.

Proof. We first remark that in the result of [16, Equation (1.3) of Theorem 1.5], the factor X can be replaced by $\pi(X)$. This comes from the bound in [16, page 1714]

$$\mathcal{S}_{V,X}(\Lambda, K) \ll (pQ)^{\varepsilon} QXp^{-\eta}$$

and an integration by parts.

Now, we wish to apply [16, Equation (1.3) of Theorem 1.5] to the trace weight $K(\ell) = \mathrm{sym}_n(\psi_p(E(\ell)))$ associated to the sheaf $\mathrm{Sym}_n(\mathcal{F})$ considered in the proof of Lemma 3.4 (and in [28]), where η here corresponds to $\eta/2$ in [16]. We need to verify that this sheaf is not exceptional in the sense of [16] and estimate its conductor. The sheaf is not exceptional because its monodromy is not abelian, as seen in the proof of [28, Lemma 3.1]. The conductor is the dimension of the H^1 which has been estimated in the proof of Lemma 3.4 and is linear in n. The result now follows. $\square$

Remark 3.13. *Although this is not explicitly stated in [16], the constant A seems to be absolute (and in fact of very moderate value). If it is worked out explicitly then Theorem 2.7 can also be made more explicit.*

We now use a different method to bound the sums in Lemma 3.12 which is more efficient for $L \geq p$. First we estimate the sums weighted by the von Mangoldt function.

Lemma 3.14. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1.1), then for any prime p, and any integers $n \geq 1, L \geq 2$, we have*

$$\sum_{\substack{1 \leq t \leq L \\ \Delta(t) \not\equiv 0 \pmod p}} \Lambda(t)\,\mathrm{sym}_n(\psi_p(E(t))) \ll n\left(Lp^{-1/2} + L^{5/6} + L^{1/2}p^{1/2}\right) L^{c/\log\log L},$$

for some absolute constant $c > 0$.

Proof. We remark that the trivial upper bound on the above sum is $O(nL)$, so we can assume $p \leq L$. First, for any integer t put $\delta(t) = 1$ if $\Delta(t) \not\equiv 0 \pmod p$, and let $\delta(t) = 0$ otherwise. We fix some real numbers $K, M \geq 1$ with $KM \leq L$. We now need to estimate the sums Σ_i, $i = 1, \ldots, 4$, of Lemma 3.11 with $\psi(t) = \mathrm{sym}_n(\psi_p(E(t)))\,\delta(t)$.

We start with the observation that the classical bound on the divisor function $\tau(k)$ for $k \leq L$, see [1, Theorem 13.12], yields

$$\sum_{\substack{d \mid k \\ d \leq K}} \mu(d) \ll \tau(k) \leq L^{c/\log\log L},$$

where c is some absolute constant.

By the prime number theorem, and using (3.5) we can estimate Σ_1 trivially as

$$\Sigma_1 \ll nM. \tag{3.6}$$

To estimate Σ_2, we choose another parameter R and write

$$\Sigma_2 = \Sigma_{2,1} + \Sigma_{2,2}, \tag{3.7}$$

where

$$\Sigma_{2,1} = \sum_{k \le R} \left| \sum_{m \le L/k} \psi(km) \right|, \quad \Sigma_{2,2} = \sum_{R < k \le KM} \left| \sum_{m \le L/k} \psi(km) \right|.$$

For $\Sigma_{2,1}$ we estimate the inner sum by Lemma 3.7 for k not divisible by p and estimate the inner sum trivially for other k. Hence, we obtain

$$\begin{aligned}\Sigma_{2,1} &\ll n \sum_{\substack{k \le R\\ p \nmid k}} \left(\frac{L}{kp^{1/2}} + p^{1/2} \log p \right) + n \sum_{\substack{k \le R\\ p \mid k}} \frac{L}{k}\\ &\ll n \left(\frac{L \log R}{p^{1/2}} + Rp^{1/2} \log p \right).\end{aligned} \tag{3.8}$$

For $\Sigma_{2,2}$ we apply Lemma 3.10 (with $\beta_v = 1$ and $\alpha_u = \pm 1$ according to the sign of the inner sum) and derive

$$\Sigma_{2,2} \ll n \left(Lp^{-1/2} + LR^{-1/2} + (KLM)^{1/2} + (Lp)^{1/2} \right) (\log L)^2. \tag{3.9}$$

We now choose $R = L^{2/3}p^{-1/3}$ and substitute the bounds (3.8) and (3.9) in (3.7). Furthermore, we also note that we can write

$$\Sigma_3 = \sum_{k \le K} \left| \sum_{w_k \le m \le L/k} \psi(km) \right|,$$

where w_k, $1 \le k \le K$, are chosen to satisfy

$$\left| \sum_{w_k \le m \le L/k} \psi(km) \right| = \max_{w \ge 1} \left| \sum_{w \le m \le L/k} \psi(km) \right|.$$

Hence, Σ_3 can be split into two sums as in (3.7), and analogues of the bounds (3.8) and (3.9) apply to Σ_3 (with K in place of KM). We also note that for $L \ge p$ we have $\log p \le \log L$ and $L^{2/3}p^{1/6} \le L^{5/6}$. Therefore, we obtain

$$\Sigma_2 + \Sigma_3 \ll n \left(Lp^{-1/2} + L^{5/6} + (KLM)^{1/2} + (Lp)^{1/2} \right) (\log L)^2. \tag{3.10}$$

In addition, notice that in the area of the summation in Σ_4 we always have $k \le L/M$ and $m \le L/K$. Hence, applying Lemma 3.10 to estimate Σ_4, we deduce

$$\Sigma_4 \ll n\left(Lp^{-1/2} + LM^{-1/2} + LK^{-1/2} + L^{1/2}p^{1/2}\right) L^{c/\log\log L}. \tag{3.11}$$

Comparing (3.10) with (3.11), we choose $K = M = L^{1/3}$ to balance these estimates, which also dominate (3.6). Then, substituting the above estimates into Lemma 3.11 we obtain

$$\sum_{\substack{1 \le t \le L \\ \Delta(t) \not\equiv 0 \pmod p}} \Lambda(t)\, \mathrm{sym}_n\left(\psi_p(E(t))\right) \ll n\left(Lp^{-1/2} + L^{5/6} + L^{1/2}p^{1/2}\right) L^{c/\log\log L}.$$

The result now follows. □

Via partial summation we are now immediately ready to obtain our main technical ingredient for the proof of Theorem 2.4.

Corollary 3.15. *If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (2.1), then for any prime p, and any integer $n \ge 1$, we have*

$$\sum_{\substack{\text{prime } \ell \le L \\ \Delta(\ell) \not\equiv 0 \pmod p}} \mathrm{sym}_n\left(\psi_p(E(\ell))\right) \ll n\left(Lp^{-1/2} + L^{5/6} + (Lp)^{1/2}\right) L^{c/\log\log L},$$

where c is some absolute constant.

3.7. **Distribution of multiplicative orders.** For integer λ and prime p with $\gcd(p, \lambda) = 1$, let $\mathrm{ord}_p\,\lambda$ denote the multiplicative order of λ modulo p. Then for any real $\alpha \in (0, 2)$, define

$$S_\alpha(x; \lambda) = \sum_{\substack{p \le x \\ \gcd(p,\lambda)=1}} \frac{1}{(\mathrm{ord}_p\,\lambda)^\alpha}.$$

It follows from [20, Corollary 5] that (only with $r = 1$)

$$S_1(x; \lambda) \ll x^{1/2} \frac{(\log\log x)^{1+\delta}}{(\log x)^{1+\delta/2}}, \tag{3.12}$$

where δ is given by (2.2).

Let

$$H_{\mathcal{P}}(x, y, 2y) = \#\{p \le x \ : \ \exists\, d \in (y, 2y],\, d \mid p - 1\}.$$

We first need the following consequence of a result of Ford [15, Theorem 6 and Corollary 2] (we remark that the extension to $y \in [x^{1/2}, x^{3/4}]$ comes from the symmetry of the divisors d and $(p-1)/d$).

Lemma 3.16. *For any $x \ge 2$ and $3 \le y \le x^{3/4}$, we have*
$$H_{\mathcal{P}}(x, y, 2y) \ll \frac{x}{(\log x)(\log y)^{\delta}(\log\log y)^{3/2}}.$$

Lemma 3.17. *For any integer λ with $|\lambda| > 1$, any real $\alpha \in (0,2)$ and $x \ge 3$, we have*
$$S_\alpha(x;\lambda) \ll_\alpha \frac{x^{1-\alpha/2}\log|\lambda|}{(\log x)^{1+(2-\alpha)\delta/2}(\log\log x)^{3(2-\alpha)/4}}.$$

Proof. Let $3 \le y < z \le x^{3/4}$. We divide $S_\alpha(x;\lambda)$ into three parts S_1, S_2 and S_3 with S_1 corresponding to $\mathrm{ord}_p\,\lambda \le y$, S_2 to $\mathrm{ord}_p\,\lambda \in (y, z]$ and S_3 to $\mathrm{ord}_p\,\lambda > z$. As usual, let $\omega(n)$ be the number of distinct prime factors of integer $n \ne 0$. Using the bound $\omega(n) \ll (\log n)/(\log\log n)$, we obtain
$$S_1 \le \sum_{m \le y} \frac{\omega(\lambda^m - 1)}{m^\alpha} \ll_\alpha \frac{y^{2-\alpha}}{\log y}\log|\lambda|.$$
Note that $\mathrm{ord}_p(\lambda) \mid p-1$. Then applying Lemma 3.16, we get
$$\begin{aligned} S_2 &\le \sum_{\substack{k\ge 0\\ 2^k y \le z}} \frac{1}{2^{k\alpha}y^\alpha} H_{\mathcal{P}}(x, 2^k y, 2^{k+1}y) \\ &\ll_\alpha \frac{x}{(\log x)y^\alpha(\log y)^\delta(\log\log y)^{3/2}}. \end{aligned}$$
In addition, we trivially have
$$S_3 \le \frac{\pi(x)}{z^\alpha}.$$
Then taking $z = x^{3/4}$ and $y = \sqrt{x}(\log x)^{-\delta/2}(\log\log x)^{-3/4}$, we have
$$S_1 + S_2 + S_3 \ll_\alpha \frac{x^{1-\alpha/2}\log|\lambda|}{(\log x)^{1+(2-\alpha)\delta/2}(\log\log x)^{3(2-\alpha)/4}},$$
which completes the proof. □

4. Proofs of Main Results

4.1. **Proof of Theorem 2.1.** Let $\mathcal{H} = \{w \in \mathcal{G} : \Delta(w) \ne 0\}$. Applying Lemma 3.5, we immediately have
$$\left|\sum_{w\in\mathcal{H}} \mathrm{sym}_n(\psi_p(E(w)))\right| \ll np^{1/2},$$
which, together with Corollary 3.2, yields
$$N_p(\alpha,\beta;\mathcal{G}) = \mu_{\mathtt{ST}}(\alpha,\beta)\#\mathcal{H} + O\left(\sqrt{p^{1/2}\#\mathcal{H}}\right).$$

We complete the proof by noticing that

$$\#\mathcal{G} - \deg \Delta \le \#\mathcal{H} \le \#\mathcal{G}.$$

4.2. **Proof of Theorem 2.2.** Let

$$\mathcal{H} = \{(u,v) : u \in \mathcal{U}, v \in \mathcal{V}, \Delta(uv) \ne 0\}.$$

Using Lemma 3.8 (with $\alpha_u = \beta_v = 1$ and $U = V = p-1$), we obtain

$$\left| \sum_{(u,v)\in\mathcal{H}} \mathrm{sym}_n(\psi_p(E(uv))) \right| \ll n\sqrt{\#\mathcal{U}\#\mathcal{V}p},$$

which, combining with Corollary 3.2, gives

$$N_p(\alpha,\beta;\mathcal{U},\mathcal{V}) = \mu_{\mathtt{ST}}(\alpha,\beta)\#\mathcal{H} + O\left((\#\mathcal{U}\#\mathcal{V}p)^{1/4}\sqrt{\#\mathcal{H}} \right).$$

We conclude the proof by noticing that

$$\#\mathcal{U}\#\mathcal{V} - \min\{\#\mathcal{U},\#\mathcal{V}\}\deg \Delta \le \#\mathcal{H} \le \#\mathcal{U}\#\mathcal{V}.$$

4.3. **Proof of Theorems 2.3 and 2.4.** Let $\mathcal{L}$ be the set of primes $\ell \le L$ such that $\Delta(\ell) \not\equiv 0 \pmod p$.

Without loss of generality we can assume that $\varepsilon \le 1/4$. We set

$$\eta = 1/48 - \varepsilon/24.$$

Applying Lemma 3.12, we derive

$$\left| \sum_{\ell\in\mathcal{L}} \mathrm{sym}_n(\psi_p(E(\ell))) \right| \ll n^A \pi(L)\left(1 + p/L\right)^{1/12} p^{-\eta}.$$

Now, combining this with Corollary 3.2, , and using that $p/L < p^{1/4-\varepsilon}$, we obtain

$$\begin{aligned} &Q_p(\alpha,\beta;L) - \mu_{\mathtt{ST}}(\alpha,\beta)\#\mathcal{L} \\ &\qquad \ll \pi(L)^{A/(A+1)} \left(\pi(L)\left(1+p/L\right)^{1/12} p^{-\eta} \right)^{1/(A+1)} \\ &\qquad = \pi(L)\left(\left(1+p/L\right)^{1/12} p^{-\eta} \right)^{1/(A+1)} \\ &\qquad \ll \pi(L)\left(\left(1+p^{1/4-\varepsilon}\right)^{1/12} p^{-\eta} \right)^{1/(A+1)} \\ &\qquad \ll \pi(L)p^{(1/48-\varepsilon/12-\eta)/(A+1)} = \pi(L)p^{-\rho}, \end{aligned}$$

where

$$\rho = \frac{\varepsilon}{24(A+1)} > 0$$

(provided that $0 < \varepsilon \le 1/4$), which completes the proof of of Theorems 2.3.

The proof is identical of of Theorem 2.4 to that of of Theorem 2.3, except that we use Corollary 3.15 instead of Lemma 3.12.

4.4. **Proof of Theorem 2.5.** We consider slightly more general settings, when $\mathcal{U}, \mathcal{V} \subseteq [1, T]$ for some positive integer $T \le x$, because some of the intermediate bounds can be of further use.

For any prime p, let

$$\mathcal{D}_p = \{(u, v) \ : \ u \in \mathcal{U}, v \in \mathcal{V}, uv \equiv 0 \pmod p\},$$

and

$$\mathcal{H}_p = \{(u, v) \ : \ u \in \mathcal{U}, v \in \mathcal{V}, \Delta(uv) \not\equiv 0 \pmod p\}.$$

We denote by $M_p(\alpha, \beta; \mathcal{U}, \mathcal{V})$ the number of pairs $(u, v) \in \mathcal{H}_p$ such that $\psi_p(E(uv)) \in [\alpha, \beta]$. Without loss of generality, we assume that

$$\#\mathcal{U} \ge \#\mathcal{V}.$$

It follows from Lemma 3.8 (with $\alpha_u = \beta_v = 1$ and $U = V = T$) and (3.5) that

$$\begin{aligned} &\left|\sum_{(u,v)\in\mathcal{H}_p} \mathrm{sym}_n(\psi_p(E(uv)))\right| \\ &\qquad \le \left|\sum_{\substack{(u,v)\in\mathcal{H}_p\\ \gcd(uv,p)=1}} \mathrm{sym}_n(\psi_p(E(uv)))\right| + \left|\sum_{\substack{(u,v)\in\mathcal{H}_p\\ \gcd(uv,p)\ne 1}} \mathrm{sym}_n(\psi_p(E(uv)))\right| \\ &\qquad \ll n(T/p+1)p^{1/2}(\#\mathcal{U}\#\mathcal{V})^{1/2} + n(T/p)\#\mathcal{U}. \end{aligned}$$

So, using Corollary 3.2, we have

$$\begin{aligned} &M_p(\alpha, \beta; \mathcal{U}, \mathcal{V}) - \mu_{\mathtt{ST}}(\alpha, \beta)\#\mathcal{H}_p \\ &\qquad \ll (\#\mathcal{H}_p)^{1/2}\Big((T/p+1)^{1/2}p^{1/4}(\#\mathcal{U}\#\mathcal{V})^{1/4} + (T/p)^{1/2}(\#\mathcal{U})^{1/2}\Big). \end{aligned}$$

Noticing

$$\#\mathcal{U}\#\mathcal{V} - \#\mathcal{D}_p - \#\mathcal{V}(T/p+1)\deg\Delta \le \#\mathcal{H}_p \le \#\mathcal{U}\#\mathcal{V},$$

we obtain

$$\begin{aligned} &M_p(\alpha, \beta; \mathcal{U}, \mathcal{V}) - \mu_{\mathtt{ST}}(\alpha, \beta)\#\mathcal{U}\#\mathcal{V} \\ &\qquad \ll \#\mathcal{D}_p + Tp^{-1}\#\mathcal{V} + (T^{1/2}p^{-1/4} + p^{1/4})(\#\mathcal{U}\#\mathcal{V})^{3/4} \\ &\qquad\qquad + T^{1/2}p^{-1/2}\#\mathcal{U}(\#\mathcal{V})^{1/2}. \end{aligned} \tag{4.1}$$

Besides, it is easy to see that

$$\sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(uv)\neq 0}} \pi_{E(uv)}(\alpha,\beta;x) = \sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(uv)\neq 0}} \sum_{\substack{p\le x\\ \Delta(uv)\not\equiv 0 \pmod p\\ \psi_p(E(uv))\in[\alpha,\beta]}} 1$$

$$= \sum_{p\le x} \sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(uv)\not\equiv 0 \pmod p\\ \psi_p(E(uv))\in[\alpha,\beta]}} 1 = \sum_{p\le x} M_p(\alpha,\beta;\mathcal{U},\mathcal{V}).$$

Moreover, we estimate the sum of $\#\mathcal{D}_p$ as follows:

$$\sum_{p\le x} \#\mathcal{D}_p \le \#\mathcal{U}\sum_{v\in\mathcal{V}}\omega(v) + \#\mathcal{V}\sum_{u\in\mathcal{U}}\omega(u) \ll \#\mathcal{U}\#\mathcal{V}\log x,$$

where, as before, $\omega(w)$ be the number of distinct prime factors of integer $w\neq 0$.

Thus, applying (4.1) we deduce that

$$\begin{aligned}
&\sum_{\substack{u\in\mathcal{U},v\in\mathcal{V}\\ \Delta(uv)\neq 0}} \pi_{E(uv)}(\alpha,\beta;x) - \mu_{\mathtt{ST}}(\alpha,\beta)\pi(x)\#\mathcal{U}\#\mathcal{V}\\
&\qquad \ll \sum_{p\le x}\Big(\#\mathcal{D}_p + Tp^{-1}\#\mathcal{V} + (T^{1/2}p^{-1/4}+p^{1/4})(\#\mathcal{U}\#\mathcal{V})^{3/4}\\
&\qquad\qquad + T^{1/2}p^{-1/2}\#\mathcal{U}(\#\mathcal{V})^{1/2}\Big)\\
&\qquad \ll \#\mathcal{U}\#\mathcal{V}\log x + T\#\mathcal{V}\log x + \pi(x)T^{1/2}x^{-1/2}\#\mathcal{U}(\#\mathcal{V})^{1/2}\\
&\qquad\qquad + \pi(x)\left(T^{1/2}x^{-1/4}+x^{1/4}\right)(\#\mathcal{U}\#\mathcal{V})^{3/4}.
\end{aligned} \tag{4.2}$$

Now, to finish the proof, we substitute $T=x$ in (4.2) and remark that $T\#\mathcal{V}\log x \le x\log x\,(\#\mathcal{U}\#\mathcal{V})^{1/2} \ll \pi(x)x^{1/4}(\#\mathcal{U}\#\mathcal{V})^{3/4}$.

4.5. **Proof of Theorem 2.6.** For any prime p, let

$$\mathcal{H}_p = \{t : 1\le t\le T, \Delta(\lambda^t)\not\equiv 0 \pmod p\}.$$

We denote by $M_p(\alpha,\beta;T)$ the number of integers $t\in\mathcal{H}_p$ such that $\psi_p(E(\lambda^t))\in[\alpha,\beta]$. If $p\nmid\lambda$, we write $T = k_p\operatorname{ord}_p\lambda + s_p$ with $0\le s_p < \operatorname{ord}_p\lambda$. Using Lemma 3.5 and Lemma 3.6, for $p\nmid\lambda$ we obtain

$$\left|\sum_{t\in\mathcal{H}_p}\operatorname{sym}_n(\psi_p(E(\lambda^t)))\right| \ll n\left(k_p\sqrt{p}+\sqrt{p}\log p\right).$$

Hence, using Corollary 3.2, we have

$$M_p(\alpha,\beta;T) = \mu_{\mathtt{ST}}(\alpha,\beta)\#\mathcal{H}_p + O\left(\sqrt{(k_p\sqrt{p}+\sqrt{p}\log p)\#\mathcal{H}_p}\right).$$

Noticing

$$T - (k_p + 1) \deg \Delta \le \#\mathcal{H}_p \le T,$$

for $p \nmid \lambda$ we have

$$M_p(\alpha, \beta; T) - \mu_{\mathtt{ST}}(\alpha, \beta) T \ll \left(k_p^{1/2} p^{1/4} + p^{1/4} (\log p)^{1/2}\right) T^{1/2}. \tag{4.3}$$

In addition, it is easy to see that

$$\begin{aligned}\sum_{\substack{1 \le t \le T \\ \Delta(\lambda^t) \ne 0}} \pi_\lambda(\alpha, \beta; t, x) &= \sum_{\substack{1 \le t \le T \\ \Delta(\lambda^t) \ne 0}} \sum_{\substack{p \le x \\ \Delta(\lambda^t) \not\equiv 0 \pmod p \\ \psi_p(E(\lambda^t)) \in [\alpha, \beta]}} 1 \\ &= \sum_{p \le x} \sum_{\substack{1 \le t \le T \\ \Delta(\lambda^t) \not\equiv 0 \pmod p \\ \psi_p(E(\lambda^t)) \in [\alpha, \beta]}} 1 = \sum_{p \le x} M_p(\alpha, \beta; T).\end{aligned}$$

For $p \mid \lambda$, we use the trivial bound $M_p(\alpha, \beta; T) \le T$. Thus, recalling (4.3) and using $k_p \le T / \operatorname{ord}_p \lambda$, we deduce that

$$\begin{aligned}&\sum_{\substack{1 \le t \le T \\ \Delta(\lambda^t) \ne 0}} \pi_\lambda(\alpha, \beta; t, x) - \mu_{\mathtt{ST}}(\alpha, \beta) \pi(x) T \\ &\quad \ll T \log |\lambda| + \sum_{\substack{p \le x \\ p \nmid \lambda}} \left(k_p^{1/2} p^{1/4} + p^{1/4} (\log p)^{1/2}\right) T^{1/2} \\ &\quad \ll_\lambda T x^{1/4} S_{1/2}(x; \lambda) + T^{1/2} x^{1/4} (\log x)^{1/2} \pi(x) \\ &\quad \ll_\lambda \frac{Tx}{(\log x)^{1+3\delta/4} (\log \log x)^{9/8}} + T^{1/2} x^{1/4} (\log x)^{1/2} \pi(x),\end{aligned}$$

where the last inequality follows from Lemma 3.17.

Recalling the condition $T \ge x^{1/2} (\log x)^{1+3\delta/2} (\log \log x)^{9/4}$, we complete the proof.

4.6. **Proof of Theorems 2.7 and 2.8.** The results follow immediately from Theorem 2.3 and Theorem 2.4 after summation over p, respectively.

5. Possible Extensions

Here we point out several further results which can be obtained within our methods. For example, we can estimate the sums

$$\begin{aligned}&\sum_{\substack{1\le t\le L\\ \Delta(t)\not\equiv 0 \pmod p}} |\mu(t)|\,\mathrm{sym}_n\left(\psi_p(E(t))\right),\\ &\sum_{\substack{1\le t\le L\\ \Delta(t)\not\equiv 0 \pmod p}} \mu(t)\,\mathrm{sym}_n\left(\psi_p(E(t))\right),\end{aligned} \tag{5.1}$$

with the Möbius function μ. Note that the first sum in (5.1) is the sum over squarefree numbers and can be reduced to the sums of Lemma 3.7 via the standard inclusion-exclusion principle. It correponds to a form of the Sato–Tate conjecture on average for curves of the family (1.2) with squarefree values of the parameter t. For the second sum in (5.1) we can use the following analogue of the Vaughan identity given in Lemma 3.11: for any complex-valued function $\psi(t)$ and any real numbers $K, M \ge 1$ with $KM \le L$ and $L \ge 2$, we have

$$\sum_{t=1}^{L} \mu(t)\psi(t) \ll \Omega_1 + \Omega_2 + \Omega_3 + \Omega_4,$$

where

$$\begin{aligned}\Omega_1 &= \left|\sum_{t\le \max\{K,M\}} \mu(t)\psi(t)\right|,\\ \Omega_2 &= \sum_{k\le KM} \tau(k)\left|\sum_{m\le L/k} \psi(km)\right|,\\ \Omega_3 &= 0,\\ \Omega_4 &= \left|\sum_{M<m\le L/K} \mu(m) \sum_{K<k\le L/m} \left(\sum_{d\mid k,\ d\le K} \mu(d)\right)\psi(km)\right|;\end{aligned}$$

see the proof of [5, Theorem 5.1].[1] So we can now proceed as in the proof of Lemma 3.14.

[1]We take the opportunity to note that in the proof of [5, Theorem 5.1], there are some absolute value symbols that should be brackets; this is inconsequential for the argument.

Acknowledgements

The research of the first author was supported by an IUF junior, the second and third authors were supported by the Australian Research Council Grant DP130100237, and the research of the fourth author was supported by the Simons Foundation Grant #234591.

References

[1] T. M. Apostol, *Introduction to analytic number theory*, Springer, New York, 1976.

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

[5] W. D. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, *Exponential sums over Mersenne numbers*, Compos. Math. **140** (2004), 15–30.

[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] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. Math. **181** (2015), 191–242.

[9] 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.

[10] 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.

[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] H. Davenport, *Multiplicative Number Theory*, Springer, New York, 2000.

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

[15] K. Ford, *The distribution of integers with a divisor in a given interval, Ann. of Math.* **168** (2008), 367–433.

[16] É. Fouvry, E. Kowalski and P. Michel, *Algebraic trace functions over the primes, Duke Math. J.* **163** (2014), 1683–1736.

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

[18] É. Fouvry and J. Pomykala, *Rang des courbes elliptiques et sommes d'exponentielles*, Monatsh. Math. **116** (1993), 111–125.

[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.-K. Indlekofer and N. M. Timofeev, *Divisors of shifted primes*, *Publ. Math. Debrecen* **60** (2002), 307–345.

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

[22] N. M. Katz, *Exponential sums over finite fields and differential equations over the complex numbers: Some interactions*, Bull. Amer. Math. Soc. **23** (1990), 269–309.

[23] N. M. Katz, *Estimates for nonsingular multiplicative character sums*, Int. Math. Res. Not. **2002** (2002), 333–349.

[24] E. Kowalski, *Elliptic curves, rank in families and random matrices*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, 7–52,

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

[26] J.-F. Mestre, *Courbes elliptiques et formules explicites* Sé minaire de Théorie des Nombres de Paris, 1981–82, Birkhaüser, Basel, 1983, 179–187.

[27] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), 209–232.

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

[29] J. S. Milne, *Lectures on Étale Cohomology*, (v2.21), 2013, available at http://www.jmilne.org/math/CourseNotes/lec.html.

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

[31] B. Poonen, *Average rank of elliptic curves [after Manjul Bhargava and Arul Shankar]*, Astérisque, No. 352 (2013), Exp. No. 1049, 187–204.

[32] M. Sha and I. E. Shparlinski, *Lang–Trotter and Sato–Tate distributions in single and double parametric families of elliptic curves*, Acta Arith. **170** (2015), 299–325.

[33] I. E. Shparlinski, *On the Sato–Tate conjecture on average for some families of elliptic curves*, Forum Math. **25** (2013), 647–664.

[34] 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.

[35] J. H. Silverman, *The average rank of an algebraic family of elliptic curves*, J. Reine Angew. Math. **504** (1998), 227–236.

[36] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, Berlin, 2009.

[37] R. Taylor, *Automorphy for some* ℓ*-adic lifts of automorphic mod* ℓ *Galois representations II*, Pub. Math. IHES **108** (2008), 183–239.

[38] R. C. Vaughan, *Sommes trigonométriques sur les nombres premiers*, C.R. Acad. Sci. Paris Sér. **A 285** (1977), 981–983.

[39] R. C. Vaughan, *An elementary method in prime number theory*, Acta Arith. **37** (1980), 111–115.

[40] R. C. Vaughan, *A new iterative method for Waring's problem*, Acta Math. **162** (1989), 1–71.

Institut de Mathématiques de Jussieu-PRG, Université Paris Diderot, Sorbonne Paris Cité, UMR 7586, Case 7012, F-75013 Paris, France
E-mail address: regis.de-la-breteche@imj-prg.fr

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

Department of Mathematics, University of Texas, Austin, TX 78712, USA
E-mail address: voloch@math.utexas.edu