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 Lang–Trotter conjecture 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

\[
\Delta(Z) \neq 0 \quad \text{and} \quad j(Z) \notin \mathbb{Q},
\]

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, we consider the elliptic curve

\( E(Z) : \quad \begin{align*}
Y^2 &= X^3 + f(Z)X + g(Z)
\end{align*} \)

over the function field \( \mathbb{Q}(Z) \), for a general background on elliptic curves we refer to [29].

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 integer or rational numbers. More precisely, motivated by the Lang–Trotter and Sato–Tate conjectures we study the distribution of the number of points and other properties of the reductions of \( E(t) \) modulo consecutive primes \( p \leq x \) for a growing parameter \( x \geq 2 \).
Let us first introduce 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 $p \leq x$ 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 $p \leq x$ with $p \nmid N_E$ and such that $\mathbb{Q}(\sqrt{a_p(E)^2 - 4p}) = \mathbb{K}$, where $\mathbb{Q}(\sqrt{a_p(E)^2 - 4p})$ is the so-called Frobenius field of $E$ with respect to $p$. In fact, it is well-known that if $E$ is with complex multiplication (CM), for any prime $p \nmid N_E$, we have

$$\mathbb{Q}(\sqrt{a_p(E)^2 - 4p}) \simeq \text{End}_{\overline{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q},$$

where $\text{End}_{\overline{\mathbb{Q}}}(E)$ 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.

Two celebrated Lang–Trotter conjectures [20] assert that if $E$ is without complex multiplication, then

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

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

Despite a series of several interesting achievements, see [9, 10, 12, 25, 28] for surveys and some recent results, these conjectures are widely open.
In addition, by Hasse’s bound, see [29], we can define the angle \( \psi_p(E) \in [0, \pi] \) via the identity
\[
\cos \psi_p(E) = \frac{a_p(E)}{2\sqrt{p}}.
\]
For real numbers \( 0 \leq \alpha < \beta \leq \pi \), we define the Sato–Tate density
\[
\mu_{ST}(\alpha, \beta) = \frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 \vartheta \, d\vartheta.
\]
We denote by \( \pi_E(\alpha, \beta; x) \) the number of primes \( p \leq x \) (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 [18], and Taylor [30], asserts that if \( E \) is not a CM curve, then
\[
\pi_E(\alpha, \beta; x) \sim \mu_{ST}(\alpha, \beta) \cdot \frac{x}{\log x}
\]
as \( x \to \infty \).

So, due to the lack of conclusive results towards the Lang–Trotter conjectures, and also the lack of explicit error term in the asymptotic formula (5), it makes sense to study \( \pi_E(\alpha; x) \) and \( \pi_E(\alpha, \beta; x) \) on average over some natural families of elliptic curves.

Here we continue to 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 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 \( p \leq x \) on average over a family of curves \( E \) is due to Fouvry and Murty [16], who have considered the average value of \( \pi_E(0; x) \) and proved the Lang–Trotter on average, for the family of curves
\[
E_{u,v} : \ Y^2 = X^3 + uX + v,
\]
where the integers \( u \) and \( v \) satisfy the inequalities \( |u| \leq U, \ |v| \leq V \).

The results of [16] is nontrivial provided that
\[
UV \geq x^{3/2+\varepsilon} \quad \text{and} \quad \min\{U, V\} \geq x^{1/2+\varepsilon}
\]
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 [16] to \( \pi_E(a; x) \) with
an arbitrary \( a \in \mathbb{Z} \), in a narrower range than that given by (7). Finally, Baier [2] gives a full analogue of the result of [16] with \( a \in \mathbb{Z} \), see also [3, 4].

The Sato–Tate conjecture on average has also been studied for the family (6), see [5, 6]. In particular, Banks and Shparlinski have shown that using bounds of multiplicative character sums and the large sieve inequality (instead of employed in [16] the exponential sum technique), one can study the Sato–Tate conjecture in a much wider range of \( U \) and \( V \) than that given by (7). Namely, the results of [6] are nontrivial when

\[
UV \geq x^{1+\varepsilon} \quad \text{and} \quad \min\{U, V\} \geq x^\varepsilon
\]

for some fixed positive \( \varepsilon > 0 \). 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 (8), see [10, 15, 26].

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 \( f \) and \( g \), are given in [27].

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

\[
\mathcal{F}(T) = \left\{ u/v \in \mathbb{Q} : \gcd(u, v) = 1, \ 1 \leq u, v \leq T \right\},
\]

of height at most \( T \). It is well known that

\[
\#\mathcal{F}(T) \sim \frac{6}{\pi^2} T^2.
\]

as \( T \to \infty \), see [17, Theorem 331].

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

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

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

\[
\sum_{\substack{t \in \mathcal{F}(T) \\ \Delta(t) \neq 0}} \pi_{E(t)}(\mathbb{K}; x) \ll T^{x^{3/2+o(1)}} + T^2 x^{2/3},
\]
where as usual we use the notation $U \ll V$ as an equivalent of $U = O(V)$. Throughout the paper the implied constants may depend on the polynomials $f(Z)$ and $g(Z)$ in (2).

1.3. Our results. We start with an improvement and generalisation of the bound (10), and later on we will find that its proof is simpler than that of (10). Namely, 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 $p \leq x$ which do not divide the conductor $N_E$ of $E$ and such that $a_p(E) = a_p$.

We say that $\mathfrak{A}$ is a 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 $\mathfrak{A} = \{a\}$ 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 $a_p = -\lfloor 2p^{1/2} \rfloor$, corresponding to curves with the largest possible number of $\mathbb{F}_p$-rational points.

**Theorem 1.** Given $T \geq 1$, if the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any $x \geq 2$ and any sequence of integers $\mathfrak{A} = \{a_p\}$, we have

$$\sum_{t \in \mathbb{F}(T)} \pi_E(t)(\mathfrak{A}; x) \ll \begin{cases} T x^{11/8+o(1)} + T^2 x^{7/8} & \text{for any } \mathfrak{A}, \\ T x^{4+o(1)} + T^2 x^{5/6} & \text{if } \mathfrak{A} \text{ is a zero sequence}. \end{cases}$$

Comparing this with (10), we can see that if $a \neq 0$ Theorem 1 improves (10) and remains nontrivial for $x^{3/8+\varepsilon} \leq T \leq x^{5/8-\varepsilon}$ for any fixed $\varepsilon > 0$. If $a = 0$ the same holds for $x^{1/3+\varepsilon} \leq T \leq x^{2/3-\varepsilon}$. Furthermore, we note that (10) is nontrivial only when $T \geq x^{1/2+\varepsilon}$.

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

(12) $f(Z) = 3Z(1728 - Z)$ and $g(Z) = 2Z(1728 - Z)^2$

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.** Given $T \geq 1$, if the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ are given by (12), then for any $x \geq 2$ and any sequence of integers $\mathfrak{A} =$
Now, we state a new result concerning the Lang-Trotter conjecture involving Frobenius fields.

**Theorem 3.** Given $T \geq 1$, if the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any $x \geq 2$ and any imaginary quadratic field $\mathbb{K}$, we have

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

Comparing this with (11), we can see that Theorem 3 improves (11) and remains nontrivial for $x^{1/3 + \varepsilon} \leq T \leq x^{2/3 - \varepsilon}$ for any fixed $\varepsilon > 0$.

Unfortunately, currently there are no asymptotic results concerning the average value of $\pi_{E(t)}(\alpha, \beta; x)$ (which is relevant to the Sato–Tate conjecture) when the parameter $t$ runs through $\mathcal{F}(T)$. Here, we consider this problem in another direction. As usual, we use $\pi(x)$ to denote the number of primes $p \leq x$.

**Theorem 4.** Suppose that the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), and for some $\varepsilon > 0$,

$$x^{1/2 + \varepsilon} \leq T \leq x^{1-\varepsilon}.$$

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

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

where $\delta > 0$ depends only on $\varepsilon$.

Note that in Theorem 4 the ranges of $x$ and $T$ are more restrictive than in other results, but it can easily be extended to just one natural restriction $T \geq x^{1/2 + \varepsilon}$.

We now recall that the common feature of the approaches of both [6] and [16] 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 as 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 [27], the family of curves (2) has been studied for specialisations t from the set
\[ t \in I(T) = \{1, \ldots, T\} \]
of T consecutive integers. In particular, in [27, Theorem 15], an asymptotic formula is given for the average value of \( \pi_{E(t)}(\alpha, \beta; x) \) over \( t \in I(T) \), provided that \( T \geq x^{1/2+\varepsilon} \), 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 [27, Theorem 15], amongst other things, is based on a result of Michel [22]. We note that unfortunately for [27, Lemma 9] a wrong reference is given, a correct one is [22, Proposition 1.1]. Here we use the similar approach to estimate the average value of \( \pi_{E(t)}(\mathfrak{A}; x) \) over \( t \in I(T) \), that is, also for a single parametric family of curves, which is relevant to the Lang–Trotter conjecture.

**Theorem 5.** Given \( T \geq 1 \), if the polynomials \( f(Z), g(Z) \in \mathbb{Z}[Z] \) satisfy (1), then for any \( x \geq 2 \) and any sequence of integers \( \mathfrak{A} = \{a_p\} \), we have
\[
\sum_{t \in I(T)} \pi_{E(t)}(\mathfrak{A}; x) \ll T \log x + T^{1/2} x^{5/4+o(1)}.
\]

**Theorem 6.** Given \( T \geq 1 \), if the polynomials \( f(Z), g(Z) \in \mathbb{Z}[Z] \) satisfy (1), then for any \( x \geq 2 \), any sequence of integers \( \mathfrak{A} = \{a_p\} \) and sets of integer \( U, V \subseteq I(T) \), we have
\[
\sum_{\substack{u \in U, v \in V \\Delta(u+v) \neq 0}} \pi_{E(u+v)}(\mathfrak{A}; x) \ll \#U \#V \log x + (\#U \#V)^{3/4} x^{5/4}.
\]

In addition to bounding the average value of \( \pi_{E(t)}(\mathfrak{A}; x) \) over \( t \in I(T) \), getting analogues of [27, Theorem 13] for this average value might be also of interest. Here, we derive an analogue of [27, Theorem 15] in the following theorem relevant to the Sato–Tate conjecture.

**Theorem 7.** Suppose that the polynomials \( f(Z), g(Z) \in \mathbb{Z}[Z] \) satisfy (1), and sets of integer \( U, V \subseteq I(T) \) are such that, for some \( \varepsilon > 0 \),
\[
\#U \#V \geq x^{1+\varepsilon} \quad \text{and} \quad T \leq x^{1-\varepsilon}.
\]
Then for any real numbers \( 0 \leq \alpha < \beta \leq \pi \), we have
\[
\frac{1}{\#U \#V} \sum_{\substack{u \in U, v \in V \\Delta(u+v) \neq 0}} \pi_{E(u+v)}(\alpha, \beta; x) = (\mu_{ST}(\alpha, \beta) + O(x^{-\delta})) \pi(x),
\]
where \( \delta > 0 \) depends only on \( \varepsilon \).

Note that in Theorem 7, since \( T^2 \geq \#U\#V \geq x^{1+\varepsilon} \), we have \( T \geq x^{(1+\varepsilon)/2} \).

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 \( Z = t \).

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

\[
\sum_{t \in F(T)} \Delta(t) \neq 0 \quad \Rightarrow \quad \pi_E(t)(\mathfrak{A}; x) = \sum_{p \leq x} \sum_{0 \leq w \leq p-1 \atop \Delta(w) \neq 0 \atop a_{w,p} = a_p} R_{T,p}(w),
\]

where to simplify the notation we denote

\[
a_{w,p} = a_p(E(w)).
\]

Notice that since \( \Delta(t) \) and \( N(t) \) have the same prime divisors for \( t \in \mathbb{Q} \), we see that for any prime \( p \), \( \Delta(t)N(t) \equiv 0 \pmod{p} \) if and only if \( \Delta(t) \equiv 0 \pmod{p} \).

2.2. Some congruences with traces. The following estimate is a direct generalisation to \( \pi_E(t)(\mathfrak{A}; x) \) of those obtained for \( \pi_E(t)(a; x) \) in the proof of [12, Theorem 2], (more precisely, see the bottom of [12, Page 1982]) and it follows immediately from the identity (14).

**Lemma 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 prime \( \ell \), we have

\[
\sum_{t \in F(T)} \pi_E(t)(\mathfrak{A}; x) \leq \sum_{p \leq x} \sum_{0 \leq w \leq p-1 \atop \Delta(w) \neq 0 \atop a_{w,p} = a_p} R_{T,p}(w).
\]

Next we need the following two bounds that have been obtained in the proof of [12, Theorem 2] from an effective version of the Chebotarev theorem given by Murty and Scherk [23, Theorem 2], see also [11, Theorem 1.2].
Lemma 9. If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any integer $a$ and prime $\ell \geq 17$ and $\ell \neq p$, we have

$$\sum_{0 \leq w \leq p-1 \atop \Delta(w) \neq 0 \pmod{p} \atop a_{w,p} \equiv a \pmod{\ell}} \frac{1}{\ell} + \begin{cases} \frac{O(\ell p^{1/2})}{\ell^{1/2}p^{1/2}} & \text{if } a \neq 0, \\ O(\ell^{1/2}p^{1/2}) & \text{if } a = 0, \end{cases}$$

where in particular the implied constants are independent of $a, p$ and $\ell$.

Lemma 10. 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 $K$, we have

$$\sum_{0 \leq w \leq p-1 \atop \Delta(w) \neq 0 \pmod{p} \atop a_{w,p} \neq 0 \pmod{p} \atop \mathbb{Q}(\sqrt{a_{w,p}^2-4p})=K} \frac{1}{\ell} + O(\ell^{1/2}p^{1/2}),$$

where in particular the implied constants are independent of $K, p$ and $\ell$.

2.3. Distribution of angles. We now consider the angles $\psi_p(E(t))$ that are given by (3).

Michel [22, 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 also denote $e_p(z) = \exp(2\pi iz/p)$.

Lemma 11. If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), we have

$$\sum_{w \in \mathbb{F}_p \atop \Delta(w) \neq 0 \pmod{p}} \frac{\sin((n+1)\psi_p(E(w)))}{\sin(\psi_p(E(w)))} e_p(mw) \ll np^{1/2},$$

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

The following lemma is a direct application of Lemma 11.

Lemma 12. If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any prime $p > T$, we have

$$\sum_{r,s \in \mathbb{F}(T) \atop \Delta(r+s) \neq 0 \pmod{p}} \frac{\sin((n+1)\psi_p(E(r+s)))}{\sin(\psi_p(E(r+s)))} \ll np^{1/2}T^3,$$

and uniformly over all integers $n \geq 1$. 
Proof. Using the orthogonality of the exponential function, we write

\[
\sum_{r,s \in \mathcal{F}(T), \Delta(r+s) \not\equiv 0 \pmod{p}} \frac{\sin((n+1)\psi_p(E(r+s)))}{\sin(\psi_p(E(r+s)))} - \sum_{w \in \mathcal{F}(T), \Delta(w) \not\equiv 0 \pmod{p}} \frac{\sin((n+1)\psi_p(E(w)))}{\sin(\psi_p(E(w)))}
\]

\[
= \sum_{w \in \mathcal{F}(T), \Delta(w) \not\equiv 0 \pmod{p}} \frac{1}{p} \sum_{m=0}^{p-1} e_p(m(w - u_1/v_1 - u_2/v_2)).
\]

So changing the order of summation we obtain:

\[
\sum_{r,s \in \mathcal{F}(T), \Delta(r+s) \not\equiv 0 \pmod{p}} \frac{\sin((n+1)\psi_p(E(r+s)))}{\sin(\psi_p(E(r+s)))} - \sum_{w \in \mathcal{F}(T), \Delta(w) \not\equiv 0 \pmod{p}} \frac{1}{p} \sum_{m=0}^{p-1} e_p(mw)
\]

\[
= \sum_{u_1/v_1 \in \mathcal{F}(T), \gcd(v_1,p)=1} e_p(-mu_1/v_1) \sum_{u_2/v_2 \in \mathcal{F}(T), \gcd(v_2,p)=1} e_p(-mu_2/v_2).
\]

Using Lemma 11, we have

\[
\sum_{r,s \in \mathcal{F}(T), \Delta(r+s) \not\equiv 0 \pmod{p}} \frac{\sin((n+1)\psi_p(E(r+s)))}{\sin(\psi_p(E(r+s)))} \ll np^{-1/2} \sum_{m=0}^{p-1} e_p(-mu_1/v_1) \sum_{u_2/v_2 \in \mathcal{F}(T), \gcd(v_2,p)=1} e_p(-mu_2/v_2).
\]

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

\[
\sum_{m=0}^{p-1} \left| \sum_{u_1/v_1 \in \mathcal{F}(T), \gcd(v_1,p)=1} e_p(-mu_1/v_1) \right|^2 \leq pT^3,
\]
and
\[
\sum_{m=0}^{p-1} \left| \sum_{\substack{u_2/v_2 \in \mathcal{F}(T) \\gcd(v_2,p)=1}} e_p(-mu_2/v_2) \right|^2 \leq pT^3,
\]
which follow from the orthogonality of the exponential function and the fact that
\[
\# \{(u_1/v_1, u_2/v_2) \in \mathcal{F}(T) \times \mathcal{F}(T) : \gcd(v_1v_2, p) = 1, \quad u_1v_2 \equiv u_2v_1 \pmod{p}\} \leq T^3,
\]
for \(p > T\).

Now, we define \(S_{f,g,p}(\mathcal{F}(T); \alpha, \beta)\) 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
\[
\alpha \leq \psi_p(E(r+s)) \leq \beta.
\]

Now, combining Lemma 12 with the technique of Niederreiter [24, Lemma 3] we derive:

**Lemma 13.** If the polynomials \(f(Z), g(Z) \in \mathbb{Z}[Z]\) satisfy (1), then for any prime \(p > T\), we have
\[
\max_{0 \leq \alpha < \beta \leq \pi} \left| S_{f,g,p}(\mathcal{F}(T); \alpha, \beta) - \mu_{\text{ST}}(\alpha, \beta)(\#\mathcal{F}(T))^2 \right| \ll p^{1/4}T^{7/2}.
\]

**Proof.** As the above, we have
\[
\# \{(r, s) \in \mathcal{F}(T) \times \mathcal{F}(T) : \Delta(r+s) \equiv 0 \pmod{p}\} \ll T^3.
\]

By [24, Lemma 3], for any odd positive integer \(k\), we have
\[
\max_{0 \leq \alpha < \beta \leq \pi} \left| S_{f,g,p}(\mathcal{F}(T); \alpha, \beta) - \mu_{\text{ST}}(\alpha, \beta)(\#\mathcal{F}(T))^2 \right| \ll \frac{(\#\mathcal{F}(T))^2}{k} + T^3 + 
\sum_{n=1}^{k} \frac{1}{n} \left| \sum_{r,s \in \mathcal{F}(T), \Delta(r+s) \not\equiv 0 \pmod{p}} \frac{\sin((n+1)\psi_p(E(r+s)))}{\sin(\psi_p(E(r+s)))} \right|.
\]

Thus, by Lemma 12 and (9), we get
\[
\max_{0 \leq \alpha < \beta \leq \pi} \left| S_{f,g,p}(\mathcal{F}(T); \alpha, \beta) - \mu_{\text{ST}}(\alpha, \beta)(\#\mathcal{F}(T))^2 \right| \ll \frac{(\#\mathcal{F}(T))^2}{k} + T^3 + kp^{1/2}T^3 \ll \frac{T^4}{k} + kp^{1/2}T^3.
\]

Taking \(k = 2 \left[ (p^{-1}T^2)^{1/4} \right] - 1\) we conclude the proof. \(\square\)
Let $\mathcal{T}_{f,g,p}(I(T); \alpha, \beta)$ be the number of integers $t \in I(T)$, where $I(T)$ is given by (13), with $\Delta(t) \not\equiv 0 \pmod{p}$, such that

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

We recall the asymptotic formula on $\mathcal{T}_{f,g,p}(I(T); \alpha, \beta)$ given in [27, Lemma 11], which in turn is based on Lemma 11, combined with the technique of Niederreiter [24, Lemma 3] and the standard reduction between complete and incomplete sums (see [19, Section 12.2]).

**Lemma 14.** If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for $p > T$, we have

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

We now give yet another application of Lemma 11.

**Lemma 15.** If the polynomials $f(Z), g(Z) \in \mathbb{Z}[Z]$ satisfy (1), then for any subsets $U, V \subseteq I(T)$ and $p > T$, we have

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

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

**Proof.** Applying the same argument as the proof of Lemma 12, we have

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

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

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

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

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

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

As before, combining Lemma 15 with the technique of Niederreiter [24, Lemma 3] we derive:
Lemma 16. If the polynomials \( f(Z), g(Z) \in \mathbb{Z}[Z] \) satisfy (1), then for any subsets \( U, V \subseteq I(T) \) and any prime \( p > T \), we have

\[
\max_{0 \leq \alpha < \beta \leq \pi} |W_{f,g,p}(U, V; \alpha, \beta) - \mu_{ST}(\alpha, \beta) \#U \#V| \ll p^{1/4}(\#U \#V)^{3/4}.
\]

Proof. Clearly, we have

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

By [24, Lemma 3], for any odd positive integer \( k \) we have

\[
\max_{0 \leq \alpha < \beta \leq \pi} |W_{f,g,p}(U, V; \alpha, \beta) - \mu_{ST}(\alpha, \beta) \#U \#V| \ll \frac{\#U \#V}{k} + (\#U \#V)^{1/2} + k\left(\frac{1}{p} \sum_{n} \frac{\sin((n + 1)\psi_p(E(u + v)))}{\sin(\psi_p(E(u + v)))}\right).\]

Thus, by Lemma 15, we get

\[
\max_{0 \leq \alpha < \beta \leq \pi} |W_{f,g,p}(U, V; \alpha, \beta) - \mu_{ST}(\alpha, \beta) \#U \#V| \ll \frac{\#U \#V}{k} + (\#U \#V)^{1/2} + k\left(p \#U \#V\right)^{1/2}.
\]

Taking \( k = 2 \left[(p^{-1} \#U \#V)^{1/4}\right] - 1 \) we conclude the proof. \( \square \)

3. Proofs of Main Results

3.1. Proof of Theorem 1. From Lemma 8, using the Cauchy inequality and then discarding the conditions \( \Delta(w) \equiv 0 \pmod{p} \) and \( a_{w,p} \equiv a_p \pmod{\ell} \), we derive

\[
\sum_{t \in F(T)} \pi_E(t)(Q; x) \leq \sum_{p \leq x} L_{T,p}^{1/2} Q_{T,p}^{1/2},
\]

where

\[
L_{T,p} = \sum_{0 \leq w \leq p-1} 1 \quad \text{and} \quad Q_{T,p} = \sum_{0 \leq w \leq p-1} R_{T,p}(w)^2.
\]
We note that \( Q_{T,p} \) is the number of solutions to the congruence
\[
\frac{u_1}{v_1} \equiv \frac{u_2}{v_2} \pmod{p},
\]
\[1 \leq u_1, u_2, v_1, v_2 \leq T, \quad \gcd(u_1, v_1) = \gcd(u_2, v_2) = 1.
\]
Dropping the condition \( \gcd(u_1, v_1) = \gcd(u_2, v_2) = 1 \), we see that \( Q_{T,p} \)
does not exceed the number of solutions to the congruence
\[
\frac{u_1 v_2}{u_2 v_1} \equiv \frac{u_2 v_1}{u_1 v_2} \pmod{p},
\]
\[1 \leq u_1, u_2, v_1, v_2 \leq T,
\]
which has been estimated as \( O(T^4/p + T^2 p^{o(1)}) \) by Ayyad, Cochrane
and Zheng [1, Theorem 1] (note that in the form of the result of [1, Theorem 1] the condition \( T < p \) is not needed). So, we have
\[
(17) \quad Q_{T,p} \ll T^4/p + T^2 p^{o(1)},
\]
where in particular the implied constant is independent of \( p \) and \( T \).

Thus, substituting the bound of (17) in (16) and using the bound of Lemma 9 with \( \ell \sim x^{1/4} \) for an arbitrary sequence \( \mathfrak{A} \) and also with \( \ell \sim x^{1/3} \) if \( \mathfrak{A} \) is a zero sequence, after simple calculations we conclude the proof.

3.2. Proof of Theorem 2. By (14) and as the proof of Theorem 1, we have
\[
(18) \quad \sum_{t \in \mathcal{F}(T), \Delta(t) \neq 0} \pi_{E(t)}(\mathfrak{A}; x) \leq \sum_{p \leq x} M_{T,p}^{1/2} Q_{T,p}^{1/2},
\]
where
\[
M_{T,p} = \sum_{0 \leq w \leq p-1} 1 \quad \text{and} \quad Q_{T,p} = \sum_{0 \leq w \leq p-1} R_{T,p}(w)^2.
\]

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 different \( \mathbb{F}_p \)-isomorphism class of elliptic curves over \( \mathbb{F}_p \). So, we have
\[
M_{T,p} \leq H(a_p, p).
\]
By [21, Proposition 1.9 (a)], for \( p \geq 5 \) 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 (18) and using the bound of \( Q_{T,p} \) in (17), we can get the desired result.

3.3. Proof of Theorem 3. As Lemma 8 and using the Cauchy inequality, we obtain

\[
\sum_{t \in \mathcal{F}(T)} \pi_{E(t)}(\mathbb{K}; x) = \sum_{p \leq x} \sum_{\Delta(t) \neq 0} R_{T,p}(w) \leq \sum_{p \leq x} N_{T,p}^{1/2} Q_{T,p}^{1/2},
\]

where

\[
N_{T,p} = \sum_{\Delta(w) \neq 0, \, \Delta(w) \equiv 0 \pmod{p}, \, a_{w,p} \neq 0} 1 \quad \text{and} \quad Q_{T,p} = \sum_{0 \leq w \leq p-1} R_{T,p}(w)^2.
\]

Then, using the bound of Lemma 10 and the bound of \( Q_{T,p} \) in (17) with \( \ell \sim x^{1/3} \), we can complete the proof.

3.4. Proof of Theorem 4. Using the same notation as in Section 2 and noticing that \( \Delta(r+s) \) and \( N(r+s) \) have the same prime divisors, we have

\[
\sum_{r,s \in \mathcal{F}(T), \, \Delta(r+s) \neq 0} \pi_{E(r+s)}(\alpha, \beta; x) = \sum_{r,s \in \mathcal{F}(T), \, \Delta(r+s) \neq 0} \sum_{p \leq x} 1 = \sum_{p \leq x} S_{f,g,p}(\mathcal{F}(T); \alpha, \beta).
\]

By Lemma 13, we get

\[
\sum_{r,s \in \mathcal{F}(T), \, \Delta(r+s) \neq 0} \pi_{E(r+s)}(\alpha, \beta; x) - \sum_{p \leq x} \mu_{\mathcal{F}}(\alpha, \beta)(\#\mathcal{F}(T))^2 \ll \sum_{p \leq T} T^4 + \sum_{T < p \leq x} p^{1/4} T^{7/2} \ll T^5 + x^{5/4} T^{7/2}.
\]

Then, the desired result follows from (9) and the assumption \( x^{1/2+\varepsilon} \leq T \leq x^{1-\varepsilon} \).
3.5. **Proof of Theorem 5.** 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

$$
\mu_{ST}(\alpha_p, \beta_p) = \frac{2}{\pi} \int_{\alpha_p}^{\beta_p} \sin^2 \theta \, d\theta = \frac{2}{\pi} \int_{\cos \beta_p}^{\cos \alpha_p} (1 - z^2)^{1/2} \, dz \leq \frac{2}{\pi} (\cos \alpha_p - \cos \beta_p) \leq \frac{4}{\pi p}.
$$

We recall the definition (15) and observe that for each elliptic curve $E(t), t \in \mathcal{I}(T)$ 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

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

Noticing that $N(t)$ and $\Delta(t)$ have the same prime divisors, we have

$$
\sum_{t \in \mathcal{I}(T) \atop \Delta(t) \neq 0} \pi_{E(t)}(\mathfrak{A}; x) = \sum_{t \in \mathcal{I}(T) \atop \Delta(t) \neq 0} \sum_{p \leq x \atop p \nmid N(t)} 1
$$

$$
= \sum_{p \leq x} \sum_{t \in \mathcal{I}(T) \atop \Delta(t) \neq 0 \mod p \atop a_{t,p} = a_p} 1 \leq \sum_{p \leq x} T_{f,g,p}(\mathcal{I}(T); \alpha_p, \beta_p).
$$

Then, combining the above results with Lemma 14, we obtain

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

$$
\ll T^2 + \sum_{p \leq x} \left( \frac{T}{p} + T^{1/2}p^{1/4+o(1)} \right)
$$

$$
\ll T \log x + T^{1/2}x^{5/4+o(1)},
$$

which completes the proof.
3.6. **Proof of Theorem 6.** As Section 3.5, using (15), we have
\[
\sum_{\substack{u \in U, v \in V \\ \Delta(u+v) \neq 0}} \pi_{E(u+v)}(\mathfrak{A}; x) = \sum_{\substack{u \in U, v \in V \\ \Delta(u+v) \neq 0 \atop \Delta(u+v) \not\equiv a \bmod p}} 1
\]
\[
= \sum_{p \leq x} \sum_{\substack{u \in U, v \in V \\ \Delta(u+v) \neq 0 \atop \Delta(u+v) \not\equiv a \bmod p}} 1 \leq \sum_{p \leq x} W_{f,g,p}(U, V; \alpha_p, \beta_p).
\]
By Lemma 16 and noticing that
\[
\mu_{ST}(\alpha, \beta) \leq \frac{4}{\pi p},
\]
we obtain
\[
\sum_{\substack{u \in U, v \in V \\ \Delta(u+v) \neq 0}} \pi_{E(u+v)}(\mathfrak{A}; x)
\]
\[
\ll \sum_{p \leq T} \#U \#V + \sum_{T < p \leq x} \left( \mu_{ST}(\alpha, \beta) \#U \#V + p^{1/4}(\#U \#V)^{3/4} \right)
\]
\[
\ll T \#U \#V + \sum_{p \leq x} \left( \#U \#V / p + p^{1/4}(\#U \#V)^{3/4} \right)
\]
\[
\ll \#U \#V \log x + (\#U \#V)^{3/4} x^{5/4},
\]
which gives the desired result.

3.7. **Proof of Theorem 7.** Using the notation in Section 2 and noticing that \(\Delta(u+v)\) and \(N(u+v)\) have the same prime divisors, we have
\[
\sum_{\substack{u \in U, v \in V \\ \Delta(u+v) \neq 0}} \pi_{E(u+v)}(\alpha, \beta; x) = \sum_{\substack{u \in U, v \in V \\ \Delta(u+v) \neq 0 \atop \psi_p(E(u+v)) \in [\alpha, \beta]}} 1
\]
\[
= \sum_{p \leq x} \#U \#V + \sum_{\substack{T < p \leq x \atop \psi_p(E(u+v)) \in [\alpha, \beta]}} 1 = \sum_{p \leq x} W_{f,g,p}(U, V; \alpha, \beta).
\]
By Lemma 16, we get
\[
\sum_{\substack{u \in U, v \in V \\ \Delta(u+v) \neq 0}} \pi_{E(u+v)}(\alpha, \beta; x) - \sum_{p \leq x} \mu_{ST}(\alpha, \beta) \#U \#V
\]
\[
\ll \sum_{p \leq T} \#U \#V + \sum_{T < p \leq x} p^{1/4}(\#U \#V)^{3/4}
\]
\[
\ll T \#U \#V + x^{5/4}(\#U \#V)^{3/4}.
\]
Then, the desired result follows from the assumptions \( \#U \#V \geq x^{1+\varepsilon} \) and \( T \leq x^{1-\varepsilon} \).

**Acknowledgements**

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 the mean value 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’, *Proc. Conf. “New Directions in the Theory of Universal Zeta- and L-Functions”*, Würzburg, Oct. 2008, Ber. Math., Shaker Verlag, Aachen, 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 representations’, *Pub. Math. IHES*, 108 (2008), 1–181.

[9] A. C. Cojocaru, ‘Questions about the reductions modulo primes of an elliptic curve’, *Proc. 7th Meeting of the Canadian Number Theory Association (Montreal, 2002)*, CRM Proceedings and Lecture Notes, Vol. 36, 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’, *Internat. Math. Res. Notices*, 2005 (2005), 3065–3080.

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

[13] C. David and F. Pappalardi, ‘Average Frobenius distribution of elliptic curves’, *Internat. Math. Res. Notices*, 4 (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] É. Fouvry and M. R. Murty, ‘On the distribution of supersingular primes’, *Canad. J. Math.*, 48 (1996), 81–104.
[17] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

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

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

[20] S. Lang and H. Trotter, *Frobenius Distributions in GL₂-Extensions*, Lecture Notes in Math. **504**, Springer-Verlag, Berlin, 1976.

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

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

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

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

[25] I. E. Shparlinski, ‘Tate–Shafarevich groups and Frobenius fields of reductions of elliptic curves’, *Quart. J. Math.*, **61** (2010), 255–263.

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

[27] 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.

[28] I. E. Shparlinski, ‘Elliptic curves over finite fields: Number theoretic and cryptographic aspects’, *Advances in Applied Mathematics, Modeling, and Computational Science*, Fields Inst. Commun., Springer-Verlag, Berlin, 2013, 65–90.

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

[30] 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