EXPERIMENTAL SUMS IN PRIME FIELDS FOR MODULAR FORMS

JITENDRA BAJPAI, SUBHAM BHAKTA AND VICTOR C. GARCÍA

ABSTRACT. The main objective of this article is to study the exponential sums associated to Fourier coefficients of modular forms supported at numbers having a fixed set of prime factors. This is achieved by establishing an improvement on Shparlinski’s bound for exponential sums attached to certain recurrence sequences over finite fields.

CONTENTS

1. Introduction 1
2. Exponential sums with linear recurrence sequences 6
3. Exponential sums for modular forms 12
4. Exponential sums for modular forms : beyond eigenforms 19
5. Exponential sums for modular forms : the inverse case 24
6. Impact on Waring-type problems 27
Acknowledgements 30
References 30

1. INTRODUCTION

Let $f$ be a modular form of weight $k \in 2\mathbb{Z}$ and level $N$ such that it has a Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z}, \quad \Im(z) \geq 0,$$

with $a(n)$ be the $n^{th}$ Fourier coefficient. In this article, we shall restrict to the family of modular forms with rational coefficients, i.e. $f(z)$ with $a(n) \in \mathbb{Q}$ for every $n$. We first consider the Hecke eigenforms in the space of cusp forms of weight $k$ for the congruence subgroup $\Gamma_1(N)$ with trivial nebentypus. When $f$ is an eigenform, it follows from Deligne-Serre that, there exist a corresponding Galois representation

$$\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_2(\mathbb{Z}_\ell)$$

such that $\text{tr}(\rho_f(\text{Frob}_p)) = a(p)$, for any prime $p$ not dividing $N$. For quick reference on the Deligne-Serre correspondence, we refer the interested reader to Chapter 3 of [7]. In particular, $a(p) \mod \ell$ is determined by the trace of Frobenius in

$$\text{GL}_2(\mathbb{Z}_\ell/\ell\mathbb{Z}) = \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Date: July 31, 2020.

2010 Mathematics Subject Classification. Primary 11F30, 11L07; Secondary 11F05, 11B37, 11F80.

Key words and phrases. Exponential Sums, Korobov’s Bound, Modular Forms.
In certain cases, Chebotarev’s density theorem says that given any \( \lambda \in \mathbb{F}_\ell \), there exist prime \( p \) such that \( a(p) \equiv \lambda \pmod{\ell} \). However, the set of such primes comes with density strictly less than 1. So what can be said for other primes? Is there an absolute integer \( s \geq 1 \) such that the congruence

\[
\sum_{i=1}^{s} a(p^{n_{i,p}}) \equiv \lambda \pmod{\ell}
\]

is solvable for any prime \( p \), and some tuple \( (n_{i,p})_{1 \leq i \leq s} \) of positive integers depending on \( p \)? If so, can we estimate number of such solutions? Let \( \tau(n) \) be the Ramanujan function, which is defined by the identity

\[
\Delta(z) = q \prod_{n \geq 1} (1 - q^n)^24 = \sum_{n \geq 1} \tau(n)q^n, \quad \text{with} \quad q = \exp(2\pi i z).
\]

In [27] Shparlinski proved that the set \( \{ \tau(n) \} \) is an additive basis modulo any prime \( \ell \), i.e. there is an absolute constant \( s \) such that the Waring-type congruence

\[
\tau(n_1) + \cdots + \tau(n_s) \equiv \lambda \pmod{\ell}
\]

has solution for any residue class \( \lambda \pmod{\ell} \). Garaev, Garcia and Konyagin (see [9]) proved that for any \( \lambda \in \mathbb{Z} \), the equation

\[
\sum_{i=1}^{s} \tau(n_i) = \lambda
\]

always has solution for \( s = 74,000 \).

Later Garcia and Nicolae (see [11]) extended such result for coefficients \( a(n) \) of normalized Hecke eigenforms of weight \( k \) in \( \mathcal{S}_k^\text{new}(\Gamma_0(N)) \). For any \( \lambda \in \mathbb{Z} \), the equation

\[
\sum_{i=1}^{s} a(n_i) = \lambda
\]

always has solution for some \( s \leq c(f) \) and \( c(f) \) satisfying

\[
c(f) \ll (2\Lambda^{3/8})^{k-1} + \varepsilon k \log(k + 1).
\]

The proof of the last two results are strongly attached to the Waring–Goldbach problem. Namely, by connecting the identity \( a(p^2) = a^2(p) - p^k - 1 \) with the solubility of the equation

\[
p_1^{k-1} + \cdots + p_s^{k-1} = N, \quad \text{for primes} \quad p_1, \ldots, p_s.
\]

We are actually studying the same problem over finite fields, and our main tool is Theorem 1 which provides a nontrivial bound for exponential sums with coefficients of modular forms. In other words, we are generalizing Shparlinski’s result to a wider class of modular forms. We shall mainly see in which cases the \( n_i \)'s can be taken to be powers of a given prime, and we shall record this in Corollary 15. To study this problem, we shall primarily focus on the exponential sum of type

\[
\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell(\xi a(p^n)) \right|
\]
whenever $f$ is a Hecke eigenform, and $p, \ell$ are primes. However, we shall also study this exponential sum for certain cusp forms which are not necessarily an eigenform.

It is well known that $a(n)$ is a multiplicative function and for any prime $p$ satisfies the relation
\begin{equation}
    a(p^{n+2}) = a(p)a(p^{n+1}) - p^{k-1}a(p^n), \quad n \geq 0.
\end{equation}
This comes from properties of Hecke operators, see Chapter 5 of [18] for a brief review.

In particular, the sequence $\{a(p^n)\}$ defines a linear recurrence sequence with order two. If $a(p) \in \mathbb{Q}$, then we can consider $a(p) \pmod{\ell} \in \mathbb{F}_\ell$ naturally. We shall shortly give a brief review of linear recurrence sequences. On the other hand, any modular form can be uniquely written as a linear combination of pairwise orthonormal Hecke eigenforms with coefficients coming from $\mathbb{C}$. Here we are concerned when all such eigenforms have integer coefficients. In this case, the sequence $\{a(p^n)\}$ is still a linear recurrence sequence of possibly higher degree.

1.1. Linear recurrence sequences and Shparlinski’s bound. We now provide a quick overview on the basic theory of linear recurrence sequences. Let $r \geq 1$ be an integer and $p$ be an arbitrary prime number. A linear recurrence sequence $\{s_n\}$ of order $r$ in $\mathbb{F}_p$ consists of a recursive relation
\begin{equation}
    s_{n+r} \equiv a_{r-1}s_{n+r-1} + \cdots + a_0s_{n} \pmod{p}, \quad n = 0, 1, 2, \ldots,
\end{equation}
and initial values $s_0, \ldots, s_{r-1} \in \mathbb{F}_p$. Here $a_0, \ldots, a_{r-1} \in \mathbb{F}_p$ are fixed. The characteristic polynomial $\omega(x)$ associated to $\{s_n\}$ is
\[\omega(x) = x^r - a_{r-1}x^{r-1} - \cdots - a_1x - a_0.\]

Under certain assumptions, linear recurrence sequences become periodic modulo $p$, see [14, Lemma 6.4] and [16, Theorem 6.11].

Let $p$ be a prime number and $\omega(x)$ be the characteristic polynomial of linear recurrence sequence $\{s_n\}$ as defined by equation (2). If $(a_0, p) = 1$ and at least one of the $s_0, \ldots, s_{r-1}$ are not divisible by $p$, then the sequence $\{s_n\}$ is periodic modulo $p$, that is for some $T \geq 1$,
\[s_{n+T} \equiv s_n \pmod{p}, \quad n = 0, 1, 2, \ldots.\]
The least positive period is denoted by $\tau$. In particular the least period satisfies $\tau \leq p^r - 1$ and $\tau$ divides $T$ for any period $T \geq 1$ of the sequence $\{s_n\}$.

In 1953, Korobov [13] obtained bounds for rational exponential sums involving linear recurrence sequences in residue classes. In particular, for the fields of order $p$, if $\{s_n\}$ is a linear recurrence sequence of order $r$ with $(a_0, p) = 1$ and period $\tau$, it follows that
\begin{equation}
    \left| \sum_{n \leq \tau} e_p(s_n) \right| \leq p^{r/2}.
\end{equation}

Note that such bound is nontrivial if $p^{r/2} < \tau$ and asymptotically effective only if $p^{r/2}/\tau \to 0$ as $p \to \infty$. Estimate (3) is optimal in general terms, indeed Korobov [14] showed that there is a linear recurrence sequence $\{s_n\}$ with length $r$ satisfying
\[\frac{1}{2}p^{r/2} < \left| \sum_{n \leq \tau} e_p(s_n) \right| \leq p^{r/2}.\]
In turn, is proven that exists a class of recurrences sequences having a better upper bound:

$$\sum_{n \leq \tau} e_p(s_n) \leq \tau^{1/2+\varepsilon},$$

however, the proof of existence is ineffective in the sense that we do not know explicit characteristics of such family, see [6, Section 5.1].

The case when the associate polynomial is irreducible in $\mathbb{F}_p[x]$, was widely studied. For instance, from a more general result due to Katz [12, Theorem 4.1.1.] it follows that if $\omega(0) = 1$ then

$$\sum_{n \leq \tau} e_p(s_n) \leq p^{(r-1)/2}.$$

Shparlinski [26] improved Korobov’s bound for all nonzero recurrence sequences with irreducible characteristic polynomial $\omega$ in $\mathbb{F}_p[x]$. From [26, Theorem 3.1] we get

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \leq \tau} e_p(\xi s_n) \right| \leq \tau p^{-\varepsilon/(r-1)} + r^{3/11} \tau^{8/11} p^{(3r-1)/22},$$

with period $\tau$ provided that

$$\max_{d < r} \gcd(\tau, p^{d} - 1) < \tau p^{-\varepsilon}.$$  

In particular, if $r$ is fixed then the upper bound is non trivial for $\tau \geq p^{r/2-1/6+\varepsilon}$. We mention the condition (4) above is essential if $\tau \leq p^{r/2+\varepsilon}$, for details see the example given by Shparlinski in [26, Section 1]. Moreover, we consider the general case when the associated polynomial is not necessarily irreducible, and we deduce the following key result.

**Theorem 1.** Let $p$ be a large prime number and $\varepsilon > \varepsilon' > 0$. Suppose that $\{s_n\}$ is a nonzero linear recurrence sequence with positive order and period $\tau$ in $\mathbb{F}_p$ such that its characteristic polynomial $\omega(x)$ has distinct roots in its splitting field, and $(\omega(0), p) = 1$. Set $\omega(x) = \prod_{i=1}^{\nu} \omega_i(x)$ as a product of distinct irreducible polynomials in $\mathbb{F}_p[x]$, and for each $i$, $\alpha_i$ denotes a root of $\omega_i(x)$. If all polynomials $\omega_i$ have the same degree, i.e. $\deg \omega_i = r > 1$, and the system $\tau_i = \text{ord} \alpha_i$, satisfies

$$\max_{d < r} \gcd(\tau_i, p^{d} - 1) < \tau_i p^{-\varepsilon}, \quad \text{at least for one } 1 \leq i \leq \nu,$$

$$\gcd(\tau_i, \tau_j) < p^{\varepsilon'}, \quad \text{for some pair } i \neq j \text{ along with } \mathbb{F}_p(\alpha_i) \cong \mathbb{F}_p(\alpha_j),$$

then there exists a $\delta = \delta(\varepsilon, \varepsilon') > 0$ such that

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \leq \tau} e_p(\xi s_n) \right| \leq \tau p^{-\delta}.$$
The result above also extends [2, Corollary] due to Bourgain, where all of the irreducible factors have degree \( r = 1 \), while our result deals with the case \( r \geq 2 \). This is useful for the next section, roughly because the characteristic polynomial associated to \{a(p^n)\} have degree two.

Theorem 1 will be essential to establish Theorem 2 and Corollaries 14 and 16. Our approach, which relies on sum-product phenomenon, provides an improvement over Shparlinski’s Theorem 3.1 of [26] for the same class of recurrence sequences, obtaining non trivial exponential sums in a larger range: \( \tau > p^{r/2-1/6+\varepsilon} \).

Actually, if \( p(r) \) denotes the least prime divisor of \( r \) then we note that any \( \tau > p^{r/p(r)+\varepsilon} \) satisfies

\[
\tau p^{-\varepsilon} > p^{r/p(r)} \geq \frac{1}{r} \max_{d \mid r} \gcd(\tau, p^d - 1).
\]

This is an improvement if \( p(r) > 2 \), in particular when \( r \) is odd, say. Now, even if we improve the range of \( \tau \), one may ask whether there is any \( \tau \) in between \( p^{r/p(r)+\varepsilon} \) and \( p^{r/2-1/6+\varepsilon} \).

Let us recall that, a newform is said to have complex multiplication (CM) by a quadratic Dirichlet character \( \phi \) if \( f = f \otimes \phi \), where we define the twist as

\[
f \otimes \phi = \sum_{n=1}^{\infty} a(n)\phi(n)q^n.
\]

Then we have the following result:

**Theorem 3.** Let \( f(z) \) be a cusp form which is not necessarily an eigenform, and can be written as a \( \mathbb{Q} \)-linear combination of newforms (with rational coefficients). Then the following is true.
(i) If at most one of the newform is without CM, then there exists a positive density set of primes \( P \) such that, for each \( p \in P \) an estimation of type (7) holds for a positive density of primes \( \ell \).

(ii) Moreover, if all such newforms are without CM, then we have a similar result under the Generalized Sato-Tate conjecture.\(^{12}\)

In both of the results above, we took a fixed prime \( p \) and looked for primes \( \ell \) for which an estimation of type (7) holds. However, these results were valid for almost all prime \( \ell \), and we do not knot explicitly which of the primes are being excluded in this process. So one may now naturally ask, what if we now fix a prime \( \ell \) randomly and vary the primes \( p \). In this regard, we have the following results.

**Theorem 4.** Let \( f(z) \) be an eigenform as in Theorem 2. Consider the set of primes, \( \mathcal{P} = \{ \ell, \text{prime} \mid (k - 1, \ell - 1) = 1, \text{ and } 2^{v_2(\ell - 1)} < \ell^{1 - 2\varepsilon} \} \). Then for any fixed \( \varepsilon > 0 \) and \( \ell \in \mathcal{P} \), the set of primes \( p \) satisfying

\[
\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} e_{\ell} (\xi a(p^n)) \right| \leq \tau \ell^{-\varepsilon}
\]

have density at least \( \frac{1}{2} + O \left( \frac{1}{\ell} \right) \).

**Theorem 5.** If \( f(z) \) is not necessarily an eigenform, and it can be written as a \( \mathbb{Q} \) linear combination of rational coefficients of newforms without CM, such that absolute values of \( p \)th Fourier coefficients of each pair does not coincide for almost all prime.\(^{3}\) Suppose that for any fixed \( \varepsilon > \varepsilon' > 0 \) and large enough prime \( \ell \), one of the following assumptions are satisfied;

A.1: There exist divisors \( d_1, d_2 \) of \( \ell - 1 \) such that 
\[
d_1 > \ell^\varepsilon, \quad d_2 > \ell^\varepsilon \quad \text{and} \quad \gcd(d_1, d_2) < \ell^{\varepsilon'}.
\]

A.2: There exist divisors \( d_1, d_2 \) of \( \ell + 1 \) such that 
\[
d_1 > \ell^\varepsilon, \quad d_2 > \ell^\varepsilon \quad \text{and} \quad \gcd(d_1, d_2) < \ell^{\varepsilon'}.
\]

Then the set of primes \( p \) satisfying (9) have positive density.

2. **Exponential sums with linear recurrence sequences**

In this section, our main goal is to prove Theorem 1, which is our main tool in establishing several important results in the article.

We already noticed that condition a) of Theorem 1 is essential. Now in the more general case some assumption other than a) is also needed. For example, let \( r = 2 \) and \( g \) be a generator of \( \mathbb{F}_\ell^* \). Then, consider the sequence

\[
s_n = \text{Tr} \left( g^{n(\ell^2 + 1)/2} - g^n \right),
\]
Then, one can show that

\[ \tau_2 = \text{ord } g = \ell^2 - 1 \text{ and } \tau_1 = \text{ord } g^{(\ell^2+1)/2} = \frac{\ell^2 - 1}{\gcd(\ell^2 - 1, (\ell^2 + 1)/2)}. \]

It is easy to see that \( \gcd(\ell^2 - 1, (\ell^2 + 1)/2) = 1 \) or 2, therefore

\[ \gcd(\tau_1, \tau_2) = \begin{cases} \ell^2 - 1 & \text{if } \gcd(\ell^2 - 1, (\ell^2 + 1)/2) = 1, \\ (\ell^2 - 1)/2 & \text{if } \gcd(\ell^2 - 1, (\ell^2 + 1)/2) = 2. \end{cases} \]

Then, one can show that

\[ \sum_{n=1}^{\ell^2-1} e_\ell(s_n) = \sum_{n=1}^{\ell^2-1} e_\ell \left( \text{Tr} \left( g^{n(\ell^2+1)/2} - g^n \right) \right) = \frac{\ell^2 - 1}{2} + \sum_{n=1}^{(\ell^2-1)/2} e_\ell \left( \text{Tr} \left( -2g^{2n+1} \right) \right). \]

Note that the exponential sum appearing on right side of the above expression is bounded by

\[ \left| \sum_{n=1}^{(\ell^2-1)/2} e_\ell \left( \text{Tr} \left( -2g^{2n+1} \right) \right) \right| \leq \max_{\xi \in F_{\ell^2}} \left| \sum_{n=1}^{(\ell^2-1)/2} e_\ell \left( \text{Tr} \left( \xi g^{2n} \right) \right) \right| \leq \ell, \]

because \( \text{ord } g^2 = (\ell^2 - 1)/2 \). Therefore the linear recurrence sequence \( \{s_n\} \) satisfies

\[ \sum_{n=1}^{\ell^2-1} e_\ell(s_n) = \frac{\ell^2 - 1}{2} + O(\ell). \]

We now need to establish some necessary background. Let \( K \) be a finite field of characteristic \( p \) and \( F \) be an extension of \( K \) with \( [F : K] = r \). The trace function \( \text{Tr}_{F/K} : F \rightarrow K \) is defined by

\[ \text{Tr}_{F/K}(z) = z + z^p + \cdots + z^{p^{r-1}}, \quad z \in F. \]

The following properties of \( \text{Tr}_{F/K}(z) \) are well known.

\begin{align*}
(10) \quad & \text{Tr}_{F/K}(az + w) = a \text{Tr}_{F/K}(z) + \text{Tr}_{F/K}(w), \quad \text{for all } a \in K, z, w \in F. \\
(11) \quad & \text{Tr}_{F/K}(a) = ra, \quad \text{for any } a \in K. \\
(12) \quad & \text{Tr}_{F/K}(z^p) = \text{Tr}_{F/K}(z), \quad \text{for any } z \in F.
\end{align*}

Throughout this section, \( F = \mathbb{F}_q, K = \mathbb{F}_p \) with \( q = p^r \) and we will simply write \( \text{Tr}(z) \) instead \( \text{Tr}_{F/K}(z) \).

Let \( \{s_n\} \) be a linear recurrence sequence of order \( r \geq 1 \) in \( \mathbb{F}_p \) with characteristic polynomial \( \omega(x) \) in \( \mathbb{F}_p[x] \). It is well known that \( n^{th} \)-term can be written in terms of the roots of the characteristic polynomial, see Theorem 6.21 in [16]. Therefore, if the roots \( \alpha_0, \ldots, \alpha_{r-1} \) of \( \omega(x) \) are all distinct in its splitting field, then

\[ s_n = \sum_{i=0}^{r-1} \beta_i \alpha_i^n, \quad \text{for } n = 0, 1, 2, \ldots, \]

with characteristic polynomial \( (x - g)(x - g^2)(x - g^{(\ell^2+1)/2})(x - g^{(\ell^2+1)/2}) \). Note that

\[ \tau_2 = \text{ord } g = \ell^2 - 1 \text{ and } \tau_1 = \text{ord } g^{(\ell^2+1)/2} = \frac{\ell^2 - 1}{\gcd(\ell^2 - 1, (\ell^2 + 1)/2)}. \]
where $\beta_0, \ldots, \beta_{r-1}$ are uniquely determined by initial values $s_0, \ldots, s_{r-1}$, and belong to the splitting field of $\omega(x)$ over $\mathbb{F}_p$.

If the characteristic polynomial $\omega$ is irreducible and $\alpha$ is a root, then its $r$ distinct conjugates are

$$\alpha, \alpha^p, \ldots, \alpha^{p^{r-2}}, \alpha^{p^{r-1}}.$$  

Hence, the coefficients $s_n$ are given by

$$s_n = \sum_{i=0}^{r-1} \beta_i \alpha^{p^i n}, \quad n = 0, 1, 2, \ldots.$$  

One of our main tools is the bound for Gauss sum in finite fields given by Bourgain and Chang [3, Theorem 2]. This will be required to prove Theorem 1. Assume that for a given $\alpha \in \mathbb{F}_q$ such that $t = \text{ord} \alpha$ satisfies

$$t > p^r \quad \text{and} \quad \max_{1 \leq d < r} \gcd(t, p^d - 1) < t p^{-\varepsilon}.$$  

Then there exists a $\delta = \delta(\varepsilon) > 0$ such that for any nontrivial additive character $\psi$ of $\mathbb{F}_q$, we have

$$\left| \sum_{n \leq t} \psi(\alpha^n) \right| \leq t p^{-\delta}.$$  

Here, we note that second assumption in (14) implies the first one whenever $r \geq 2$.

2.1. Proof of Theorem 1. We proceed by induction over $\nu$. Before that, following properties (10) and (11) of trace function we get

$$s_n = \text{Tr} \left( r^{-1} s_n \right) = r^{-1} \text{Tr} \left( \sum_{i=1}^{\nu} (\beta_{i,0} \alpha_i^n + \ldots + \beta_{i,t_i-1} \alpha_i^{p^{t_i-1} n}) \right) = r^{-1} \sum_{i=1}^{\nu} \sum_{j=0}^{t_i-1} \text{Tr} \left( \beta_{i,j} \alpha_i^{p^j n} \right).$$  

Set $r = [\mathbb{F}_p(\alpha_1, \ldots, \alpha_\nu) : \mathbb{F}_p]$, then $z^{p^n} = z$ for any $z \in \mathbb{F}_p(\alpha_1, \ldots, \alpha_\nu)$, in particular $\text{Tr} \left( z^{p^n} \right) = \text{Tr} \left( z \right)$. Then for each pair $(i, j)$, raising each argument $\beta_{i,j} \alpha_i^{p^j n}$ to the power $p^{r-j}$

$$\text{Tr} \left( \beta_{i,j} \alpha_i^{p^j n} \right) = \text{Tr} \left( \beta_{i,j}^{p^{r-j}} \alpha_i^{p^{j} n} \right) = \text{Tr} \left( \beta_{i,j}^{p^{r-j}} \alpha_i^{p^j n} \right) = \text{Tr} \left( \beta_{i,j}^{p^{r-j}} \alpha_i^{n} \right).$$

This implies that

$$s_n = r^{-1} \sum_{i=1}^{\nu} \sum_{j=0}^{t_i-1} \text{Tr} \left( \beta_{i,j}^{p^{r-j}} \alpha_i^n \right) = r^{-1} \sum_{i=1}^{\nu} \text{Tr} \left( \left( \sum_{j=0}^{t_i-1} \beta_{i,j}^{p^{r-j}} \right) \alpha_i^n \right).$$

$$= \text{Tr} \left( \gamma_1 \alpha_i^n \right) + \ldots + \text{Tr} \left( \gamma_\nu \alpha_i^n \right),$$

where $\gamma_i = r^{-1} \sum_{j=0}^{t_i-1} \beta_{i,j}^{p^{r-j}}$, for each $1 \leq i \leq \nu$.

The case $\nu = 1$ follows by Bourgain–Chang [3, Theorem 2]. We shall now proceed inductively, and $\nu = 2$ will be the base case. We start with denoting $h = \gcd(\tau_1, \tau_2)$. It is clear
that $\text{lcm}(\tau_1, \tau_2) = \tau_1 \tau_2 / h$ is a period of $s_n$, then

$$\left| \sum_{n \leq \frac{\tau_1 \tau_2}{h}} e_p(\xi s_n) \right| = \frac{\tau}{\tau_1 \tau_2 / h} \left| \sum_{n \leq \frac{\tau_1 \tau_2}{h}} e_p(\xi s_n) \right| .$$

Hence, it is enough to prove that

$$\left| \sum_{n \leq \frac{\tau_1 \tau_2}{h}} e_p(\xi s_n) \right| \leq \frac{\tau_1 \tau_2}{h} p^{-\delta}, \quad \text{with } (\xi, p) = 1,$$

for some $\delta = \delta(\varepsilon) > 0$. We have

$$\left| \sum_{n \leq \frac{\tau_1 \tau_2}{h}} e_p(\xi s_n) \right| = \left| \sum_{u=0}^{h-1} \sum_{n \leq \frac{\tau_1 \tau_2}{h}} e_p(\xi s_{nh+u}) \right| \leq \sum_{u=0}^{h-1} \left| \sum_{n \leq \frac{\tau_1 \tau_2}{h}} e_p(\xi s_{nh+u}) \right| .$$

(16)

Let $(n_1, n_2)$ be a tuple with $n_i \leq \frac{\tau_1}{h}$. Since $\gcd(\frac{\tau_1}{h}, \frac{\tau_2}{h}) = 1$, by Chinese reminder theorem, there exist integers $m_1, m_2$ with $\gcd(m_1, \frac{\tau_1}{h}) = \gcd(m_2, \frac{\tau_2}{h}) = 1$, such that

(17) \quad $\left\{ n \pmod{\frac{\tau_1 \tau_2}{h^2}} : 1 \leq n \leq \frac{\tau_1 \tau_2}{h^2} \right\} = \left\{ \frac{n_1 m_1 \tau_1}{h} + n_2 m_2 \frac{\tau_2}{h} \pmod{\frac{\tau_1 \tau_2}{h}} : 1 \leq n_i \leq \frac{\tau_1}{h} \right\} .$

Moreover, the pair $(m_1, m_2)$ has the following property: given $(n_1, n_2)$, with $1 \leq n_i \leq \tau_i / h$, then $n = n_1 \frac{\tau_1}{h} + n_2 \frac{\tau_2}{h}$ satisfies

$$n \equiv n_1 \pmod{\frac{\tau_1}{h}} \text{ and } n \equiv n_2 \pmod{\frac{\tau_2}{h}},$$

and $n$ is unique modulus $\frac{\tau_1 \tau_2}{h^2}$. Since $\frac{\tau_1}{h} = \text{ord} \alpha_1^h$ and $\frac{\tau_2}{h} = \text{ord} \alpha_2^h$ then

(18) \quad $\alpha_i^{h n_i} = \alpha_i^{h (n_1 \frac{\tau_1}{h} + n_2 \frac{\tau_2}{h})} = \alpha_i^{h n_i}, \quad 1 \leq i \leq 2.$

Combining (17) and (18) we have

$$\left| \sum_{n \leq \frac{\tau_1 \tau_2}{h^2}} e_p(\xi s_{nh+u}) \right| = \sum_{n_1 \leq \frac{\tau_1}{h}} e_p \left( \text{Tr} \left( \xi \gamma_1 \alpha_1^{n_1 h+u} \right) \right) \times \sum_{n_2 \leq \frac{\tau_2}{h}} e_p \left( \text{Tr} \left( \xi \gamma_2 \alpha_2^{n_2 h+u} \right) \right) ,$$

(19)

with $\gamma_i' = \xi \gamma_1 \alpha_1^{u}, \gamma_i'' = \xi \gamma_2 \alpha_2^u$ in $\mathbb{F}_p(\alpha_1, \alpha_2)$. Since $\{s_n\}$ is a nonzero sequence then $\gamma_i' \neq 0$, at least for some $1 \leq i \leq 2$. We may assume all of them are nonzero. For each $e_p \left( \text{Tr} \left( \xi \gamma_i' \right) \right)$ it corresponds a nontrivial additive character $\psi_i(z)$ in $\mathbb{F}_p(\alpha_1, \alpha_2) \cong \mathbb{F}_p(\alpha_1)$, we say, because $\mathbb{F}_p(\alpha_1) \cong \mathbb{F}_p(\alpha_2)$. In order to satisfy condition (14) we first recall assumptions $h < p''$. 


\( \varepsilon > \varepsilon' > 0 \) and \( \max_{d \leq r} \gcd(\tau_i, p^d - 1) < \tau_ip^{-\varepsilon} \) for some \( i = 1, 2 \). Then, for any \( d|r \) with \( 1 \leq d < r \) and some \( i = 1, 2 \) we have
\[
\gcd\left( \frac{\tau_i}{p^d - 1} \right) \leq \gcd(\alpha_i, p^d - 1) < \tau_i p^{-\varepsilon} < \frac{\tau_i}{h}p^{-(\varepsilon-\varepsilon')}.
\]

Therefore, by Bourgain–Chang [3, Theorem 2] it follows that
\[
\sum_{n_i \leq \tau r^h} e_p\left( \text{Tr} \left( \gamma_i^{n_i/h} \right) \right) = \sum_{n_i \leq \tau r^h} |\psi(\alpha_i^{n_i/h})| \leq \frac{\tau_i}{h} p^{-\delta}, \text{ for some } 1 \leq i \leq 2.
\]

Thus, combining above equation with (16) and (19) we get
\[
\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \leq \tau} e_p(\xi s_n) \right|^{2t} = \sum_{m \leq \tau} \left| \sum_{n \leq \tau} e_p(\xi s_{m+n}) \right|^{2t} = \sum_{m \leq \tau} \left| \sum_{n \leq \tau} e_p(\xi(\text{Tr}(\gamma_1^{m+n} + \cdots + \text{Tr}(\gamma_\nu^{m+n}))) \right|^{2t} \leq \sum_{n_1 \leq \tau} \sum_{n_2 \leq \tau} \sum_{m \leq \tau} e_p \left( \xi \sum_{i=1}^{\nu} \left( \text{Tr}(\gamma_i^{n_1} + \cdots + \gamma_i^{n_2}) \right) \right) .
\]

Rising to the power \( 2t \) we have
\[
\tau^{2t} \left| \sum_{n \leq \tau} e_p(\xi s_n) \right|^{4t^2} \leq \tau^{2t(2t-1)} \sum_{n_1 \leq \tau} \cdots \sum_{n_2 \leq \tau} \sum_{m \leq \tau} e_p \left( \xi \sum_{i=1}^{\nu} \left( \text{Tr}(\gamma_i^{n_1} + \cdots + \gamma_i^{n_2}) \right) \right) .
\]

Given \( (\lambda_1, \cdots, \lambda_\nu) \in \mathbb{F}_q^\nu \), by \( J_t(\lambda_1, \cdots, \lambda_\nu) \) we denote the number of solutions of the system
\[
\begin{align*}
\alpha_1^{n_1} + \cdots + \alpha_1^{n_2t} &= \alpha_1^{n_1+1} + \cdots + \alpha_1^{n_{2t}} + \lambda_1 \\
& \quad \vdots \\
\alpha_\nu^{n_1} + \cdots + \alpha_\nu^{n_2t} &= \alpha_\nu^{n_{t+1}} + \cdots + \alpha_\nu^{n_{2t}} + \lambda_\nu
\end{align*}
\]

with \( 1 \leq n_1, \cdots, n_{2t} \leq \tau \). Therefore
\[
(20) \left| \sum_{n \leq \tau} e_p(\xi s_n) \right|^{4t^2} \leq \tau^{4t^2-4t} \sum_{\lambda_1 \in \mathbb{F}_q} \cdots \sum_{\lambda_\nu \in \mathbb{F}_q} J_t(\lambda_1, \cdots, \lambda_\nu) \sum_{m \leq \tau} e_p \left( \xi \sum_{i=1}^{\nu} \left( \text{Tr}(\gamma_i \lambda_i \alpha_i^{m}) \right) \right) .
\]
Note that writing $J_t(\lambda_1 \cdots, \lambda_\nu)$ in terms of character sums it follows that

$$J_t(\lambda_1 \cdots, \lambda_\nu) = \frac{1}{q^\nu} \sum_{\psi \in \mathbb{F}_q} \cdots \sum_{\nu \in \mathbb{F}_q} \left| \sum_{n \leq \tau} \psi_1(\alpha_1^n) \cdots \psi_\nu(\alpha_\nu^n) \right|^{2t} \times \psi_1(\lambda_1) \cdots \psi_\nu(\lambda_\nu)$$

$$\leq \frac{1}{q^\nu} \sum_{\psi \in \mathbb{F}_q} \cdots \sum_{\nu \in \mathbb{F}_q} \left| \sum_{n \leq \tau} \psi_1(\alpha_1^n) \cdots \psi_\nu(\alpha_\nu^n) \right|^{2t}$$

$$\leq J_t(0, \ldots, 0) =: J_{t, \nu}.$$

In particular, we note that $J_{t, \nu} \leq J_{t, \nu-1}$. From (20) it follows that

$$\left| \sum_{n \leq \tau} e_p(\xi s_n) \right|^{4t^2} \leq \tau^{4t^2-4t} J_{t, \nu} \sum_{m_1 \leq \tau} \cdots \sum_{m_\nu \leq \tau} \sum_{\lambda_1 \in \mathbb{F}_q} \cdots \sum_{\nu \in \mathbb{F}_q} e_p \left( \sum_{i=1}^\nu \text{Tr}(\xi \beta_i \alpha_i^{m_1} + \cdots - \alpha_i^{m_\nu}) \right).$$

Note that $a \gamma \lambda$, with $a \gamma \neq 0$, runs over $\mathbb{F}_q$ as $\lambda$ does, then $e_p(\text{Tr}(a \theta \lambda z))$ runs through all additive characters $\psi$ in $\mathbb{F}_q$, evaluated at $z$. Then the above expression can be written as

$$\left| \sum_{n \leq \tau} e_p(\xi s_n) \right|^{4t^2} \leq \tau^{4t^2-4t} J_{t, \nu} \sum_{m_1 \leq \tau} \cdots \sum_{m_\nu \leq \tau} \sum_{\psi \in \mathbb{F}_q} \left( \sum_{\lambda_1 \in \mathbb{F}_q} \cdots \sum_{\nu \in \mathbb{F}_q} e_p \left( \sum_{i=1}^\nu \text{Tr}(\alpha_i^{m_1} + \cdots - \alpha_i^{m_\nu}) \right) \right).$$

(21)

We now require an estimate for $J_{t, \nu-1}$. Writing it as sum of characters

$$J_{t, \nu-1} = \frac{1}{q^{\nu-1}} \sum_{\lambda_1 \in \mathbb{F}_q} \cdots \sum_{\nu-1 \in \mathbb{F}_q} \left| \sum_{m \leq \tau} e_p \left( \text{Tr}(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m) \right) \right|^{2t}$$

$$= \frac{\tau^{2t}}{q^{\nu-1}} + O \left( \left( \max_{(\lambda_1, \ldots, \lambda_{\nu-1}) \in \mathbb{F}_q^{\nu-1}} \left| \sum_{m \leq \tau} e_p \left( \text{Tr}(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m) \right) \right| \right)^{2t} \right).$$

(22)

Finally, we note that $s_m' = \text{Tr}(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m)$ defines a linear recurrence sequence with period $\tau'$ dividing $\tau$, which in particular satisfies induction hypothesis. Therefore

$$\left| \sum_{m \leq \tau} e_p \left( \text{Tr}(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m) \right) \right| \leq \tau p^{-\delta'},$$

for some $\delta' = \delta'(\varepsilon) > 0$. Now, taking $t > d(\nu - 1)/2\delta'$ (where $d = [\mathbb{F}_q : \mathbb{F}_p]$) and combining with (22) we get

$$J_{t, \nu-1} \ll \frac{\tau^{2t}}{q^{\nu-1}}.$$
We conclude the proof combining the above estimate with (21) to get

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \leq \tau} e_p (\xi s_n) \right| \leq \tau p^{-\delta},$$

with $\delta = -\frac{d(\nu-2)}{4\tau^2}.$

The following is an immediate corollary of this theorem which will be quite handy in establishing several results in Section 3 and Section 6.

**Corollary 6.** Suppose that $\{s_n\}$ is a nonzero linear recurrence sequence of order $r \geq 2$ such that its characteristic polynomial $\omega(x)$ is irreducible in $\mathbb{F}_p[x]$. If its period $\tau$ satisfies

$$\max_{d<r \atop d | \tau} \gcd(\tau, p^d - 1) < \tau p^{-\varepsilon},$$

then there exists a $\delta = \delta(\varepsilon) > 0$ such that

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \leq \tau} e_p (\xi s_n) \right| \leq \tau p^{-\delta}.$$

### 3. Exponential sums for modular forms

In this section, we study the effect of recurrence sequence and Theorem 1 in the behaviour of the exponential sums attached to certain Fourier coefficients of modular forms. As a consequence, we obtain interesting results which have been summarized earlier in form of Theorem 2 and Theorem 3.

#### 3.1. Order of the roots of characteristic polynomial

Let $f$ be a normalized modular form of weight $k \in 2\mathbb{Z}$, without complex multiplication, and $a(n)$ be its $n^{th}$-Fourier coefficient. In other words, there exists no positive integer $D$ such that $a(p) = 0$ for all prime $p$ with $\left( \frac{D}{p} \right) = -1$. We recall that $\{a(p^n)\}_{n \in \mathbb{N}}$ is a recurrence sequence of order 2, see (1). The aim of this section is to study exponential sums with the sequence $\{a(p^n)\}$ in $\mathbb{F}_\ell$ for primes $p$ and $\ell$. In particular, we establish Theorem 2. Before going into the proof of this theorem, we develop a useful tool which will be quiet handy in what follows. We state it in the form of following lemma.

**Lemma 7.** Let $\omega(x) = x^2 + ax + b \in \mathbb{Z}[x]$ be a quadratic polynomial with $b \neq 0$ having roots $\alpha, \beta$ such that, none of $\alpha, \beta$ or $\alpha\beta^{-1}$ is a root of unity. For any prime $\ell$ let $\alpha_\ell, \beta_\ell$ be its roots in the splitting field of $\omega$ over $\mathbb{F}_\ell$. Then, given $0 < \varepsilon < 1/2$, for $\pi(y)(1 + O(y^{2\varepsilon - 1}\log y))$ many primes $\ell \leq y$ we have

$$\text{ord } \alpha_\ell > \ell^\varepsilon, \quad \text{ord } \beta_\ell > \ell^\varepsilon \quad \text{and} \quad \text{ord } (\alpha_\ell\beta_\ell^{-1}) > \ell^\varepsilon.$$

\(^4\)We need to consider the base case $\nu = 2$ as otherwise $\delta$ would be 0.

\(^5\)Here $\pi(y)$ denotes the number of primes up to $y$, which is asymptotically equivalent to $\frac{y}{\log y}$. 

Proof. It is clear that $\omega \pmod{\ell}$ has a distinct roots for all but finitely many primes $\ell$, since $a^2 - 4b \neq 0$ is given. For all such prime $\ell$, let $\alpha_\ell$ and $\beta_\ell$ be the distinct roots in its splitting field. Given a large positive parameter $T$, consider the polynomial

$$G_T(x) = \prod_{t \leq T} (x^t - 1)(x^{2t} - b^t) \in \mathbb{Z}[x].$$

Note that $\ell$ divides $\text{Res}(\omega, G_T)$ if and only if $\omega \pmod{\ell}$ and $G_T \pmod{\ell}$ have common roots in some finite extension of $\mathbb{F}_\ell$. Clearly $\alpha_\ell$ or $\beta_\ell$ are common roots of $\omega$ and $G_T$ if $\text{ord} \alpha_\ell$ or $\text{ord} \beta_\ell$ are less than $T$. We also note that $\text{ord} (\alpha_\ell \beta_\ell^{-1}) \leq T$ if and only if $\alpha_\ell^{2t} - b^t = 0$ (or $\beta_\ell^{2t} - b^t = 0$), for some $t \leq T$, because $\alpha_\ell \beta_\ell = b$.

Now, Sylvester matrix of $\omega$ and $G_T$ is a square matrix with order $2 + \deg G_T \ll T^2$, and entries bounded by an absolute constant $M$ (which depends on $a, b$ and not on $\ell$ or the parameter $T$). Then, its determinant

$$|\text{Res}(\omega, G_T)| \leq T^{2!} \times M^{T^2} \ll M^{2T^2 \log T}.$$  

Note that $\text{Res}(\omega, G_T)$ is zero, if and only if, $\alpha_\ell^{t} = 1$, $\beta_\ell^{t} = 1$ or $(\alpha \beta_\ell)^t = 1$ for some $t \leq T$, which following our assumption can not happen. In particular, the resultant has at most $O(T^2)$ prime divisors. In particular this shows that the cardinality of the set of primes

$$|\{\ell | \text{ord} \alpha_\ell \leq T \text{ or } \text{ord} \beta_\ell \leq T \text{ or } \text{ord} \alpha_\ell \beta_\ell^{-1} \leq T\}| = O(T^2).$$

Choosing $T = y^\varepsilon$ the number of primes $\ell \leq y$ such that

$$\text{ord} \alpha_\ell \leq \ell^\varepsilon \text{ or } \text{ord} \beta_\ell \leq \ell^\varepsilon \text{ or } \text{ord} (\alpha_\ell \beta_\ell^{-1}) \leq \ell^\varepsilon$$

is $O(y^{2\varepsilon})$. \hfill \Box

Let us now proceed to prove the main results of this section.

3.2. Proof of Theorem 2. The characteristic polynomial of $(1)$ is

$$(23) \quad \omega(x) = x^2 - a(p)x + p^{k-1},$$

and has discriminant $a^2(p) - 4p^{k-1}$. We note that in our case the discriminant does not vanish, otherwise $|a(p)| = 2p^{(k-1)/2}$ with $a(p)$ being integer and $p^{(k-1)/2}$ irrational. Now, let us denote by $\mathbb{P}$ the set of all primes and $\mathcal{P}$ the set of primes such that $a(p^n) \neq 0$ for all integers $u \geq 1$. We divide the proof for primes $p \in \mathcal{P}$ and $p \in \mathbb{P} \setminus \mathcal{P}$.

Following from the part 3 of Theorem B in $[1]$ (i.e. proof of Sato-Tate conjecture), we know that $a(p^n) \neq 0$, for all $u \geq 1$, and almost all primes $p$ in $\mathbb{P}$, then $\mathcal{P}$ has density one in $\mathbb{P}$. Since $a^2(p) - 4p^{k-1} \neq 0$, for any $p \in \mathcal{P}$, we write $a^2(p) - 4p^{k-1} = u^2 D_p$, with $D_p < 0$ square-free and $u \neq 0$. We now split the cases according to $D_p \pmod{\ell}$ is quadratic residue, zero or non quadratic residue modulo $\ell$.

Set

$$\mathbb{P} \cap \mathcal{P} = \mathbb{P}_0 \cup \mathbb{P}_1 \cup \mathbb{P}_{-1}, \quad \text{where } \mathbb{P}_\nu = \left\{ \ell \in \mathbb{P} \cap \mathcal{P} : \left( \frac{D_p}{\ell} \right) = \nu \right\}.$$  

For $\nu = 0, 1, -1$, we also define

$$\mathbb{P}_\nu(x) = \mathbb{P}_\nu \cap [1, x], \quad \pi_\nu(x) = |\mathbb{P}_\nu(x)| \text{ and } \kappa_\nu = \lim_{x \to \infty} \frac{\pi_\nu(x)}{\pi(x)}.$$  

It is clear that $\pi_\nu(x) = \pi(x)(\kappa_\nu + o(1))$, and $\kappa_0 + \kappa_1 + \kappa_{-1} = 1$.  


Note that for a given \( p \), the associated polynomial \( \omega(x) \) (mod \( \ell \)) has a single root in \( \mathbb{F}_\ell \) if and only if \( D_\ell = 0 \) (mod \( \ell \)). Since such equation has finitely many solutions for \( \ell \), we get \( \kappa_0 = 0 \). On another hand, Chebotarev’s density theorem implies the uniform distribution of primes \( \ell \) such that \( P(x) \) (mod \( \ell \)) is irreducible or has distinct roots in \( \mathbb{F}_\ell \). Equivalently, the primes \( \ell \) satisfying \( \left( \frac{D_\ell}{\ell} \right) = \pm 1 \) are distributed in the same proportion, therefore \( \kappa_{-1} = \kappa_1 = 1/2 \). Now we turn to establish nontrivial exponential sums for \( \{ a(p^n) \} \) (mod \( \ell \)) with \( \ell \in \mathbb{P}_\nu \) for \( \nu = \pm 1 \).

**Case 1.** \( \ell \in \mathbb{P}_{-1} \): In this case the associated polynomial (23) is irreducible modulo \( \ell \). We want to show that the inequality (7) is satisfied by almost all primes \( \ell \) in \( \mathbb{P}_{-1} \). Let \( \alpha \) and \( \beta = \alpha^\ell \) be the conjugate roots of (23) in its splitting field \( \mathbb{F}_\ell(\alpha) \). For a given \( \varepsilon > 0 \) from Lemma 7 there exists a subset of \( \mathbb{P}_{-1} \), with density \( 1/2 \) in \( \mathbb{P} \) such that

\[
\text{Case 1. } \ell \in \mathbb{P}_{-1}: \text{ In this case the associated polynomial (23) is irreducible modulo } \ell. \text{ We want to show that the inequality (7) is satisfied by almost all primes } \ell \text{ in } \mathbb{P}_{-1}. \text{ Let } \alpha \text{ and } \beta = \alpha^\ell \text{ be the conjugate roots of (23) in its splitting field } \mathbb{F}_\ell(\alpha). \text{ For a given } \varepsilon > 0 \text{ from Lemma 7 there exists a subset of } \mathbb{P}_{-1}, \text{ with density } 1/2 \text{ in } \mathbb{P} \text{ such that}
\]

\[
(24) \quad \text{ord } \alpha^\ell = \text{ord } \alpha > \ell^\varepsilon \quad \text{and} \quad \text{ord } \alpha\beta = \text{ord } \alpha^{1-\ell} > \ell^\varepsilon.
\]

Combining the identity

\[
\text{ord } \alpha^{\ell-1} = \text{ord } \alpha / \text{gcd}(\text{ord } \alpha, \ell - 1)
\]

with the second inequality of (24), we get

\[
\text{gcd}(\text{ord } \alpha, \ell - 1) = \frac{\text{ord } \alpha}{\text{ord } \alpha^{\ell-1}} = \frac{\text{ord } \alpha}{\text{ord } \alpha^{1-\ell}} < (\text{ord } \alpha)^{1-\varepsilon}.
\]

This finishes the first part of the proof of (i) in Theorem 2.

**Case 2.** \( \ell \in \mathbb{P}_1 \): Let \( \alpha, \beta \) be the roots of \( \omega(x) \) (mod \( \ell \)) inside \( \mathbb{F}_\ell^* \). From (13) it follows that for \( n \geq 0 \),

\[
a(p^n) = c\alpha^n + d\beta^n \pmod{\ell},
\]

for some constants \( c, d \) in \( \mathbb{F}_\ell \), with \( (\alpha, \beta) \neq (0, 0) \). It is clear that \( \ell - 1 \) is a period of the sequence \( a(p^n) \) (mod \( \ell \)), then \( \tau \) divides \( \ell - 1 \). We have

\[
\sum_{n \leq \tau} e_{\ell}(\xi a(p^n)) = \frac{\tau}{\ell - 1} \sum_{n \leq \ell - 1} e_{\ell}(\xi a(p^n)) = \frac{\tau}{\ell - 1} \sum_{n \leq \ell - 1} e_{\ell}(\xi(c\alpha^n + d\beta^n)).
\]

From Lemma 7, there is a subset of \( \mathbb{P}_1 \) with density \( 1/2 \) in \( \mathbb{P} \) such that \( \text{ord } \alpha, \text{ord } \beta \) and \( \text{ord } (\alpha\beta) \) are bigger than \( \ell^\varepsilon \). It follows from Bourgain (see [2, Corollary]) that there exists \( \delta = \delta(\varepsilon) > 0 \) such that

\[
\max_{(c,d) \in \mathbb{F}_\ell \times \mathbb{F}_\ell} \left| \sum_{n \leq \ell - 1} e_{\ell}(c\alpha^n + d\beta^n) \right| \leq \ell^{1-\delta}.
\]

Hence, (i) of Theorem 2 holds.

Now, assume that \( p \) belongs to the exceptional set \( \mathbb{P} \setminus \mathbb{P}_1 \), i.e. \( a(p^n) = 0 \) for some \( u \geq 1 \). We consider \( u = u(p) \) to be the least such integer. Since the discriminant is nonzero (the roots \( \alpha \) and \( \beta \) of (23) are distinct), from basic methods we get

\[
a(p^n) = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} = 0.
\]
Therefore, we have
\[ \alpha \] which is absurd as
\[ \text{get trivially} \]
upto \( u \)

First of all observe that
\[ (25) \]

Due to Lemma \( (26) \)

Next argument applies to the positive sign case as well. Since we are assuming that this sign is negative. Moreover, it is easy to see that our
\[ \text{for any} \ n \ \text{we may assume that} \]

Set \( b(u + 1) = a(p^u) \), then it follows that for all \( n \geq 1 \) we have
\[ b(n(u + 1)) = a(p^{n(u+1)-1}) = \frac{\alpha^n(u+1) - \beta^n(u+1)}{\alpha - \beta} = 0. \]

Therefore,
\[ \sum_{n \leq \tau} e_\ell (\xi a(p^n)) = \sum_{n=0}^{\tau-1} e_\ell (\xi b(n + 1)) = \sum_{n=0}^{\tau/(u+1)} \sum_{\ell \leq n} e_\ell (\xi b(n(u + 1) + \epsilon)) + O(u) \]

\[ (25) \]

\[ = \frac{\tau}{u+1} + \sum_{\ell \leq n} e_\ell (\xi b(n(u + 1) + \epsilon)) + O(u). \]

First of all observe that \( u \) is odd. As otherwise, if \( u \) is even then we would get
\[ \alpha^{u+1} + \beta^{u+1} = 2\alpha^{u+1} = \pm2p^{\frac{(u+1)(-1)}{2}}, \]

which is absurd as \( \alpha^{u+1} + \beta^{u+1} \) is an integer but \( \frac{(u+1)(-1)}{2} \) is not. Now, for any \( 0 < \epsilon < u+1 \) we have
\[ b((u + 1)n + \epsilon) = \alpha^{(u+1)n}(\alpha^\epsilon - \beta^\epsilon) = \pm p^{\frac{(u+1)(-1)}{2}} a(p^{\epsilon-1}), \]

where the sign on the right hand side above depends on the sign of \( \alpha^{u+1} \). Without loss of generality, we are assuming that this sign is negative. Moreover, it is easy to see that our next argument applies to the positive sign case as well. Since \( u \) is fixed, so are all the \( \epsilon \)'s upto \( u - 1 \). In particular, we may consider large \( \ell \)'s for which all of the \( a(p^\epsilon) \neq 0 \ (\mod \ell) \) for any \( 1 \leq \epsilon \leq u - 1 \). Then, we have
\[ \sum_{n=0}^{\tau/(u+1)} e_\ell (\xi b(n(u + 1) + \epsilon)) = \sum_{n=0}^{\tau/(u+1)} e_\ell (\xi (-p)^{\frac{(u+1)(-1)n}{2}} a(p^{\epsilon-1})). \]

Due to Lemma \( 7 \), we may assume that \( t_u = \text{ord} (-p^{k-1}(u+1)/2) > \ell^{2\epsilon} \) holds for \( \pi(y)(1 + y^{2\epsilon-1} \log y) \) many primes \( \ell \leq y \). Now, by \([4, \text{Theorem} 6]\) it follows that
\[ (26) \]

\[ \left| \sum_{n \leq t_u} e_\ell (\xi (-p)^{\frac{(u+1)(-1)n}{2}} a(p^{\epsilon-1})) \right| \leq t_u \ell^{-\delta}, \quad \text{for some} \ \delta = \delta(\varepsilon) > 0. \]

Writing \( \left\lceil \tau/(u+1) \right\rceil = qt_u + r \), with \( 0 \leq r < t_u \) it follows that
\[ \sum_{n \leq \tau/(u+1)} e_\ell (\xi \alpha^{(u+1)n} a(p^{\epsilon-1})) = q \sum_{n \leq t_u} e_\ell (\xi \alpha^{(u+1)n} a(p^{\epsilon-1})) + \]

\[ + \sum_{n \leq \tau} e_\ell (\xi \alpha^{(u+1)n} a(p^{\epsilon-1})). \]

The estimate \( \left| \sum_{n \leq t_u} e_\ell (\xi \alpha^{(u+1)n} a(p^{\epsilon-1})) \right| \leq t_u \ell^{-\epsilon} \) follows from \( (26) \). If \( r \leq \ell^{\delta} \), then we get trivially \( \left| \sum_{n \leq \tau} e_\ell (\xi \alpha^{(u+1)n} a(p^{\epsilon-1})) \right| \leq \ell^{\delta} \). If \( \ell^{\delta} \leq r \leq t_u \), then from \( (26) \) it follows that
\[ \left| \sum_{n \leq \tau} e_\ell (\xi \alpha^{(u+1)n} a(p^{\epsilon-1})) \right| \leq t_u \ell^{-\delta}. \]
Therefore
\[
\left| \sum_{n \leq \tau} e_{\ell} \left( \xi \alpha^{(u+1)n} a(p^{\ell-1}) \right) \right| \leq \ell^\varepsilon + t_u \ell^{-\delta}.
\]

We also note that \( t_u \ell^{-\delta} \geq \ell^\varepsilon \) for \( \varepsilon \) small enough, since from [4, Theorem 6] \( \delta = \exp(-C_1 \varepsilon - C_2) \) for some absolute constants \( C_1, C_2 > 0 \). Thus,
\[
\left| \sum_{n \leq \tau/(u+1)} e_{\ell} \left( \xi \alpha^{(u+1)n} a(p^{\ell-1}) \right) \right| \leq q t_u \ell^{-\delta} \ll \frac{\tau}{u+1} \ell^{-\delta}.
\]

Finally, combining the above inequality with (25) we obtain
\[
\max_{\xi \in \mathbb{S}_\ell^*} \left| \sum_{n \leq \tau} e_{\ell} (\xi \alpha^n) \right| = \frac{\tau}{u+1} + O \left( \tau \ell^{-\delta} \right).
\]

This conclude the proof for all exceptional set of primes \( p \in \mathbb{P} \setminus \mathcal{P} \).

**Remark 1.** In the proof of Case 2 part (i) of Theorem 2, we only needed the fact that \( \tau \) divides \( \ell - 1 \). However, how often is this \( \tau \) actually \( \ell - 1 \)? At the moment we do not have an answer to that, but \( \tau \) divides \( \text{lcm}(\text{ord} \alpha, \text{ord} \beta) \) and we claim that the former is exactly \( \ell - 1 \) for a positive density of primes under the assumption of GRH. Because,
\[
\text{ord} (p^{k-1}) = \text{ord} (\alpha \beta) \leq \ell - 1,
\]
and since \( k - 1 \) is always odd, by Artin’s primitive root conjecture \( \text{lcm}(\text{ord} \alpha, \text{ord} \beta) = \ell - 1 \) for a positive density of primes \( \ell \). But in our case, we needed the primes \( \ell \) to be in \( \mathbb{P}_1 \). In particular, here we need to look for primes \( \ell \) which are congruent to \( a' \) (mod \( D_p \)) for some \( a' \) with \( \left( \frac{D_p}{\ell} \right) = +1 \) such that modulo these primes \( p^{k-1} \) is a primitive root. Indeed, this problem was first considered by Lenstra, and under GRH he found the corresponding density (see [15]). Later Moree did a more delicate analysis, and showed that the density is positive when \( (a' - 1, |D_p|, k - 1) = 1 \), see Theorem 1.2 of [19] for more details. In particular, \( \text{ord} (p^{k-1}) = \ell - 1 \) for a positive density of primes \( \ell \in \mathbb{P}_1 \), provided that \( (a' - 1, |D_p|, k - 1) = 1 \). For instance, this is always true for \( k = 2 \).

### 3.3. Consequences of Theorem 2

As one of the consequences of Theorem 2, we can consider the problem where the exponential sum runs over numbers up to some stage having only one prime factor. More precisely, we prove

**Corollary 8.** Let \( f \) be a normalized eigenform of weight \( k \) and level \( N \) with integer coefficient. Then for a given \( 0 < \varepsilon < 1/2 \), there exists a \( \delta(\varepsilon) > 0 \) such that for many large enough primes \( \ell \) and \( x \), we have the following estimates:
\[
\max_{\xi \in \mathbb{S}_\ell} \left| \sum_{p^n \leq x} e_{\ell} (\xi \alpha(p^n)) \right| = \begin{cases} 
O \left( (\log x/\log p)^{1-\delta/(2+\delta)} \right) & \text{if } p \notin \mathcal{P} \\
\frac{1}{u+1} \log x + O \left( (\log x/\log p)^{1-\delta/(2+\delta)} \right) & \text{if } p \in \mathcal{P}.
\end{cases}
\]
Proof. Following Theorem 2, we have

$$\max_{\xi \in \mathbb{F}_r} \left| \sum_{p^n \leq \tau} e_\ell (\xi a(p^n)) \right| \leq \frac{\tau}{\ell^\delta}. \tag{27}$$

For large enough \(x\), consider any prime

$$\ell \in \left[ \left( \log x/ \log p \right)^{1/2-\delta/4+2\delta}, 2(\log x/ \log p)^{1/2-\delta/4+2\delta} \right].$$

Then, we have \(\tau \leq \ell^2 < \log x/ \log p\). In particular,

$$\max_{\xi \in \mathbb{F}_r} \left| \sum_{p^n \leq x} e_\ell (\xi a(p^n)) \right| \leq \frac{\log x}{\ell^\delta \log p} + O \left( \ell^2 \right) = O \left( (\log x/ \log p)^{1-\delta/(2+\delta)} \right).$$

Finally, Lemma 7 allows us to pick many such \(\ell\) so that an estimation of type (27) holds.

On the other hand, if \(p \in \mathcal{P}\) is fixed, then again by Theorem 2 we have

$$\max_{\xi \in \mathbb{F}_r} \left| \sum_{p^n \leq \tau} e_\ell (\xi a(p^n)) \right| = \frac{\tau}{u+1} + O \left( \frac{\tau}{\ell^\delta} \right),$$

for some \(u\) depending on \(p\). We now get the desired result arguing similarly as in the previous paragraph, with the same choices of primes \(\ell\).

Corollary 9. Let \(f\) be a normalized eigenform of weight \(k\) and level \(N\) with integer coefficients. For almost all primes \(\ell\) we have the following property. Given \(0 < \varepsilon < 1/2\) and \(p_1, \cdots, p_\nu\) be any set of distinct primes such that \(a(p_i^n) \neq 0\) for all \(u \geq 1\) and \(1 \leq i \leq \nu\), there exists a \(\delta = \delta(\varepsilon) > 0\) such that

$$\max_{\xi \in \mathbb{F}_r} \left| \sum_{n_1 \leq \tau_1} \cdots \sum_{n_\nu \leq \tau_\nu} e_\ell (\xi a(p_1^{n_1} \cdots p_\nu^{n_\nu})) \right| \leq \tau_1 \cdots \tau_\nu \ell^{-\delta}.$$

Proof. We proceed by induction. Case \(\nu = 1\) is done by Theorem 2. Now, by multiplicativity it follows that

$$\left| \sum_{n_1 \leq \tau_1} \cdots \sum_{n_\nu \leq \tau_\nu} e_\ell (\xi a(p_1^{n_1} \cdots p_\nu^{n_\nu})) \right| \leq \sum_{n_1 \leq \tau_1} \left| \sum_{n_2 \leq \tau_2} \cdots \sum_{n_\nu \leq \tau_\nu} e_\ell (\xi a(p_1^{n_1}) a(p_2^{n_2} \cdots p_\nu^{n_\nu})) \right|$$

$$\leq \tau_2 \cdots \tau_\nu \sum_{a(p_1^{n_1})=0} 1 + \sum_{n_1 \leq \tau_1} \left| \sum_{n_2 \leq \tau_2} \cdots \sum_{n_\nu \leq \tau_\nu} e_\ell (\xi a(p_1^{n_1}) a(p_2^{n_2} \cdots p_\nu^{n_\nu})) \right|.$$

By induction hypothesis, the second term on the right hand side of the above equation is bounded by \(\tau_1 \cdots \tau_\nu \ell^{-\delta}\), for some \(\delta > 0\) depending on \(\varepsilon\). On the other hand, note that
\[
\sum_{a(p_1^{n_1})=0}^{n_1 \leq \tau_1} 1 \text{ counts the number of solutions of the congruence } a(p_1^{n_1}) \equiv 0 \pmod{\ell}, \quad n_1 \leq \tau_1.
\]

Writing it as exponential sum and by Theorem 1, we get
\[
\sum_{a(p_1^{n_1})=0}^{n_1 \leq \tau_1} 1 = \frac{1}{\ell} \sum_{x=0}^{\ell-1} \sum_{n_1 \leq \tau_1} \mathbf{e}_\ell(x(a(p_1^{n_1})))
\]
\[
= \frac{\tau_1}{\ell} + O\left( \max_{x \in F_\ell^*} \left| \sum_{n_1 \leq \tau_1} \mathbf{e}_\ell(x(a(p_1^{n_1}))) \right| \right)
\]
\[
= \frac{\tau_1}{\ell} + O(\tau_1 \ell^{-\delta}) \leq 2\tau_1 \ell^{-\delta},
\]
since the explicit constant in Theorem 1 was exactly 1. Therefore
\[
\left| \sum_{n_1 \leq \tau_1} \cdots \sum_{n_\nu \leq \tau_\nu} \mathbf{e}_\ell(a(p_1^{n_1} \cdots p_\nu^{n_\nu})) \right| \leq \tau_2 \cdots \tau_\nu \left( 2\tau_1 \ell^{-\delta} \right) + \tau_1 \tau_2 \cdots \tau_\nu \ell^{-\delta},
\]
for some \( \delta = \delta(\varepsilon) > 0 \). This shows that
\[
\max_{\xi \in F_\ell^*} \left| \sum_{n_1 \leq \tau_1} \cdots \sum_{n_\nu \leq \tau_\nu} \mathbf{e}_\ell(\xi a(p_1^{n_1} \cdots p_\nu^{n_\nu})) \right| \leq 3\tau_1 \cdots \tau_\nu \ell^{-\delta}.
\]
holds for almost all prime \( \ell \) and this completes the proof. \( \square \)

We have another consequence of the arguments used to prove Theorem 2, which is the following

**Corollary 10.** Let \( \{s_n\} \) be a sequence in \( \mathbb{Z} \), whose characteristic polynomial \( \omega(x) \in \mathbb{Z}[x] \) is irreducible. Suppose that the Galois group generated by the roots of \( \omega \) is cyclic. Then, for a given \( 0 < \varepsilon < 1/2 \) there exists a \( \delta := \delta(\varepsilon) > 0 \) such that the set of primes \( \ell \) for which the following estimate
\[
\max_{\xi \in F_\ell^*} \left| \sum_{n_1 \leq \tau_1} \cdots \sum_{n_\nu \leq \tau_\nu} \mathbf{e}_\ell(\xi s_n) \right| \leq \tau \ell^{-\delta}
\]
holds, have positive density, where \( \tau \) is given by the order of \( \{s_n\} \) modulo \( \ell \).

**Proof.** First of all, \( \omega \) has distinct roots in \( F_\ell \) for all but finitely many primes \( \ell \). From the given condition, the Galois extension, say \( \mathbb{Q}_f \), generated by the roots of \( \omega \) is a cyclic extension. In particular if a prime \( \ell \) remains inert in \( \mathbb{Q}_\omega \), then \( \omega(x) \pmod{\ell} \) is irreducible. By Chebotarev’s density theorem, the set of such primes have positive density. Now we want to verify the conditions of Theorem 1. First of all, writing
\[
\omega(x) = \prod_{i=0}^{r-1} (x - \alpha^i)
\]
we get \( \omega(0) = (-\alpha)^1 + \ell^2 + \cdots + \ell^{r-1} \), where \( r \) is given by the degree of \( \omega \). We can make 
\((\omega(0), \ell) = 1\), for all but finitely many \( \ell \)'s, and in that case we have
\[
\ell^e < \text{ord}(\alpha^1 + \ell^2 + \cdots + \ell^{r-1}) < \text{ord}(\alpha) = \tau,
\]
for almost all \( \ell \), follows from \([5]\). On the other hand, we need condition \((b)\) of Theorem 1 for \( d = 1 \). We have gcd(ord \( \alpha, \ell - 1 \) = \( \frac{\text{ord} \alpha}{\text{ord} \alpha - 1} \). The proof is now complete if \( \text{ord}(\alpha^{\ell-1}) > \ell^e \) holds for almost all primes \( \ell \). Note that
\[
\alpha^{(\ell-1)t} = 1 \implies \alpha^{rt} = \left( \prod_{i=0}^{r-1} \alpha^i \right)^t \implies \alpha^{2rt} = \omega(0)^{2t}.
\]

Now, we consider \( R(T) = \text{Res} \left( \omega(x), \prod_{\ell \leq T} (x^{2rt} - \omega(0)^{2t}) \right) \), and argue similarly as in the proof of Lemma 7.

\[\square\]

4. Exponential sums for modular forms: beyond eigenforms

We shall now prove Theorem 3. Write
\[
a_f(p^n) = \sum_{i=1}^{r} a_i a_f(p^n),
\]
for some \( a_i \in \mathbb{Q} \), where \( f_i \)'s are newforms and at most one of them is without CM. The characteristic polynomial of \( a_f(p^n) \) is given by product of characteristic polynomial of \( a_f(p^n)'s \). Denote \( D_i(p) \) to be their discriminant respectively. Consider
\[
S_1 = \left\{ \ell \mid \left( \frac{D_i(p)}{\ell} \right) = 1, \forall 1 \leq i \leq r \right\}.
\]
It is clear that \( S_1 \) has positive density. We denote \( \omega^{(i,p)} \) be the characteristic polynomial of \( a_f(p^n) \), and its roots by \( \alpha^{(i,p)}, \beta^{(i,p)} \). So for any \( \ell \in S_1 \), we can write
\[
\omega^{(p)}(x) \pmod{\ell} = \prod_{1 \leq i \leq r} \left( x - \alpha^{(i,p)}_\ell \right) \left( x - \beta^{(i,p)}_\ell \right),
\]
where all of \( \alpha^{(i,p)}_\ell, \beta^{(i,p)}_\ell \)'s are all in \( \mathbb{F}_\ell \). Now, we consider the set
\[
S_2 = \left\{ p \mid \alpha^{(i,p)}(\beta^{(j,p)})^{-1} \text{ are not root of unity, } \forall i, j \right\} \cup \left\{ p \mid \alpha^{(i,p)}(\alpha^{(j,p)})^{-1} \text{ are not root of unity, } \forall i \neq j \right\}.
\]

Lemma 11. For any prime \( p \in S_2 \),
\[
\text{ord}(\alpha^{(i,p)}(\beta^{(j,p)})^{-1}) > \ell^e, \text{ ord}(\alpha^{(i,p)}) > \ell^e \text{ and ord}(\beta^{(j,p)}) > \ell^e,
\]
for all \( 1 \leq i, j \leq r \), and
\[
\text{ord}(\alpha^{(i,p)}(\alpha^{(j,p)})^{-1}) > \ell^e, \text{ for all } 1 \leq i \neq j \leq r,
\]
hold for \( \pi(y)(1 + y^{2e-1} \log y) \) many primes \( \ell \leq y \).
Proof. It is enough to prove the result for \( i, j \in \{1, 2\} \). From the assumption, it is clear that \( \alpha^{(1,p)}, \alpha^{(2,p)}, \beta^{(1,p)}, \beta^{(2,p)} \)'s are pairwise distinct. We can furthermore, choose large enough \( \ell \) such that all of \( \alpha^{(1,p)}_\ell, \alpha^{(2,p)}_\ell, \beta^{(1,p)}_\ell, \beta^{(2,p)}_\ell \)'s are pairwise distinct. Consider the Galois extension \( K = \mathbb{Q}(\alpha^{(1,p)}, \alpha^{(2,p)}) \). Let \( \mathfrak{L} \) be a prime ideal lying over \( \ell \) in \( \mathcal{O}_K \). It is clear that,

\[
\{\alpha^{(1,p)}_\ell, \alpha^{(2,p)}_\ell, \beta^{(1,p)}_\ell, \beta^{(2,p)}_\ell\} = \{\alpha^{(1,p)}, \alpha^{(2,p)}, \beta^{(1,p)}, \beta^{(2,p)}\} \pmod{\mathfrak{L}},
\]

because both of the sets serve as a set of roots of the equation \( \omega(x) \pmod{\mathfrak{L}} \) and \( \omega(x) \pmod{\ell} \), respectively. Note that \( \omega(x) \pmod{\mathfrak{L}} \) coincides with \( \omega(x) \pmod{\ell} \). The right hand side above does not depend on the choice of prime \( \mathfrak{L} \) lying over \( \ell \), so there is no problem in working with a fixed \( \mathfrak{L} \) lying over \( \ell \). It is now clear that,

\[
\{\alpha^{(1,p)}_\ell(\beta^{(j,p)}_\ell)^{-1}\} = \{\alpha^{(1,p)}(\beta^{(j,p)})^{-1}\} \pmod{\mathfrak{L}}.
\]

Consider

\[
R(T) = \text{Res} \left( \omega_1(x), g_T(x) \right),
\]

where \( \omega_1(x) = (x - \alpha^{(1,p)})(x - \beta^{(1,p)}) \) and

\[
g_T(x) = \prod_{t \leq T} \left( x^t - \alpha^{(2,p)}(x^t) \right) \left( x^t - \beta^{(2,p)}(x^t) \right).
\]

It is clear that \( R(T) \neq 0 \) for any \( T \in \mathbb{N} \) as \( p \in S_2 \) by assumption. Now consider the set,

\[
\{ \ell \mid \text{ord} \left( \alpha^{(i,p)}_\ell(\beta^{(j,p)}_\ell)^{-1}\right), \text{ord} \left( \alpha^{(i,p)}_\ell(\alpha^{(j,p)}_\ell)^{-1}\right) \leq T \text{ for some } i \neq j \in \{1, 2\} \}.
\]

For any prime \( \ell \) in the set above, and for any prime \( \mathfrak{L} \) in \( \mathcal{O}_K \) lying over \( \ell \), \( \omega_1(x) \pmod{\mathfrak{L}} \) and \( g_T(x) \pmod{\mathfrak{L}} \) have a common root. Therefore, \( R(T) \pmod{\mathfrak{L}} = 0 \). Since both \( \omega_1 \) and \( g_T(x) \) are in \( \mathbb{Z}[x] \), it is clear that \( R(T) \in \mathbb{Z} \), and so \( R(T) \pmod{\ell} = 0 \) as well. Now one can argue similarly as in Lemma 7. This shows that

\[
\text{ord} \left( \alpha^{(i,p)}_\ell(\beta^{(j,p)}_\ell)^{-1}\right) > \ell^\varepsilon, \quad \text{and } \text{ord} \left( \alpha^{(i,p)}_\ell(\alpha^{(j,p)}_\ell)^{-1}\right) > \ell^\varepsilon
\]

holds for all \( i \neq j \in \{1, 2\} \), and for almost all primes \( \ell \). Rest of the proof follows from Lemma 7 immediately. \( \square \)

We shall now give a short overview of Sato-Tate distribution. When \( f \) is newform without \( CM \), then Sato-Tate conjecture says that \( \frac{a(p)}{2p^{1/2}} \)'s are equidistributed in \([-1, +1]\) with respect to measure

\[
\mu_{\text{non-CM}} = \frac{2}{\pi} \int \sin^2(\theta) \, d\theta.
\]

On the other hand if \( f \) has \( CM \), then the corresponding Sato-Tate distribution is

\[
\mu_{CM} = \frac{1}{2\pi} \int \frac{dx}{\sqrt{1 - x^2}} = \frac{1}{2\pi} \int 1 \, d\theta,
\]

on \([0, \pi] - \{\pi\}\). Moreover at \( \theta_p = \frac{\pi}{2}, a(p) \) becomes zero and it is known that set of such primes \( p \) have density exactly \( \frac{1}{2} \). Now consider the \( L \)-function defined by

\[
L(s, \text{Sym}^m f) = \prod_{p \text{ not dividing } N} \prod_{j=0}^{m} \left( 1 - \alpha^i_p \beta^{m-i} p^{-s} \right)^{-1}.
\]
Serre in [24] showed that if for all integer $m \geq 0, L(s, \text{Sym}^m(f))$ extends analytically to $\text{Re}(s) \geq 1$ and does not vanish there, then the Sato–Tate conjecture holds true for $f$. Note that Barnet-Lamb et al. have proved the conjecture in [1] working with this $L$-function.

However, we will make use of (what is now widely known in the community as) Generalized Sato-Tate conjecture (GST). This is stated as follows: if we have newforms $f_1, f_2, \cdots, f_r$, then their Sato-Tate distributions are independent to each other provided the $L$-function

$$L(s, \text{Sym}^m f_1 \otimes \cdots \otimes \text{Sym}^m f_r)$$

extends to $\text{Re}(s) \geq 1$ and does not vanish, for all integers $m_1, \cdots, m_r$.

Now, assuming the GST conjecture, we have the following result.

**Lemma 12.** Density of $S_2$ is positive if all of $f_i$’s are newforms without CM.

**Proof.** We start by writing

$$\alpha^{(j,p)} = p^{\frac{k-1}{2}} e^{i\theta_{j,p}}, \beta^{(j,p)} = p^{\frac{k-1}{2}} e^{-i\theta_{j,p}}, \forall 1 \leq j \leq r.$$

So, the problem reduced to study the set of primes

$$(28) \quad \{p \mid \theta_{1,p} \pm \theta_{j,p} \in \mathbb{Q} \times \pi, \text{ for some } 1 \leq i, j \leq r\}$$

It follows from the discussion above that the density of this set is given by

$$\left(\frac{2}{\pi}\right)^r \int \cdots \int_{S} \sin^2(\theta_1) \sin^2(\theta_2) \cdots \sin^2(\theta_r) \, d\theta_1 \, d\theta_2 \cdots \, d\theta_r,$$

where $S = \{(\theta_1, \theta_2, \cdots, \theta_r) \in [0, \pi]^r \mid \theta_i \pm \theta_j \in \mathbb{Q} \times \pi \text{ for some } 1 \leq i, j \leq r\}$.

**Case 1, $r = 1$ :** If $\alpha_p^{(1,p)} \beta_p^{-(-1,p)}$ is a root of unity then this implies $\theta_{1,p} \in \pi \times \mathbb{Q}$. By Sato-Tate, density of such primes is bounded by

$$\frac{2}{\pi} \int_{\theta \in \pi \times \mathbb{Q}} \sin^2(\theta) \, d\theta.$$ 

Since the integral above runs over a set of measure zero, the integral is zero, and this proves the case.

**Case 2, $r = 2$ :** In this case, we need to carry out the integral

$$\iint_{S_0} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2,$$

where $S_0 = \{(\theta_1, \theta_2) \in [0, \pi]^2 \mid \theta_1 \pm \theta_2 \in \mathbb{Q} \times \pi\}$. It is evident that

$$\iint_{S_0} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2 = \iint_{\theta_1 + \theta_2 \in \mathbb{Q} \times \pi} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2 + \iint_{\theta_1 - \theta_2 \in \mathbb{Q} \times \pi} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2,$$
as $\mathbb{Q} \times \mathbb{Q}$ has zero measure. Now we can write,

$$
\iint_{\theta_1 - \theta_2 \in \mathbb{Q} \times \pi} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2 = \int_{\theta_1 = \theta_2} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2 + \iint_{\theta_1 \neq \theta_2 \in \mathbb{Q} \times \pi} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2.
$$

Note that,

$$
\iint_{\theta_1 = \theta_2} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2 = \int_0^\pi \sin^4(\theta) \, d\theta = \frac{3\pi}{8}.
$$

On the other hand,

$$
\left| \iint_{\theta_1 - \theta_2 \in (a,b)} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2 \right| \leq \int_0^b \int_a^b \sin^2(\theta) \sin^2(\theta + t) \, d\theta \, dt \ll |b - a|,
$$

for any $b > a$. In particular,

$$
\iint_{\theta_1 \neq \theta_2 \in \mathbb{Q} \times \pi} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2 \ll \sum_{k=1}^{\infty} \frac{\varepsilon}{2^k},
$$

for any $\varepsilon > 0$. The last implication above follows from the standard argument to show a countable set always has zero measure. Hence,

$$
\iint_{\theta_1 - \theta_2 \in \mathbb{Q} \times \pi} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2 = \int_0^\pi \sin^4(\theta) \, d\theta = \frac{3\pi}{8}.
$$

Now,

$$
\iint_{\theta_1 + \theta_2 \in \mathbb{Q} \times \pi} \sin^2(\theta_1) \sin^2(\theta_2) \, d\theta_1 \, d\theta_2 = \int_{\mathbb{Q} \times \pi} \int_0^\pi \sin^2(\theta - t) \sin^2(\theta) \, dt \, d\theta,
$$

and this is zero by the previous argument. In particular this shows density of $S$ is strictly less than 1, and hence density of $S_2$ is positive in this case.

**Case 3, $r > 2$**: Following the pattern of the arguments in the previous paragraph, it is evident that the integral over $S$ contributes only when at least two of $\theta_i$ and $\theta_j$’s are same. From now on, we work with this set $S$. In order to show density of $S_2$ is positive, it is enough to show that

$$
\left( \frac{2}{\pi} \right)^r \int_{S} \sin^2(\theta_1) \sin^2(\theta_2) \cdots \sin^2(\theta_r) \, d\theta_1 \, d\theta_2 \cdots \, d\theta_r < 1.
$$

So for the sake of contradiction, assume that

$$
\left( \frac{2}{\pi} \right)^r \int_{S^c} \sin^2(\theta_1) \sin^2(\theta_2) \cdots \sin^2(\theta_r) \, d\theta_1 \, d\theta_2 \cdots \, d\theta_r = 0,
$$

where $S^c$ is the complement of $S$.
where $S^c$ denotes the complement of $S$. Now, for any small $\varepsilon > 0$, we have
\begin{equation}
(29) \quad \prod_{i=0}^{\nu-1} \left( \frac{\pi}{2} - \varepsilon + \frac{i\varepsilon}{\nu}, \frac{\pi}{2} - \varepsilon + \frac{(i+1)\varepsilon}{\nu} \right),
\end{equation}
and it is clear that
\[
0 < \left( \frac{2}{\pi} \right)^r \int_{S_0} \cdots \int \sin^2(\theta_1) \sin^2(\theta_2) \cdots \sin^2(\theta_r) \, d\theta_1 \, d\theta_2 \cdots d\theta_r,
\]
for any small enough $\varepsilon > 0$. This completes the proof. \(\square\)

Let us again go back to the discussion on $L$-functions that we initiated earlier. If one of the $f_i$ is with CM, then we know due to Ribet ([22]) that $L$-function of $f_i$ comes from $L$-function associated to a Hecke character. Now suppose that at most one of the $f_i$ is without CM. Then without loss of generality we can write
\[
L(s, \text{Sym}^{m_1} f_1 \cdots \text{Sym}^{m_r} f_r) = L(s, \text{Sym}^{m_1} f_1 \otimes \text{Sym}^{m_2} \psi_2 \otimes \cdots \otimes \text{Sym}^{m_r} \psi_r),
\]
where $\psi_i$’s are the corresponding Hecke characters. It follows from the work of Barnet-Lamb et al. (see Theorem B.3 of [1]) that for any odd $m$, there exist a Galois extension $K$ over $\mathbb{Q}$ such that the base change $\text{Sym}^m f|_K$ is automorphic. Following the arguments given in page 643 of [21] one can write
\[
L(s, \text{Sym}^{m_1} f_1 \otimes \text{Sym}^{m_2} \psi_2 \otimes \cdots \otimes \text{Sym}^{m_r} \psi_r) = \prod_{i} (L(s, (\text{Sym}^{m_i} f)|_{K_{H_i}} \otimes \chi_i \otimes \text{Sym}^{m_2} \psi_2 \otimes \cdots \otimes \text{Sym}^{m_r} \psi_r)^{a_i},
\]
where $H_i$’s are nilpotent subgroups of $\text{Gal}(K/\mathbb{Q})$ and $a_i$’s are integers. In particular, we now have a meromorphic continuation to $\text{Re}(s) \geq 1$. It is known that any automorphic $L$-function is non vanishing on $\text{Re}(s) = 1$, in particular we now have the desired analytic continuation to $\text{Re}(s) \geq 1$ for any odd $m_1$. Now if $m_1$ is even, we argue inductively as in [21]. The point is, similarly as in [21] (page 643 – 644), we need to study non vanishing of a Rankin-Selberg $L$-function on $\text{Re}(s) = 1$, which can be done by using Shahidi’s result on Rankin-Selberg $L$-function. See (e) at page 418 of [25].

**Lemma 13.** If at most one of the $f_i$ is without CM and others are with CM then density of $S_2$ is positive, unconditionally.

**Proof.** Following the discussion above, we unconditionally obtain the required measure, given by
\[
\mu_{f_1, f_2, \cdots, f_r} = \frac{2}{\pi} \times \frac{1}{(2\pi)^{r-1}} \int_{\theta_1, \theta_2, \cdots, \theta_r} \sin^2 \theta_1 \, d\theta_1 \, d\theta_2 \cdots d\theta_r.
\]
Following the similar arguments as in the previous lemma, we need to show
\[
\mu_{f_1, f_2, \cdots, f_r}(S_0^c) > 0
\]
where
\[
S_0 = \left\{ (\theta_1, \theta_2, \cdots, \theta_r) \in [0, \pi]^r \mid \theta_i \pm \theta_j \in \mathbb{Q} \times \pi \text{ for some } 1 \leq i, j \leq r, \text{ at least one of } \theta_j \text{ is } \frac{\pi}{2} \right\},
\]
and it follows similarly, that counting measure of $S_0$ is same as counting measure of its subset which consists of points whose at least two coordinates coincides. Hence, the
complement of this set has same measure as $S_0^c$, and we are done by considering the set defined by (29). □

**Proof of Theorem 3.** Let $p \in S_2$ be a fixed prime, then we can write

$$\sum_{i=1}^{r} a_i a_f(p^n) \mod \ell = \sum_{i=1}^{r} a_i^{(\ell)} \left( e^{i,\ell} \alpha^{n(i,\ell)} + d^{i,\ell} \beta^{n(i,\ell)} \right),$$

where $a_i^{(\ell)}, e^{i,\ell}$ and $d^{i,\ell}$ are all in $\mathbb{F}_\ell$. On the other hand all $\alpha^{(i,\ell)}$ and $\beta^{(i,\ell)}$'s are in $\mathbb{F}_\ell$, as $\ell \in S_1$. Part (i) follows by [2, Corollary] joint with Lemma 11 and Lemma 12. Part (ii) follows from Lemma 13 and [2, Corollary]. □

**Remark 2.** In Lemma 12, we believe that it is possible to obtain a concrete description of the density in terms of $c_k$’s, where $c_k = \int_{0}^{\pi} \sin^{2k}(\theta) d\theta$. We have done this for $r = 2$.

**Remark 3.** Case 1 of Lemma 12 shows part (i) of Theorem 2 occurs for almost all prime $p$, when $f$ is a newform without CM.

5. **Exponential sums for modular forms: the inverse case**

One may now ask that for a given prime $\ell$ and small enough $\delta$, how many primes $p$ are there for which an estimate like (7) holds. Our attempt to answer this question is summarized in the form of Theorem 4 and Theorem 5. Let us begin with the proof of Theorem 4.

**Proof of Theorem 4.** For any prime $p$, we first denote roots of $x^2 - a(p)x + p^{k-1}$ (mod $\ell$) by $a_p^{(\ell)}, b_p^{(\ell)}$. Recall that from Deligne-Serre correspondence, we have the associated Galois representation

$$\rho_f: \text{Gal} \left( \overline{\mathbb{Q}}/\mathbb{Q} \right) \longrightarrow \text{GL}_2 \left( \mathbb{Q}_\ell \right),$$

such that $a(p) = \text{tr} \left( \rho_f(Frob_p) \right)$. It is clear that the characteristic polynomial of $\rho_f(Frob_p)$ (mod $\ell$) is same as $x^2 - a(p)x + p^{k-1}$ (mod $\ell$). Following Ribet, see Theorem 3.1 of [23], it is known that the image of this representation is $\left\{ A \in \text{GL}_2 \left( \mathbb{Z}_\ell \right) \mid \det(A) \in (\mathbb{Z}_\ell^*)^{k-1} \right\}$. The condition $(k, \ell - 1) = 1$ implies that the induced Galois representation

$$\rho_{f,\ell}: \text{Gal} \left( \overline{\mathbb{Q}}/\mathbb{Q} \right) \longrightarrow \text{GL}_2 \left( \mathbb{F}_\ell \right),$$

is surjective, and the eigenvalues of the matrix $\rho_{f,\ell}(\text{Frob}_p) \in \text{GL}_2(\mathbb{F}_\ell)$ are $a_p^{(\ell)}$ and $b_p^{(\ell)}$. From the proof of Theorem 2, we know an estimate of type (7) holds provided that,

$$\text{ord} \left( \alpha_p^{(\ell)} \right) > \ell^\varepsilon, \quad \text{ord} \left( \beta_p^{(\ell)} \right) > \ell^\varepsilon, \quad \text{and} \quad \text{ord} \left( \alpha_p^{(\ell)} \beta_p^{(\ell)} \right) > \ell^\varepsilon.$$

Let us define,

$$C = \left\{ A \in \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \mid \text{ord} \left( \lambda_{1,A} \right), \text{ord} \left( \lambda_{2,A} \right), \text{ord} \left( \lambda_{1,A} \lambda_{2,A}^{-1} \right) > \ell^\varepsilon \right\},$$

where $\lambda_{1,A}, \lambda_{2,A}$ are the eigenvalues of $A$ in $\mathbb{F}_\ell$ or $\mathbb{F}_\ell^\varepsilon$. The problem is now about computing the density of primes $p$ for which the corresponding $\rho_{f,\ell}(\text{Frob}_p)$ is in $C$. Note that $C$ is a subset of $\text{GL}_2(\mathbb{F}_\ell)$ stable under conjugation. Hence, by Chebotarev’s density theorem, the required density is $\frac{|C|}{|\text{GL}_2(\mathbb{F}_\ell)|}$. For each $a, b \in \mathbb{F}_\ell$, let $C_{a,b}$ be the conjugacy class of $\left( \begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix} \right)$.
It is known that \(|C_{a,b}| = (\ell + 1)\ell\). Any element \(\lambda \in \mathbb{F}_2 \setminus \mathbb{F}_r\) can be written as \(x + \epsilon y\) where \(x, y \in \mathbb{F}_r\), with \(y \neq 0\) and \(\epsilon\) be a root of \(x^2 - \sigma\), where \(\sigma\) is a generator of \(\mathbb{F}_r\). Then the conjugacy class of matrices in \(\text{GL}_2(\mathbb{F}_r)\) having eigenvalue \(x + \epsilon y\) can be represented by \((\begin{smallmatrix} x & \epsilon y \\ y & x \end{smallmatrix})\) which we denote by \(c_\lambda\). It is known that \(|C_\lambda| = \ell(\ell - 1)\). Now, we consider the following sets:

\[
S_1 = \{a, b \in \mathbb{F}_r \mid \text{ord}(a) > \ell^\epsilon, \text{ord}(b) > \ell^\epsilon, \text{ord}(ab^{-1}) > \ell^\epsilon\},
\]

\[
S_2 = \left\{\lambda \in \mathbb{F}_2 \setminus \mathbb{F}_r \mid \text{ord}(\lambda) > \ell^\epsilon, \text{ord}(\lambda^{\ell-1}) > \ell^\epsilon\right\},
\]

and realize that \(|C| = \frac{1}{2}\left(\ell^2 + \ell(\ell - 1)\right)\). This boils down to the problem of counting \(S_1\) and \(S_2\). First let us compute \(|S_2|\). Take \(\tau\) to be a generator of \(\mathbb{F}_r\), then any \(\lambda \in S_2\) is of the form \(\tau^\ell\), with \((i, d) = 1\). Moreover, we also have a order restriction on \(\lambda^{\ell-1}\), which implies \(\delta(d,\ell) > \ell^\epsilon\). Hence,

\[
|S_2| = \sum_{\frac{d|\ell^2-1}{(d,\ell-1)} > \ell^\epsilon} \phi(d) = \ell^2 + O\left(\sum_{\frac{d|\ell^2-1}{(d,\ell-1)} < \ell^\epsilon} \phi(d)\right).
\]

If \(d\) is odd, dividing \(\ell^2 - 1\) and \(\frac{d}{(d,\ell-1)} < \ell^\epsilon\), then it can be written as \(AB\) such that \(A \mid \ell - 1, B \mid \ell + 1\) and so \(B < \ell^\epsilon\). In particular, any such \(d\) is less than \(\ell^\epsilon + 1\). Therefore,

\[
\sum_{\frac{d|\ell^2-1}{(d,\ell-1)} < \ell^\epsilon} \phi(d) \leq \ell^\epsilon + 1 \ell^2 - 1 = O\left(\ell^{1+\epsilon + \frac{2\epsilon}{\log \log \ell}}\right),
\]

where \(\phi(d)\) is the divisor function, and here we are using the well known upper bound on divisor function (see [20] for instance). On the other hand if we consider even \(d\)’s, arguing same as before, the condition \(\frac{d}{(d,\ell-1)} < \ell^\epsilon\) implies \(d \leq 2^{\nu_2(\ell-1)}\ell^{1+\epsilon}\). Hence,

\[
\sum_{\frac{d|\ell^2-1}{(d,\ell-1)} < \ell^\epsilon} \phi(d) = O\left(\ell^{1+\epsilon + \frac{2\epsilon}{\log \log \ell}} \times 2^{\nu_2(\ell^2-1)}\right) = O\left(\ell^{2-\epsilon}\right),
\]

as \(\ell\) satisfies \(\nu_2(\ell^2-1) < \ell^{1-2\epsilon}\). Therefore, the required density is at least

\[
\frac{1}{2}(\ell + 1)\frac{|S_1|}{|\text{GL}_2(\mathbb{F}_r)|} \geq \frac{\ell^4 + O\left(\ell^{1-\epsilon}\right)}{2\ell^4} \geq \frac{1}{2} + O\left(\ell^{-\epsilon}\right).
\]

**Remark 4.** Recall the set \(\mathfrak{P}\) from Theorem 4. This set has density at least \(\frac{1}{2}\). For instance, all but finitely many primes congruent to \(8i \pm 3\) mod \(8(k-1)\), for all \(0 \leq i \leq k-2\) is there.

**Proof of Theorem 5.** We first start with considering the map

\[
\rho_{f,\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F}_r),
\]
defined by

\[ \sigma \mapsto \begin{pmatrix} \rho_{f_1}(\sigma) & & \\ & \rho_{f_2}(\sigma) & \\ & & \ddots \\ & & & \rho_{f_r}(\sigma) \end{pmatrix}. \]

It is clear that the image of this representation is contained in \( \Delta_r(\ell) \), where

\[ \Delta_r(\ell) = \left \{ \begin{pmatrix} g_1 & & \\ & g_2 & \\ & & \ddots \\ & & & g_r \end{pmatrix} \mid \det(g_1) = \det(g_2) = \cdots = \det(g_r) \right \}. \]

It is in fact the case that the image is contained in \( \Delta_r^{(k-1)}(\ell) \), where \( \Delta_r^{(k-1)}(\ell) \) denotes the set of matrices in \( \Delta_r(\ell) \) in which, determinant of each block is a \( (k-1) \)th power. If this image is not exactly \( \Delta_r^{(k-1)}(\ell) \), then by the argument of Masser-Wüstholz at page 252 of [17] we get quadratic characters \( \chi_{i,j} \) of \( \Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \) such that

\[ \rho_{f_i}(\text{Frob}_p) \text{ is conjugate to } \chi_{i,j}(\text{Frob}_p) \rho_{f_j}(\text{Frob}_p) \text{ in } \GL_2(\mathbb{F}_\ell), \]

for all \( 1 \leq i < j \leq r \).

If \( \chi_{i,j} \) is trivial for some \( i < j \), then we immediately get \( a_{f_i}(p) = a_{f_j}(p) \) for all primes \( p \) not dividing \( N \). However, this implies that \( a_{f_i} = a_{f_j} \) since \( f_i, f_j \) are normalized eigenforms. If \( \chi_{i,j} \) is not trivial, then it definitely becomes trivial over a quadratic extension of \( \mathbb{Q} \). This says that for a set of primes with density \( \frac{1}{2} \), \( a_{f_i}(p) \) and \( a_{f_j}(p) \) coincides, where as for the other set of primes they are of opposite sign. Since, we are excluding this situation from the beginning, therefore we may assume

\[ \text{im}(\rho_{f,\ell}) = \Delta_r^{(k-1)}(\ell). \]

Hence the required density is at least

\[ \frac{|C_r^{k-1}(\ell)|}{|\Delta_r^{(k-1)}(\ell)|}, \]

where \( C_r^{k-1}(\ell) \) is the conjugacy classes of elements in \( \Delta_r^{(k-1)}(\ell) \) whose eigenvalues satisfy the conditions of Theorem 1. To finish the proof, we only need to show that this set is non empty. To show non-emptyness, we can simply use Bourgain [2, Corollary]. For instance we can try to get an element \( (a_1, a_2, \cdots, a_r) \in (\mathbb{F}_\ell^*)^r \) such that

\[ \ord(a_i) > \ell^\varepsilon \text{ and } \max_{i \neq j} \gcd(\ord(a_i), \ord(a_j)) \ll \ell^{\varepsilon'}, \]

and then consider the matrix given by

\[ \begin{pmatrix} A_1 & & \\ & A_2 & \\ & & \ddots \\ & & & A_r \end{pmatrix}, \]

where \( A_i = \begin{pmatrix} a_i & a_{i-1} \end{pmatrix} \). However, our Theorem 1 allows us to take a much larger class of elements, which gives a larger density. For instance, we could consider a tuple \((a_1, a_2, \cdots, a_r)\) satisfying

\[ \ord(a_1) > \ell^\varepsilon, \quad \ord(a_2) > \ell^\varepsilon, \quad \gcd(\ord(a_1), \ord(a_2)) < \ell^{\varepsilon'}, \]

and choose \( a_3, a_4, \cdots, a_r \) freely over \( \mathbb{F}_\ell^* \). We can do this because of the the assumption A.1 on \( \ell \).

In fact, we can do even better. We want to choose \((k-1)\)th power of some elements in \( \mathbb{F}_\ell^* \), which we denote by \( \alpha, \beta \), whose orders divide \( \ell + 1 \) satisfying

\[ \ord(\alpha) > \ell^\varepsilon, \quad \ord(\beta) > \ell^\varepsilon, \quad \gcd(\ord(\alpha), \ord(\beta)) < \ell^{\varepsilon'}. \]
Since $k$ is fixed, this is possible to do large enough $\ell$ satisfying $\ell^k \gg k$, under the assumption A.2. Then one can simply consider an element of the form \[
\left( \begin{array}{ccc}
A'_1 & & \\
& A'_2 & \\
& & \ddots \\
& & & A'_n
\end{array} \right),
\]
where $A'_1$ having eigenvalues $\alpha, \alpha^\ell$, $A'_2$ having eigenvalues $\beta, \beta^\ell$ and $A'_3, \ldots, A'_n$ are any matrices having same determinant as $A'_1, A'_2$. This matrix is indeed in $\Delta^{(k-1)}(\ell)$ because $\alpha^{\ell+1} = \beta^{\ell+1}$ and it is in $C^{(k-1)}(\ell)$ because the eigenvalues of this matrix satisfy the conditions of Theorem 1.

6. Impact on Waring-type problems

Given a sequence of integers $\{x_n\}$ one of the classical questions in additive number theory consists on decide whether $\{x_n\}$ is an additive basis in $\mathbb{Z}$ or residue classes, i.e. is there an absolute integer $k \geq 1$ such that any residue class $\lambda$ modulo $p$ can represented as

$$x_{n_1} + \cdots + x_{n_k} \equiv \lambda \pmod{p},$$

for infinitely many primes $p$? For instance, it is easy to see that the Fibonacci sequence

$$F_{n+2} = F_{n+1} + F_n, \quad \text{with } F_0 = 0, F_1 = 1,$$

is not an additive basis in $\mathbb{Z}$, however the third author proved, [10, Theorem 2.2], that for $\pi(X)/(1 + o(1))$ primes $p \leq X$, every residue class modulo $p$ can be written as

$$F_{n_1} + \cdots + F_{n_{16}} \equiv \lambda \pmod{p},$$

provided with $n_1, \ldots, n_{16} \leq N^{1/2+o(1)}$. The method is based on distribution properties of sparse sequences for almost all primes and particular identities of Lucas sequence. It does not seem easy to extend such ideas for general linear recurrence sequences.

In the present section we combine Theorem 1 with analytic classic tools to prove that $\{s_n\}$ is an additive basis modulo primes under some assumptions. Moreover, we discuss on advantages of getting nontrivial exponential sums to prove it.

6.1. Waring-type problems with recurrence sequences. Let $\{s_n\}$ be a nonzero linear recurrence sequence modulo $p$ as in (2) with order $r$, $(a_0, p) = 1$ and period $\tau$. Given an integer $k \geq 2$, for any $\lambda$ residue class modulo $p$ we denote by $T_k(\lambda)$ the number of solutions of the congruence

$$s_{n_1} + \cdots + s_{n_k} \equiv \lambda \pmod{p},$$

with $1 \leq n_1, \ldots, n_k \leq \tau$. Then writing $T_k(\lambda)$ in terms of exponential sums we get

$$T_k(\lambda) = \frac{1}{p} \sum_{a=0}^{p-1} \sum_{n_1 \leq \tau} \cdots \sum_{n_k \leq \tau} e_p \left( a(s_{n_1} + \cdots + s_{n_k} - \lambda) \right).$$
Taking away the term \( a = 0 \) and using triangle inequality it is clear that

\[
T_k(\lambda) = \frac{\tau^k}{p} + \frac{1}{p} \sum_{a=1}^{p-1} \sum_{n_1 \leq \tau} \cdots \sum_{n_k \leq \tau} e_p(a(s_{n_1} + \cdots + s_{n_k} - \lambda))
\]

\[
= \frac{\tau^k}{p} + \frac{q''}{p} \sum_{a=1}^{p-1} \sum_{n_1 \leq \tau} \cdots \sum_{n_k \leq \tau} e_p(a(s_{n_1} + \cdots + s_{n_k}))
\]

\[
= \frac{\tau^k}{p} + \left( \sum_{n \leq \tau} \left| \sum_{a \in \mathbb{F}_p^*} e_p(a s_n) \right| \right)^k,
\]

(30)

where \( \theta, \theta' \) and \( \theta'' \) are complex numbers with \(|\theta|, |\theta'|, |\theta''| \leq 1\). Assume that we have an exponential sum bound of the type

\[
\max_{a \in \mathbb{F}_p} \left| \sum_{n \leq \tau} e_p(a s_n) \right| \leq R.
\]

Then, combining (30) and (31) we get

\[
T_k(\lambda) = \frac{\tau^k}{p} + \theta R^k = \frac{\tau^k}{p} \left( 1 + \theta (R/\tau)^k p \right).
\]

Now, if \((R/\tau)^k p\) goes to zero as \( p \) does, we obtain an effective asymptotic formula for \( T_k(\lambda) \).

In particular \( T_k > 0 \) for \( p \) large enough. For instance, if \( \tau \geq p^{r/2+\varepsilon} \) we employ Korobov’s bound (3) with \( R = p^{r/2} \) to get

\[
T_k(\lambda) = \frac{\tau^k}{p} \left( 1 + \theta(p^{r/2}/\tau)^k p \right) = \frac{\tau^k}{p} \left( 1 + \theta p^{1-k\varepsilon} \right),
\]

therefore \( T_k(\lambda) = \frac{\tau^k}{p}(1 + o(1)) \) for \( k > 1/\varepsilon \) in the range \( \tau \geq p^{r/2+\varepsilon} \). If the characteristic polynomial \( \omega(x) \) of \( \{s_n\} \) is irreducible with \( \deg(\omega) \geq 2 \) and the least period \( \tau \) satisfies \( \gcd(\tau, p^d - 1) < \tau p^{-\delta} \) for any divisor \( d < r \) of \( r \), then by Theorem 1 we choose \( R = \tau p^{-\delta} \) for some positive \( \delta = \delta(\varepsilon) \), to get

\[
T_k(\lambda) = \frac{\tau^k}{p} \left( 1 + \theta(\tau p^{-\delta}/\tau)^k p \right) = \frac{\tau^k}{p} \left( 1 + \theta (p^{1-k\delta}) \right).
\]

Thus, \( T_k(\lambda) > 0 \) for \( k > 1/\delta \) and \( \max_{d < r \mid r} \gcd(\tau, p^d - 1) < \tau p^{-\varepsilon} \), in particular in the range \( \tau > p^r \). We first summarize the above discussion in the following corollary.

**Corollary 14.** Let \( p \) be a prime number, \( \varepsilon > 0 \) and \( \{s_n\} \) be a linear recurrence sequence of order \( r \geq 2 \). If the characteristic polynomial \( f(x) \) in \( \mathbb{F}_p[x] \) is irreducible with \( (f(0), p) = 1 \), and the least period \( \tau \) satisfies

\[
\max_{d < r \mid r} \gcd(\tau, p^d - 1) < \tau p^{-\varepsilon},
\]
then exists an integer \( k_0 = k_0(\varepsilon) > 0 \) such that for any \( k \geq k_0 \) and every integer \( \lambda \), if \( T_k(\lambda) \) denotes the number of solutions of the congruence
\[
s_{n_1} + \cdots + s_{n_k} \equiv \lambda \pmod{p}, \quad 1 \leq n_1, \ldots, n_k \leq \tau,
\]
then \( T_k(\lambda) = \frac{\tau}{p^k} (1 + o(1)) \).

6.2. Waring-type problems: modular forms. Let us recall our discussion at page 2 on Waring problem for modular forms. Fix any \( 0 < \varepsilon < \frac{1}{2} \), then there exists a \( \delta \) depending only on \( \varepsilon \) such that
\[
\max_{\xi \in F} \left| \sum_{n \leq \tau} e_\ell(\xi a(p^n)) \right| \leq \tau \ell^{-\delta},
\]
holds for almost all primes \( p \) and \( \ell \). We obtain this from Theorem 2, and Remark 3. In particular this shows that \( T_k(\lambda) > 0 \) for any \( \lambda \in F, \) and \( k > 1/\delta \). Moreover, this \( k \) does not depend on choice of the eigenform because, \( \delta \) does not. More precisely, we have the following result.

**Corollary 15.** There exists an absolute constant \( k \) such that, for any integer \( \lambda \) and any newform without CM and with integer Fourier coefficients, the equation
\[
\sum_{i=1}^{k} a(p^n_i) = \lambda
\]
is solvable modulo \( \ell \) for almost all primes \( p \) and \( \ell \).

6.3. Bound of non-linearity of a recurrence sequence. Let \( \{s_n\} \) be a linear recurrence sequence modulo \( p \) as in (2) with order \( r, \) \( (a_0, p) = 1 \) and period \( \tau \). For \( 0 \leq b \leq p^r - 1 \), let us define the sum
\[
W(b) = \sum_{n \leq \tau} e_p(s_n + (b, n)),
\]
where \( (b, n) \) denotes the inner product \( (b, n) = b_0n_0 + \cdots + b_{r-1}n_{r-1} \) assuming that \( 0 \leq b, n \leq p^r - 1 \) are written in its \( p \)-ary expansion
\[
b = b_0 + b_1p + \cdots + b_{r-1}p^{r-1}, \quad n = n_0 + n_1p + \cdots + n_{r-1}p^{r-1}.
\]
Bounds for \( W(b) \) have cryptographic significance, see [28] and references therein. Shparlinski and Winterhof [28, Theorem 1] proved that
\[
\max_{0 \leq b \leq p^r - 1} |W(b)| \ll \tau^{3/4} p^{r^{1/4}} / p^{r/8},
\]
whenever the characteristic polynomial of \( \{s_n\} \) is irreducible. Such bound is asymptotically effective if \( rp^{r/2}/\tau \to 0 \). Combining Corollary 6 and the ideas of Shparlinski–Winterhof we are able to improve such bound for a large class of recurrence sequences in the range \( \tau > p^r \). For example, assuming hypothesis of Corollary 6, if \( r \) is fixed then \( |W(b)| \ll \tau p^{-\delta'} \) as \( p \to \infty \) for some \( \delta' > 0 \). In general we get \( |W(b)| = o(\tau) \) if \( r \log p/p^{\delta'} \to 0 \) as \( p \to \infty \). More precisely
Corollary 16. Let \( p \) be a prime number, \( \varepsilon > 0 \) and \( \{ s_n \} \) be a linear recurrence sequence of order \( r \geq 1 \). If the characteristic polynomial \( f(x) \) in \( \mathbb{F}_p[x] \) is irreducible polynomial with \( (f(0), p) = 1 \), and the least period \( \tau \) satisfies
\[
\tau > p^\varepsilon, \quad \text{and} \quad \max_{d < r} \left( \frac{\tau}{d} p^d - 1 \right) < \tau p^{-\varepsilon},
\]
then there exists a \( \delta = \delta(\varepsilon) > 0 \) such that
\[
\max_{0 \leq b \leq p^{r-1}} \left| \sum_{n \leq \tau} e_p \left( s_n + \langle b, n \rangle \right) \right| \leq \tau p^{-\delta/4} (r \log p)^{1/4} \left( 1 + \tau p^{-\delta/4} (r \log p)^{1/4} \right).
\]

Proof. The proof follows the same steps given by Shparlinski and Winterhof [28, Theorem 1]. We just need to employ the bound given by 6 instead Korobov’s one.

\[\square\]

Note. we have an improvement on the bound of Shparlinski-Winterhof if
\[
\tau \leq \frac{p^{r/2+\delta^*}}{\log p}.
\]

We claim that there are many \( \tau \)'s with such property. For any natural number \( r \) and prime \( p \), get an element \( \alpha \) of order \( n \) (later we shall specify what is \( n \)) in \( \mathbb{F}_p^* \). Note that \( f(x) = \prod_{i=0}^{r-1} (x - \alpha^i) \in \mathbb{F}_p[x] \) of degree \( r \). Note that \( f \) is irreducible if,
\[
n \mid p^r - 1, \text{ and } n \mid p^d - 1, \forall d < r, d \mid r.
\]
In particular, we may force \( n \) to satisfy \( n \mid p^r - 1 \) and \( (n,r/d) = 1 \) for all \( d \mid r \). Among many such examples, we may consider \( n = q \), a prime and \( r = \phi(q) \).

Acknowledgements
Authors would like to thank Igor Shparlinski and Will Sawin for useful suggestions on various occasions during the writing of the article.

In addition, authors would like to thank the Georg-August University Göttingen, Germany, where most of the discussion and work took place, for its hospitality and extend their thanks to Harald Helfgott for the support and encouragement.

The work of the first author is financially supported by the ERC Consolidator grants 648329 and 681207. The work of the second author is financially supported by ERC Consolidator grant 648329.

References
[1] 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(1):29–98, 2011. 13, 21, 23
[2] J. Bourgain. Mordell’s exponential sum estimate revisited. J. Amer. Math. Soc., 18(2):477–499, 2005. 5, 14, 24, 26
[3] J. Bourgain and M.-C. Chang. A Gauss sum estimate in arbitrary finite fields. C. R. Math. Acad. Sci. Paris, 342(9):643–646, 2006. 8, 10
[4] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin. Estimates for the number of sums and products and for exponential sums in fields of prime order. J. London Math. Soc. (2), 73(2):380–398, 2006. 15, 16
[5] P. Erdös and M. R. Murty. On the order of \( a \) (mod \( p \)). In Number theory (Ottawa, ON, 1996), volume 19 of CRM Proc. Lecture Notes, pages 87–97. Amer. Math. Soc., Providence, RI, 1999. 19
[6] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003. 4

[7] A. Ferraguti. Galois representation attached to type $(1, \chi)$ modular forms. 2011. 1

[8] M. Z. Garaev. Sums and products of sets and estimates for rational trigonometric sums in fields of prime order. *Uspekhi Mat. Nauk*, 65(4(394)):5–66, 2010. 10

[9] M. Z. Garaev, V. K. Garsiya, and S. V. Konyagin. The Waring problem with Ramanujan’s $r$-function. *Izv. Ross. Akad. Nauk Ser. Mat.*, 72(1):39–50, 2008. 2

[10] V. C. García. On the distribution of sparse sequences in prime fields and applications. *J. Théor. Nombres Bordeaux*, 25(2):317–329, 2013. 27

[11] V. C. García and F. Nicolae. Additive bases with coefficients of newforms. *Forum Math.*, 30(5):1079–1087, 2018. 2

[12] N. M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988. 4

[13] N. M. Korobov. The distribution of non-residues and of primitive roots in recurrence series. *Doklady Akad. Nauk SSSR (N.S.)*, 88:603–606, 1953. 3

[14] N. M. Korobov. *Exponential sums and their applications*, volume 80 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1992. Translated from the 1989 Russian original by Yu. N. Shakhov. 3

[15] H. W. Lenstra, Jr. On Artin’s conjecture and Euclid’s algorithm in global fields. *Invent. Math.*, 42:201–224, 1977. 16

[16] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, 1986. 3, 7

[17] J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original. 21

[18] I. E. Shparlinski. On the nonlinearity of linear recurrence sequences. *Appl. Math. Lett.*, 19(4):340–344, 2006. 29, 30

J. Bajpai: Mathematisches Institut, Georg-August-Universität Göttingen, Germany.
E-mail address: jitendra@math.uni-goettingen.de
S. Bhakta: Mathematisches Institut, Georg-August-Universität Göttingen, Germany. E-mail address: subham.bhakta@mathematik.uni-goettingen.de

V. C. García: Universidad Autónoma Metropolitana, México. E-mail address: vceh@azc.uam.mx