J. Bajpai et al. *Res. Number Theory* (2022) 8:18
https://doi.org/10.1007/s40993-022-00310-3

Research in Number Theory

RESEARCH

Exponential sums in prime fields for modular forms

Jitendra Bajpai[1], Subham Bhakta[2*] and Victor C. García[3]

*Correspondence:
subham.bhakta@mathematik.uni-goettingen.de
[12]Mathematisches Institut, Georg-August-Universität Göttingen, Göttingen, Germany
Full list of author information is available at the end of the article

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 linear recurrence sequences over finite fields.

Keywords: Linear recurrence sequence, Exponential sums, Modular forms

Mathematics Subject Classification: Primary 11F30, 11L07; Secondary 11P05, 11B37, 11F80

Contents

Springer

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 nth Fourier coefficient. In this article, we shall restrict to the family of modular forms with rational coefficients, that is, $f(z)$ with $a(n) \in \mathbb{Q}$ for every n. We first consider Hecke eigenforms or simply 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 with integer Fourier coefficients, it follows from Deligne-Serre that for any prime ℓ, there exists a corresponding Galois representation

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

such that $\mathrm{tr}(\rho_f^{(\ell)}(\mathrm{Frob}_p)) = a(p)$, for any prime $p \nmid N\ell$. For a quick reference about this correspondence, we refer the interested reader to [8, Chapter 3].

In particular, $a(p) \pmod{\ell}$ is determined by the trace of the corresponding Frobenius element in $\mathrm{GL}_2(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$. In certain cases, Chebotarev's density theorem implies that given any $\lambda \in \mathbb{F}_\ell$, there exists a prime p such that $a(p) \equiv \lambda \pmod{\ell}$. However, the set of such primes p come with density strictly less than 1. So what about the other primes p? In this context, we address the following Waring-type question.

Question *Does there exist an absolute constant s such that for any given primes p and* ℓ*, any element of* $\mathbb{F}_\ell$ *can be written as a sum of at most s elements of the set* $\{a(p^n)\}_{n\geq 1}$?

A related question was studied by Shparlinski in [24] for the Ramanujan's τ function, where $\tau(n)$ is defined by the identity

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

In [24], it is proved that the set $\{\tau(n)\}_{n\geq 1}$ is an additive basis modulo any prime ℓ, that is, there exists an absolute constant s such that the Waring-type congruence

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

is solvable for any residue class $\lambda \pmod{\ell}$.

Shparlinski's work was later generalized by Garaev, García and Konyagin over the global field $\mathbb{Q}$. More precisely, in [10], the authors proved that for any $\lambda \in \mathbb{Z}$, the equation

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

always has a solution for s =74,000.

Later García and Nicolae [12] extended this result for coefficients $a(n)$ of normalized Hecke eigenforms of weight k in $S_k^{\mathrm{new}}(\Gamma_0(N))$. More precisely, they proved that for any $\lambda \in \mathbb{Z}$, the equation

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

always has a solution for some $s \leq c(f)$ with $c(f)$ satisfying

$$c(f) \ll (2N^{3/8})^{\frac{k-1}{2}+\varepsilon} k^{\frac{3}{16}k+O(1)+\varepsilon} \log(k+1).$$

The proof of the above two results are connected to the identity $a(p^2) = a^2(p) - p^{k-1}$ and the solubility of the equation

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

We are studying the finite field version of this additivity problem by obtaining nontrivial exponential sums associated with coefficients of modular forms, in the sense of [24]. We are working with the class of forms that García and Nicolae [12] considered, but with Fourier coefficients evaluated only at prime powers. Our results are recorded in Corollaries 15 and 16. Our main tool is Theorem 1 which provides a nontrivial bound for exponential sums with coefficients of modular forms. To study this problem, we shall primarily focus on the exponential sums of type

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell \left(\xi a(p^n) \right) \right|$$

where p, ℓ are primes, and τ is a suitable parameter which we shall specify later. This is done in Theorems 2 and 3.

When f is a normalized eigenform, it is well known that $a(n)$ is a multiplicative function and for any prime $p \nmid N$ satisfies the relation

$$a(p^{n+2}) = a(p)a(p^{n+1}) - p^{k-1}a(p^n), \quad n \ge 0. \tag{1}$$

Moreover, we have $a(p^n) = a(p)^n$ for any prime $p \mid N$. These facts come from the properties of Hecke operators, see [5, Proposition 5.8.5]. If $a(p) \in \mathbb{Q}$, then one can consider $a(p) \pmod{\ell} \in \mathbb{F}_\ell$ naturally for any large enough prime ℓ. For instance, ℓ can be taken to be any prime not dividing the denominators of the Fourier coefficients. On the other hand, any cuspform can be uniquely written as a $\mathbb{C}$-linear combination of pairwise orthogonal eigenforms with Fourier coefficients coming from $\mathbb{C}$. See [5, Chapter 5] for a brief review of the Hecke theory of modular forms. However, here we are concerned with all such cuspforms which can be uniquely written as a $\mathbb{Q}$-linear combination of pairwise orthogonal eigenforms with Fourier coefficients coming from $\mathbb{Q}$. Note that, in this case, the sequence $\{a(p^n)\}$ is a linear recurrence sequence of possibly higher degree. We now turn to discuss the basic theory of linear recurrence sequences. We will also discuss the bounds of their associated exponential sums.

1.1 Linear recurrence sequences and exponential sums

Let $r \ge 1$ 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

$$s_{n+r} \equiv a_{r-1}s_{n+r-1} + \cdots + a_0 s_n \pmod{p}, \quad \text{with } n = 0, 1, 2, \ldots, \tag{2}$$

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

$$\omega(x) = x^r - a_{r-1}x^{r-1} - \cdots - a_1 x - a_0.$$

We see from Eq. (1) that $\{a(p^n)\}$ is a linear recurrence sequence of order 2 when f is an eigenform. We shall prove the results in Sect. 2, by studying exponential sums associated to a much more general class of linear recurrence sequences.

Under certain assumptions, linear recurrence sequences become periodic modulo p, see [15, Lemma 6.4] and [18, Theorem 6.11].

Let p be a prime number and $\omega(x)$ be the characteristic polynomial of a linear recurrence sequence $\{s_n\}$ defined by Eq. (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 $T \geq 1$,

$$s_{n+T} \equiv s_n \pmod{p}, \qquad n = 0, 1, 2, \ldots .$$

The least positive period is denoted by τ. Moreover, $\tau \leq p^r - 1$ and τ divides T for any period $T \geq 1$ of the sequence $\{s_n\}$.

In 1953, Korobov [16] 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 τ, it follows that

$$\left| \sum_{n \leq \tau} \mathbf{e}_p(s_n) \right| \leq p^{r/2}. \tag{3}$$

Note that such a 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 [15] showed that there is a linear recurrence sequence $\{s_n\}$ with length r satisfying

$$\frac{1}{2} p^{r/2} < \left| \sum_{n \leq \tau} \mathbf{e}_p(s_n) \right| \leq p^{r/2}.$$

In turn, for any given $\varepsilon > 0$, it has been proved that there exists a class of linear recurrence sequences with a better upper bound

$$\left| \sum_{n \leq \tau} \mathbf{e}_p(s_n) \right| \leq \tau^{1/2+\varepsilon}.$$

However, the proof of the existence is ineffective in the sense that we do not know any explicit characteristics of such family, see [7, Section 5.1].

The case when the associated polynomial $\omega(x)$ is irreducible in $\mathbb{F}_p[x]$, was widely studied. In particular, from a more general result due to Katz [14, Theorem 4.1.1] it follows that if $\omega(0) = 1$ then

$$\left| \sum_{n \leq \tau} \mathbf{e}_p(s_n) \right| \leq p^{(r-1)/2}.$$

Shparlinski [23] improved Korobov's bound for all nonzero linear recurrence sequences with irreducible characteristic polynomial $\omega(x)$ in $\mathbb{F}_p[x]$. From [23, Theorem 3.1] we get

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

for any given $\varepsilon > 0$ and with period τ satisfying that

$$\max_{\substack{d < r \\ d \mid r}} \gcd(\tau, p^d - 1) < \tau p^{-\varepsilon}. \tag{4}$$

In particular, if r is fixed then the upper bound is non trivial for $\tau \geq p^{r/2-1/6+\varepsilon}$.

We already pointed out that the inequality (3) is nontrivial for $\tau > p^{r/2+\varepsilon}$, so the most important case occurs when $\tau \leq p^{r/2+\varepsilon}$. If $\tau \leq p^{r/2+\varepsilon}$, then condition (4) is needed to obtain a non trivial bound suggested by an example given in [23, Section 1]. In this particular example, the exponential sums of type

$$\left|\sum_{n=1}^{(p^m-1)/2} \mathbf{e}_p\left(\mathrm{Tr}(ag^{2n})\right)\right| = \frac{(p^m-1)}{2},$$

are considered for certain a in $\mathbb{F}_{p^m}^*$ with g a generator of $\mathbb{F}_{p^m}^*$ and m be any even integer. It is worth noting that $\{\mathrm{Tr}(ag^{2n})\}$ is indeed a linear recurrence sequence of order m in $\mathbb{F}_p$.

Moreover, we consider the general case when the associated polynomial $\omega(x)$ is not necessarily irreducible, and 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 τ in $\mathbb{F}_p$ such that its characteristic polynomial $\omega(x)$ has distinct roots in its splitting field, and $(\omega(0), p) = 1$. Set $\omega(x) = \prod_i^{\nu} \omega_i(x)$ as a product of distinct irreducible polynomials in $\mathbb{F}_p[x]$, and for each i, α_i denotes a root of $\omega_i(x)$. If all polynomials $\omega_i(x)$ have the same degree, i.e.* $\deg \omega_i(x) = r > 1$, *and the system $\tau_i = \operatorname{ord} \alpha_i$, satisfies*

$$(a)\ \max_{\substack{d<r\\ d|r}} \gcd(\tau_i, p^d - 1) < \tau_i p^{-\varepsilon}, \quad \text{for any } 1 \le i \le \nu,$$

$$(b)\ \gcd(\tau_i, \tau_j) < p^{\varepsilon'}, \text{ for some pair } i \neq j \textit{ along with } \mathbb{F}_p(\alpha_i) \cong \mathbb{F}_p(\alpha_j), \tag{5}$$

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

$$\max_{\xi \in \mathbb{F}_p^*} \left|\sum_{n \le \tau} \mathbf{e}_p(\xi s_n)\right| \le \tau p^{-\delta}. \tag{6}$$

It turns out that, this extends [2, Corollary] due to Bourgain, where all of the irreducible factors have degree $r = 1$, while Theorem 1 deals with the case $r \ge 2$.

This will be of immense use in what follows, roughly because the characteristic polynomial associated to $\{a(p^n)\}$ have degree two.

Theorem 1 will be essential to establish Theorem 2 and Corollaries 12 and 17. Our approach, which relies on the sum-product phenomenon, provides an improvement over Theorem 3.1 of [23] for the same class of linear recurrence sequences, obtaining non trivial exponential sums in a larger range. To be more precise, if $p(r)$ denotes the least prime divisor of r then any $\tau > p^{r/p(r)+\varepsilon}$ satisfies

$$\tau p^{-\varepsilon} > p^{r/p(r)} \ge \max_{\substack{d<r\\ d|r}} \gcd(\tau, p^d - 1).$$

In particular, our result works for any $\tau > p^{r/p(r)+\varepsilon}$, while bound in [23] is nontrivial if $\tau > p^{r/2-1/6+\varepsilon}$. This is an improvement if $p(r) > 2$, more precisely when r is odd.

1.2 Main results for exponential sum with modular forms

We now quickly discuss the main results obtained in this article. In the list, our first result is the following:

Theorem 2 *Let $f(z)$ be an eigenform with rational coefficients $a(n)$. Let $\mathcal{P}$ be the set of primes p such that $a(p^u) \neq 0$ for any $u \in \mathbb{N}$. Then the following is true.*

(i) *The set of primes $\mathcal{P}$ satisfies that given $p \in \mathcal{P}$, for any $0 < \varepsilon < 1/2$ there exists a $\delta = \delta(\varepsilon) > 0$ such that the following estimate*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) \right| \le \tau \ell^{-\delta}, \tag{7}$$

holds for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \le y$, where the least period τ of the linear recurrence sequence $\{a(p^n)\} \pmod{\ell}$ depends on both p and ℓ, and $\pi(y)$ denotes the number of primes up to y which is asymptotically equivalent to $\frac{y}{\log y}$.

(ii) *For the exceptional set of primes $p \notin \mathcal{P}$, let u be the least natural number such that $a(p^u) = 0$. Then for any $0 < \varepsilon < 1/2$, there exists a $\delta = \delta(\varepsilon) > 0$ such that the following estimate*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) \right| = \frac{\tau}{u+1} + O(\tau \ell^{-\delta} + u). \tag{8}$$

holds for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \le y$.

Roughly speaking, a newform of level N is a normalized eigenform which is not a cuspform of level N' for any proper divisor N' of N. For details and basics on modular forms, we refer the reader to [5]. A newform is said to have complex multiplication (CM) by a quadratic Dirichlet character ϕ if $f = f \otimes \phi$, where we define the twist as

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

In part (i) of Theorem 2, the condition $a(p^u) \neq 0$ holds for almost all prime p provided that f is a newform without CM. This is a consequence of Sato-Tate conjecture and we shall discuss this again in the proof of Lemma 11. In particular, we have a non trivial estimate for the following exponential sum

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) \right| . \tag{9}$$

Let us recall that any general cusp form f can be uniquely written as $\mathbb{C}$-linear combination of eigenforms. These eigenforms will be called as components of f. We then 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. Suppose that there are r_2 many components with CM, then under the assumption of GST hypothesis*[1] *there exists a set of primes p with density at least 2^{-r_2} such that for any $0 < \varepsilon < 1/2$ there exists a $\delta = \delta(\varepsilon) > 0$ for which the following estimate*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) \right| \le \tau \ell^{-\delta}, \tag{10}$$

holds for $c_f \pi(y) + O(y^{2\varepsilon})$ many primes $\ell \le y$, where $c_f > 0$ is a constant.

[1] See Sect. 4.1 for the discussion about GST hypothesis.

In both of the above theorems, we took a fixed prime p and looked for primes ℓ for which a non trivial estimate to (9) holds. However, these results are valid for almost all primes ℓ, and we do not know explicitly which of the primes are being excluded in this process. Thus, one may naturally ask, what if we now fix a prime ℓ and find out for how many primes p the sum at (9) is non trivial. In this regard, we have the following results.

Theorem 4 *Let $f(z)$ be a newform of weight k, without CM, and with integer Fourier coefficients. Consider the set $\mathfrak{P} = \left\{\ell \text{ prime} \mid (k-1, \ell-1) = 1\right\}$. Then, for any fixed $\varepsilon > 0$ and any large enough $\ell \in \mathfrak{P}$, the set of primes p satisfying*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) \right| \le \tau \ell^{-\delta} \tag{11}$$

have density at least $1 + O_\varepsilon\left(\frac{1}{\ell^{1-3\varepsilon}}\right)$, where $\delta = \delta(\varepsilon)$ is same as in Theorem 1.

Intuitively, this theorem can be regarded as the inverse of Theorem 2, and in this analogy, the following result as the inverse of Theorem 3. Just for the sake of simplicity we are assuming $(k-1, \ell-1) = 1$, which can be easily avoided and will be evident from the proof of the following theorem.

Theorem 5 *If $f(z)$ is a cuspform, and can be written as $\mathbb{Q}$ linear combination of r many newforms without CM and with integer coefficients, such that all of these components satisfies GST hypothesis. Then, for any fixed $\varepsilon > 0$ and large enough ℓ, the set of primes p satisfying*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) \right| \le \tau \ell^{-\delta} \tag{12}$$

have density at least $2^{-r} + O_\varepsilon\left(\frac{1}{\ell^{1-2\varepsilon}}\right)$, where $\delta = \delta(\varepsilon)$ is same as in Theorem 1.

1.3 Waring type problems over finite fields

Given a sequence $\{x_n\}$, one of the classical questions are to decide whether $\{x_n\}$ is an additive basis. More precisely, is there an absolute constant $k \ge 1$ such that any residue class λ modulo p can be represented as

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

for infinitely many primes p?

In this article, we are concerned about the case when $\{x_n\}$ is a linear recurrence sequence in $\mathbb{F}_p$. For a simple sequence $2^n \pmod{p}$, it follows combining a result of Erdős and Murty [6] and a result of Glibichuk [13] that for almost all primes p, every residue class modulo p can be represented in the following form

$$2^{n_1} + \cdots + 2^{n_8} \pmod{p},$$

for certain positive integers $n_1, \cdots, n_8$.

Note that $2^n \pmod{p}$ is a linear recurrence sequence of order 1. For higher order cases, one can ask about the classical case of Fibonacci sequences. The third author proved in [11, Theorem 2.2], that given a parameter $N \to \infty$, for $\pi(N)(1 + o(1))$ primes $p \le N$, every residue class modulo p can be written as

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

provided that $n_1, \ldots, n_{16} \leq N^{1/2+o(1)}$. The method is based on the 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 this article, we prove that if $\{s_n\}$ is a linear recurrence sequence in $\mathbb{Z}$, whose characteristic polynomial $\omega(x) \in \mathbb{Z}[x]$ is monic, irreducible, and having prime degree, then there exists an absolute constant k such that every residue class $\lambda (\operatorname{mod} p)$ can be represented as

$$s_{n_1} + \cdots + s_{n_k} \equiv \lambda \,(\operatorname{mod} p),$$

for a set of primes p with positive density. We record this in Theorem 13 in Sect. 6.

2 Exponential sums with linear recurrence sequences

In this section, our main goal is to prove Theorem 1, which is one of our key tool in establishing several important results of this article. Recalling the example of Shparlinski in [23, Section 1], we already noticed in Sect. 1.1 that, condition (a) of Theorem 1 is needed if $\omega(x)$ is irreducible in $\mathbb{F}_p[x]$. We shall discuss more about this condition later in Remark 1.

Now, we illustrate with an example that all of the $\gcd(\tau_i, \tau_j)'s$ cannot be too large. In other words, we need condition (b) (or some other condition) to obtain a non trivial bound in Theorem 1. For example, let $r = 2$ and g be a generator of $\mathbb{F}_{\ell^2}^*$. Then, consider the sequence

$$s_n = \operatorname{Tr}\left(g^{n(\ell^2+1)/2} - g^n\right),$$

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

$$\tau_2 = \operatorname{ord} g = \ell^2 - 1 \text{ and } \tau_1 = \operatorname{ord} g^{(\ell^2+1)/2} = \tfrac{\ell^2-1}{\gcd(\ell^2-1,(\ell^2+1)/2)}.$$

It is easy to see that $\gcd(\ell^2-1, (\ell^2+1)/2) = 1$, so $\gcd(\tau_1, \tau_2) = \ell^2 - 1$. On another hand we note that $\gcd(\tau_1, \ell-1) = \ell - 1$. Then, one can show that

$$\begin{aligned}
\sum_{n=1}^{\ell^2-1} \mathbf{e}_{\ell}\left(s_n\right) &= \sum_{n=1}^{\ell^2-1} \mathbf{e}_{\ell}\left(\operatorname{Tr}\left(g^{n(\ell^2+1)/2} - g^n\right)\right) \\
&= \sum_{n=1}^{(\ell^2-1)/2} \mathbf{e}_{\ell}\left(\operatorname{Tr}\left(g^{2n(\ell^2+1)/2} - g^{2n}\right)\right) \\
&\quad + \sum_{n=1}^{(\ell^2-1)/2} \mathbf{e}_{\ell}\left(\operatorname{Tr}\left(g^{(2n-1)(\ell^2+1)/2} - g^{2n-1}\right)\right) \\
&= \frac{\ell^2-1}{2} + \sum_{n=1}^{(\ell^2-1)/2} \mathbf{e}_{\ell}\left(\operatorname{Tr}\left(-2g^{2n-1}\right)\right) = \frac{\ell^2-1}{2} + \sum_{h \in H} \mathbf{e}_{\ell}\left(\operatorname{Tr}\left(-2gh\right)\right),
\end{aligned}$$

where $H = \langle g^2 \rangle$.

Let p be any prime and q be any power of p. Then, the classical theorem about additive sums for one-variable polynomial, due to A. Weil (see [17, Theorem 3.2]), states that, for a given polynomial $f(x) \in \mathbb{F}_q[x]$ with degree d, $d < q$, $\gcd(d, q) = 1$ and a nontrivial additive character ψ in $\mathbb{F}_q$, we have

$$\left|\sum_{x \in \mathbb{F}_q} \psi(f(x))\right| \leq (d-1)\sqrt{q}. \tag{13}$$

Consider

$$1+2\sum_{h\in H}\mathbf{e}_\ell\left(\operatorname{Tr}(-2gh)\right)=\sum_{x\in\mathbb{F}_{\ell^2}}\psi(x^2),$$

where $\psi(\omega)=\mathbf{e}_\ell\left(\operatorname{Tr}(-2g\omega)\right)$ is a nonzero additive character of $\mathbb{F}_{\ell^2}$. Applying (13) with $f(x)=x^2$, it follows that

$$\left|\sum_{h\in H}\mathbf{e}_\ell\left(\operatorname{Tr}(-2gh)\right)\right|\le\left|\sum_{x\in\mathbb{F}_{\ell^2}}\psi(x^2)\right|\le\ell.$$

Therefore, the linear recurrence sequence $\{s_n\}$ satisfies

$$\sum_{n=1}^{\ell^2-1}\mathbf{e}_\ell\left(s_n\right)=\frac{\ell^2-1}{2}+O(\ell).$$

We now need to discuss 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 $\operatorname{Tr}_{F/K}:F\to K$ is defined by

$$\operatorname{Tr}_{F/K}(z)=z+z^p+\cdots+z^{p^{r-1}},\qquad z\in F.$$

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

$$\operatorname{Tr}_{F/K}(az+w)=a\operatorname{Tr}_{F/K}(z)+\operatorname{Tr}_{F/K}(w),\quad\text{for all } a\in K,\ z,w\in F. \tag{14}$$

$$\operatorname{Tr}_{F/K}(a)=ra,\quad\text{for any}\quad a\in K. \tag{15}$$

$$\operatorname{Tr}_{F/K}(z^p)=\operatorname{Tr}_{F/K}(z),\quad\text{for any}\quad z\in F. \tag{16}$$

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

Let $\{s_n\}$ be a linear recurrence sequence of order $r\ge 1$ in $\mathbb{F}_p$ with characteristic polynomial $\omega(x)$ in $\mathbb{F}_p[x]$. It is well known that nth-term can be written in terms of the roots of the characteristic polynomial, see Theorem 6.21 in [18]. Therefore, if the roots $\alpha_0,\ldots,\alpha_{r-1}$ of $\omega(x)$ are all distinct in its splitting field, then

$$s_n=\sum_{i=0}^{r-1}\beta_i\alpha_i^n,\quad\text{for } n=0,1,2,\ldots, \tag{17}$$

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 $\omega(x)$ is irreducible and α 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

$$s_n=\sum_{i=0}^{r-1}\beta_i\alpha^{p^in},\qquad n=0,1,2,3,\ldots.$$

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 $\alpha\in\mathbb{F}_q$ and $\varepsilon>0$, such that $\operatorname{ord} \alpha = t$ satisfies

$$t > p^{\varepsilon} \quad \text{and} \quad \max_{\substack{1 \le d < r \\ d \mid r}} \gcd(t, p^d - 1) < tp^{-\varepsilon}. \tag{18}$$

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

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

Note that the second assumption in (18) implies the first one whenever $r \ge 2$.

2.1 Proof of Theorem 1

We proceed by induction over ν. Before that, following properties (14) and (15) of trace function we write

$$\begin{aligned} s_n &= \operatorname{Tr}\left(r^{-1} s_n\right) = r^{-1} \operatorname{Tr}\left(\sum_{i=1}^{\nu} (\beta_{i,0}\alpha_i^n + \cdots + \beta_{i,r-1}\alpha_i^{p^{r-1}n}) \right) \\ &= r^{-1} \sum_{i=1}^{\nu} \sum_{j=0}^{r-1} \operatorname{Tr}\left(\beta_{i,j}\alpha_i^{p^j n}\right). \end{aligned}$$

By the assumption, $[\mathbb{F}_p(\alpha_i) : \mathbb{F}_p] = r$ for any $1 \le i \le \nu$. In other words, any such α_i is in $\mathbb{F}_{p^r}$. We then have, $r = [\mathbb{F}_p(\alpha_1, \ldots, \alpha_\nu) : \mathbb{F}_p]$ and $z^{p^r} = z$ for any $z \in \mathbb{F}_p(\alpha_1, \ldots, \alpha_\nu)$. In addition, from (16) it follows that, $\operatorname{Tr}(z^p) = \operatorname{Tr}(z)$ for any $z \in \mathbb{F}_p(\alpha_1, \ldots, \alpha_\nu)$. Then, for each pair (i, j), raising each argument $\beta_{i,j}\alpha_i^{p^j n}$ to the power p^{r-j}

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

This implies that

$$\begin{aligned} s_n &= r^{-1} \sum_{i=1}^{\nu} \sum_{j=0}^{r-1} \operatorname{Tr}\left(\beta_{i,j}^{p^{r-j}} \alpha_i^n\right) = r^{-1} \sum_{i=1}^{\nu} \operatorname{Tr}\left(\left(\sum_{j=0}^{r-1} \beta_{i,j}^{p^{r-i}} \right) \alpha_i^n \right) \\ &= \operatorname{Tr}\left(\gamma_1 \alpha_1^n\right) + \cdots + \operatorname{Tr}\left(\gamma_\nu \alpha_\nu^n\right), \end{aligned} \tag{19}$$

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

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

$$\left| \sum_{n \le \tau} \mathbf{e}_p\left(\xi s_n\right) \right| = \frac{\tau}{\tau_1 \tau_2 / h} \left| \sum_{n \le \frac{\tau_1\tau_2}{h}} \mathbf{e}_p\left(\xi s_n\right) \right|.$$

Hence, it is enough to prove that

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

for some $\delta = \delta(\varepsilon) > 0$. Dividing the range of the sum $n \le \tau_1\tau_2/h$ into the form $n = mh+u_0$ with $m \le \tau_1\tau_2/h^2$ and $0 \le u_0 \le h-1$, we have

$$\begin{aligned}\left|\sum_{n\le\frac{\tau_1\tau_2}{h}} \mathbf{e}_p\left(\xi s_n\right)\right| &= \left|\sum_{u_0=0}^{h-1}\sum_{n\le\frac{\tau_1\tau_2}{h^2}} \mathbf{e}_p\left(\xi s_{nh+u_0}\right)\right| \le \sum_{u_0=0}^{h-1}\left|\sum_{n\le\frac{\tau_1\tau_2}{h^2}} \mathbf{e}_p\left(\xi s_{nh+u_0}\right)\right| \\ &\le h \times \max_{0\le u_0\le h-1}\left|\sum_{n\le\tau_1\tau_2/h^2} \mathbf{e}_p\left(\xi s_{nh+u_0}\right)\right|. \qquad (20)\end{aligned}$$

Let (n_1, n_2) be a tuple with $n_i \le \frac{\tau_i}{h}$. Since $\gcd(\frac{\tau_1}{h}, \frac{\tau_2}{h}) = 1$, by Chinese remainder 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

$$\left|\left\{n \left(\bmod \tfrac{\tau_1\tau_2}{h^2}\right) : 1 \le n \le \frac{\tau_1\tau_2}{h^2}\right\}\right| = \left|\left\{n_1m_1\tfrac{\tau_2}{h} + n_2m_2\tfrac{\tau_1}{h} \left(\bmod \tfrac{\tau_1\tau_2}{h^2}\right) : 1 \le n_i \le \frac{\tau_i}{h}\right\}\right|. \qquad (21)$$

Moreover, the pair (m_1, m_2) has the following property: given (n_1, n_2), with $1 \le n_i \le \tau_i/h$, then $n = n_1m_1\frac{\tau_2}{h} + n_2m_2\frac{\tau_1}{h}$ satisfies

$$n \equiv n_1 \left(\bmod \tfrac{\tau_1}{h}\right) \text{ and } n \equiv n_2 \left(\bmod \tfrac{\tau_2}{h}\right),$$

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

$$\alpha_i^{hn} = \alpha_i^{h\left(n_1m_1\frac{\tau_2}{h}+n_2m_2\frac{\tau_1}{h}\right)} = \alpha_i^{hn_i}, \quad 1 \le i \le 2. \qquad (22)$$

Combining (21) and (22), we have

$$\begin{aligned}\left|\sum_{n\le\frac{\tau_1\tau_2}{h^2}} \mathbf{e}_p\left(\xi s_{nh+u_0}\right)\right| &= \left|\sum_{n_1\le\frac{\tau_1}{h}} \mathbf{e}_p\left(\operatorname{Tr}\left(\xi\gamma_1\alpha_1^{n_1h+u_0}\right)\right)\right| \\ &\quad\times \left|\sum_{n_2\le\frac{\tau_2}{h}} \mathbf{e}_p\left(\operatorname{Tr}\left(\xi\gamma_2\alpha_2^{n_2h+u_0}\right)\right)\right| \\ &= \left|\sum_{n_1\le\frac{\tau_1}{h}} \mathbf{e}_p\left(\operatorname{Tr}\left(\gamma_1'\alpha_1^{n_1h}\right)\right)\right| \times \left|\sum_{n_2\le\frac{\tau_2}{h}} \mathbf{e}_p\left(\operatorname{Tr}\left(\gamma_2'\alpha_2^{n_2h}\right)\right)\right|, \qquad (23)\end{aligned}$$

with $\gamma_1' = \xi\gamma_1\alpha_1^{u_0}, \gamma_2' = \xi\gamma_2\alpha_2^{u_0}$ in $\mathbb{F}_p(\alpha_1, \alpha_2)$. Since $\{s_n\}$ is a nonzero sequence, therefore $\gamma_i' \ne 0$, at least for some $1 \le i \le 2$. First, let us assume that $\gamma_1', \gamma_2' \ne 0$.

Each $\mathbf{e}_p\left(\operatorname{Tr}\left(\xi\gamma_i'z\right)\right)$ corresponds to a nontrivial additive character, say $\psi_i(z)$, in $\mathbb{F}_p(\alpha_i) = \mathbb{F}_{p^r}$. In order to satisfy condition (18), we first recall assumptions $h < p^{\varepsilon'}$, $\varepsilon > \varepsilon' > 0$ and $\max_{\substack{d<r\\ d|r}} \gcd(\tau_i, p^d-1) < \tau_i p^{-\varepsilon}$ for some $i \in \{1, 2\}$. Without loss of generality, let us assume that $i = 1$. Then, for any $d|r$ with $1 \le d < r$, we have

$$\gcd\left(\tfrac{\tau_1}{h}, p^d-1\right) \le \gcd(\tau_1, p^d-1) < \tau_1 p^{-\varepsilon} < \frac{\tau_1}{h}p^{-(\varepsilon-\varepsilon')}.$$

Therefore, by Bourgain and Chang [3, Theorem 2] it follows that

$$\left|\sum_{n_1\le\tau_1/h} \mathbf{e}_p\left(\operatorname{Tr}\left(\gamma_1'\alpha_1^{n_1h}\right)\right)\right| = \left|\sum_{n_1\le\tau_1/h} \psi_1(\alpha_1^{n_1h})\right| \le \frac{\tau_1}{h}p^{-\delta}.$$

On the other hand, bounding trivially we have

$$\left|\sum_{n_2\le\tau_2/h}\mathbf{e}_p\left(\mathrm{Tr}\left(\gamma_2'\alpha_2^{n_2h}\right)\right)\right| = \left|\sum_{n_2\le\tau_2/h}\psi_2(\alpha_2^{n_2h})\right| \le \frac{\tau_2}{h}.$$

Thus, combining above equations with (20) and (23) we get

$$\max_{\xi\in\mathbb{F}_p^*}\left|\sum_{n\le\frac{\tau_1\tau_2}{h}}\mathbf{e}_p\left(\xi s_n\right)\right| \le h\times\frac{\tau_1\tau_2}{h^2}p^{-\delta} = \frac{\tau_1\tau_2}{h}p^{-\delta}.$$

Now, let us assume that one of the $\lambda_i' = 0$, say for $i = 2$. Arguing exactly as few lines above, it follows from assumption (a) that

$$\left|\sum_{n_1\le\tau_1/h}\mathbf{e}_p\left(\mathrm{Tr}\left(\gamma_1'\alpha_1^{n_1h}\right)\right)\right| \le \frac{\tau_1}{h}p^{-\delta}, \quad \text{and} \quad \left|\sum_{n_2\le\tau_2/h}\mathbf{e}_p\left(\mathrm{Tr}\left(\gamma_2'\alpha_2^{n_2h}\right)\right)\right| = \frac{\tau_2}{h}.$$

Hence, the desired bound follows. This conclude the case $\nu = 2$.

Now, we proceed by induction over ν, and assume Theorem 1 to be true up to $\nu - 1$. We follow the idea due to Garaev [9, Section 4.4]. Considering (19) and periodicity, for any $t \ge 1$ we get

$$\begin{aligned}
\tau\left|\sum_{n\le\tau}\mathbf{e}_p\left(\xi s_n\right)\right|^{2t} &= \sum_{m\le\tau}\left|\sum_{n\le\tau}\mathbf{e}_p\left(\xi s_{m+n}\right)\right|^{2t}\\
&= \sum_{m\le\tau}\left|\sum_{n\le\tau}\mathbf{e}_p\left(\xi(\,\mathrm{Tr}\left(\gamma_1\alpha_1^{m+n}\right) + \cdots + \,\mathrm{Tr}\left(\gamma_\nu\alpha_\nu^{m+n}\right))\right)\right|^{2t}\\
&\le \sum_{n_1\le\tau}\cdots\sum_{n_{2t}\le\tau}\left|\sum_{m\le\tau}\mathbf{e}_p\left(\xi\sum_{i=1}^{\nu}\mathrm{Tr}\left(\gamma_i\alpha_i^m\left(\alpha_i^{n_1} + \cdots - \alpha_i^{n_{2t}}\right)\right)\right)\right|.
\end{aligned}$$

Raising to the power $2t$, and applying Cauchy–Schwarz, we have

$$\begin{aligned}
\tau^{2t}\left|\sum_{n\le\tau}\mathbf{e}_p\left(\xi s_n\right)\right|^{4t^2} &\le \tau^{2t(2t-1)}\\
&\quad\times\sum_{n_1\le\tau}\cdots\sum_{n_{2t}\le\tau}\left|\sum_{m\le\tau}\mathbf{e}_p\left(\xi\sum_{i=1}^{\nu}\mathrm{Tr}\left(\gamma_i\alpha_i^m\left(\alpha_i^{n_1} + \cdots - \alpha_i^{n_{2t}}\right)\right)\right)\right|^{2t}.
\end{aligned}$$

Given $(\lambda_1, \cdots, \lambda_\nu) \in \mathbb{F}_q^\nu$, let $J_t(\lambda_1, \cdots, \lambda_\nu)$ denote the number of solutions of the system

$$\begin{cases}
\alpha_1^{n_1} + \cdots + \alpha_1^{n_t} = \alpha_1^{n_{t+1}} + \cdots + \alpha_1^{n_{2t}} + \lambda_1\\
\quad\vdots \qquad \vdots \qquad\qquad \vdots \qquad \vdots \qquad \vdots\\
\alpha_\nu^{n_1} + \cdots + \alpha_\nu^{n_t} = \alpha_\nu^{n_{t+1}} + \cdots + \alpha_\nu^{n_{2t}} + \lambda_\nu
\end{cases}$$

with $1 \le n_1, \cdots, n_{2t} \le \tau$. Therefore,

$$\begin{aligned}
\left|\sum_{n\le\tau}\mathbf{e}_p\left(\xi s_n\right)\right|^{4t^2} &\le \tau^{4t^2-4t}\sum_{\lambda_1\in\mathbb{F}_q}\cdots\sum_{\lambda_\nu\in\mathbb{F}_q}J_t(\lambda_1, \cdots, \lambda_\nu)\\
&\quad\times\left|\sum_{m\le\tau}\mathbf{e}_p\left(\xi\sum_{i=1}^{\nu}\mathrm{Tr}\left(\gamma_i\lambda_i\alpha_i^m\right)\right)\right|^{2t}.
\end{aligned} \tag{24}$$

Note that writing $J_\nu(\lambda_1 \cdots, \lambda_\nu)$ in terms of character sums, it follows that

$$\begin{aligned} J_t(\lambda_1 \cdots, \lambda_\nu) &= \frac{1}{q^\nu} \sum_{x_1 \in \mathbb{F}_q} \cdots \sum_{x_\nu \in \mathbb{F}_q} \left| \sum_{n \le \tau} \mathbf{e}_p\left(\operatorname{Tr}\left(x_1 \alpha_1^n\right)\right) \cdots \mathbf{e}_p\left(\operatorname{Tr}\left(x_\nu \alpha_\nu^n\right)\right) \right|^{2t} \\ &\quad \times \mathbf{e}_p\left(\operatorname{Tr}\left(x_1 \lambda_1\right)\right) \cdots \mathbf{e}_p\left(\operatorname{Tr}\left(x_\nu \alpha_\nu^n\right)\right) \\ &\le \frac{1}{q^\nu} \sum_{x_1 \in \mathbb{F}_q} \cdots \sum_{x_\nu \in \mathbb{F}_q} \left| \sum_{n \le \tau} \mathbf{e}_p\left(\operatorname{Tr}\left(x_1 \alpha_1^n\right)\right) \cdots \mathbf{e}_p\left(\operatorname{Tr}\left(x_\nu \alpha_\nu^n\right)\right) \right|^{2t} \\ &\le J_t(0, \ldots, 0) =: J_{t,\nu}. \end{aligned}$$

In particular, we note that $J_{t,\nu} \le J_{t,\nu-1}$. From (24), it follows that

$$\begin{aligned} &\left| \sum_{n \le \tau} \mathbf{e}_p\left(\xi s_n\right) \right|^{4t^2} \\ &\quad \le \tau^{4t^2 - 4t} J_{t,\nu} \sum_{m_1 \le \tau} \cdots \sum_{m_{2t} \le \tau} \sum_{\lambda_1 \in \mathbb{F}_q} \cdots \sum_{\lambda_\nu \in \mathbb{F}_q} \mathbf{e}_p\left(\sum_{i=1}^{\nu} \operatorname{Tr}\left(\xi \gamma_i \lambda_i (\alpha_i^{m_1} + \cdots - \alpha_i^{m_{2t}})\right) \right). \end{aligned}$$

Note that $a\gamma\lambda$, with $a\gamma \ne 0$, runs over $\lambda \in \mathbb{F}_q$, then $\mathbf{e}_p\left(\operatorname{Tr}\left(a\theta\lambda z\right)\right)$ runs through all additive characters ψ in $\widehat{\mathbb{F}}_q$, evaluated at z. Then, the above expression can be written as

$$\begin{aligned} \left| \sum_{n \le \tau} \mathbf{e}_p\left(\xi s_n\right) \right|^{4t^2} &\le \tau^{4t^2 - 4t} J_{t,\nu} \sum_{m_1 \le \tau} \cdots \sum_{m_{2t} \le \tau} \prod_{i=1}^{\nu} \left(\sum_{x \in \mathbb{F}_q} \mathbf{e}_p\left(x(\alpha_i^{m_1} + \cdots - \alpha_i^{m_{2t}})\right) \right) \\ &\le \tau^{4t^2 - 4t} q^\nu J_{t,\nu}^2 \le \tau^{4t^2 - 4t} q^\nu J_{t,\nu-1}^2. \end{aligned} \tag{25}$$

We now require an estimate for $J_{t,\nu-1}$, and write

$$\begin{aligned} J_{t,\nu-1} &= \frac{1}{q^{\nu-1}} \sum_{\lambda_1 \in \mathbb{F}_q} \cdots \sum_{\lambda_{\nu-1} \in \mathbb{F}_q} \left| \sum_{m \le \tau} \mathbf{e}_p\left(\operatorname{Tr}\left(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m\right)\right) \right|^{2t} \\ &= \frac{\tau^{2t}}{q^{\nu-1}} + O\left(\left(\max_{\substack{(\lambda_1, \ldots, \lambda_{\nu-1}) \in \mathbb{F}_q^{\nu-1} \\ (\lambda_1, \ldots, \lambda_{\nu-1}) \ne 0}} \left| \sum_{m \le \tau} \mathbf{e}_p\left(\operatorname{Tr}\left(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m\right)\right) \right| \right)^{2t} \right). \end{aligned} \tag{26}$$

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

$$\left| \sum_{m \le \tau} \mathbf{e}_p\left(\operatorname{Tr}\left(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m\right)\right) \right| \le \tau p^{-\delta'},$$

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 (26), we get

$$J_{t,\nu-1} \ll \frac{\tau^{2t}}{q^{\nu-1}}.$$

We conclude the proof combining the above estimate with (25) to get[2]

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \le \tau} \mathbf{e}_p\left(\xi s_n\right) \right| \le \tau p^{-\delta}, \quad \text{with} \quad \delta = \tfrac{d(\nu-2)}{4t^2}.$$

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

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

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

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

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

Remark 1 It is possible to relax the condition (a) by assuming that

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

holds for some $1 \le i \le \nu$ for which $\lambda_i' \ne 0$, where λ_i' is defined in the proof of Theorem 1. Also, note that $\lambda_i' = 0$ if and only if $\lambda_i = 0$.

Since $\{s_n\}$ is a nonzero linear recurrence sequence, there exists some $1 \le i \le \nu$ for which $\lambda_i \ne 0$. We discussed in Sect. 1.1 that why (a) (or some other condition) is needed to prove the irreducible case of Theorem 2. Now, for the reducible case, some of the λ_i could be 0. For the worst case scenario, let us assume that only one of them is nonzero, say for $i = 1$. Then, it follows from (19) that, we are back to considering the irreducible case and then we need the condition (a) for $i = 1$. In particular, we need (a) (or some other condition) for each irreducible component of the underlying $\omega(x)$.

3 Exponential sums for modular forms

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

3.1 Order of the roots of the characteristic polynomial

In the case of normalized eigenforms, the sequence $\{a(p^n)\}$ defines a linear recurrence sequence of order two when $p \nmid N$, otherwise it is of order one. This is one of the tools for Theorem 2. However, we do not need to assume that the form is normalized because the normalizing factor is in $\mathbb{Q}$, and we can realize that to be an element of $\mathbb{F}_\ell^*$ for any large enough prime ℓ. Before going into the proof of this theorem, we develop a tool which will be quite useful throughout. We state it in the form of following lemma.

[2] To get a non trivial estimate, we must have a non zero δ. This is true when $\nu > 2$. Hence our induction step starts from $\nu = 2$.

Lemma 7 *Let $\omega(x) = x^2 + ax + b \in \mathbb{Z}[x]$ be a quadratic polynomial with $b \neq 0$ and let α, β be its roots such that none of the α, β or $\alpha\beta^{-1}$ is a root of unity. For any prime ℓ, let α_ℓ, β_ℓ be its roots in the splitting field of $\omega(x)$ over $\mathbb{F}_\ell$.*

Then, given $0 < \varepsilon < 1/2$, for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \leq y$, we have

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

Proof Given a large positive parameter T, we begin by considering the polynomial

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

It is clear that $\omega(x) \pmod{\ell}$ has distinct roots for all but finitely many primes ℓ, since $a^2 - 4b \neq 0$. For any such prime ℓ, let α_ℓ and β_ℓ be the distinct roots in its splitting field. We now consider the resultant $\operatorname{Res}(\omega(x), G_T(x))$, and note that

$$\operatorname{Res}(\omega(x), G_T(x)) \pmod{\ell} = \prod_{1 \leq i \leq 3T}(\alpha_\ell - \mu_i)(\beta_\ell - \mu_i),$$

where each μ_i is a root of $G_T(x)$ in its splitting field over $\mathbb{F}_\ell$.

In particular, $\operatorname{Res}(\omega(x), G_T(x)) \equiv 0 \pmod{\ell}$ if and only if $\omega(x) \pmod{\ell}$ and $G_T(x) (\bmod\ \ell)$ have common roots in some finite extension of $\mathbb{F}_\ell$. Additionally, since $\alpha_\ell\beta_\ell = b$, it follows that $\operatorname{ord}(\alpha_\ell\beta_\ell^{-1}) \leq T$ if and only if $\alpha_\ell^{2t} - b^t = 0$ (or $\beta_\ell^{2t} - b^t = 0$), for some $t \leq T$. Therefore, α_ℓ (or β_ℓ) is a common root of $\omega(x) \pmod{\ell}$ and $G_T(x) \pmod{\ell}$ if $\operatorname{ord}\alpha_\ell$ or $\operatorname{ord}(\alpha_\ell\beta_\ell^{-1})$ (or $\operatorname{ord}\beta_\ell$ or $\operatorname{ord}(\alpha_\ell\beta_\ell^{-1})$) is less than T. Now, the Sylvester matrix of $\omega(x)$ and $G_T(x)$ is a square matrix of order $2 + \deg(G_T(x)) \ll T^2$, and entries bounded by an absolute constant M (which depends on a, b and not on ℓ or the parameter T). Then, by Hadamard's inequality, the determinant

$$\operatorname{Res}(\omega(x), G_T(x)) \leq T^{T^2} \times M^{T^2} \ll M^{2T^2\log T}.$$

Note that $\operatorname{Res}(\omega(x), G_T(x))$ is zero if and only if $\alpha^t = 1, \beta^t = 1$ or $(\alpha\beta^{-1})^t = 1$ for some $t \leq T$, which, following our assumption, can not happen. In particular, the resultant has at most $O\left(T^2\right)$ many distinct prime divisors. This shows that

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

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

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

is $O\left(y^{2\varepsilon}\right)$. □

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

3.2 Proof of Theorem 2

If $p \mid N$, then $a(p^n) = a(p)^n$ for any n. We only need to consider

$$\max_{\xi \in \mathbb{F}_\ell^*}\left|\sum_{n \leq \tau}\mathbf{e}_\ell\left(\xi a(p)^n\right)\right|. \tag{27}$$

If $p \notin \mathcal{P}$, then there exists u such that $a(p^u) = 0$. Since $p \mid N$, we have $a(p) = 0$. In this case, the sum is $O(1)$ because we have $\tau = 1$.

On the other hand, if $p \in \mathcal{P}$, then for any prime ℓ large enough τ is simply the order of $a(p) \pmod \ell$ in $\mathbb{F}_\ell^*$. Due to Lemma 7, we may assume that $\tau > p^\varepsilon$ holds for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell < y$. Hence, this case is settled down by [4, Theorem 6].

Let us now consider the case $p \nmid N$. The characteristic polynomial of (1) is

$$\omega(x) = x^2 - a(p)x + p^{k-1}, \tag{28}$$

and has discriminant $a^2(p) - 4p^{k-1}$. We note that in our case the discriminant does not vanish, otherwise $|a(p)| = 2p^{(k-1)/2}$ is absurd, with $a(p)$ being integer and $p^{(k-1)/2}$ irrational. Let $\mathbb{P}$ be the set of all primes. We divide the proof for primes $p \in \mathcal{P}$ and $p \in \mathbb{P} \setminus \mathcal{P}$. 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 $u \neq 0$. Let us split the cases according to $D_p \pmod \ell$ is quadratic residue, zero or non quadratic residue modulo ℓ. Set

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

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

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

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

Case 1. $\boldsymbol{\ell \in \mathbb{P}_{-1}}$**:**

we want to show that the inequality (7) is satisfied by $\frac{\pi(y)}{2} + O(y^{2\varepsilon})$ many primes $\ell \leq y$ in $\mathbb{P}_{-1}$. In this case the associated polynomial (28) is irreducible modulo ℓ, then the idea is to employ Corollary 6. Let α and $\beta = \alpha^\ell$ be the conjugate roots of (28) in its splitting field $\mathbb{F}_\ell(\alpha)$. For a given $\varepsilon > 0$, from Lemma 7 it follows that for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \leq y$, the following inequalities

$$\operatorname{ord} \alpha^\ell = \operatorname{ord} \alpha > \ell^\varepsilon \quad \text{and} \quad \operatorname{ord} \alpha\beta^{-1} = \operatorname{ord} \alpha^{1-\ell} > \ell^\varepsilon \tag{29}$$

hold. Combining the identity

$$\operatorname{ord} \alpha^{\ell-1} = \frac{\operatorname{ord} \alpha}{\gcd(\operatorname{ord} \alpha, \ell - 1)}$$

with the second inequality of (29), we get

$$\gcd(\operatorname{ord} \alpha, \ell - 1) = \frac{\operatorname{ord} \alpha}{\operatorname{ord} \alpha^{\ell-1}} = \frac{\operatorname{ord} \alpha}{\operatorname{ord} \alpha^{1-\ell}} < (\operatorname{ord} \alpha)\ell^{-\varepsilon}.$$

Applying Corollary 6 we complete the proof of this case.

Case 2. $\ell \in \mathbb{P}_1$:
let α, β be the roots of $\omega(x) (\bmod\, \ell)$ inside $\mathbb{F}_\ell^*$. From (17) it follows that for $n \geq 0$, $a(p^n) \equiv c\alpha^n + d\beta^n (\bmod\, \ell)$, 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 $a(p^n) (\bmod\, \ell)$, and hence τ divides $\ell - 1$. We have

$$\sum_{n \leq \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) = \frac{\tau}{\ell - 1} \sum_{n \leq \ell - 1} \mathbf{e}_\ell\left(\xi a(p^n)\right) = \frac{\tau}{\ell - 1} \sum_{n \leq \ell - 1} \mathbf{e}_\ell\left(\xi (c\alpha^n + b\beta^n)\right).$$

From Lemma 7, there is a subset of $\mathbb{P}_1$ with $\frac{\pi(y)}{2} + O(y^{2\varepsilon})$ many primes $\ell \leq y$ such that $\operatorname{ord} \alpha$, $\operatorname{ord} \beta$ and $\operatorname{ord} (\alpha\beta^{-1})$ are bigger than ℓ^ε. It follows from [2, Corollary, page 479] that there exists a $\delta = \delta(\varepsilon) > 0$ such that

$$\max_{\substack{(c,d) \in \mathbb{F}_\ell \times \mathbb{F}_\ell \\ (c,d) \neq (0,0)}} \left| \sum_{n \leq \ell - 1} \mathbf{e}_\ell\left(c\alpha^n + d\beta^n\right) \right| \leq \ell^{1-\delta}.$$

Hence, *(i)* of Theorem 2 holds. Now, assume that p belongs to the exceptional set $\mathbb{P} \setminus \mathcal{P}$, that is $a(p^u) = 0$ for some $u \geq 1$. We consider $u = u(p)$ to be the least such integer. Since the discriminant is nonzero (the roots α and β of (28) are distinct), we get[3]

$$a(p^u) = \frac{\alpha^{u+1} - \beta^{u+1}}{\alpha - \beta} = 0.$$

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,

$$\begin{aligned}
\sum_{n \leq \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) &= \sum_{n=0}^{\tau - 1} \mathbf{e}_\ell\left(\xi b(n + 1)\right) = \left(\sum_{n=0}^{\lfloor \tau/(u+1) \rfloor} \sum_{e=0}^{u} \mathbf{e}_\ell\left(\xi b(n(u + 1) + e)\right) \right) \\
&\quad + O(u) \\
&= \left(\sum_{n=0}^{\lfloor \tau/(u+1) \rfloor} \mathbf{e}_\ell\left(\xi b(n(u + 1))\right) + \sum_{e=1}^{u} \sum_{n=0}^{\lfloor \tau/(u+1) \rfloor} \mathbf{e}_\ell\left(\xi b(n(u + 1) + e)\right) \right) \\
&\quad + O(u) \\
&= \lfloor \frac{\tau}{u + 1} \rfloor + \left(\sum_{e=1}^{u} \sum_{n=0}^{\lfloor \tau/(u+1) \rfloor} \mathbf{e}_\ell\left(\xi b(n(u + 1) + e)\right) \right) + O(u). \qquad (30)
\end{aligned}$$

First of all observe that u is odd. As otherwise, if u is even then we would get

$$\alpha^{u+1} + \beta^{u+1} = 2\alpha^{u+1} = \pm 2 p^{\frac{(u+1)(k-1)}{2}},$$

which is absurd as $\alpha^{u+1} + \beta^{u+1}$ is a rational, but $p^{\frac{(u+1)(k-1)}{2}}$ is not. Now, for any $0 < e < u+1$ we have

$$b((u + 1)n + e) = \alpha^{(u+1)n} \frac{(\alpha^e - \beta^e)}{\alpha - \beta} = \left(\pm p^{\frac{(u+1)(k-1)}{2}}\right)^n a(p^{e-1}),$$

where the sign on the right hand side above depends on the sign of α^{u+1}. Without loss of generality, we are assuming that this sign is negative. It is easy to see that our next

[3] The explicit expression of $a(p^u)$ can be obtained by using induction on u along with the fact that $\alpha + \beta = a(p)$, $\alpha\beta = p^{k-1}$ and the recurrence relation at (1).

argument applies to the positive sign case as well. Since u is fixed, so are all the e's up to $u-1$. In particular, we may consider large primes ℓ for which all of the $a(p^e) \not\equiv 0 (\mathrm{mod}\, \ell)$ for any $1 \le e \le u-1$. Then, we have

$$\sum_{n=0}^{\tau/(u+1)} \mathbf{e}_\ell\left(\xi b(n(u+1)+e)\right) = \sum_{n=0}^{\tau/(u+1)} \mathbf{e}_\ell\left(\xi \left(-p^{\frac{(u+1)(k-1)}{2}}\right)^n a(p^{e-1})\right).$$

Due to Lemma 7, we may assume that $t_u = \operatorname{ord}(-p^{(k-1)(u+1)/2}) > \ell^\varepsilon$ holds for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \le y$. Now, by [4, Corollary 1] it follows that

$$\left|\sum_{n\le t} \mathbf{e}_\ell\left(\xi \left(-p^{\frac{(u+1)(k-1)}{2}}\right)^n a(p^{e-1})\right)\right| \le t\ell^{-\delta}, \quad \text{for some } \delta = \delta(\varepsilon/2) > 0, \tag{31}$$

and for any $t_u \ge t > \ell^\varepsilon$.

Writing $[\tau/(u+1)] = qt_u + r$, with $0 \le r < t_u$ it follows that

$$\sum_{n\le \tau/(u+1)} \mathbf{e}_\ell\left(\xi\alpha^{(u+1)n} a(p^{e-1})\right) = q \sum_{n\le t_u} \mathbf{e}_\ell\left(\xi\alpha^{(u+1)n} a(p^{e-1})\right) + \sum_{n\le r} \mathbf{e}_\ell\left(\xi\alpha^{(u+1)n} a(p^{e-1})\right).$$

The estimate $\left|\sum_{n\le t_u} \mathbf{e}_\ell\left(\xi\alpha^{(u+1)n} a(p^{e-1})\right)\right| \le t_u\ell^{-\delta}$ follows from (31). If $r \le \ell^{\varepsilon/2}$, then we get trivially $\left|\sum_{n\le r} \mathbf{e}_\ell\left(\xi\alpha^{(u+1)n} a(p^{e-1})\right)\right| \le \ell^{\varepsilon/2}$. If $\ell^{\varepsilon/2} \le r < t_u$, then from (31) it follows that

$$\left|\sum_{n\le r} \mathbf{e}_\ell\left(\xi\alpha^{(u+1)n} a(p^{e-1})\right)\right| \le t_u\ell^{-\delta}.$$

Therefore,

$$\left|\sum_{n\le r} \mathbf{e}_\ell\left(\xi\alpha^{(u+1)n} a(p^{e-1})\right)\right| \le \max\left\{\ell^{\varepsilon/2}, t_u\ell^{-\delta}\right\}.$$

Recalling that $t_u \ge \ell^\varepsilon$, we can also assume that $t_u\ell^{-\delta} \ge \ell^{\varepsilon/2}$ by taking small enough δ. Thus,

$$\left|\sum_{n\le \tau/(u+1)} \mathbf{e}_\ell\left(\xi\alpha^{(u+1)n} a(p^{e-1})\right)\right| \le (qt_u + t_u)\ell^{-\delta} \ll \frac{\tau}{u+1}\ell^{-\delta}.$$

Finally, combining the above inequality with (30) we obtain

$$\begin{aligned}\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n\le\tau} \mathbf{e}_\ell\left(\xi a(p^n)\right)\right| &= \left\lfloor \frac{\tau}{u+1} \right\rfloor + O\left(\tau\ell^{-\delta} + u\right) \\ &= \frac{\tau}{u+1} + O\left(\tau\ell^{-\delta} + u\right).\end{aligned}$$

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

3.3 Consequences of Theorem 2

Let us consider an exponential sum of type $S(p,x,\alpha) = \sum_{p^n \le x} \mathbf{e}(\alpha a(p^n))$, for $\alpha \in [0,1]$. As one of the consequences of Theorem 2, we want to study this exponential sum when α is a rational whose denominator is a prime. In this regard, we have the following result.

Corollary 8 *Let f be an eigenform of weight k and level N with rational coefficient. Then for a given $0 < \varepsilon < 1/2$, there exists a $\delta(\varepsilon) > 0$ such that for at least $\gg \frac{(\log x)^{1-\delta/(2+\delta)}}{\log\log x}$ many primes ℓ, we have the following estimates:*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{p^n \le x} \mathbf{e}_\ell\left(\xi a(p^n)\right) \right| = \begin{cases} O\left((\log x/\log p)^{1-\delta/(2+\delta)}\right) & \text{if} \quad p \notin \mathcal{P} \\ \frac{1}{u+1}\frac{\log x}{\log p} + O\left((\log x/\log p)^{1-\delta/(2+\delta)}\right) & \text{if} \quad p \in \mathcal{P} \end{cases}.$$

Proof Consider the same $\delta := \delta(\varepsilon)$ as in Theorem 2 and any prime

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

Following Theorem 2, we have

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) \right| \le \frac{\tau}{\ell^\delta} \tag{32}$$

holds, for at least $\gg \frac{(\log x)^{1-\delta/(2+\delta)}}{\log\log x}$ primes ℓ. For these primes, we also have $\tau \le \ell^2 < \frac{\log x}{\log p}$. In particular,

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

On the other hand, let $p \in \mathcal{P}$ be a prime, then by Theorem 2 we have

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) \right| = \frac{\tau}{u+1} + O\left(\frac{\tau}{\ell^\delta} + u\right),$$

holds, for some u depending on p, and for at least $\gg \frac{(\log x)^{1-\delta/(2+\delta)}}{\log\log x}$ primes ℓ. Due to Lemma 7, we can assume that $\tau > \ell^\delta$ holds by choosing small enough δ, for at least $\gg \frac{(\log x)^{1-\delta/(2+\delta)}}{\log\log x}$ primes ℓ. Arguing similarly as in the previous case, we get the desired main term, and the error term that we get

$$O\left(\frac{\log x}{\ell^\delta \log p} + \frac{u \log x}{\tau \log p}\right) = O\left(\frac{\log x}{\ell^\delta \log p}\right) = O\left((\log x/\log p)^{1-\delta/(2+\delta)}\right),$$

where the last equality holds because $\tau > \ell^\delta$. □

Corollary 9 *Let f be an eigenform of weight k and level N with rational coefficients. For $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \le y$ we have the following property. Given $0 < \varepsilon < 1/2$ and $p_1, \cdots, p_\nu$ be any set of distinct primes such that $a(p_i^u) \ne 0$ for all $u \ge 1$ and $1 \le i \le \nu$, there exists a $\delta = \delta(\varepsilon) > 0$ such that*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n_1 \le \tau_1} \cdots \sum_{n_\nu \le \tau_\nu} \mathbf{e}_\ell\left(\xi a(p_1^{n_1} \cdots p_\nu^{n_\nu})\right) \right| \le \tau_1 \cdots \tau_\nu \ell^{-\delta}.$$

Proof Set

$$S_\nu(\xi) = \left| \sum_{n_1 \le \tau_1} \cdots \sum_{n_\nu \le \tau_\nu} \mathbf{e}_\ell \left(\xi a(p_1^{n_1} \cdots p_\nu^{n_\nu}) \right) \right|.$$

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

$$\begin{aligned} |S_\nu(\xi)| &\le \sum_{n_1 \le \tau_1} \left| \sum_{n_2 \le \tau_2} \cdots \sum_{n_\nu \le \tau_\nu} \mathbf{e}_\ell \left(\xi a(p_1^{n_1}) a(p_2^{n_2} \cdots p_\nu^{n_\nu}) \right) \right| \\ &\le \tau_2 \cdots \tau_\nu \sum_{\substack{n_1 \le \tau_1 \\ a(p_1^{n_1}) \equiv 0 \,(\mathrm{mod}\, \ell)}} 1 + \sum_{\substack{n_1 \le \tau_1 \\ a(p_1^{n_1}) \not\equiv 0 \,(\mathrm{mod}\, \ell)}} \left| \sum_{n_2 \le \tau_2} \cdots \sum_{n_\nu \le \tau_\nu} \mathbf{e}_\ell \left(\xi a(p_1^{n_1}) a(p_2^{n_2} \cdots p_\nu^{n_\nu}) \right) \right| \end{aligned}$$

By induction hypothesis, the second term on the right hand side of the above equation is bounded by $\tau_1 \tau_2 \cdots \tau_\nu \ell^{-\delta}$, for some $\delta > 0$ depending on ε. On the other hand, note that $\sum_{\substack{n_1 \le \tau_1 \\ a(p_1^{n_1}) \equiv 0 \,(\mathrm{mod}\, \ell)}} 1$ counts the number of solutions of the congruence

$$a(p_1^n) \equiv 0 \,(\mathrm{mod}\, \ell), \qquad n \le \tau_1.$$

Writing it as exponential sum we get

$$\begin{aligned} \sum_{\substack{n_1 \le \tau_1 \\ a(p_1^{n_1}) \equiv 0 \,(\mathrm{mod}\, \ell)}} 1 &= \frac{1}{\ell} \sum_{x=0}^{\ell-1} \sum_{n_1 \le \tau_1} \mathbf{e}_\ell \left(x(a(p_1^{n_1})) \right) \\ &= \frac{\tau_1}{\ell} + O\left(\max_{x \in \mathbb{F}_\ell^*} \left| \sum_{n_1 \le \tau_1} \mathbf{e}_\ell \left(x(a(p_1^{n_1})) \right) \right| \right). \end{aligned}$$

We can bound the error term by Theorem 2 and without loss of generality assuming $\delta < 1$, we get the sum above is simply $\frac{\tau_1}{\ell} + O(\tau_1 \ell^{-\delta})$. This is further bounded by $2\tau_1 \ell^{-\delta}$, because the explicit constant in Theorem 2 is exactly 1. Therefore,

$$|S_\nu(\xi)| \le \tau_2 \cdots \tau_\nu \left(2\tau_1 \ell^{-\delta} \right) + \tau_1 \tau_2 \cdots \tau_\nu \ell^{-\delta},$$

for some $\delta = \delta(\varepsilon) > 0$. This shows that the inequality

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n_1 \le \tau_1} \cdots \sum_{n_\nu \le \tau_\nu} \mathbf{e}_\ell \left(\xi a(p_1^{n_1} \cdots p_\nu^{n_\nu}) \right) \right| \le 3\tau_1 \cdots \tau_\nu \ell^{-\delta}$$

holds for almost all prime ℓ and this completes the proof because we can remove the extra factor 3 by taking primes ℓ large enough. □

4 Exponential sums for modular forms: beyond eigenforms

We shall now prove Theorem 3. Write

$$a_f(p^n) = \sum_{i=1}^{r} a_i a_{f_i}(p^n),$$

where $a_i \in \mathbb{Q}$, and f_i is a newform with rational coefficients for every $1 \le i \le r$. Let $\omega^{(i,p)}$ be the characteristic polynomial of $a_{f_i}(p^n)$ and $D_i(p)$ be its discriminant.

Consider

$$\mathcal{S}_1 = \left\{ \ell \text{ prime} \mid \left(\frac{D_i(p)}{\ell}\right) = 1, \forall 1 \le i \le r \right\}.$$

It is clear that $\mathcal{S}_1$ has positive density. One can verify this by considering primes congruent to 1 modulo $8\prod_{i=1}^{r} D_i(p)$. This works well because, we then have

$$\left(\frac{-1}{\ell}\right) = 1, \left(\frac{2}{\ell}\right) = 1 \text{ and } \left(\frac{\ell}{\text{odd}(D_i(p))}\right) = 1, \forall 1 \le i \le r,$$

where odd(.) denotes odd part of the corresponding number. These conditions altogether imply $\ell \in \mathcal{S}_1$. Let $\alpha^{(i,p)}$ and $\beta^{(i,p)}$ be the roots of $\omega^{(i,p)}$. So for any $\ell \in \mathcal{S}_1$, we can write

$$\omega^{(i,p)}(x) \,(\text{mod}\,\ell) = \prod_{1\le i\le r} \left(x - \alpha_\ell^{(i,p)}\right)\left(x - \beta_\ell^{(i,p)}\right),$$

where for every i, j, $\alpha_\ell^{(i,p)}, \beta_\ell^{(j,p)}$ are in $\mathbb{F}_\ell$. Now, we consider the set of primes

$$\mathcal{S}_2 = \left\{p \text{ prime} \mid \alpha^{(i,p)}(\beta^{(j,p)})^{-1} \text{ is not root of unity}, \forall\, i, j\right\}$$
$$\cup \left\{p \text{ prime} \mid \alpha^{(i,p)}(\alpha^{(j,p)})^{-1} \text{ is not root of unity}, \forall i \ne j\right\}.$$

Lemma 10 *For any prime $p \in \mathcal{S}_2$, the following inequalities are true for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \le y$.*

(1) $\text{ord}\,(\alpha_\ell^{(i,p)}(\beta_\ell^{(j,p)})^{-1}) > \ell^\varepsilon$, $\text{ord}\,(\alpha_\ell^{(i,p)}) > \ell^\varepsilon$ *and* $\text{ord}\,(\beta_\ell^{(j,p)}) > \ell^\varepsilon$, *for all* $1 \le i, j \le r$, *and*

(2) $\text{ord}\,(\alpha_\ell^{(i,p)}(\alpha_\ell^{(j,p)})^{-1}) > \ell^\varepsilon$, *for all* $1 \le i \ne j \le r$,

Proof It is enough to prove the result only for $i, j \in \{1, 2\}$. Consider the Galois extension $K = \mathbb{Q}\left(\alpha^{(1,p)}, \alpha^{(2,p)}\right)$. Let $\mathfrak{L}$ be a prime ideal lying over ℓ in $\mathcal{O}_K$. It is clear that

$$\{\alpha_\ell^{(1,p)}, \alpha_\ell^{(2,p)}, \beta_\ell^{(1,p)}, \beta_\ell^{(2,p)}\} = \{\alpha^{(1,p)}, \alpha^{(2,p)}, \beta^{(1,p)}, \beta^{(2,p)}\}(\text{mod}\,\mathfrak{L}), \tag{33}$$

because both of these sets serve as a set of roots of the equation $\omega(x)\,(\text{mod}\,\ell)$ and $\omega(x)\,(\text{mod}\,\mathfrak{L})$ respectively. Note that $\omega(x)\,(\text{mod}\,\mathfrak{L})$ coincides with $\omega(x)\,(\text{mod}\,\ell)$. It follows from (33) that the right hand side does not depend on the choice of prime $\mathfrak{L}$ lying over ℓ, so there is no problem in working with a fixed $\mathfrak{L}$ lying over ℓ. It is now clear that,

$$\left\{\alpha_\ell^{(i,p)}(\beta_\ell^{(j,p)})^{-1}\right\}_{1\le i,j\le 2} = \left\{\alpha^{(i,p)}(\beta^{(j,p)})^{-1}\right\}_{1\le i,j\le 2} (\text{mod}\,\mathfrak{L}).$$

Consider $R(T) = \text{Res}\,(\omega_1(x), g_T(x))$, where $\omega_1(x) = \left(x - \alpha^{(1,p)}\right)\left(x - \beta^{(1,p)}\right)$ and

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

It is clear that $R(T) \ne 0$ for any $T \in \mathbb{N}$ as $p \in \mathcal{S}_2$ by assumption. Now, consider the set of primes

$$\left\{\ell \text{ prime} \mid \text{ord}\left(\alpha_\ell^{(i,p)}(\beta_\ell^{(j,p)})^{-1}\right), \text{ord}\left(\alpha_\ell^{(i,p)}(\alpha_\ell^{(j,p)})^{-1}\right) \le T \text{ for some } i \ne j \in \{1, 2\}\right\}. \tag{34}$$

For any prime ℓ in the set above, and for any prime $\mathfrak{L}$ in $\mathcal{O}_K$ lying over ℓ, $\omega_1(x)\,(\text{mod}\,\mathfrak{L})$ and $g_T(x)\,(\text{mod}\,\mathfrak{L})$ have a common root, Therefore, $R(T)(\text{mod}\,\mathfrak{L}) = 0$. Since both $\omega_1(x)$

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 estimate the number of prime divisors of $R(T)$ similar to as in Lemma 7. This shows that

$$\operatorname{ord}\left(\alpha_\ell^{(i,p)}(\beta_\ell^{(j,p)})^{-1}\right) > \ell^{\varepsilon}, \text{ and } \operatorname{ord}\left(\alpha_\ell^{(i,p)}(\alpha_\ell^{(j,p)})^{-1}\right) > \ell^{\varepsilon}$$

holds for all $i \neq j \in \{1, 2\}$, and $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \leq y$. Rest of the cases can be dealt with Lemma 7. □

4.1 GST: Beyond Sato-Tate

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

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

On the other hand, if f is with CM, then the corresponding Sato-Tate distribution is

$$\mu_{CM} = \frac{1}{2\pi} \int \frac{\mathrm{d}x}{\sqrt{1-x^2}} = \frac{1}{2\pi} \int 1\, \mathrm{d}\theta,$$

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

$$L(s, \mathrm{Sym}^m f) = \prod_{p \nmid N} \prod_{i=0}^{m} \left(1 - \alpha_p^i \beta_p^{m-i} p^{-s}\right)^{-1},$$

where α_p, β_p are normalized roots of (28). In other words, if $\widetilde{\alpha}_p, \widetilde{\beta}_p$ are the roots of (28), then we define $\alpha_p = \frac{\widetilde{\alpha}_p}{p^{\frac{k-1}{2}}}, \beta_p = \frac{\widetilde{\beta}_p}{p^{\frac{k-1}{2}}}$. Serre in [22] showed that if for all integer $m \geq 0$, $L(s, \mathrm{Sym}^m(f))$ extends analytically to $\mathrm{Re}(s) \geq 1$ 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, to estimate the size of $\mathcal{S}_2$ we will have more than one newform to play with, and it will be helpful to have their distributions independent. ***This independency property is stated as Generalized Sato-Tate (GST) hypothesis.*** In this article, we shall always work with the newforms that obey this hypothesis. For example, in Theorem 3, it is assumed that all the associated newforms satisfy the GST hypothesis.

4.2 A consequence of GST

To prove Theorem 3, we need to study the set $\mathcal{S}_2$. We have that luxury when the associated newforms satisfy GST.

Lemma 11 *Suppose that there are r_1 many components without CM and r_2 many components with CM in f. Then under the GST hypothesis, density of $\mathcal{S}_2$ is 2^{-r_2}.*

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

$$\left\{p \text{ prime} \mid \theta_{i,p} \pm \theta_{j,p} \in \mathbb{Q} \times \pi,\ \text{for some } 1 \leq i, j \leq r\right\}. \tag{35}$$

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

$$\left(\frac{2}{\pi}\right)^{r_1}\left(\frac{1}{2\pi}\right)^{r_2}\underset{S}{\int\cdots\int}\sin^2(\theta_1)\sin^2(\theta_2)\cdots\sin^2(\theta_{r_1})\,\mathrm{d}\theta_1\,\mathrm{d}\theta_2\cdots\,\mathrm{d}\theta_r, \tag{36}$$

where $S=\left\{(\theta_1,\theta_2,\cdots,\theta_r)\in[0,\pi]^r \mid \theta_i\pm\theta_j\in\mathbb{Q}\times\pi \text{ for some } 1\leq i,j\leq r\right\}$. Just for the sake of simplicity and to have a feel of what is going on, let us first do the case when there is only one component.

Case 1 $r=1$: suppose that the given component is without *CM*. If $\alpha_p^{(1,p)}\beta_p^{-(1,p)}$ is a root of unity then this implies that $\theta_{1,p}\in\pi\times\mathbb{Q}$. By Sato-Tate, density of such primes is bounded by

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

Since the integral above runs over a set of measure zero, the integral is zero, and for this particular case density of $\mathcal{S}_2$ is indeed 1. Now, suppose that the given component is with *CM*. In this case, the density of $\mathcal{S}_2$ is

$$\left(\frac{1}{2\pi}\right)\int_{\theta\in[0,\pi]\setminus\pi\times\mathbb{Q}}\sin^2(\theta)\,\mathrm{d}\theta=\frac{1}{2}.$$

Case 2 $r\geq 2$: for this general case, it is enough to show that the integral over S in (36) is zero. This is because, due to GST, we are now working with the measure

$$\left(\frac{2}{\pi}\right)^{r_1}\left(\frac{1}{2\pi}\right)^{r_2}\int\cdots\int\sin^2(\theta_1)\sin^2(\theta_2)\cdots\sin^2(\theta_{r_1})\,\mathrm{d}\theta_1\,\mathrm{d}\theta_2\cdots\,\mathrm{d}\theta_r, \tag{37}$$

and with respect to this measure, $[0,\pi]^r$ has measure $\left(\frac{1}{2}\right)^{r_2}$. We can write $S=\bigcup_{1\leq i,j\leq r}S_{i,j}$, where the set $S_{i,j}$ is defined to be the tuples for which $\theta_i\pm\theta_j\in\mathbb{Q}\times\pi$. It is now enough to show that each of these sets $S_{i,j}$ has a zero measure. Note that the integral over $S_{i,j}$ is crudely bounded by $\iint_{S_{i,j}}1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j$. It is evident that

$$\iint_{S_{i,j}}1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j=\iint_{\theta_i+\theta_j\in\mathbb{Q}\times\pi}1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j+\iint_{\theta_i-\theta_j\in\mathbb{Q}\times\pi}1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j,$$

as $\mathbb{Q}\times\mathbb{Q}$ has zero measure. We now note that

$$\iint_{\theta_i-\theta_j\in(a,b)}1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j\leq\int_0^\pi\int_a^b 1\,\mathrm{d}t\,\mathrm{d}\theta\ll|b-a|, \tag{38}$$

for any $b>a$. In particular, for any $\varepsilon>0$,

$$\iint_{\theta_i-\theta_j\in\mathbb{Q}\times\pi}1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j\ll\sum_{k=1}^{\infty}\frac{\varepsilon}{2^k}=\varepsilon.$$

The last implication above follows from the standard argument to show a countable set always has a zero measure. In particular, the second integral of (38) is zero. On the other hand, just by replacing θ_j with $\pi - \theta_j$, we get

$$\iint_{\theta_i+\theta_j \in \mathbb{Q}\times\pi} 1 \, \mathrm{d}\theta_i \, \mathrm{d}\theta_j = - \iint_{\theta_i-\theta_j \in \mathbb{Q}\times\pi} 1 \, \mathrm{d}\theta_i \, \mathrm{d}\theta_j.$$

This just shows that the integral over $S_{i,j}$ at (38) is zero, which completes the proof. □

4.3 Proof of Theorem 3

Let $p \in \mathcal{S}_2$ be a prime, then we can write

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

where $a_i^{(\ell)}$, $c^{(i,\ell)}$ and $d^{(i,\ell)}$ are all in $\mathbb{F}_\ell$. On the other hand, all the roots $\alpha^{(i,\ell)}$ and $\beta^{(i,\ell)}$ are in $\mathbb{F}_\ell$, as $\ell \in \mathcal{S}_1$. The proof now follows by [2, Corollary, p. 479] combining with Lemmas 10 and 11. □

Remark 2 It is known, due to Thorner, that GST holds for $r = 2$ when both f_1 and f_2 are without *CM* and not twist-equivalent. We say that f_1 and f_2 are twist-equivalent if there exists a primitive Dirichlet character χ such that $f_1 = f_2 \otimes \chi$. For more details, we refer the reader to Theorem 1.3 in [27].

5 Exponential sums for modular forms: the inverse case

One may now ask that for a given prime ℓ and small enough ε, 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 Theorems 4 and 5. Let us begin with the proof of Theorem 4.

5.1 Proof of Theorem 4

For any prime p, let us denote the roots of $x^2 - a(p)x + p^{k-1} \, (\mathrm{mod}\ \ell)$ by $\alpha_p^{(\ell)}, \beta_p^{(\ell)}$. Recall that from Deligne-Serre correspondence, we have the associated Galois representation

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

such that $a(p) = \mathrm{tr}\left(\rho_f^{(\ell)}(\mathrm{Frob}_p)\right)$ for any prime $p \nmid N\ell$. It is clear that the characteristic polynomial of $\rho_f^{(\ell)}(\mathrm{Frob}_p) (\mathrm{mod}\ \ell)$ is same as $x^2 - a(p)x + p^{k-1} \, (\mathrm{mod}\ \ell)$. Following Ribet [21, Theorem 3.1], it is known that the image of this representation is $\left\{A \in \mathrm{GL}_2\left(\mathbb{Z}_\ell\right) \mid \det(A) \in (\mathbb{Z}_\ell^*)^{k-1}\right\}$, except possibly for finitely many primes ℓ. In particular, the condition $(k-1, \ell-1) = 1$ implies that the induced Galois representation

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

is surjective for any large prime ℓ, and the eigenvalues of the matrix $\rho_{f,\ell}(\mathrm{Frob}_p) \in \mathrm{GL}_2\left(\mathbb{F}_\ell\right)$ are $\alpha_p^{(\ell)}$ and $\beta_p^{(\ell)}$. From the proof of Theorem 2, we know that an estimate of type (7) holds provided that,

$$\mathrm{ord}\,(\alpha_p^{(\ell)}) > \ell^\varepsilon, \ \mathrm{ord}\,(\beta_p^{(\ell)}) > \ell^\varepsilon, \ \text{and} \ \mathrm{ord}\,(\alpha_p^{(\ell)}(\beta_p^{(\ell)})^{-1}) > \ell^\varepsilon.$$

Let us define,

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

where $\lambda_{1,A}, \lambda_{2,A}$ are the eigenvalues of A in $\mathbb{F}_{\ell^2}^*$. Now the problem is about computing the density of primes p for which the corresponding $\rho_{f,\ell}\left(\mathrm{Frob}_p\right)$ is in C. Note that C is a subset of $\mathrm{GL}_2(\mathbb{F}_\ell)$ stable under conjugation. Hence, by Chebotarev's density theorem, the required density is at least $\frac{|C|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|}$. For each $a \neq b \in \mathbb{F}_\ell^*$, let $C_{a,b}$ be the conjugacy class of $\left(\begin{smallmatrix} a & 0 \\ 0 & b\end{smallmatrix}\right)$. It is known that $|C_{a,b}| = (\ell+1)\ell$. For any element λ in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$, we denote c_λ to be the conjugacy class of matrices in $\mathrm{GL}_2\left(\mathbb{F}_\ell\right)$ having eigenvalue λ. It is known that $|C_\lambda| = \ell(\ell-1)$. Now, we consider the following sets:

$$S_1 = \left\{a, b \in \mathbb{F}_\ell^* \mid \mathrm{ord}\,(a) > \ell^\varepsilon,\ \mathrm{ord}\,(b) > \ell^\varepsilon,\ \mathrm{ord}\,(ab^{-1}) > \ell^\varepsilon\right\},$$
$$S_2 = \left\{\lambda \in \mathbb{F}_{\ell^2}^* \setminus \mathbb{F}_\ell^* \mid \mathrm{ord}\,(\lambda) = \mathrm{ord}\,(\lambda^\ell) > \ell^\varepsilon,\ \mathrm{ord}\,(\lambda^{\ell-1}) > \ell^\varepsilon\right\},$$

and realize that $|C| = \frac{1}{2}((\ell+1)\ell|S_1| + \ell(\ell-1)|S_2|)$. This reduced to the problem of estimating S_1 and S_2. Let us first estimate S_1. Take σ to be a generator of $\mathbb{F}_\ell^*$. For any divisor d of $\ell-1$, the set of all elements of $\mathbb{F}_\ell^*$ having order exactly d is of the form $\sigma^{\frac{\ell-1}{d}i}$ with $(i,d) = 1$. In particular, the number of elements of $\mathbb{F}_\ell^*$ with order greater than ℓ^ε is given by

$$\sum_{\substack{d \mid \ell-1 \\ d > \ell^\varepsilon}} \phi(d) = \ell + O\left(\sum_{\substack{d \mid \ell-1 \\ d < \ell^\varepsilon}} \phi(d)\right) = \ell + O\left(\ell^\varepsilon d(\ell-1)\right) = \ell + O_\varepsilon\left(\ell^{2\varepsilon}\right),$$

where $d(\cdot)$ is the divisor function, and here we are using the well known upper bound on divisor function (see [20]) for any prime ℓ large enough. Now note that $\mathrm{ord}\left(ab^{-1}\right) < \ell^\varepsilon$ implies that ab^{-1} belongs to a set with only $\sum_{k \mid \ell-1, k < \ell^\varepsilon} \phi(k)$ many elements. By the argument above, this set has only $O_\varepsilon\left(\ell^{2\varepsilon}\right)$ many elements. This observation implies that

$$\left|\left\{a, b \in \mathbb{F}_\ell^* \mid \mathrm{ord}\,(a),\ \mathrm{ord}\,(b), \mathit{or}\ \mathrm{ord}\,(ab^{-1}) < \ell^\varepsilon\right\}\right| = O_\varepsilon(\ell^{2\varepsilon+1}).$$

In particular, we then have $|S_1| = \ell^2 + O_\varepsilon(\ell^{2\varepsilon+1})$.

Let us now estimate $|S_2|$. Take τ to be a generator of $\mathbb{F}_{\ell^2}^*$, then any $\lambda \in S_2$, of order d, is of the form $\tau^{\frac{\ell^2-1}{d}i}$, with $(i,d) = 1$. We also have an order restriction on $\lambda^{\ell-1}$, which implies that $\frac{d}{(d,\ell-1)} > \ell^\varepsilon$. Hence,

$$|S_2| = \sum_{\substack{d \mid \ell^2-1 \\ \frac{d}{(d,\ell-1)} > \ell^\varepsilon}} \phi(d) = \ell^2 + O\Bigg(\sum_{\substack{d \mid \ell^2-1 \\ \frac{d}{(d,\ell-1)} < \ell^\varepsilon}} \phi(d)\Bigg).$$

Note that, the condition $\frac{d}{(d,\ell-1)} < \ell^\varepsilon$ implies that $d < \ell^{\varepsilon+1}$. Therefore,

$$\sum_{\substack{d \mid \ell^2-1 \\ \frac{d}{(d,\ell-1)} < \ell^\varepsilon}} \phi(d) \leq \ell^{\varepsilon+1} d(\ell^2-1) = O_\varepsilon\left(\ell^{1+3\varepsilon}\right).$$

Therefore, the required density is at least

$$\frac{1}{2}(\ell-1)\ell\frac{|S_1|}{|\mathrm{GL}_2\left(\mathbb{F}_\ell\right)|} + \frac{1}{2}(\ell+1)\ell\frac{|S_2|}{|\mathrm{GL}_2\left(\mathbb{F}_\ell\right)|} = 1 + O_\varepsilon\left(\frac{1}{\ell^{1-3\varepsilon}}\right).$$

□

5.2 Proof of Theorem 5

Let $\rho_{f,\ell} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_{2r}\left(\mathbb{F}_\ell\right)$ be the map defined by

$$\sigma \mapsto \begin{pmatrix} \rho_{f_{1,\ell}}(\sigma) & & & \\ & \rho_{f_{2,\ell}}(\sigma) & & \\ & & \ddots & \\ & & & \rho_{f_{r,\ell}}(\sigma) \end{pmatrix}.$$

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 in $\mathbb{F}_\ell^*$. Due to [21, Theorem 3.1], we may assume that for any prime ℓ large enough, the image of each $\rho_{f_{i,\ell}}$ is $\Delta_1^{(k-1)}(\ell)$, which coincides with the set of matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose determinants are a $(k-1, \ell-1)$th power in $\mathbb{F}_\ell^*$. If the image of $\rho_{f,\ell}$ is not exactly $\Delta_r^{(k-1)}(\ell)$, then by [19, Lemma 5.1] we get a set of quadratic characters $\{\chi_{i,j,\ell}\}_{1\le i,j\le r}$ of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ such that

$$\rho_{f_i,\ell}\left(\mathrm{Frob}_p\right) \text{ is conjugate to } \chi_{i,j,\ell}\left(\mathrm{Frob}_p\right)\rho_{f_j,\ell}\left(\mathrm{Frob}_p\right) \text{ in } \mathrm{GL}_2(\mathbb{F}_\ell),$$

for all $1 \le i, j \le r$. In particular, $a_i(p) = \pm a_j(p) (\mathrm{mod}\ \ell)$, for all $1 \le i, j \le r$, and any prime $p \nmid N\ell$. This implies that $\alpha_\ell^{(i,p)} + \beta_\ell^{(i,p)} = \pm(\alpha_\ell^{(j,p)} + \beta_\ell^{(j,p)})$. Moreover, we also know that

$$\alpha_\ell^{(i,p)}\beta_\ell^{(i,p)} = \alpha_\ell^{(j,p)}\beta_\ell^{(j,p)} = p^{k-1} \,(\mathrm{mod}\ \ell).$$

In particular, this means that

$$\{\alpha_\ell^{(i,p)}, \beta_\ell^{(i,p)}\} = \pm\{\alpha_\ell^{(j,p)}, \beta_\ell^{(j,p)}\}, \forall 1 \le i, j \le r, \text{and for any prime } p \nmid N\ell. \tag{39}$$

Due to GST, for a positive density of primes p, none of these

$$\{\alpha^{(i,p)}\beta^{-(j,p)}\}_{1\le i,j\le 2} \quad \text{or} \quad \pm\{\alpha^{(i,p)}, \alpha^{-(j,p)}\}_{1\le i\ne j\le 2}$$

are roots of unity. For those primes p, following the arguments in the proof of Lemma 10, and considering the set in (34), each element of the set $\{\alpha_\ell^{(i,p)}\beta_\ell^{-(j,p)}\}_{1\le i,j\le 2}$ has order larger than 4 except for finitely many primes ℓ. We then have a contradiction to (39), and hence we may assume that the image of $\rho_{f,\ell}$ is indeed $\Delta_r^{(k-1)}(\ell)$ for any prime ℓ large enough.

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 union of conjugacy classes of elements in $\Delta_r^{(k-1)}(\ell)$ whose eigenvalues satisfy the conditions of Theorem 1. Note that any tuple $(a_1, a_2, \cdots, a_{2r}) \in (\mathbb{F}_\ell^*)^{2r}$ with $\mathrm{ord}\,(a_i) > \ell^\varepsilon$, $\mathrm{ord}\,(a_i a_j^{-1}) > \ell^\varepsilon, \forall i \ne j$ and $a_i a_{i+1} = a_j a_{j+1}, \forall i, j$ odd, satisfies that $\prod_{i,\text{ odd}} C_{a_i, a_{i+1}} \subseteq C_r^{k-1}(\ell)$. We call these tuples *nice* and we want to count them. First of all note that,

$$\{(a_1, a_2, \cdots, a_{2r}) \in (\mathbb{F}_\ell^*)^{2r} \mid a_i a_{i+1} = a_j a_{j+1}, \forall i, j \text{ odd}\} = \frac{(\ell-1)^{r+1}}{(\ell-1, k-1)}.$$

On the other hand, for any $(k-1)$th power λ in $\mathbb{F}_\ell^*$, note that $ab = \lambda$ and $\mathrm{ord}\,(ab^{-1}) < \ell^\varepsilon$ imply $\mathrm{ord}\,(a^2\lambda^{-1}) < \ell^\varepsilon$. From the proof of Theorem 4, for a fixed λ, the number of such a

is $O_\varepsilon(\ell^{2\varepsilon})$. Moreover, $\operatorname{ord}(a) < \ell^\varepsilon$ or $\operatorname{ord}(b) < \ell^\varepsilon$ holds for only $O_\varepsilon(\ell^{2\varepsilon})$ many elements a or b. In particular, the number of tuples that does not come into our consideration is

$$\sum_{\lambda,\ (k-1)\text{th power}} O_\varepsilon(\ell^{r-1+2\varepsilon}) = O_\varepsilon\left(\frac{\ell^{r+2\varepsilon}}{(k-1, \ell-1)}\right).$$

In particular, we then have

$$\begin{aligned} |C_r^{k-1}(\ell)| &\geq \sum_{(a_1,a_2,\cdots,a_r)\ \text{nice}} \left(\prod_{i\ \text{odd}} |C_{a_i,a_{i+1}}|\right) \\ &= \left(\frac{\ell(\ell+1)}{2}\right)^r \left(\frac{(\ell-1)^{r+1}}{(\ell-1, k-1)} + O_\varepsilon\left(\frac{\ell^{r+2\varepsilon}}{(k-1,\ell-1)}\right)\right). \end{aligned} \tag{40}$$

The extra factor $\left(\frac{\ell(\ell+1)}{2}\right)^r$ is coming because each conjugacy class $C_{a_{i,i+1}}$ has $\ell(\ell+1)$ many elements and taking into consideration that $C_{a_i,a_{i+1}} = C_{a_{i+1},a_i}, \forall i$ odd, the extra factor $\frac{1}{2}$ is coming for each component. The proof is now complete because $|\Delta_r^{(k-1)}(\ell)| = \left(\frac{|\mathrm{GL}_2(\mathbb{F}_\ell)|}{\ell-1}\right)^r \frac{\ell-1}{(\ell-1,k-1)}$. □

6 Impact on Waring-type problems

In the present section we combine Theorem 1 with classical analytical tools to prove that a linear recurrence sequence $\{s_n\}$ is an additive basis over prime fields, under some assumptions. Moreover, we discuss about the advantages of nontrivial exponential sums obtained in Theorem 1 to prove it.

6.1 Waring-type problems with linear recurrence sequences

Let $\{s_n\}$ be a nonzero linear recurrence sequence modulo ℓ as in (2) with order r, period τ and $(a_0, \ell) = 1$. Given an integer $k \geq 2$, for any residue class $\lambda (\operatorname{mod} \ell)$, we denote by $T_k(\lambda)$ the number of solutions of the congruence

$$s_{n_1} + \cdots + s_{n_k} \equiv \lambda \,(\operatorname{mod} \ell), \quad \text{with} \quad 1 \leq n_1, \ldots, n_k \leq \tau.$$

Then, writing $T_k(\lambda)$ in terms of exponential sums, we get

$$T_k(\lambda) = \frac{1}{\ell}\sum_{\xi=0}^{\ell-1}\sum_{n_1\leq\tau}\cdots\sum_{n_k\leq\tau} \mathbf{e}_\ell\left(\xi(s_{n_1}+\cdots+s_{n_k}-\lambda)\right).$$

Taking away the term $\xi = 0$ and using triangle inequality, it is clear that

$$\begin{aligned} \left|T_k(\lambda) - \frac{\tau^k}{\ell}\right| &= \frac{1}{\ell}\left|\sum_{\xi=1}^{\ell-1}\sum_{n_1\leq\tau}\cdots\sum_{n_k\leq\tau} \mathbf{e}_\ell\left(\xi(s_{n_1}+\cdots+s_{n_k}-\lambda)\right)\right| \\ &\leq \frac{1}{\ell}\sum_{\xi=1}^{\ell-1}\left|\sum_{n_1\leq\tau}\cdots\sum_{n_k\leq\tau} \mathbf{e}_\ell\left(\xi(s_{n_1}+\cdots+s_{n_k})\right)\right| \\ &\leq \frac{1}{\ell}\sum_{\xi=1}^{\ell-1}\left(\left|\sum_{n_1\leq\tau}\mathbf{e}_\ell\left(\xi s_{n_1}\right)\right|\cdots\left|\sum_{n_k\leq\tau}\mathbf{e}_p\left(\xi s_{n_k}\right)\right|\right) \\ &\leq \left(\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n\leq\tau}\mathbf{e}_\ell\left(\xi s_n\right)\right|\right)^k. \end{aligned} \tag{41}$$

Assume that we have an exponential sum bound of the type

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi s_n\right) \right| \le R. \tag{42}$$

Then, combining (41) and (42) we get $\left|T_k(\lambda) - \frac{\tau^k}{\ell}\right| \le R^k$. Now, if $(R/\tau)^k \ell$ goes to zero as $\ell \to \infty$, we obtain an effective asymptotic formula for $T_k(\lambda)$. In particular, $T_k(\lambda) > 0$ for ℓ large enough. For instance, if $\tau \ge \ell^{r/2+\varepsilon}$ we employ Korobov's bound (3) with $R = \ell^{r/2}$ to get

$$\left| T_k(\lambda) - \frac{\tau^k}{\ell} \right| \le \frac{\tau^k}{\ell}\left((\ell^{r/2}/\tau)^k \ell \right) \le \frac{\tau^k}{\ell}\left(\ell^{1-k\varepsilon} \right),$$

therefore $T_k(\lambda) = \frac{\tau^k}{\ell}(1 + o(1))$ for $k > 1/\varepsilon$ in the range $\tau \ge \ell^{r/2+\varepsilon}$. If the characteristic polynomial $\omega(x)$ of $\{s_n\}$ is irreducible with $\deg(\omega) \ge 2$ and the least period τ satisfies $\gcd(\tau, \ell^d - 1) < \tau \ell^{-\varepsilon}$ for any divisor $d < r$ of r, then by Corollary 6 we choose $R = \tau \ell^{-\delta}$ for some positive $\delta = \delta(\varepsilon)$, to get

$$\left| T_k(\lambda) - \frac{\tau^k}{\ell} \right| \le \frac{\tau^k}{\ell}\left((\tau \ell^{-\delta}/\tau)^k \ell \right) = \frac{\tau^k}{\ell}\left(\ell^{1-k\delta} \right).$$

Thus, $T_k(\lambda) > 0$ when $k > 1/\delta$ and $\max_{\substack{d<r\\ d|r}} \gcd(\tau, \ell^d - 1) < \tau \ell^{-\varepsilon}$. Let us summarize the above discussion in the form of following corollary.

Corollary 12 *Let ℓ be a prime number, $k > 0$ be any integer, $\varepsilon > 0$, and $\{s_n\}$ be a linear recurrence sequence of order $r \ge 2$ in $\mathbb{F}_\ell$. If the characteristic polynomial $\omega(x)$ in $\mathbb{F}_\ell[x]$ is irreducible with $(\omega(0), \ell) = 1$, the least period τ satisfies*

$$\max_{\substack{d<r\\ d|r}}(\tau, \ell^d - 1) < \tau \ell^{-\varepsilon},$$

and for every integer λ, let $T_k(\lambda)$ denote the number of solutions of the congruence

$$s_{n_1} + \cdots + s_{n_k} \equiv \lambda \pmod{\ell}, \quad \text{with} \quad 1 \le n_1, \ldots, n_k \le \tau,$$

then there exists an integer $k_0 > 0$ such that for any $k \ge k_0$, $T_k(\lambda) = \frac{\tau^k}{\ell}(1 + o(1))$.

We are now ready to prove the main result of this section.

Theorem 13 *Let $\{s_n\}$ be a linear recurrence sequence in $\mathbb{Z}$, whose characteristic polynomial $\omega(x) \in \mathbb{Z}[x]$ is monic, irreducible, and having prime degree. Then for a set of primes ℓ with positive density, the sequence $\{s_n\}$ is an additive basis modulo ℓ. More precisely, there exists an absolute constant c such that the Waring-type congruence*

$$s_{n_1} + \cdots + s_{n_c} \equiv \lambda \pmod{\ell}$$

is solvable for any residue class $\lambda \pmod{\ell}$.

Proof Let $\mathbb{Q}_\omega$ denote the splitting field of ω and G_ω be $\mathrm{Gal}\,(\mathbb{Q}_\omega/\mathbb{Q})$. Note that $\deg(\omega)$ divides $|G_\omega|$ and G_ω is contained in the symmetric group $S_{\deg(\omega)}$. By the Cauchy's theorem, there exists an element in G_ω of order $\deg(\omega)$. In particular, there is a $\deg(\omega)$-cycle in G_ω because $\deg(\omega)$ is prime. By Chebotarev's density theorem, the set of such primes ℓ for which $\omega(x) \pmod{\ell}$ is irreducible, have positive density, see Theorem of Frobenius in [26, Page 11]. We are now interested to work with these primes.

Let α be a root of $\omega(x)(\bmod \ell)$, and τ be the period of sequence $\{s_n\}(\bmod \ell)$. We then have $\tau = \operatorname{ord}(\alpha)$. Since $\omega(x)(\bmod \ell)$ is irreducible, one can write

$$\omega(x)(\bmod \ell) = \prod_{i=0}^{\deg(\omega)-1} \left(x - \alpha^{\ell^i}\right),$$

and in particular, $\omega(0)(\bmod \ell) = (-\alpha)^{1+\ell+\ell^2+\dots+\ell^{\deg(\omega)-1}}$. Note that $(\omega(0), \ell) = 1$, for all but finitely many primes ℓ. We now need to verify the condition of Corollary 12 for $d = 1$ because $\deg(\omega)$ is prime. Observe that $\gcd(\operatorname{ord}\alpha, \ell - 1) = \frac{\operatorname{ord}\alpha}{\operatorname{ord}\alpha^{\ell-1}}$. Fix any $0 < \varepsilon < 1/2$, and now the proof is complete if $\operatorname{ord}\left(\alpha^{\ell-1}\right) > \ell^{\varepsilon}$ holds for almost all primes ℓ.

For any integer t, we have the following

$$\alpha^{(\ell-1)t} = 1 \implies \alpha^{rt} = \left(\prod_{i=0}^{r-1} \alpha^{\ell^i}\right)^t \implies \alpha^{2rt} = \omega(0)^{2t}.$$

In particular, α is a root of both $\omega(x)(\bmod \ell)$ and $\prod_{t \le T}\left(x^{2rt} - \omega(0)^{2t}\right)(\bmod \ell)$.

Now, given a large positive parameter T, we consider the resultant

$$R(T) = \operatorname{Res}\left(\omega(x), \prod_{t \le T}\left(x^{2rt} - \omega(0)^{2t}\right)\right).$$

Counting the number of distinct prime factors of the resultant as in the proof of Lemma 7, we see that $|\{\ell \text{ prime} \mid \operatorname{ord}(\alpha^{\ell-1}) \le T\}| = O(T^2)$. For any large $y > 0$, taking $T = y^{\varepsilon}$, we see that there exists a δ such that

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi s_n\right) \right| \le \tau \ell^{-\delta}$$

holds, for at least $c_\omega \pi(y) + O(y^{2\varepsilon})$ many primes $\ell \le y$, for some constant (which depends only on ω) $c_\omega > 0$. Now, the proof follows immediately from Corollary 12. □

For further explanation, one can consider the following example.

Example 14 Consider the classical case of Fibonacci sequence $\{F_n\}$. In the beginning of this section, the result of the third author is discussed for this special case. We can however get a slightly weaker result from Corollary 12. In this case, the characteristic polynomial is $x^2 - x - 1$. It is of course a monic, irreducible and of a prime degree. This polynomial is irreducible modulo prime ℓ, iff we have the Legendre symbol $\left(\frac{5}{\ell}\right) = -1$. The set of such primes have density 1/2. Corollary 12 says, for almost all of these primes, $\{F_n\}$ is an additive basis modulo ℓ. For the other set of primes, we use Lemma 7. Given any $0 < \varepsilon < 1/2$, for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \le y$, we have

$$\operatorname{ord}\alpha_\ell > \ell^{\varepsilon}, \qquad \operatorname{ord}\beta_\ell > \ell^{\varepsilon} \quad \text{and} \quad \operatorname{ord}\left(\alpha_\ell \beta_\ell^{-1}\right) > \ell^{\varepsilon},$$

where α_ℓ and β_ℓ are the roots of $x^2 - x - 1(\bmod \ell)$. It then follows from [2, Corollary, page 479] that there exists a $\delta = \delta(\varepsilon) > 0$ such that

$$\max_{\substack{(c,d) \in \mathbb{F}_\ell \times \mathbb{F}_\ell \\ (c,d) \ne (0,0)}} \left| \sum_{n \le \ell - 1} \mathbf{e}_\ell\left(c\alpha^n + d\beta^n\right) \right| \le \ell^{1-\delta}.$$

In particular, we then have

$$\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n\le\tau}\mathbf{e}_\ell\left(\xi F_n\right)\right|\le\tau\ell^{-\delta},$$

which guarantees the existence of an absolute constant, as we saw in the proof of Theorem 13. With this, we have an inexplicit result for the Fibonacci sequences compared to what the third author had in [11]. However, Theorem 13 provides a general result for a large class of linear recurrence sequences.

6.2 Waring-type problems for modular forms

Let us recall our discussion from the introduction about Waring problem for modular forms. In this section, we are assuming that the modular form is a newform without *CM*. Fix any $0<\varepsilon<\frac{1}{2}$, say $\varepsilon=\frac{1}{3}$. Then taking $\delta:=\delta(\varepsilon)$ as in Theorem 2, the following estimate

$$\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n\le\tau}\mathbf{e}_\ell\left(\xi a(p^n)\right)\right|\le\tau\ell^{-\delta},$$

holds for almost all primes p and ℓ. The discussion in Sect. 6.1 shows that $T_s(\lambda)>0$ for any $\lambda\in\mathbb{F}_\ell$, and $s>1/\delta$, where $T_s(\lambda)$ is the number of solutions of the congruence

$$a(p^{n_1})+\cdots+a(p^{n_s})\equiv\lambda\ (\mathrm{mod}\ \ell),\quad \text{with}\quad 1\le n_1,\ldots,n_s\le\tau.$$

Moreover, this s does not depend on the choice of the eigenform because δ does not. More precisely, we have the following result.

Corollary 15 *Let f be a newform without CM and with rational Fourier coefficients. We say, a proposition $\mathcal{Q}_f(p,\ell,s)$ is true if and only if, any element of $\mathbb{F}_\ell$ can be written as a sum of at most s elements of the set $\{a(p^n)\}_{n\ge0}$. Then, there is an absolute constant s_0 such that $\mathcal{Q}_f(p,\ell,s_0)$ is true for almost all primes p and ℓ. Moreover, s_0 does not depend on the choice of f.*

As an immediate consequence of Theorem 4, we obtain the following result.

Corollary 16 *Suppose the newform is without CM and with integer Fourier coefficients. Then there exists an absolute constant s_0 such that, for any large prime ℓ satisfying the coprimality condition $(\ell-1,k-1)=1$, the proposition $\mathcal{Q}_f(p,\ell,s_0)$ is true for a set of primes p with density at least $1+O\left(\frac{1}{\sqrt{\ell}}\right)$. Moreover, s_0 does not depend on the choice of f.*

6.3 Bound of non-linearity of a linear recurrence sequence

Let $\{s_n\}$ be a linear recurrence sequence modulo ℓ as in (2) with order r, $(a_0,\ell)=1$ and period τ. For $0\le b\le\ell^r-1$, let us define the sum

$$W(b)=\sum_{n\le\tau}\mathbf{e}_\ell\left(s_n+\langle b,n\rangle\right),$$

where $\langle b,n\rangle$ denotes the inner product $\langle b,n\rangle=b_0n_0+\cdots+b_{r-1}n_{r-1}$ assuming that $0\le b,n\le\ell^r-1$ are written in its ℓ–ary expansion

$$b=b_0+b_1\ell+\cdots+b_{r-1}\ell^{r-1},\qquad n=n_0+n_1\ell+\cdots+n_{r-1}\ell^{r-1}.$$

Bounds for $W(b)$ have cryptographic significance, see [25] and references therein. Shparlinski and Winterhof [25, Theorem 1] proved that

$$\max_{0\leq b\leq \ell^r-1} |W(b)| \ll \tau^{3/4} r^{1/4} \ell^{r/8},$$

whenever the characteristic polynomial of $\{s_n\}$ is irreducible. Such bound is asymptotically effective if $r\ell^{r/2}/\tau \to 0$. Combining Corollary 6 and the ideas of [25], we are able to improve such bound for a large class of linear recurrence sequences in the range $\tau > \ell^{\varepsilon}$. For example, assuming hypothesis of Corollary 6, if r is fixed then $|W(b)| \ll \tau \ell^{-\delta'}$ as $\ell \to \infty$ for some $\delta' > 0$. In general, we get $|W(b)| = o(\tau)$ if $r \log \ell/\ell^{\delta'} \to 0$ as $\ell \to \infty$. More precisely,

Corollary 17 *Let ℓ 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 $\mathbb{F}_\ell[x]$ is irreducible polynomial with $(f(0), \ell) = 1$, and the least period τ satisfies*

$$\tau > \ell^{\varepsilon}, \quad \text{and} \quad \max_{\substack{d<r\\ d|r}}(\tau, \ell^d - 1) < \tau \ell^{-\varepsilon},$$

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

$$\max_{0\leq b\leq \ell^r-1} \left|\sum_{n\leq\tau} \mathbf{e}_\ell\left(s_n + \langle b, n\rangle\right)\right| \leq \tau \ell^{-\delta/4}(r\log \ell)^{1/4}\left(1 + \ell^{-\delta/4}(r\log\ell)^{1/4}\right).$$

Proof The proof follows the same steps as given in [25, Theorem 1]. We just need to employ the bound given by Corollary 6 instead of Korobov's bound. □

Note. We have an improvement on the bound [25, Theorem 1] , if $\tau \leq \frac{\ell^{r/2+\delta}}{\log \ell}$. Clearly there are many such cases, for instance, one can consider any element in $\mathbb{F}_\ell^*$ of order smaller than $\ell^{\frac{1}{2}}$.

Acknowledgements
Authors would like to thank Igor Shparlinski for useful suggestions through personal communications and Will Sawin for helpful comments through MathOverflow, during the writing of the article. In addition, authors would like to thank University of Göttingen, 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 supported by the ERC Consolidator grants 648329 (codename GRANT, with H. Helfgott as PI) and 681207 (codename GrDyAP, with A. Thom as PI), the second author is supported by the ERC Consolidator grant 648329 and the third author was supported by Project CB005-16 UAM-A.

Funding Open Access funding enabled and organized by Projekt DEAL.

Author details
[1]Max-Planck-Institut für Mathematik Bonn, Germany, [2]Mathematisches Institut, Georg-August-Universität Göttingen, Göttingen, Germany, [3]Universidad Autónoma Metropolitana, CDMX(Mexico city), Mexico.

Received: 28 December 2020 Accepted: 13 January 2022 Published online: 22 February 2022

References
1. Barnet-Lamb, T., Geraghty, D., Harris, M., Taylor, R.: A family of Calabi–Yau varieties and potential automorphy II. Publ. Res. Inst. Math. Sci. **47**(1), 29–98 (2011)
2. Bourgain, J.: Mordell's exponential sum estimate revisited. J. Am. Math. Soc. **18**(2), 477–499 (2005)
3. Bourgain, J., Chang, M.-C.: A Gauss sum estimate in arbitrary finite fields. C. R. Math. Acad. Sci. Paris **342**(9), 643–646 (2006)
4. Bourgain, J., Glibichuk, A.A., Konyagin, S.V.: Estimates for the number of sums and products and for exponential sums in fields of prime order. J. Lond. Math. Soc. (2) **73**(2), 380–398 (2006)
5. Diamond, F., Shurman, J.: A first course in modular forms, volume 228 of Graduate Texts in Mathematics. Springer, New York (2005)

6. Erdős, P., Murty, M.R.: On the order of $a(\bmod p)$. In: Number theory (Ottawa, ON, 1996), volume 19 of CRM Proc. Lecture Notes, pp. 87–97. Amer. Math. Soc., Providence (1999)
7. Everest, G., van der Poorten, A., Shparlinski, I., Ward, T.: Recurrence sequences, volume 104 of Mathematical Surveys and Monographs. American Mathematical Society, Providence (2003)
8. Ferraguti, A.: Galois representation attached to type $(1, \chi)$ modular forms. (2011)
9. Garaev, M.Z.: 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. Garaev, M.Z., García, V.C., Konyagin, S.V.: The Waring problem with Ramanujan's τ-function. Izv. Ross. Akad. Nauk Ser. Mat. **72**(1), 39–50 (2008)
11. García, V.C.: On the distribution of sparse sequences in prime fields and applications. J. Théor. Nombres Bordeaux **25**(2), 317–329 (2013)
12. García, V.C., Nicolae, F.: Additive bases with coefficients of newforms. Forum Math. **30**(5), 1079–1087 (2018)
13. Glibichuk, A.A.: Combinatorial properties of sets of residues modulo a prime and the Erdös–Graham problem. Mat. Zametki **79**(3), 384–395 (2006)
14. Katz, N.M.: Gauss sums, Kloosterman sums, and monodromy groups, volume 116 of Annals of Mathematics Studies. Princeton University Press, Princeton (1988)
15. Korobov, N.M.: 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
16. Korobov, N.M.: The distribution of non-residues and of primitive roots in recurrence series. Doklady Akad. Nauk SSSR (N.S.) **88**, 603–606 (1953)
17. Kowalski, E.: Exponential sums over finite fields: elementary methods. https://people.math.ethz.ch/~kowalski/exponential-sums-elementary.pdf (2021)
18. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge (1986)
19. Masser, D.W., Wüstholz, G.: Galois properties of division fields of elliptic curves. Bull. Lond. Math. Soc. **25**(3), 247–254 (1993)
20. Murty, M.R.: Problems in analytic number theory, volume 206 of Graduate Texts in Mathematics. Readings in Mathematics. 2nd ed. Springer, New York (2008)
21. Ribet, K.A.: On l-adic representations attached to modular forms. II. Glasgow Math. J. **27**, 185–194 (1985)
22. Serre, J.-P.: 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
23. Shparlinski, I.E.: Bounds of Gauss sums in finite fields. Proc. Am. Math. Soc. **132**(10), 2817–2824 (2004)
24. Shparlinski, I.E.: On the value set of the Ramanujan function. Arch. Math. (Basel) **85**(6), 508–513 (2005)
25. Shparlinski, I.E., Winterhof, A.: On the nonlinearity of linear recurrence sequences. Appl. Math. Lett. **19**(4), 340–344 (2006)
26. Stevenhagen, P., Lenstra, H.W., Jr.: Chebotarëv and his density theorem. Math. Intelligencer **18**(2), 26–37 (1996)
27. Thorner, J.: Effective forms of the Sato–Tate conjecture. arXiv (2020)

Publisher's Note