

# ON THE EXPONENTIAL LARGE SIEVE INEQUALITY FOR SPARSE SEQUENCES MODULO PRIMES

MEI-CHU CHANG, BRYCE KERR, AND IGOR E. SHPARLINSKI

ABSTRACT. We complement the argument of M. Z. Garaev (2009) with several other ideas to obtain a stronger version of the large sieve inequality with sparse exponential sequences of the form  $\lambda^{s_n}$ . In particular, we obtain a result which is non-trivial for monotonically increasing sequences  $\mathcal{S} = \{s_n\}_{n=1}^\infty$  provided  $s_n \leq n^{2+o(1)}$ , whereas the original argument of M. Z. Garaev requires  $s_n \leq n^{15/14+o(1)}$  in the same setting. We also give an application of our result to arithmetic properties of integers with almost all digits prescribed.

## 1. INTRODUCTION

The classical large sieve inequality, giving upper bounds on average values of various exponential and similar Dirichlet polynomials, such as

$$\sum_{q=1}^Q \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^q \left| \sum_{s=1}^S \alpha_s \exp(2\pi ias/q) \right|^2 \quad \text{and} \quad \sum_{q=1}^Q \sum_{\substack{\chi \bmod q \\ \chi \text{ prim.}}} \left| \sum_{s=1}^S \alpha_s \chi(s) \right|^2,$$

with primitive multiplicative characters  $\chi$  modulo  $q$  and arbitrary complex weights  $\{\alpha_s\}_{n=1}^S$ , has proved to be an extremely useful and versatile tool in analytic number theory and harmonic analysis, see, for example, [13, 17, 18].

Furthermore, if the weights  $\alpha_s$  are supported only on elements of some sequence  $\mathcal{S} = \{s_n\}_{n=1}^T$ , which naturally occurs in many number theoretic applications, then the above sums can be written as

$$(1.1) \quad \sum_{q=1}^Q \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^q \left| \sum_{n \leq T} \gamma_n \mathbf{e}_q(s_n) \right|^2 \quad \text{and} \quad \sum_{q=1}^Q \sum_{\substack{\chi \bmod q \\ \chi \text{ prim.}}} \left| \sum_{n \leq T} \gamma_n \chi(s_n) \right|^2,$$

where  $\gamma_n = \alpha_{s_n}$  and

$$\mathbf{e}_q(z) = \exp(2\pi iz/q).$$

---

2010 *Mathematics Subject Classification.* 11L07, 11N36.

*Key words and phrases.* exponential sums, sparse sequences, large sieve.

However, the power of general bounds rapidly diminishes when the sequence  $\mathcal{S}$  becomes sparse.

Partially motivated by this phenomenon, and partially by applications to Mersenne numbers, Garaev and Shparlinski [10, Theorem 3.1] have introduced a modification of the large sieve, for both exponential and Dirichlet polynomials with arguments that contain exponentials from extremely sparse sequences.

In particular, in the setting of [10], the arguments of the exponentials and characters appearing in (1.1) contain exponential functions  $\lambda^{s_n}$  with elements of  $\mathcal{S}$  rather than the elements of  $\mathcal{S}$  themselves. In the case of exponential polynomials, Garaev [9] has introduced a new approach, which has led to a stronger version of the exponential large sieve inequality, improving some of the results of [10], see also [1, Lemma 2.11] and [22, Theorem 1] for several other bounds of this type. Furthermore, stronger versions of the exponential large sieve inequality for special sequences  $\mathcal{S}$ , such as  $T$  consecutive integers or the first  $T$  primes, can also be found in [1, 10], with some applications given in [21].

Here we continue this direction and concentrate on the case of general sequences  $\mathcal{S}$  without any arithmetic restriction. We introduce several new ideas which allow us to improve some results of Garaev [9]. For example, we make use of the bound of [15, Theorem 5.5] on exponential sums over small multiplicative subgroups modulo  $p$ , which hold for almost all primes  $p$ , see Lemma 3.2. We also make the method more flexible so it now applies to much sparser sequences  $\mathcal{S}$  than in [9]. We believe these ideas may find more applications in similar problems.

More precisely, let us fix some integer  $\lambda \geq 2$ . For each prime number  $p$ , we let  $t_p$  denote the order of  $\lambda \pmod p$ . For real  $X$  and  $\Delta$  we define the set

$$\mathcal{E}_\Delta(X) = \{p \leq X : t_p \geq \Delta\}.$$

Note that by a result of Erdős and Murty [8], see also (2.8), for  $\Delta = X^{1/2}$ , almost all primes  $p \leq X$  belong to  $\mathcal{E}_\Delta(X)$ .

For integer  $T$  and two sequences of complex weights  $\Gamma = \{\gamma_n\}_{n=1}^T$  and integers  $\mathcal{S} = \{s_n\}_{n=1}^T$  we define the sums

$$V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) = \sum_{p \in \mathcal{E}_\Delta(X)} \max_{\gcd(a,p)=1} \left| \sum_{n \leq T} \gamma_n \mathbf{e}_p(a\lambda^{s_n}) \right|^2.$$

These sums majorize the ones considered by Garaev [9] where each term is divided by the divisor function  $\tau(p-1)$  of  $p-1$ . Here we obtain a new bound of the sums  $V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta)$  which in particular improves some bounds of Garaev [9].

The argument of Garaev [9] reduces the problem to bounding Gauss sums for which he uses the bound of Heath-Brown and Konyagin [12], that is, the admissible pair (2.1), which is defined below. In particular, for  $V_\lambda(\Gamma, \mathcal{S}; T, X, X^{1/2})$  the result of Garaev [9] is nontrivial provided

$$(1.2) \quad S \leq X^{15/14+o(1)}.$$

Our results by-pass significantly the threshold (1.2) and allow us to replace 15/14 with any fixed  $\vartheta < 2$ .

Our improvement is based on a modification of the argument of Garaev [9] which allows us to use the bounds of short sums with exponential functions, given in [15, Theorem 5.5], see also Lemma 3.2 below. This alone allows us to extend the result of [9] to sparse sequences  $\mathcal{S}$ , roughly growing at most  $s_n \leq n^{7/6-\varepsilon}$  for any fixed  $\varepsilon > 0$  in the same scenario where the result of [9] limits the growth to  $s_n \leq n^{15/14-\varepsilon}$ . Furthermore, using bounds of exponential sums over small subgroups of finite fields, in particular that of Bourgain, Glibichuk and Konyagin [5] we relax the condition on  $\mathcal{S}$  to  $s_n \leq n^{3/2-\varepsilon}$ .

Using a different argument which combines a bound of Bourgain and Chang [4] for Gauss sums modulo a product of two primes with a duality principle for bilinear forms, we obtain another, although less explicit bound which allows the elements to grow as fast as  $s_n \leq n^{2-\varepsilon}$ . Furthermore, for this result we do not need to limit the summation to primes from  $\mathcal{E}_\Delta(X)$  but can consider all primes from  $p \leq X$ , in which case we denote

$$V_\lambda(\Gamma, \mathcal{S}; T, X) = \sum_{p \in X} \max_{\gcd(a,p)=1} \left| \sum_{n \leq T} \gamma_n \mathbf{e}_p(a\lambda^{s_n}) \right|^2.$$

We also give an application of our new estimate to investigating arithmetic properties of integers with almost all digits prescribed in some fixed base. To simplify the exposition, we only consider binary expansions (and hence we talk about bits rather than binary digits). Namely, for an integer  $S \geq 1$ , an  $S$ -bit integer  $a$  and a sequence of integers  $\mathcal{S} = \{s_n\}_{n=1}^T$  with  $0 \leq s_1 < \dots < s_T \leq S$ , we denote by  $\mathcal{N}(a; \mathcal{S})$  the set of  $S$ -bit integers  $z$  whose bits on all positions  $j = 1, \dots, S$  (counted from the right) must agree with those of  $a$  except maybe when  $j \in \mathcal{S}$ .

We first recall that Bourgain [2, 3] has recently obtained several very strong results about the distribution of prime numbers among the elements of  $\mathcal{N}(a; \mathcal{S})$ , see also [11]. However, in the setting of the strongest result in this direction from [3], the set  $\mathcal{S}$  of “free” positions has to be very massive, namely its cardinality has to satisfy  $T \geq (1 - \kappa)S$  for

some small (and unspecified) absolute constant  $\kappa > 0$ . In the case of square-free numbers instead of prime numbers, a similar result has been obtained in [6] with any fixed  $\kappa < 2/5$  (one can also find in [6] some results on the distribution of the value of the Euler function and quadratic non-residues in  $\mathcal{N}(a; \mathcal{S})$ ). Here we address a problem at the other extreme, and relax the strength of arithmetic conditions on the elements from  $\mathcal{N}(a; \mathcal{S})$  but instead consider much sparser sets  $\mathcal{S}$  of available positions. In particular, we show that the product of the elements from  $\mathcal{N}(a; \mathcal{S})$  contains significantly more prime divisors than a typical integer of comparable size.

## 2. MAIN RESULTS

Throughout the paper, the letter  $p$  always denotes a prime number.

As usual  $A = O(B)$ ,  $A \ll B$ ,  $B \gg A$  are all equivalent to  $|A| \leq c|B|$  for some *absolute* constant  $c > 0$ , whereas  $A = o(B)$  means that  $A/B \rightarrow 0$ .

We say that a pair  $(\alpha, \beta)$  is *admissible* if for any prime  $p$  and any integer  $\lambda$  with  $\gcd(\lambda, p) = 1$  we have

$$\max_{(a,p)=1} \left| \sum_{z=1}^t \mathbf{e}_p(a\lambda^z) \right| \leq t^\alpha p^{\beta+o(1)},$$

as  $p \rightarrow \infty$ , where  $t$  is the multiplicative order of  $\lambda$  modulo  $p$ .

Concerning admissible pairs, Korobov [16] has shown that the pair

$$(\alpha, \beta) = (0, 1/2),$$

is admissible. For shorter ranges of  $t$ , Korobov's bound has been improved by Heath-Brown and Konyagin [12] who show that the pairs

$$(2.1) \quad (\alpha, \beta) = (5/8, 1/8),$$

and

$$(2.2) \quad (\alpha, \beta) = (3/8, 1/4),$$

are admissible.

More recently Shkredov [19, 20] has shown that the pair

$$(2.3) \quad (\alpha, \beta) = (1/2, 1/6),$$

is admissible, which improves on the pairs (2.1) and (2.2) in the medium range of  $t$ .

Furthermore, the truly remarkable result of Bourgain, Glibichuk and Konyagin [5] implies that for any  $\zeta > 0$  there is some  $\vartheta > 0$  that depends only on  $\zeta$  such that

$$(2.4) \quad (1 - \vartheta, \zeta\vartheta),$$

is admissible.

Our first result is as follows.

**Theorem 2.1.** *Suppose that for an admissible pair  $(\alpha, \beta)$  and some positive numbers  $\eta$  and  $\delta$ , we have*

$$(2.5) \quad \frac{\beta + \eta}{1 - \alpha} \leq \frac{1}{2} - \delta.$$

Suppose further that  $S$ ,  $T$  and  $X$  are parameters satisfying

$$(2.6) \quad T^{1+1/(3-2\alpha)} \geq SX^{2\eta}.$$

Let  $\Delta > 1$  and integer  $k \geq 1$  satisfy

$$(2.7) \quad X \leq \left( \left( \frac{T}{SX^{2\eta}} \right)^{1/(3-2\alpha)} \Delta \right)^k.$$

Then for any sequence of complex numbers  $\Gamma = \{\gamma_n\}_{n=1}^T$  with  $|\gamma_n| \leq 1$  and integers  $\mathcal{S} = \{s_n\}_{n=1}^T$  with  $0 \leq s_1 < \dots < s_T \leq S$  we have

$$\begin{aligned} V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \\ \leq \left( X + TX^{-\delta/(k^2+2)} + (S^{2-2\alpha}TX^{-2\eta})^{1/(3-2\alpha)} \right) TX^{1+o(1)}. \end{aligned}$$

We note that under (2.6) the condition (2.7) also follows from a simpler inequality

$$X \leq \left( T^{-1/(3-2\alpha)^2} \Delta \right)^k.$$

Considering the strength of Theorem 2.1, we take  $\Delta = X^{1/2}$  and  $T = X^{1+\varepsilon}$ . Using the admissible pair of Heath-Brown and Konyagin (2.1), we obtain a power saving in Theorem 2.1 provided  $S \leq X^{7/6-\varepsilon}$ , improving of Garaev's range of  $S \leq X^{15/14-\varepsilon}$ . With the same choice of parameters and using the admissible pair (2.4) of Bourgain, Glibichuk and Konyagin [5], we obtain a power saving in Theorem 2.1 provided  $S \leq X^{3/2-\varepsilon}$ .

Using a different method we can set  $\Delta = 1$  and also extend the range of  $S$  for which we may obtain a nontrivial bound for  $V_\lambda(\Gamma, \mathcal{S}; T, X)$  at the cost of making the power saving explicit.

**Theorem 2.2.** *There exists some absolute constant  $\rho > 0$  such that*

$$V_\lambda(\Gamma, \mathcal{S}; T, X) \leq \left( X^{1-\rho}T^2 + X^{3/2}T^{3/2} + X^{3/4}T^{7/8}S^{1/4} \right) X^{o(1)}.$$

Comparing the bound of Theorem 2.2 with the trivial bound  $XT^2$ , we see that it is nontrivial provided

$$T > X^{1+\varepsilon} \quad \text{and} \quad S < TX^{1+\varepsilon},$$

which on taking  $T = X^{1+\varepsilon}$ , we obtain a power saving in Theorem 2.2 provided  $S \leq T^{2-\varepsilon}$ .

For a sequence of points  $\mathcal{A} = \{a_n\}_{n=1}^T$  we define the discrepancy  $D$  of  $\mathcal{A}$  by

$$D = \sup_{0 \leq a \leq b \leq 1} \left| \frac{A(a, b)}{T} - (b - a) \right|,$$

where  $A(a, b)$  denotes the number of points of  $\mathcal{A}$  falling in the interval  $[a, b] \in [0, 1]$ . Garaev [9] combines his bound for  $V_\lambda(\Gamma, \mathcal{S}, T, X, \Delta)$  with a result of Erdős and Murty [8], which in particular implies that

$$(2.8) \quad \mathcal{E}_{X^{1/2}, X} = (1 + o(1)) \frac{X}{\log X}, \quad X \rightarrow \infty,$$

and the Erdős-Turán inequality (see for example [7]). This allows Garaev [9, Section 3] to show that for any  $\varepsilon > 0$  there is some  $\delta > 0$  such that for almost all primes  $p \leq X$ , the sequence

$$(2.9) \quad A(\lambda, p) = \left\{ \frac{\lambda^{s_n}}{p} \bmod 1 \right\}_{1 \leq n \leq T},$$

with  $T = \lceil X(\log X)^{2+\varepsilon} \rceil$ , has discrepancy

$$D \leq (\log T)^{-\delta},$$

provided  $S \leq X^{15/14+o(1)}$  as  $X \rightarrow \infty$ .

For comparison with our bound, Theorem 2.2 produces the following result. For any  $\varepsilon > 0$  and almost all primes  $p \leq X$ , the sequence (2.9) with  $T = \lceil X^{1+\varepsilon} \rceil$  has discrepancy

$$D \leq T^{-\delta},$$

provided that  $S \leq X^{2-\varepsilon}$  as  $X \rightarrow \infty$ .

We now give an application of Theorem 2.2 to the numbers with prescribed digits, namely to the integers from the set  $\mathcal{N}(a; \mathcal{S})$ , defined in Section 1. We denote by  $\omega(k)$  the number of distinct prime divisors of an integer  $k \geq 1$ .

**Theorem 2.3.** *Let us fix some  $\varepsilon > 0$ . For any sequence of integers  $\mathcal{S} = \{s_n\}_{n=1}^T$  with  $0 \leq s_1 < \dots < s_T \leq S$  with*

$$S \leq T^{2-\varepsilon},$$

*and any  $S$ -bit integer  $a$ , letting*

$$P(a; \mathcal{S}) = \prod_{z \in \mathcal{N}(a; \mathcal{S})} z,$$

*we have*

$$\omega(P(a; \mathcal{S})) \gg T^{1+\delta},$$

for some  $\delta > 0$  which depends only on  $\varepsilon$ .

Considering Theorem 2.3, we first recall a classic result of Hardy and Ramanujan, which states that for any function  $\psi(x) \rightarrow \infty$ , the number of positive integers  $n \leq x$  such that

$$|\omega(n) - \log \log n| > \psi(n)(\log \log n)^{1/2},$$

is  $o(x)$ , see, for example [13, Corollary 1.4]. Since we have

$$2^{2^T S} \ll P(a; \mathcal{S}) \ll 2^{2^T S},$$

an application of Theorem 2.3 gives

$$\omega(P(a; \mathcal{S})) \geq (\log \log P(a; \mathcal{S}))^{1+\delta},$$

for some  $\delta > 0$ . In particular, the above inequality implies that the product  $P(a; \mathcal{S})$  has a much larger number of prime factors than one usually expects from an integer of similar size.

### 3. PRELIMINARY RESULTS

We recall that  $A \ll B$  and  $A = O(B)$  are both equivalent to the inequality  $|A| \leq cB$  for some constant  $c$ , which throughout the paper may depend on  $q$  and occasionally, where obvious, on the integer parameter  $k \geq 1$ .

We also use  $\Sigma^*$  to indicate that the summation is taken over a reduced residue system. That is, for any function  $\psi$  and integer  $k$ , we have

$$\sum_{c \bmod k}^* \psi(c) = \sum_{\substack{c=1 \\ \gcd(c,k)=1}}^k \psi(c).$$

We need the following simplified form of the large sieve inequality, see [13, Theorem 7.11].

**Lemma 3.1.** *For any  $K \geq 1$  and increasing sequence of integers  $\mathcal{S} = \{s_n\}_{n=1}^T$  with  $\max_{s \in \mathcal{S}} s = S$ , we have*

$$\sum_{k \leq K} \sum_{c \bmod k}^* \left| \sum_{n \leq T} \gamma_n \mathbf{e}_k(cs_n) \right|^2 \ll (K^2 + S)T.$$

The following is [15, Theorem 5.5].

**Lemma 3.2.** *For each integer  $t$  and prime  $\ell \equiv 1 \pmod t$  we fix some element  $g_{t,\ell}$  of multiplicative order  $t$  modulo  $\ell$ . Then, for any fixed integer  $k \geq 2$  and an arbitrary  $U > 1$ , the bound*

$$\max_{(a,\ell)=1} \left| \sum_{x=0}^{t-1} \mathbf{e}_\ell(ag_{t,\ell}^x) \right| \ll t\ell^{1/2k^2} (t^{-1/k} + U^{-1/k^2}),$$

holds for all primes  $\ell \equiv 1 \pmod t$  except at most  $U/\log U$  of them.

**Lemma 3.3.** *Let  $\lambda$  be a fixed integer. For any  $Z > 0$  we have*

$$\#\{p \text{ prime} : \text{ord}_p \lambda \leq Z\} \ll Z^2.$$

*Proof.* If  $\text{ord}_p \lambda = y$  then  $\lambda^y - 1 \equiv 0 \pmod p$ . This implies that

$$\#\{p \text{ prime} : \text{ord}_p \lambda < Z\} \leq \omega \left( \prod_{1 \leq z \leq Z} (\lambda^z - 1) \right),$$

where as before,  $\omega(k)$  denotes the number of distinct prime divisors of an integer  $k \geq 1$ . Hence,

$$\#\{p \text{ prime} : \text{ord}_p \lambda < Z\} \ll \log \prod_{1 \leq z \leq Z} (\lambda^z - 1) \leq \log \left( \lambda^{Z^2/2} \right) \ll Z^2,$$

which gives the desired result.  $\square$

The following is a special case of [4, Corollary 4.2].

**Lemma 3.4.** *Let  $p_1$  and  $p_2$  be primes and let  $\mathcal{H}$  be a subgroup of  $\mathbb{Z}_q^*$ , where  $q = p_1 p_2$  such that*

$$\#\{\mathcal{H} \pmod{p_\nu}\} \geq q^\delta, \quad \nu = 1, 2$$

for some fixed  $\delta > 0$ . Then

$$\max_{\gcd(a,q)=1} \left| \sum_{h \in \mathcal{H}} \mathbf{e}_q(ah) \right| \leq (\#\mathcal{H})^{1-\rho},$$

for some  $\rho > 0$  which depends only on  $\delta > 0$ .

## 4. PROOF OF THEOREM 2.1

**4.1. Initial transformations.** Let

$$\sigma_p(a) = \sum_{n \leq T} \gamma_n \mathbf{e}_p(a \lambda^{s_n}).$$

It is also convenient to define  $a_p$  as any integer  $a \in \{1, \dots, p-1\}$  with

$$(4.1) \quad |\sigma_p(a_p)| = \max_{\gcd(a,p)=1} |\sigma_p(a)|,$$

so that

$$V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) = \sum_{p \in \mathcal{E}_\Delta(X)} |\sigma_p(a_p)|^2.$$

However, it is more convenient to work with the sums where each term is divided by the divisor function  $\tau(p-1)$ . We define

$$W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) = \sum_{p \in \mathcal{E}_\Delta(X)} \frac{1}{\tau(p-1)} |\sigma_p(a)|^2,$$



and note the inequality  $\tau(n) = n^{o(1)}$  implies that

$$V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \leq W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) X^{o(1)}.$$

Hence it is enough to prove

$$(4.2) \quad W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \leq \left( X + \frac{S^{1-1/(3-2\alpha)} T^{1/(3-2\alpha)}}{X^{2\eta/(3-2\alpha)}} + \frac{T}{X^{\delta/(k^2+2)}} \right) T X^{1+o(1)},$$

where  $\alpha, \beta, \delta, \eta$  satisfy (2.5) and  $(\alpha, \beta)$  is an admissible pair.

Fix some  $p \leq X$  and consider  $\sigma_p(a_p)$ . We split  $s_n$  into arithmetic progressions mod  $t_p$ . Using the orthogonality of exponential functions, we obtain

$$\begin{aligned} \sigma_p(a_p) &= \sum_{x=1}^{t_p} \sum_{\substack{n \leq T \\ s_n \equiv x \pmod{t_p}}} \gamma_n \mathbf{e}_p(a_p \lambda^{s_n}) \\ &= \frac{1}{t_p} \sum_{x=1}^{t_p} \sum_{b=1}^{t_p} \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p}(b(s_n - x)) \mathbf{e}_p(a_p \lambda^x), \end{aligned}$$

and hence

$$\begin{aligned} \sigma_p(a_p) &= \frac{1}{t_p} \sum_{d|t_p} \sum_{x=1}^{t_p} \sum_{\substack{b=1 \\ \gcd(b, t_p)=d}}^{t_p} \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p}(b(s_n - x)) \mathbf{e}_p(a_p \lambda^x) \\ &= \frac{1}{t_p} \sum_{d|t_p} \sum_{x=1}^{t_p} \sum_{b \pmod{(t_p/d)}^*} \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - x)) \mathbf{e}_p(a_p \lambda^x). \end{aligned}$$

Let  $\xi > 0$  be a real parameter to be chosen later. We set

$$D_p = \xi t_p,$$

and partition summation over  $d$  according to  $D_p$ . This gives

$$(4.3) \quad |\sigma_p(a_p)| \leq |\sigma_{p,1}(a_p)| + |\sigma_{p,2}(a_p)|,$$

where

$$(4.4) \quad \sigma_{p,1}(a_p) = \frac{1}{t_p} \sum_{\substack{d|t_p \\ d \leq D_p}} \sum_{x=1}^{t_p} \sum_{b \pmod{(t_p/d)}^*} \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - x)) \mathbf{e}_p(a_p \lambda^x),$$

and

$$\sigma_{p,2}(a_p) = \frac{1}{t_p} \sum_{\substack{d|t_p \\ d > D_p}} \sum_{x=1}^{t_p} \sum_{b \pmod{(t_p/d)}^*} \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - x)) \mathbf{e}_p(a_p \lambda^x).$$

The equation (4.3) implies that

$$|\sigma_p(a_p)|^2 \ll |\sigma_{p,1}(a_p)|^2 + |\sigma_{p,2}(a_p)|^2,$$

which on averaging over  $p \leq X$  gives

$$(4.5) \quad W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \ll \Sigma_1 + \Sigma_2,$$

where

$$(4.6) \quad \begin{aligned} \Sigma_1 &= \sum_{p \in \mathcal{E}_\Delta(X)} \frac{1}{\tau(p-1)} |\sigma_{p,1}(a_p)|^2, \\ \Sigma_2 &= \sum_{p \in \mathcal{E}_\Delta(X)} \frac{1}{\tau(p-1)} |\sigma_{p,2}(a_p)|^2. \end{aligned}$$

**4.2. The sum  $\Sigma_1$ .** To bound  $\Sigma_1$  we use the argument of Garaev [9, Theorem 3.1]. Fix some  $p \leq X$  and consider  $\sigma_{p,1}(a_p)$ . From (4.4) and the Cauchy-Schwarz inequality

$$\begin{aligned} |\sigma_{p,1}(a_p)|^2 &= \left| \frac{1}{t_p} \sum_{\substack{d|t_p \\ d \leq D_p}} \sum_{x=1}^{t_p} \sum_{b \bmod (t_p/d)}^* \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - x)) \mathbf{e}_p(a_p \lambda^x) \right|^2 \\ &\leq \frac{\tau(t_p)}{t_p} \sum_{\substack{d|t_p \\ d \leq D_p}} \sum_{x=1}^{t_p} \left| \sum_{b \bmod (t_p/d)}^* \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - x)) \right|^2. \end{aligned}$$

Expanding the square and interchanging summation gives

$$\begin{aligned} |\sigma_{p,1}(a_p)|^2 &\leq \frac{\tau(t_p)}{t_p} \sum_{\substack{d|t_p \\ d \leq D_p}} \sum_{b_1, b_2 \bmod (t_p/d)}^* \\ &\quad \sum_{n_1, n_2 \leq T} \gamma_{n_1} \bar{\gamma}_{n_2} \mathbf{e}_{t_p/d}(b_1 s_{n_1} - b_2 s_{n_2}) \sum_{x=1}^{t_p} \mathbf{e}_{t_p/d}(x(b_2 - b_1)). \end{aligned}$$

By the orthogonality of exponential functions, the inner sum vanishes unless  $b_1 = b_2$ . Hence

$$\begin{aligned} |\sigma_{p,1}(a_p)|^2 &\leq \tau(t_p) \sum_{\substack{d|t_p \\ d \leq D_p}} \sum_{b \bmod (t_p/d)}^* \sum_{n_1, n_2 \leq T} \gamma_{n_1} \bar{\gamma}_{n_2} \mathbf{e}_{t_p/d}(b(s_{n_1} - s_{n_2})) \\ &\leq \tau(p-1) \sum_{\substack{d|t_p \\ d \leq D_p}} \sum_{b \bmod (t_p/d)}^* \left| \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b s_n) \right|^2, \end{aligned}$$

where we have used the inequality

$$\tau(t_p) \leq \tau(p-1),$$

since  $t_p \mid (p-1)$ . Summing over  $p \leq X$  we see that

$$\Sigma_1 \leq \sum_{p \leq X} \sum_{\substack{d \mid t_p \\ d \leq D_p}} \sum_{b \bmod (t_p/d)}^* \left| \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(bs_n) \right|^2.$$

We define the sequence of numbers  $X_j$  for  $1 \leq j \leq J$ , where

$$(4.7) \quad J = \left\lceil \frac{\log(X/\Delta)}{\log 2} \right\rceil,$$

by

$$(4.8) \quad X_1 = \Delta, \quad X_j = \min\{2X_{j-1}, X\}, \quad 2 \leq j \leq J,$$

and partition the set of primes  $p \leq X$  into the sets

$$(4.9) \quad \mathcal{R}_j = \{p \leq X : X_j \leq t_p < X_{j+1}\}.$$

Writing

$$\Sigma_{1,j} = \sum_{p \in \mathcal{R}_j} \sum_{\substack{d \mid t_p \\ d \leq D_p}} \sum_{b \bmod (t_p/d)}^* \left| \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(bs_n) \right|^2,$$

we have

$$(4.10) \quad \Sigma_1 \ll \sum_{j=1}^J \Sigma_{1,j}.$$

For each integer  $r$ , we define the set  $\mathcal{Q}(r)$  by

$$(4.11) \quad \mathcal{Q}(r) = \{p \leq X : t_p = r\},$$

so that, replacing  $t_p$  with  $r$  for  $p \in \mathcal{Q}(r)$ , we obtain

$$\begin{aligned} \Sigma_{1,j} &\leq \sum_{X_j \leq r < 2X_j} \sum_{p \in \mathcal{Q}(r)} \sum_{\substack{d \mid r \\ d \leq D_p}} \sum_{b \bmod (r/d)}^* \left| \sum_{n \leq T} \gamma_n \mathbf{e}_{r/d}(bs_n) \right|^2 \\ &= \sum_{X_j \leq r < 2X_j} \#\mathcal{Q}(r) \sum_{\substack{d \mid r \\ d \leq D_p}} \sum_{b \bmod (r/d)}^* \left| \sum_{n \leq T} \gamma_n \mathbf{e}_{r/d}(bs_n) \right|^2. \end{aligned}$$

For each prime  $p \in \mathcal{Q}(r)$  we have  $r \mid (p-1)$  and hence for  $X_j \leq r < 2X_j$  we also have

$$\#\mathcal{Q}(r) \leq \frac{X}{r} \leq \frac{X}{X_j} \quad \text{and} \quad D_p < 2\xi X_j.$$

This implies that

$$\begin{aligned} \Sigma_{1,j} &\leq \frac{X}{X_j} \sum_{X_j \leq r < 2X_j} \sum_{\substack{d|r \\ d \leq 2\xi X_j}} \sum_{b \bmod (r/d)}^* \left| \sum_{n \leq T} \gamma_n \mathbf{e}_{r/d}(bs_n) \right|^2 \\ &= \frac{X}{X_j} \sum_{d \leq 2\xi X_j} \sum_{\substack{X_j \leq r < 2X_j \\ d|r}} \sum_{b \bmod (r/d)}^* \left| \sum_{n \leq T} \gamma_n \mathbf{e}_{r/d}(bs_n) \right|^2, \end{aligned}$$

and hence

$$(4.12) \quad \Sigma_{1,j} \leq \frac{X}{X_j} \sum_{d \leq 2\xi X_j} F_j(d),$$

where  $F_j(d)$  is given by

$$F_j(d) = \sum_{X_j/d \leq m < 2X_j/d} \sum_{b \bmod m}^* \left| \sum_{n \leq T} \gamma_n \mathbf{e}_m(bs_n) \right|^2.$$

An application of Lemma 3.1 gives

$$F_j(d) \ll \left( \frac{X_j^2}{d^2} + S \right) T,$$

which combined with (4.12) implies that

$$\Sigma_{1,j} \leq \frac{X}{X_j} \sum_{d \leq 2\xi X_j} \left( \frac{X_j^2}{d^2} + S \right) T \ll \frac{X}{X_j} (X_j^2 + 2\xi X_j S) T,$$

and hence by (4.10)

$$(4.13) \quad \Sigma_1 \ll \sum_{j=1}^J \frac{X}{X_j} (X_j^2 + \xi X_j S) T \ll X(X + \xi S \log X) T.$$

**4.3. The sum  $\Sigma_2$ .** Fix some  $p \leq X$  and consider  $\sigma_{p,2}(a_p)$ . For each value of  $d$  in the outermost summation we split summation over  $x$  into arithmetic progressions mod  $t_p/d$ . Recalling that  $\sigma_{p,2}(a_p)$  is given by

$$\sigma_{p,2}(a_p) = \frac{1}{t_p} \sum_{\substack{d|t_p \\ d > D_p}} \sum_{x=1}^{t_p} \sum_{b \bmod (t_p/d)}^* \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - x)) \mathbf{e}_p(a_p \lambda^x),$$

we see that

$$\begin{aligned} \sigma_{p,2}(a_p) &= \frac{1}{t_p} \sum_{\substack{d|t_p \\ d > D_p}} \sum_{y=1}^{t_p/d} \sum_{b \bmod (t_p/d)}^* \\ &\quad \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - y)) \sum_{z=1}^d \mathbf{e}_p(a_p \lambda^y \lambda^{zt_p/d}), \end{aligned}$$

and hence

$$\begin{aligned} |\sigma_{p,2}(a_p)| &\leq \frac{1}{t_p} \sum_{\substack{d|t_p \\ d > D_p}} \sum_{y=1}^{t_p/d} \left| \sum_{b \bmod (t_p/d)}^* \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - y)) \right| \\ &\quad \times \left| \sum_{z=1}^d \mathbf{e}_p(a_p \lambda^y \lambda^{zt_p/d}) \right| \\ &\leq \sum_{\substack{d|t_p \\ d > D_p}} \frac{1}{t_p} \sum_{y=1}^{t_p/d} \left| \sum_{b \bmod (t_p/d)}^* \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - y)) \right| \\ &\quad \times \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zt_p/d}) \right|, \end{aligned}$$

where  $f_{d,p}$  is chosen to satisfy

$$\left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zt_p/d}) \right| = \max_{\gcd(a,p)=1} \left| \sum_{z=1}^d \mathbf{e}_p(a \lambda^{zt_p/d}) \right|.$$

Let

$$U(p, d) = \frac{1}{t_p} \sum_{y=1}^{t_p/d} \left| \sum_{\substack{b=1 \\ \gcd(b, t_p/d)=1}}^{t_p/d} \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - y)) \right|,$$

so that

$$(4.14) \quad |\sigma_{p,2}(a_p)| \leq \sum_{\substack{d|t_p \\ d > D_p}} U(p, d) \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zt_p/d}) \right|.$$

We consider bounding the terms  $U(p, d)$ . By the Cauchy-Schwarz inequality

$$\begin{aligned} U(p, d)^2 &\leq \frac{1}{dt_p} \sum_{y=1}^{t_p/d} \left| \sum_{\substack{b=1 \\ \gcd(b, t_p/d)=1}}^{t_p/d} \sum_{n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b(s_n - y)) \right|^2 \\ &= \frac{1}{dt_p} \sum_{1 \leq n_1, n_2 \leq T} \sum_{\substack{b_1, b_2=1 \\ \gcd(b_1 b_2, t_p/d)=1}}^{t_p/d} \gamma_{n_1} \bar{\gamma}_{n_2} \mathbf{e}_{t_p/d}(b_1 s_{n_1} - b_2 s_{n_2}) \\ &\qquad \qquad \qquad \times \sum_{y=1}^{t_p/d} \mathbf{e}_{t_p/d}(y(b_1 - b_2)). \end{aligned}$$

Using the orthogonality of exponential functions again, we see that the last sum vanishes unless  $b_1 = b_2$ . This gives

$$U(p, d)^2 \leq \frac{1}{d^2} \sum_{1 \leq n_1, n_2 \leq T} \sum_{\substack{b=1 \\ \gcd(b, t_p/d)=1}}^{t_p/d} \gamma_{n_1} \bar{\gamma}_{n_2} \mathbf{e}_{t_p/d}(b(s_{n_1} - s_{n_2})).$$

After rearranging and extending the summation over  $b$  to the complete residue system modulo  $t_p/d$ , we derive

$$\begin{aligned} U(p, d)^2 &\leq \frac{1}{d^2} \sum_{\substack{b=1 \\ \gcd(b, t_p/d)=1}}^{t_p/d} \sum_{1 \leq n_1, n_2 \leq T} \gamma_{n_1} \bar{\gamma}_{n_2} \mathbf{e}_{t_p/d}(b(s_{n_1} - s_{n_2})) \\ &= \frac{1}{d^2} \sum_{\substack{b=1 \\ \gcd(b, t_p/d)=1}}^{t_p/d} \left| \sum_{1 \leq n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b s_n) \right|^2 \\ &\leq \frac{1}{d^2} \sum_{b=1}^{t_p/d} \left| \sum_{1 \leq n \leq T} \gamma_n \mathbf{e}_{t_p/d}(b s_n) \right|^2 = \frac{t_p}{d^3} V(t_p/d), \end{aligned}$$

where for an integer  $r \geq 1$  we define

$$(4.15) \quad V(r) = \#\{(n_1, n_2) \in [1, T]^2 : s_{n_1} \equiv s_{n_2} \pmod{r}\}.$$

Substituting this in (4.14) gives

$$|\sigma_{p,2}(a_p)| \leq t_p^{1/2} \sum_{\substack{d|t_p \\ d > D_p}} \frac{1}{d^{3/2}} V(t_p/d)^{1/2} \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{z t_p/d}) \right|.$$

Summing over  $p \leq X$  gives

$$\Sigma_2 \leq \sum_{p \in \mathcal{E}_\Delta(X)} \frac{t_p}{\tau(p-1)} \left( \sum_{\substack{d|t_p \\ d > D_p}} \frac{1}{d^{3/2}} V(t_p/d)^{1/2} \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zt_p/d}) \right| \right)^2,$$

which by the Cauchy-Schwarz inequality implies that

$$\begin{aligned} \Sigma_2 &\leq \sum_{p \in \mathcal{E}_\Delta(X)} \frac{t_p \tau(t_p)}{\tau(p-1)} \sum_{\substack{d|t_p \\ d > D_p}} \frac{1}{d^3} V(t_p/d) \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zt_p/d}) \right|^2 \\ &\leq \sum_{p \in \mathcal{E}_\Delta(X)} t_p \sum_{\substack{d|t_p \\ d > D_p}} \frac{1}{d^3} V(t_p/d) \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zt_p/d}) \right|^2. \end{aligned}$$

At this point our strategy is to rearrange summation so we may apply Lemma 3.2. We define the sequence  $X_j$  as in (4.8), we let  $\mathcal{Q}(r)$  be given by (4.11) and for each integer  $r$  we define the following subsets  $\mathcal{S}_i(r)$  of  $\mathcal{Q}(r)$

$$\mathcal{S}_i(r) = \{p : 2^i \leq p \leq 2^{i+1} \text{ and } t_p = r\}.$$

Writing

$$\Sigma_{2,i,j} = \sum_{X_j \leq r \leq X_{j+1}} r \sum_{p \in \mathcal{S}_i(r)} \sum_{\substack{d|r \\ d > D_p}} \frac{1}{d^3} V(r/d) \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zr/d}) \right|^2,$$

the above implies that

$$\Sigma_2 \leq \sum_{i=1}^J \sum_{j: X_j \ll 2^i} \Sigma_{2,i,j}.$$

To further transform the sums  $\Sigma_{2,i,j}$ , define the numbers  $Z_j$  by

$$(4.16) \quad Z_j = \xi X_j, \quad j = 1, \dots, J,$$

so that

$$\Sigma_{2,i,j} \ll X_j \sum_{X_j \leq r \leq X_{j+1}} \sum_{p \in \mathcal{S}_i(r)} \sum_{\substack{d|r \\ d > Z_j}} \frac{1}{d^3} V(r/d) \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zr/d}) \right|^2.$$

After interchanging summation, we arrive at

$$(4.17) \quad \Sigma_{2,i,j} \ll X_j \sum_{Z_j < d \leq X_{j+1}} \frac{1}{d^3} \sum_{\substack{X_j \leq r \leq X_{j+1} \\ d|r}} V(r/d) \\ \sum_{p \in \mathcal{S}_i(r)} \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zr/d}) \right|^2.$$

Let  $\rho$  be a parameter to be chosen later. We now partition summation over  $i$  and  $j$  in  $\Sigma_2$  as follows

$$(4.18) \quad \Sigma_2 \leq \Sigma_2^{\leq} + \Sigma_2^{\geq},$$

where

$$\Sigma_2^{\leq} = \sum_{i=1}^J \sum_{j: X_j \leq 2^{i\rho}} \Sigma_{2,i,j} \quad \text{and} \quad \Sigma_2^{\geq} = \sum_{i=1}^J \sum_{j: 2^{i\rho} \leq X_j \ll 2^i} \Sigma_{2,i,j}.$$

To estimate  $\Sigma_2^{\leq}$ , we first fix some  $j$  with  $X_j \leq 2^{i\rho}$ . Considering the inner summation over  $p$ , we partition  $\mathcal{S}_i(r)$  according to Lemma 3.2. Let

$$U_i(r) = \frac{2^{i(1-1/(k^2+2))}}{r^{1-2/(k^2+2)}},$$

and for integer  $k$  we define the sets  $\mathcal{S}_i^{(1)}(r)$  and  $\mathcal{S}_i^{(2)}(r)$  by

$$\mathcal{S}_i^{(1)}(r) = \left\{ p \in \mathcal{S}_i(r) : \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zr/d}) \right| \leq d 2^{i/2k^2} \left( d^{-1/k} + U_i(r)^{-1/k^2} \right) \right\}, \\ \mathcal{S}_i^{(2)}(r) = \mathcal{S}_i(r) \setminus \mathcal{S}_i^{(1)}(r).$$

Lemma 3.2 implies that

$$\#\mathcal{S}_i^{(2)}(r) \ll \frac{U_i(r)}{\log U_i(r)}.$$

Considering  $\mathcal{S}_i^{(1)}(r)$  and using the fact that  $r \mid p-1$  for  $p \in \mathcal{S}_i(r)$  gives

$$(4.19) \quad \#\mathcal{S}_i^{(1)}(r) \leq \#\mathcal{S}_i(r) \ll \frac{2^i}{r},$$



which implies that

$$\sum_{p \in \mathcal{S}_i(r)} \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zr/d}) \right|^2 \ll d^2 \left( \frac{2^{i(1+1/k^2)}}{r} (d^{-2/k} + U_i(r)^{-2/k^2}) + \frac{U_i(r)}{\log U_i(r)} \right).$$

Recalling the choice of  $U_i(r)$  we see that

$$\sum_{p \in \mathcal{S}_i(r)} \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zr/d}) \right|^2 \ll \frac{d^2 2^{i(1-1/(k^2+2))}}{r^{1-2/(k^2+2)}} + \frac{d^{2-2/k} 2^{i(1+1/k^2)}}{r},$$

which on assuming that

$$(4.20) \quad X \leq (\xi \Delta)^k,$$

simplifies to

$$(4.21) \quad \sum_{p \in \mathcal{S}_i(r)} \left| \sum_{z=1}^d \mathbf{e}_p(f_{d,p} \lambda^{zr/d}) \right|^2 \ll \frac{d^2 2^{i(1-1/(k^2+2))}}{r^{1-2/(k^2+2)}}.$$

Hence considering  $\Sigma_{2,i,j}$ , we have

$$\begin{aligned} \Sigma_{2,i,j} &\ll X_j 2^{i(1-1/(k^2+2))} \sum_{Z_j < d \leq X_{j+1}} \frac{1}{d} \sum_{\substack{X_j \leq r \leq X_{j+1} \\ d|r}} \frac{V(r/d)}{r^{1-2/(k^2+2)}} \\ &\ll X_j 2^{i(1-1/(k^2+2))} \sum_{Z_j < d \leq X_{j+1}} \frac{1}{d^{2-2/(k^2+2)}} \sum_{X_j/d \leq r \leq X_{j+1}/d} \frac{V(r)}{r^{1-2/(k^2+2)}}, \end{aligned}$$

after the change of variable  $r \rightarrow dr$ . Writing

$$W_j(d) = \sum_{X_j/d \leq r \leq X_{j+1}/d} \frac{V(r)}{r^{1-2/(k^2+2)}},$$

the above implies

$$(4.22) \quad \Sigma_{2,i,j} \ll X_j 2^{i(1-1/(k^2+2))} \sum_{Z_j < d \leq X_{j+1}} \frac{W_j(d)}{d^{2-2/(k^2+2)}}.$$

Considering the sum  $W_j(d)$  and recalling the definition of  $V(r)$  given by (4.15), we have

$$\begin{aligned} W_j(d) &= \sum_{X_j/d \leq r \leq X_{j+1}/d} \sum_{\substack{1 \leq n_1, n_2 \leq T \\ s_{n_1} \equiv s_{n_2} \pmod r}} \frac{1}{r^{1-2/(k^2+2)}} \\ &\ll \left(\frac{d}{X_j}\right)^{1-2/(k^2+2)} \sum_{1 \leq n_1, n_2 \leq T} \sum_{\substack{X_j/d \leq r \leq X_{j+1}/d \\ s_{n_1} \equiv s_{n_2} \pmod r}} 1. \end{aligned}$$

Considering the last sum on the right, we have

$$\sum_{1 \leq n_1, n_2 \leq T} \sum_{\substack{X_j/d \leq r \leq X_{j+1}/d \\ s_{n_1} \equiv s_{n_2} \pmod r}} 1 \ll \frac{TX^j}{d} + \sum_{1 \leq n_1 < n_2 \leq T} \sum_{\substack{X_j/d \leq r \leq X_{j+1}/d \\ s_{n_1} \equiv s_{n_2} \pmod r}} 1.$$

Since the term

$$\sum_{\substack{X_j/d \leq r \leq X_{j+1}/d \\ s_{n_1} \equiv s_{n_2} \pmod r}} 1,$$

is bounded by the number of divisors of  $s_{n_2} - s_{n_1}$ , we see that

$$\sum_{\substack{X_j/d \leq r \leq X_{j+1}/d \\ s_{n_1} \equiv s_{n_2} \pmod r}} 1 = S^{o(1)},$$

and hence

$$(4.23) \quad \sum_{1 \leq n_1, n_2 \leq T} \sum_{\substack{X_j/d \leq r \leq X_{j+1}/d \\ s_{n_1} \equiv s_{n_2} \pmod r}} 1 \ll \left(\frac{X_j}{d} + TS^{o(1)}\right) T,$$

which gives

$$W_j(d) \leq \left(\frac{d}{X_j}\right)^{1-2/(k^2+2)} \left(\frac{X_j}{d} + TS^{o(1)}\right) T.$$

Substituting the above into (4.22) we get

$$\begin{aligned} \Sigma_{2,i,j} &\ll X_j^{1+2/(k^2+2)} 2^{i(1-1/(k^2+2))} T \sum_{Z_j < d \leq X_{j+1}} \frac{1}{d^2} \\ &\quad + X_j^{2/(k^2+2)} 2^{i(1-1/(k^2+2))} T^2 S^{o(1)} \sum_{Z_j < d \leq X_{j+1}} \frac{1}{d}, \end{aligned}$$

which simplifies to

$$\begin{aligned}\Sigma_{2,i,j} &\leq \frac{X_j^{1+2/(k^2+2)} 2^{i(1-1/(k^2+2))} T}{Z_j} + X_j^{2/(k^2+2)} 2^{i(1-1/(k^2+2))} T^2 (SX)^{o(1)} \\ &\leq X_j^{2/(k^2+2)} 2^{i(1-1/(k^2+2))} \left( \frac{1}{\xi} + T \right) T (SX)^{o(1)},\end{aligned}$$

on recalling the choice of  $Z_j$  given by (4.16).

We now assume that

$$(4.24) \quad \xi \geq \frac{1}{T}.$$

Without loss of generality, we can also assume that  $S = X^{O(1)}$  and thus  $(SX)^{o(1)} = X^{o(1)}$ . Hence, the above bounds further simplify to

$$\Sigma_{2,i,j} \leq T^2 X_j^{2/(k^2+2)} 2^{i(1-1/(k^2+2))} X^{o(1)}.$$

Summing over  $i$  and  $j$  with  $X_j \leq 2^{i\rho}$  we arrive at

$$\Sigma_2^{\leq} \leq T^2 X^{o(1)} \sum_{i=1}^J \sum_{j: X_j \leq 2^{i\rho}} X_j^{2/(k^2+2)} 2^{i(1-1/(k^2+2))},$$

and hence

$$(4.25) \quad \Sigma_2^{\leq} \leq T^2 X^{1-(1-2\rho)/(k^2+2)} X^{o(1)}.$$

We next consider  $\Sigma_2^{\geq}$ . We begin our treatment of  $\Sigma_2^{\geq}$  in a similar fashion to  $\Sigma_2^{\leq}$ . In particular, we use (4.17) and the assumption that  $(\alpha, \beta)$  is admissible to obtain

$$(4.26) \quad \Sigma_{2,i,j} \leq 2^{i(2\beta+o(1))} X_j \sum_{X_j \leq r \leq X_{j+1}} \#\mathcal{S}_{i,j}(r) \sum_{\substack{d|r \\ d > Z_j}} \frac{1}{d^{3-2\alpha}} V(r/d),$$

as  $i \rightarrow \infty$ .

Using (4.19) and then rearranging the order of summation, the above reduces to

$$\begin{aligned}\Sigma_{2,i,j} &\leq 2^{i(1+2\beta+o(1))} \sum_{X_j \leq r \leq X_{j+1}} \sum_{\substack{d|r \\ d > Z_j}} \frac{1}{d^{3-2\alpha}} V(r/d) \\ &\leq 2^{i(1+2\beta+o(1))} \sum_{Z_j < d \leq X_{j+1}} \frac{1}{d^{3-2\alpha}} W_j(d),\end{aligned}$$

where

$$W_j(d) = \sum_{X_j/d \leq r \leq X_{j+1}/d} V(r).$$

We see from the definition (4.15) that

$$W_j(d) = \sum_{1 \leq n_1, n_2 \leq T} \sum_{\substack{X_j/d \leq r \leq X_{j+1}/d \\ s_{n_1} \equiv s_{n_2} \pmod{r}}} 1 \leq \left( \frac{X_j}{d} + TS^{o(1)} \right) T,$$

and hence

$$\begin{aligned} \Sigma_{2,i,j} &\leq 2^{i(1+2\beta+o(1))} T \left( X_j \sum_{Z_j < d \leq X_{j+1}} \frac{1}{d^{4-2a}} + TS^{o(1)} \sum_{Z_j \leq d \leq X_{j+1}} \frac{1}{d^{3-2\alpha}} \right) \\ &\leq 2^{i(1+2\beta+o(1))} T \left( \frac{X_j}{Z_j^{3-2\alpha}} + \frac{TS^{o(1)}}{Z_j^{2-2a}} \right). \end{aligned}$$

Since obviously  $S \leq X^{O(1)}$ , we can replace both  $2^{o(i)}$  and  $S^{o(1)}$  with  $X^{o(1)}$ . Recalling the choice of  $Z_j$  and the assumption (4.24), we get

$$\Sigma_{2,i,j} \ll \frac{2^{i(1+2\beta)} T}{\xi^{2(1-\alpha)} X_j^{2(1-\alpha)}} (\xi^{-1} + T) X^{o(1)} \leq \frac{2^{i(1+2\beta)} T^2}{\xi^{2(1-\alpha)} X_j^{2(1-\alpha)}} X^{o(1)}.$$

This implies that

$$\begin{aligned} \Sigma_2^{\geq} &\leq \frac{1}{\xi^{2(1-\alpha)}} T^2 X^{o(1)} \sum_{i=1}^J \sum_{j: 2^i \rho \leq X_j \leq 2^{i+1} \rho} \frac{2^{i(1+2\beta)}}{X_j^{2(1-\alpha)}} \\ (4.27) \quad &\leq T^2 \frac{X^{1+2(\beta+\eta-\rho(1-\alpha))}}{\xi^{2(1-\alpha)}} X^{o(1)}. \end{aligned}$$

Substituting the bounds (4.25) and (4.27) in (4.18), we see that

$$(4.28) \quad \Sigma_2 \leq \left( \frac{1}{X^{(1-2\rho)/(k^2+2)}} + \frac{X^{2(\beta-\rho(1-\alpha))}}{\xi^{2(1-\alpha)}} \right) T^2 X^{1+o(1)}.$$

**4.4. Concluding the proof.** Substituting (4.13) and (4.28) in (4.5), gives

$$\begin{aligned} W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \\ \leq \left( X + \xi S + \frac{T}{X^{(1-2\rho)/(k^2+2)}} + \frac{TX^{2(\beta-\rho(1-\alpha))}}{\xi^{2(1-\alpha)}} \right) TX^{1+o(1)}. \end{aligned}$$

Let  $\eta > 0$  be a parameter and make the substitution

$$\rho = \frac{\beta + \eta}{1 - \alpha}.$$

The above transforms into

$$\begin{aligned} & W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \\ & \leq \left( X + \xi S + \frac{T}{X^{(1-2(\beta+\eta))/(1-\alpha)/(k^2+2)}} + \frac{T}{\xi^{2(1-\alpha)} X^{2\eta}} \right) T X^{1+o(1)}. \end{aligned}$$

Next we choose

$$\xi = \left( \frac{T}{S X^{2\eta}} \right)^{1/(3-2\alpha)},$$

to balance the second and fourth terms. This gives

$$\begin{aligned} & W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \\ & \leq \left( X + \frac{S^{1-1/(3-2\alpha)} T^{1/(3-2\alpha)}}{X^{2\eta/(3-2\alpha)}} + \frac{T}{X^{(1-2(\beta+\eta))/(1-\alpha)/(k^2+2)}} \right) T X^{1+o(1)}. \end{aligned}$$

We now note that the assumption (2.5) implies that

$$\begin{aligned} & W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \\ & \leq \left( X + (S^{2-2\alpha} T X^{-2\eta})^{1/(3-2\alpha)} + \frac{T}{X^{\delta/(k^2+2)}} \right) T X^{1+o(1)}. \end{aligned}$$

which is the desired bound.

Finally, to complete the proof, it remains to note that (4.20) is satisfied by the assumption (2.7) and (4.24) is satisfied by (2.6).

## 5. PROOF OF THEOREM 2.2

**5.1. Initial transformations.** As before, for each prime  $p$  we define the number  $a_p$  by (4.1). Taking  $Z = X^{1/4}$  in Lemma 3.3 and recalling that  $t_p$  denotes the order of  $\lambda \bmod p$ , we have

$$\begin{aligned} (5.1) \quad V_\lambda(\Gamma, \mathcal{S}; T, X) & \leq X^{1/2} T^2 + V_\lambda(\Gamma, \mathcal{S}; T, X, X^{1/4}) \\ & = X^{1/2} T^2 + \sum_{p \in \mathcal{E}_{X^{1/4}}(X)} |\sigma_p(a_p)|^2. \end{aligned}$$

We define the sequence of numbers  $X_j$ , as in (4.8) with  $\Delta = X^{1/4}$ . We also define the sets  $\mathcal{R}_j$  as in (4.9) for  $j = 1, \dots, J$  with  $J$  given by (4.7).

Hence, partitioning summation over  $p$  in (5.1) according to  $\mathcal{R}_j$  gives,

$$V_\lambda(\Gamma, \mathcal{S}; T, X) \ll X^{1/2} T^2 + \sum_{j=1}^J W_j,$$

where

$$W_j = \sum_{p \in \mathcal{R}_j} |\sigma_p(a_p)|^2.$$

We define the number  $Y$  by

$$(5.2) \quad Y = \frac{X^{3/4}S^{1/4}}{T^{1/4}},$$

and let  $I$  be the largest integer  $j$  with  $X_j \leq Y$  (since  $S \geq T$  we obviously have  $Y \geq X^{3/4} > X^{1/4}$  so  $I$  is correctly defined).

We now further partition the summation over  $j$  and re-write (5.1) as

$$(5.3) \quad V_\lambda(\Gamma, \mathcal{S}; T, X) \leq X^{1/2}T^2 + W^{\leq} + W^{\geq},$$

where

$$(5.4) \quad W^{\leq} = \sum_{j=1}^I W_j \quad \text{and} \quad W^{\geq} = \sum_{j=I+1}^J W_j.$$

**5.2. The sum  $W^{\leq}$ .** We fix some  $j$  with  $X^{1/4} \leq X_j < Y$ . Considering  $W_j$ , we define the sets

$$(5.5) \quad \mathcal{V}_j(r) = \{p \in \mathcal{R}_j : t_p = r\},$$

so that

$$(5.6) \quad W_j = \sum_{X_j < r \leq 2X_j} U_{j,r},$$

where  $U_{j,r}$  is given by

$$U_{j,r} = \sum_{p \in \mathcal{V}_j(r)} |\sigma_p(a_p)|^2.$$

For each  $p \in \mathcal{V}_j(r)$  we define the complex number  $c_{j,r,p}$  by

$$c_{j,r,p} = \frac{\bar{\sigma}_p(a_p)}{\left(\sum_{p \in \mathcal{V}_j(r)} |\sigma_p(a_p)|^2\right)^{1/2}},$$

so that

$$(5.7) \quad \sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}|^2 = 1,$$

and writing

$$U_{j,r}^* = \sum_{p \in \mathcal{V}_j(r)} \sum_{1 \leq n \leq T} c_{j,r,p} \gamma_n \mathbf{e}_p(a_p \lambda^{sn}),$$

we see that

$$(5.8) \quad |U_{j,r}^*| = U_{j,r}^{1/2}.$$

We have

$$U_{j,r}^* = \sum_{0 \leq x < r} \sum_{p \in \mathcal{V}_j(r)} b_r(x) c_{j,r,p} \mathbf{e}_p(a_p \lambda^x),$$

where

$$(5.9) \quad b_r(x) = \sum_{\substack{1 \leq n \leq T \\ s_n \equiv x \pmod{r}}} \gamma_n,$$

and hence by the Cauchy-Schwarz inequality

$$|U_{j,r}^*|^2 \leq \sum_{0 \leq x < r} |b_r(x)|^2 \sum_{0 \leq x < r} \left| \sum_{p \in \mathcal{V}_j(r)} c_{j,r,p} \mathbf{e}_p(a_p \lambda^x) \right|^2.$$

Expanding the square and interchanging summation gives

$$|U_{j,r}^*|^2 \leq \sum_{0 \leq x < r} |b_r(x)|^2 \sum_{p_1, p_2 \in \mathcal{V}_j(r)} |c_{j,r,p_1}| |c_{j,r,p_2}| \left| \sum_{0 \leq x < r} \mathbf{e}_{p_1 p_2}((a_{p_1} p_2 - a_{p_2} p_1) \lambda^x) \right|,$$

which implies that

$$\begin{aligned} |U_{j,r}^*|^2 &\leq r \sum_{0 \leq x < r} |b_r(x)|^2 \sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}|^2 \\ &\quad + \sum_{0 \leq x < r} |b_r(x)|^2 \sum_{\substack{p_1, p_2 \in \mathcal{V}_j(r) \\ p_1 \neq p_2}} |c_{j,r,p_1}| |c_{j,r,p_2}| \max_{(a, p_1 p_2)=1} \left| \sum_{0 \leq x < r} \mathbf{e}_{p_1 p_2}(a \lambda^x) \right|. \end{aligned}$$

Since

$$t_{p_1} = t_{p_2} = r,$$

the set

$$H = \{ \lambda^x \pmod{p_1 p_2} : 0 \leq x < r \},$$

is a subgroup of  $\mathbb{Z}_{p_1 p_2}^*$  and from the inequalities

$$r \geq X^{1/4} > (p_1 p_2)^{1/8},$$

we see that the conditions of Lemma 3.4 are satisfied. An application of Lemma 3.4 gives

$$\begin{aligned} |U_{j,r}^*|^2 &\leq r \sum_{0 \leq x < r} |b_r(x)|^2 \sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}|^2 \\ &\quad + \sum_{0 \leq x < r} |b_r(x)|^2 \left( \sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}| \right)^2 r^{1-\varrho}, \end{aligned}$$

which by the Cauchy-Schwarz inequality implies that

$$|U_{j,r}^*|^2 \leq \sum_{0 \leq x < r} |b_r(x)|^2 \sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}|^2 (r + |\mathcal{V}_j(r)| r^{1-\varrho}),$$

and hence by (5.7)

$$|U_{j,r}^*|^2 \leq \sum_{0 \leq x < r} |b_r(x)|^2 (r + |\mathcal{V}_j(r)|r^{1-\ell}).$$

Since

$$(5.10) \quad |\mathcal{V}_j(r)| \leq \frac{X}{r},$$

we get

$$(5.11) \quad |U_{j,r}^*|^2 \leq \left(r + \frac{X}{r^\ell}\right) \sum_{0 \leq x < r} |b_r(x)|^2.$$

Recalling (5.9) and the assumption each  $|\gamma_n| \leq 1$ , we see that

$$\sum_{0 \leq x < r} |b_r(x)|^2 = \sum_{1 \leq n_1, n_2 \leq T} \gamma_{n_1} \bar{\gamma}_{n_2} \sum_{\substack{0 \leq x < r \\ s_{n_1} \equiv x \pmod r \\ s_{n_2} \equiv x \pmod r}} 1 = V(r),$$

where  $V(r)$  is defined by (4.15). By (5.11) we have

$$|U_{j,r}^*|^2 \leq V(r) \left(r + \frac{X}{r^\ell}\right),$$

and hence by (5.8)

$$|U_{j,r}| \leq V(r) \left(r + \frac{X}{r^\ell}\right).$$

Combining the above with (5.6) gives

$$(5.12) \quad W_j \leq \sum_{X_j < r \leq 2X_j} V(r) \left(X_j + \frac{X}{X_j^\ell}\right).$$

As in the proof of Theorem 2.1, see (4.23), we have

$$\begin{aligned} \sum_{X_j < r \leq 2X_j} V(r) &\ll X_j T + \sum_{\substack{1 \leq n_1, n_2 \leq T \\ n_1 \neq n_2}} \sum_{\substack{X_j < r \leq 2X_j \\ s_{n_1} \equiv s_{n_2} \pmod r}} 1 \\ &\leq (X_j + TS^{o(1)})T \leq T^{2+o(1)}, \end{aligned}$$

where we have used the assumption  $S \leq T^2$  and  $T > X$  as otherwise Theorem 2.2 is trivial. Substituting the above into (5.12) gives

$$W_j \leq \left(X_j + \frac{X}{X_j^\ell}\right) T^{2+o(1)},$$

and hence by (5.4)

$$(5.13) \quad W \leq (Y + XX_1^{-\ell}) T^{2+o(1)} \leq (Y + X^{1-\ell/4}) T^{2+o(1)}.$$



5.3. **The sum  $W^\geq$ .** We fix some  $j$  with  $Y \leq X_j \leq X$  and arrange  $W_j$  as follows

$$W_j = \sum_{p \in \mathcal{R}_j} |\sigma_p(a_p)|^2 \leq T \sum_{p \in \mathcal{R}_j} |\sigma_p(a_p)|,$$

and hence there exists some sequence of complex numbers  $c_{j,p}$  with  $|c_{j,p}| = 1$  such that

$$W_j \leq T \sum_{p \in \mathcal{R}_j} \sum_{1 \leq n \leq T} c_{j,p} \gamma_n \mathbf{e}_p(a_p \lambda^{s_n}).$$

An application of the Cauchy-Schwarz inequality gives

$$W_j^2 \leq T^3 \sum_{1 \leq n \leq T} \left| \sum_{p \in \mathcal{R}_j} c_{j,p} \mathbf{e}_p(a_p \lambda^{s_n}) \right|^2.$$

Since the sequence  $s_n$  is increasing and bounded by  $S$ , we see that

$$W_j^2 \leq T^3 \sum_{1 \leq s \leq S} \left| \sum_{p \in \mathcal{R}_j} c_{j,p} \mathbf{e}_p(a_p \lambda^s) \right|^2 \ll \frac{T^3}{S} \sum_{-S \leq r, s \leq S} \left| \sum_{p \in \mathcal{R}_j} c_{j,p} \mathbf{e}_p(a_p \lambda^{r+s}) \right|^2,$$

so that writing

$$\mathbf{W}_j = \sum_{-S \leq r, s \leq S} \left| \sum_{p \in \mathcal{R}_j} c_{j,p} \mathbf{e}_p(a_p \lambda^{r+s}) \right|^2,$$

the above implies

$$(5.14) \quad W_j^2 \leq \frac{T^3}{S} \mathbf{W}_j.$$

Considering  $\mathbf{W}_j$ , expanding the square and interchanging summation gives

$$\begin{aligned} \mathbf{W}_j &\leq \sum_{p_1, p_2 \in \mathcal{R}_j} \left| \sum_{-S \leq r, s \leq S} \mathbf{e}_{p_1 p_2}((a_{p_1} p_2 - a_{p_2} p_1) \lambda^{r+s}) \right| \\ &\leq S^2 |\mathcal{R}_j| + \sum_{\substack{p_1, p_2 \in \mathcal{R}_j \\ p_1 \neq p_2}} \sum_{-S \leq r \leq S} \left| \sum_{-S \leq s \leq S} \mathbf{e}_{p_1 p_2}(a_{p_1 p_2} \lambda^{r+s}) \right|, \end{aligned}$$

for some integers  $a_{p_1 p_2}$  with  $\gcd(a_{p_1 p_2}, p_1 p_2) = 1$ . By (5.5) and (5.10)

$$|\mathcal{R}_j| = \sum_{X_j < r \leq 2X_j} |\mathcal{V}_j(r)| \ll X,$$

and hence

$$(5.15) \quad \mathbf{W}_j \ll S^2 X + \sum_{\substack{p_1, p_2 \in \mathcal{R}_j \\ p_1 \neq p_2}} Z(p_1, p_2).$$

where

$$Z(p_1, p_2) = \sum_{-S \leq r \leq S} \left| \sum_{-S \leq s \leq S} \mathbf{e}_{p_1 p_2}(a_{p_1 p_2} \lambda^{r+s}) \right|.$$

Considering  $Z(p_1, p_2)$ , by the Cauchy-Schwarz inequality, we have

$$\begin{aligned} Z(p_1, p_2)^2 &\ll S \sum_{-S \leq r \leq S} \left| \sum_{-S \leq s \leq S} \mathbf{e}_{p_1 p_2}(a_{p_1 p_2} \lambda^r \lambda^s) \right|^2 \\ &\ll S \left( 1 + \frac{S}{\text{ord}_{p_1 p_2}(\lambda)} \right) \sum_{u \bmod p_1 p_2} \left| \sum_{-S \leq s \leq S} \mathbf{e}_{p_1 p_2}(a_{p_1 p_2} u \lambda^s) \right|^2. \end{aligned}$$

Now, since

$$\begin{aligned} &\sum_{u \bmod p_1 p_2} \left| \sum_{-S \leq s \leq S} \mathbf{e}_{p_1 p_2}(a_{p_1 p_2} u \lambda^s) \right|^2 \\ &= \sum_{-S \leq s_1, s_2 \leq S} \sum_{u \bmod p_1 p_2} \mathbf{e}_{p_1 p_2}(a_{p_1 p_2} u (\lambda^{s_1} - \lambda^{s_2})) \\ &\ll p_1 p_2 S \left( 1 + \frac{S}{\text{ord}_{p_1 p_1}(\lambda)} \right), \end{aligned}$$

we see that

$$Z(p_1, p_2)^2 \ll p_1 p_2 S^2 \left( 1 + \frac{S}{\text{ord}_{p_1 p_1}(\lambda)} \right)^2 \leq X^2 S^2 \left( 1 + \frac{S}{\text{ord}_{p_1 p_2}(\lambda)} \right)^2.$$

Since  $t_{p_1}, t_{p_2} \geq X_j$ , we have

$$\text{ord}_{p_1 p_2}(\lambda) = \text{lcm}(t_{p_1}, t_{p_2}) = \frac{t_{p_1} t_{p_2}}{\text{gcd}(t_{p_1}, t_{p_2})} \geq \frac{X_j^2}{\text{gcd}(p_1 - 1, p_2 - 1)},$$

which implies

$$Z(p_1, p_2)^2 \leq X^2 S^2 \left( 1 + \frac{\text{gcd}(p_1 - 1, p_2 - 1) S}{X_j^2} \right)^2,$$

which after substituting the above in (5.15) gives

$$\mathbf{W}_j \ll S^2 X + X S \sum_{\substack{p_1, p_2 \in \mathcal{R}_j \\ p_1 \neq p_2}} 1 + \frac{X S^2}{X_j^2} \sum_{\substack{p_1, p_2 \in \mathcal{R}_j \\ p_1 \neq p_2}} \text{gcd}(p_1 - 1, p_2 - 1).$$

We have

$$\sum_{\substack{p_1, p_2 \in \mathcal{R}_j \\ p_1 \neq p_2}} 1 \leq |\mathcal{R}_j|^2 \ll X^2,$$

and

$$\begin{aligned} \sum_{\substack{p_1, p_2 \in \mathcal{R}_j \\ p_1 \neq p_2}} \gcd(p_1 - 1, p_2 - 1) &\ll \sum_{1 \leq x_1 < x_2 \leq X} \gcd(x_1, x_2) \\ &= \sum_{1 \leq d \leq X} d \sum_{\substack{1 \leq x_1 < x_2 \leq X/d \\ (x_1, x_2) = 1}} 1 \ll X^{2+o(1)}, \end{aligned}$$

so that

$$\mathbf{W}_j \ll S^2 X + S X^3 + \frac{S^2 X^{3+o(1)}}{X_j^2}.$$

Combining the above with (5.14) gives

$$W_j^2 \ll S X T^3 + X^3 T^3 + \frac{S X^{3+o(1)} T^3}{X_j^2},$$

which simplifies to

$$W_j \leq X^{3/2} T^{3/2} \left( 1 + \frac{S^{1/2}}{X_j} \right) X^{o(1)},$$

since we may assume  $S \leq X^{2+o(1)}$ . By (5.4) we have

$$(5.16) \quad W^{\geq} \ll X^{3/2} T^{3/2} \left( 1 + \frac{S^{1/2}}{Y} \right) X^{o(1)},$$

**5.4. Concluding the proof.** Substituting (5.13) and (5.16) in (5.3) we derive

$$\begin{aligned} &V_\lambda(\Gamma, \mathcal{S}; T, X) \\ &\leq X^{1/2} T^2 + (Y + X^{1-\varrho}) T^{2+o(1)} + X^{3/2} T^{3/2} \left( 1 + \frac{S^{1/2}}{Y} \right) X^{o(1)}. \end{aligned}$$

Recalling the choice of  $Y$  in (5.2) the above simplifies to

$$\begin{aligned} &V_\lambda(\Gamma, \mathcal{S}; T, X) \\ &\leq (X^{1/2} T^2 + X^{1-\varrho/4} T^2 + X^{3/2} T^{3/2} + X^{3/4} T^{7/8} S^{1/4}) X^{o(1)}, \end{aligned}$$

and the result follows with  $\rho = \varrho/4$  (as clearly  $\varrho \leq 1$  and thus  $\rho < 1/2$ )

## 6. PROOF OF THEOREM 2.3

First we note that without loss of generality we may assume the binary digits of  $a$  are zeros on all positions  $j \in \mathcal{S}$ .

For a prime  $p$ , let  $N_p(a; \mathcal{S})$  be the number of  $z \in \mathcal{N}(a; \mathcal{S})$  with  $p \mid z$ . One can easily see that  $N_p(a; \mathcal{S})$  is the number of solutions to the congruence

$$a + \sum_{n=1}^T d_n 2^{s_n} \equiv 0 \pmod{p}, \quad d_n \in \{0, 1\}, \quad n = 1, \dots, T.$$

We now proceed similarly to the proof of [15, Theorem 18.1]. Using the orthogonality of exponential functions, we write

$$\begin{aligned} N_p(a; \mathcal{S}) &= \frac{1}{p} \sum_{b=0}^{p-1} \sum_{(d_1, \dots, d_T) \in \{0, 1\}^T} \mathbf{e}_p \left( b \left( \sum_{n=1}^T d_n 2^{s_n} + a \right) \right) \\ &= 2^T p^{-1} + \frac{1}{p} \sum_{b=1}^{p-1} \sum_{(d_1, \dots, d_T) \in \{0, 1\}^T} \mathbf{e}_p \left( b \left( \sum_{n=1}^T d_n 2^{s_n} + a \right) \right) \\ &= 2^T p^{-1} + \frac{1}{p} \sum_{b=1}^{p-1} \mathbf{e}_p(ab) \prod_{n=1}^T (1 + \mathbf{e}_p(b 2^{s_n})). \end{aligned}$$

Therefore,

$$(6.1) \quad |N_{n,p}(a) - 2^T p^{-1}| \leq Q_p,$$

where

$$Q_p = \max_{b=1, \dots, p-1} \left| \prod_{n=1}^T (1 + \mathbf{e}_p(b 2^{s_n})) \right|.$$

Using [15, Equation (18.2)] we write

$$(6.2) \quad Q_p \leq \exp(O(M_p \log(T/M_p + 1))),$$

where

$$M_p = \max_{\gcd(b,p)=1} \left| \sum_{n \leq T} \mathbf{e}_p(a \lambda^{s_n}) \right|.$$

Now, by Theorem 2.2 if we fix some  $\varepsilon_0 > 0$ , then there is some  $\kappa > 0$  such that if

$$X = T^{1/(1+\varepsilon_0)}, \quad \Delta = X^{1/2} \quad \text{and} \quad S \leq X^{2-\varepsilon_0},$$

then we have

$$\sum_{p \in \mathcal{E}_\Delta(X)} M_p^2 \leq T^2 X^{1-\kappa}.$$

Since  $S \leq T^{2-\varepsilon}$ , to satisfy the above conditions, it is enough to define  $\varepsilon_0$  by the equation

$$\frac{2 - \varepsilon_0}{1 + \varepsilon_0} = 2 - \varepsilon$$

or, more explicitly,

$$\varepsilon_0 = \frac{\varepsilon}{3 - \varepsilon}.$$

Combining this with (2.8), we see that for all but  $o(X/\log X)$  primes  $p \leq X$  we have  $M_p \leq TX^{-\kappa/3}$ . For each of these primes  $p$ , a combination of (6.1) and (6.2) implies that  $N_p(a; \mathcal{S}) > 0$  (provided that  $p$  is large enough), which concludes the proof.

## 7. POSSIBLE IMPROVEMENTS

We note that one can get an improvement of Theorem 2.1 by using a combination of different admissible pairs depending on the range of  $d$  in our treatment of the sum (4.17) in and thus making the choice of  $\alpha$  and  $\beta$  in (4.26) dependent on  $i$  and  $j$ .

In particular, one can use the admissible pairs (2.1), (2.2), (2.3) and (2.4) as well the admissible pairs given by Konyagin [14] and Shteinikov [23] for small values of  $d$  in (4.17).

## ACKNOWLEDGEMENT

This work was partially supported by the NSF Grant DMS 1600154 (for M.-C. C.) and by the ARC Grant DP170100786 (for I. S.).

## REFERENCES

- [1] W. D. Banks, M. Z. Garaev, F. Luca and I. E. Shparlinski, ‘Uniform distribution of fractional parts related to pseudoprimes’, *Canad. J. Math.*, **61** (2009), 481–502. (p. 2)
- [2] J. Bourgain, ‘Prescribing the binary digits of primes’, *Israel J. Math.*, **194** (2013), 935–955. (p. 3)
- [3] J. Bourgain, ‘Prescribing the binary digits of primes, II’, *Israel J. Math.*, **206** (2015), 165–182. (p. 3)
- [4] J. Bourgain and M.-C. Chang, ‘Exponential sum estimates over subgroups and almost subgroups of  $\mathbb{Z}_Q^*$ , where  $Q$  is composite with few prime factors’, *Geom. Funct. Anal.*, **16** (2006), 327–366. (pp. 3 and 8)
- [5] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, ‘Estimates for the number of sums and products and for exponential sums in fields of prime order’, *J. Lond. Math. Soc.*, **73** (2006), 380–398. (pp. 3, 4, and 5)
- [6] R. Dietmann, C. Elsholtz and I. E. Shparlinski, ‘Prescribing the binary digits of squarefree numbers and quadratic residues’, *Trans. Amer. Math. Soc.*, (to appear). (p. 4)
- [7] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*. Lecture Notes in Mathematics 1651, Springer-Verlag, New York, 2000. (p. 6)

- [8] P. Erdős and M. R. Murty, ‘On the order of  $a \bmod p$ .’. In: Number theory, CRM Proc. Lecture Notes 19, American Mathematical Society, Providence, PI, 1999, pp. 87–97. (pp. [2](#) and [6](#))
- [9] M. Z. Garaev, ‘The large sieve inequality for the exponential sequence  $\lambda^{\mathcal{O}(n^{15/14+o(1)})}$  modulo primes’, *Canad. J. Math.*, **61**, (2009), 336–350. (pp. [2](#), [3](#), [6](#), and [10](#))
- [10] M. Z. Garaev and I. E. Shparlinski, ‘The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes’, *Intern. Math. Research Notices*, **39** (2005), 2391–2408. (p. [2](#))
- [11] G. Harman and I. Katai, ‘Primes with preassigned digits II’, *Acta Arith.*, **133** (2008), 171–184. (p. [3](#))
- [12] D. R. Heath–Brown and S. V. Konyagin, ‘New bounds for Gauss sums derived from  $k$ th powers, and for Heilbronn’s exponential sum’, *Quart. J. Math.*, **51**, (2000), 221–235. (pp. [3](#) and [4](#))
- [13] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004. (pp. [1](#) and [7](#))
- [14] S. V. Konyagin, ‘Bounds of exponential sums over subgroups and Gauss sums’, *Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications*, Moscow Lomonosov State Univ., Moscow, 2002, 86–114 (in Russian). (p. [29](#))
- [15] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999. (pp. [2](#), [3](#), [7](#), and [28](#))
- [16] N. M. Korobov, ‘On the distribution of digits in periodic fractions’, *Matem. Sbornik*, **89**, (1972), 654–670 (in Russian). (p. [4](#))
- [17] E. Kowalski, *The large sieve and its applications. Arithmetic geometry, random walks and discrete groups*, Cambridge Tracts in Math. 175. Cambridge Univ. Press, Cambridge, 2008. (p. [1](#))
- [18] O. Ramaré, *Arithmetical aspects of the large sieve inequality*, Harish-Chandra Research Institute Lecture Notes, 1. Hindustan Book Agency, New Delhi, 2009. (p. [1](#))
- [19] I. D. Shkredov, ‘Some new inequalities in additive combinatorics’, *Moscow J. Comb. and Number Theory*, **3** (2013), 237–288. (p. [4](#))
- [20] I. D. Shkredov, ‘On exponential sums over multiplicative subgroups of medium size’, *Finite Fields Appl.* **30**, (2014) 72–87. (p. [4](#))
- [21] I. E. Shparlinski, ‘Exponential sums and prime divisors of sparse integers’, *Period. Math. Hungarica*, **57** (2008), 93–99. (p. [2](#))
- [22] I. E. Shparlinski, ‘Bilinear sums with exponential functions’, *Proc. Amer. Math. Soc.*, **137** (2009), 2217–2224. (p. [2](#))
- [23] Y. N. Shteinikov, ‘Estimates of trigonometric sums over subgroups and some of their applications’, *Matem. Zametki*, **98** (2015), 606–625 (in Russian). (p. [29](#))

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA. RIVERSIDE,  
CA 92521, USA

*E-mail address:* `mcc@math.ucr.edu`

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,  
SYDNEY, NSW 2052, AUSTRALIA

*E-mail address:* `bryce.kerr89@gmail.com`

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,  
SYDNEY, NSW 2052, AUSTRALIA

*E-mail address:* `igor.shparlinski@unsw.edu.au`