Canad. J. Math. Vol. **61** (2), 2009 pp. 336–350

The Large Sieve Inequality for the Exponential Sequence $\lambda^{[O(n^{15/14+o(1)})]}$ Modulo Primes

M. Z. Garaev

Abstract. Let λ be a fixed integer exceeding 1 and s_n any strictly increasing sequence of positive integers satisfying $s_n \le n^{15/14+o(1)}$. In this paper we give a version of the large sieve inequality for the sequence λ^{s_n}. In particular, we obtain nontrivial estimates of the associated trigonometric sums "on average" and establish equidistribution properties of the numbers $\lambda^{s_n}, n \le p(\log p)^{2+\varepsilon}$, modulo p for most primes p.

1 Introduction

Studying trigonometric sums with exponential functions is a traditional question with a variety of results and numerous applications, for a detailed description see the Introduction of [10] and extensive references therein. Recently, in a series of works, spectacular results in this area have been obtained [3–5]. One such result, given by Bourgain, Glibichuk, and Konyagin [4], states that there exist positive constants C_1, C_2, and C_3 such that for $\delta > 0$, $\mathcal{A} \subset \mathbb{Z}_p^*$ with $|\mathcal{A}| \ge p^\delta$ and any $k \ge \delta^{-C_3}$ the following bound holds:

$$\max_{(a,p)=1} \Big| \sum_{x_1,\dots,x_k \in \mathcal{A}} e^{2\pi i a x_1 \dots x_k/p} \Big| < |\mathcal{A}|^k p^{-\gamma}, \quad \gamma = \exp(-C_1/\delta^{C_2}).$$

Here p denotes a prime number, $\mathbb{Z}_p^*$ is a multiplicative group of nonzero elements of the field $\mathbb{Z}_p$, and $|\mathcal{A}|$ is the cardinality of $\mathcal{A}$. Its direct consequence is the bound of the type

$$\max_{(a,p)=1} \Big| \sum_{z=1}^{t} e^{2\pi i a \lambda^z/p} \Big| < t p^{-\gamma} \tag{1.1}$$

for $t > p^\delta$, where t denotes the multiplicative order of λ modulo p, (see also [4, Corollary 1] for the estimate of incomplete sums). The best previously known result gave a nontrivial estimate only for $t > p^{1/4+\delta}$, (see [14]).

Deep results in this spirit have been obtained by Bourgain [3] for double trigonometric sums with exponential functions over short intervals. Among many other

Received by the editors May 3, 2006; revised September 28, 2006.
The author was supported by the Project PAPIIT-IN105605 from the UNAM.
AMS subject classification: Primary: 11L07; secondary: 11N36.
Keywords: Large sieve, exponential sums.

applications, these results, in combination with the approach of [1], have been used to obtain equidistribution properties of Mersenne numbers $M_q = 2^q - 1, q < N$, modulo p for most primes p, provided $N > t^{2+\varepsilon}$, where t is the multiplicative order of 2 modulo p, (see [3, Theorem 6, Corollaries 7, 8] for the precise statements).

An alternative approach has been suggested in [10], based on the large sieve inequality, to obtain nontrivial estimates of trigonometric sums with exponential functions and to investigate the problem of distribution of $\lambda^n \pmod p, n \in \mathcal{S}$, for general sets $\mathcal{S}$, "on average" over primes p. From the result of Erdős and Murty [8] we know that for a fixed λ the estimate $t_p > X^{1/2+o(1)}$ holds for almost all primes $p \le X$, where $t_p = t_p(\lambda)$ denotes the multiplicative order of λ modulo p. This has been used in [10] to obtain a nontrivial bound for the exponential sum

$$\max_{(a,p)=1} \Big| \sum_{n \in \mathcal{S}_N} \mathbf{e}_p(a\lambda^n) \Big|$$

for $\pi(X) + o(\pi(X))$ primes $p \le X$, provided that $\mathcal{S}_N \subset [1, N]$ is sufficiently dense (that is $|\mathcal{S}_N| > N^{1+o(1)}$) and N is of the size $X^{1+o(1)}$.

The result in [10] does not apply to sparser sets $\mathcal{S}_N$, but it is shown that such results can be obtained conditionally; for example, assuming the truth of the Extended Riemann Hypothesis one can get nontrivial results for sparse sets of cardinality as small as $|\mathcal{S}_N| \ge N^{1/2+\varepsilon}$.

In this paper we provide a new argument which allows us to deal with sparse sets $\mathcal{S}_N$ unconditionally and which improves the corresponding result of [10] for dense sets $\mathcal{S}_N$ too. In particular, we obtain equidistribution properties of $\lambda^n \pmod p, n \in \mathcal{S}_N$, with $|\mathcal{S}_N| > N^{14/15-o(1)}$. Furthermore, while the result of [10] only applies for the set of primes $p \le X$ with $t_p > X^{1/2}(\log X)^c$, $c > 0$, our results work when $t_p > \Delta$, where, depending on how sparse the set $\mathcal{S}_N$ is, Δ varies in $(X^{1/3+\varepsilon}, X^{1/2+o(1)}]$. This is important in obtaining sharp estimates for the exceptional set of primes p in the equidistribution problem of the sequence $\lambda^n \pmod p$, $n \in \mathcal{S}_N$, and in obtaining exponential cancellations in upper bound estimates for the associated trigonometric sums. In particular, Theorem 3.1 with $\Delta \approx X^{1/2}(\log X)^{-10}$ has found its appliction in [2], where equidistribution properties of sequences related to pseudoprimes have been established.

The underlying idea of our approach is to tie our problem to the set of exponent pairs for Gauss sums via the large sieve inequality, see Section 7 for the definition. The results of this paper correspond to the pair due to Heath-Brown and Konyagin. We show that further improvements can be obtained if one knows how to complement in a specific way the set of exponent pairs for Gauss sums given by Konyagin [14]. In particular, we establish a connection between our problem and the conjecture of Montgomery, Vaughan, and Wooley [15].

2 Notation

Throughout the paper the following notations will be used:

λ denotes a fixed positive integer, $\lambda \ge 2$;

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

X and T are large parameters, T is an integer;

$\Delta > X^{1/3}$ is a parameter;

s_n, $n = 1, 2, \dots$, is a strictly increasing sequence of positive integers (which may depend on the parameters X, T, Δ);

γ_n, $n = 1, 2, \dots$, are any complex coefficients (which may depend on the parameters X, T, Δ) with $|\gamma_n| \le 1$;

p and q always denote prime numbers;

$t_p = t_p(\lambda)$ denotes the multiplicative order of λ modulo p;

$\mathcal{E} = \mathcal{E}(\Delta, X) = \{p : p \le X, t_p > \Delta\}$; that is the set of all primes p, $p \le X$, with $t_p > \Delta$;

For integers a and b, their greatest common divisor is denoted by (a, b).

Given a set $\mathcal{X}$ we use $|\mathcal{X}|$ to denote its cardinality. As usual, $\pi(X)$ denotes the number of primes not exceeding X, and $\tau(n)$ denotes the number of positive integer divisors of n. We also follow the standard abbreviation $e_m(z) = e^{2\pi i z/m}$.

In what follows, we use the Landau symbol 'o', as well as the Vinogradov symbols '$\ll$' and '$\gg$' with their usual meanings. The implied constants may depend on the small positive quantity ε, λ, and other fixed constants, and also on the choice of the function $\nu(n)$ (in Corollary 3.2 below, see also (3.1)).

3 Results

The following statement is the main result of our paper. We recall that $s_1, s_2, \dots$, is any sequence of strictly increasing positive integers.

Theorem 3.1 *For any $L > 0$ the following bound holds:*

$$\sum_{p\in\mathcal{E}} \frac{1}{\tau(p-1)} \max_{(a,p)=1} \Big| \sum_{n\le T} \gamma_n \mathbf{e}_p(a\lambda^{s_n}) \Big|^2 \ll (X + s_T X^{1/7}\Delta^{-3/7}L + TL^{-7/4})XT.$$

If we optimize the choice of L, then the estimate can be reformulated in the form

$$\sum_{p\in\mathcal{E}} \frac{1}{\tau(p-1)} \max_{(a,p)=1} \Big| \sum_{n\le T} \gamma_n \mathbf{e}_p(a\lambda^{s_n}) \Big|^2 \ll (1 + (s_T^7 T^4 X^{-10}\Delta^{-3})^{1/11})X^2T.$$

As we have already mentioned in the Introduction, the result of [8] implies that for $\pi(X)(1+o(1))$ primes p, $p \le X$, the inequality $t_p > X^{1/2+g(X)}$ holds for any given function $g(x) = o(1)$. With this in mind, assume that the sequence s_n satisfies the condition

$$s_n \le n^{15/14+\nu_n}, \quad \lim_{n\to\infty} \nu_n = 0, \tag{3.1}$$

where ν_n is an absolutely fixed sequence (which, therefore, does not depend on the parameters T, X, Δ). Set $T = [X(\log X)^{2+\varepsilon}]$ and define $L = T^{|\nu_T|}(\log T)^{10}$, $\Delta =$

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

$T^{1/2}L^7$. Obviously, $L^7 = X^{o(1)}$, $\Delta = X^{1/2+o(1)}$ as $X \to \infty$. Therefore, $|\mathcal{E}| = \pi(X)(1 + o(1))$. Incorporating this choice of the parameters in Theorem 3.1, we obtain

$$\sum_{p\in\mathcal{E}} \frac{1}{\tau(p-1)} \max_{(a,p)=1} \Big| \sum_{n\le T} \gamma_n \mathbf{e}_p(a\lambda^{s_n}) \Big|^2 \ll X^2T + XT^2(\log T)^{-10} \ll XT^2(\log T)^{-2-\varepsilon}.$$

Next, let $\mathcal{E}'$ be the subset of $\mathcal{E}$ with $\tau(p-1) < (\log X)^{1+\varepsilon/2}$. From the Titchmarsh bound

$$\sum_{p\le X} \tau(p-1) \ll X \tag{3.2}$$

(see for example [11, Theorem 3.9] or [16, Chapter 5, Theorem 7.1]) it follows that the inequality $\tau(p-1) \ll (\log X)^{1+\varepsilon/2}$ holds for $\pi(X)(1 + O((\log X)^{-\varepsilon/2}))$ primes $p,\ p \le X$. That is, we still have $|\mathcal{E}'| = \pi(X)(1 + o(1))$. Now, we restrict the range of summation over p in the above bound to $\mathcal{E}'$. Then

$$\sum_{p\in\mathcal{E}'} \max_{(a,p)=1} \Big| \sum_{n\le T} \gamma_n \mathbf{e}_p(a\lambda^{s_n}) \Big|^2 \ll \pi(X)T^2(\log T)^{-\varepsilon/2}.$$

From this, by taking $\gamma_n = 1$, we deduce the following consequence.

Corollary 3.2 *Let s_n satisfy the condition* (3.1) *and let $T = [X(\log X)^{2+\varepsilon}]$. Then the inequality*

$$\max_{(a,p)=1} \Big| \sum_{n\le T} e^{2\pi i \frac{a\lambda^{s_n}}{p}} \Big| \ll T(\log T)^{-\varepsilon/5}$$

holds for all primes $p,\ p \le X$, except at most $o(\pi(X))$ of them.

We recall that the *discrepancy* D of a sequence of N points $(x_j)_{j=1}^N$ of the unit interval $[0, 1)$ is defined as

$$D = \sup_{0\le a,b\le 1} \Big| \frac{A(a,b)}{N} - (b-a) \Big|,$$

where $A(a, b)$ is the number of points of this sequence which belong to $[a, b)$.

Now let $D(p, X)$ denote the discrepancy of the fractional parts $\{\lambda^{s_n}/p\}$, $n \le X(\log X)^{2+\varepsilon}$, where s_n satisfies the condition (3.1). According to the well-known Erdős–Turán relation between the discrepancy and the associated exponential sums (see, for example, [7]), we derive from Corollary 3.2 that for $\pi(X)(1 + o(1))$ primes $p,\ p \le X$, the following bound holds with some $\varepsilon_1 > 0$: $D(p, X) \ll (\log X)^{-\varepsilon_1}$. In other words, the numbers $\lambda^{s_n}, n \le X(\log X)^{2+\varepsilon}$ are uniformly distributed modulo p for any given $\varepsilon > 0$. In particular, one can take $s_n = [q_n^c]$, where $1 \le c \le 15/14$ and q_n denotes the n-th prime number.

The following statement is an analogy of Theorem 3.1, where the range of summation over n now depends on p.

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

Theorem 3.3 *Let T_p, $p \in \mathcal{E}$, be any positive integers with $T_p \le T$ and let $\mathcal{E}_1 \subset \mathcal{E}$. For any positive numbers L and K the following bound holds:*

$$\sum_{p\in\mathcal{E}_1}\frac{1}{\tau(p-1)}\max_{(a,p)=1}\Big|\sum_{n\le T_p}\gamma_n\mathbf{e}_p(a\lambda^{s_n})\Big|^2 \ll (X+s_TX^{1/7}\Delta^{-3/7}L+TL^{-7/4})XT(\log K)^2+\frac{T^2}{K^2}\sum_{p\in\mathcal{E}_1}\frac{1}{\tau(p-1)}.$$

Taking $\mathcal{E}_1=\mathcal{E}$ and $K=T$ and observing that the last term never dominates, we see that Theorem 3.3 extends Theorem 3.1 to more general sums at the cost of the slight factor $(\log T)^2$. In some applications one can further relax this factor by special choices of $\mathcal{E}_1$ and K.

One may want to have an explicit estimate for $|\overline{\mathcal{E}}|$, where $\overline{\mathcal{E}}=\{p:\ p\le X, p\notin\mathcal{E}\}$. In this connection we remark that the argument given in [8] immediately yields the bound

$$|\overline{\mathcal{E}}| \ll \frac{\Delta^2}{\log\Delta}.$$

Indeed

$$\prod_{p\in\overline{\mathcal{E}}} p \mid \prod_{k\le\Delta}(\lambda^k-1),$$

Therefore, if $\omega(n)$ denotes the number of prime divisors of n, then we have

$$|\overline{\mathcal{E}}| \ll \omega\Big(\prod_{k\le\Delta}(\lambda^k-1)\Big) \ll \frac{\Delta^2}{\log\Delta},$$

where we have used the well-known estimate $\omega(n)\ll(\log n)(\log\log n)^{-1}$.

For $\Delta=X^{1/2+o(1)}$ one can use the results from [13] and [9].

4 Lemmas

We need the version of the large sieve inequality applied to our situation (recall that $|\gamma_n|\le 1$).

Lemma 4.1 *For any $K\ge 1$ the following estimate holds:*

$$\sum_{k\le K}\sum_{\substack{1\le c\le k\\(c,k)=1}}\Big|\sum_{n\le T}\gamma_n\mathbf{e}_k(cs_n)\Big|^2 \ll (K^2+s_T)T.$$

For the proof, see [6, pp. 153–154].

The following statement is due to Heath-Brown and Konyagin [12].

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

Lemma 4.2 *Let an integer* θ *be of multiplicative order* t *modulo* p*. Then the following bound holds:*

$$\max_{(a,p)=1}\left|\sum_{z=1}^{t}\mathbf{e}_p(a\theta^z)\right| \ll \min\{p^{1/2}, p^{1/4}t^{3/8}, p^{1/8}t^{5/8}\}.$$

Instead of Lemma 4.2 one can use the estimate (1.1), which however does not improve our final results.

5 Proof of Theorem 3.1

For $L \le 1$ the estimate of Theorem 3.1 is trivial. Therefore, we will suppose that $L > 1$.

Let

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

For each residue class $x \pmod{t_p}$ we first collect together the values of n for which $s_n \equiv x \pmod{t_p}$ and then express this condition by virtue of rational exponential sums. Then

$$\sigma_p(a) = \sum_{x=1}^{t_p}\sum_{\substack{n\le T\\ t_p\mid s_n-x}}\gamma_n\mathbf{e}_p(a\lambda^{s_n}) = \frac{1}{t_p}\sum_{x=1}^{t_p}\sum_{b=1}^{t_p}\sum_{n\le T}\gamma_n\mathbf{e}_{t_p}(b(s_n-x))\mathbf{e}_p(a\lambda^x).$$

For each divisor $d|t_p$ we collect together the values of b with $(b,t_p)=d$. Thus

$$\sigma_p(a) = \frac{1}{t_p}\sum_{d\mid t_p}\sum_{x=1}^{t_p}\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(c(s_n-x))\mathbf{e}_p(a\lambda^x).$$

We treat the cases of big and small values of d separately. For big values of d we will enjoy the summation over x in a proper way to get cancellations that are sufficient to our purposes. The small values of d are treated in a different way. Thus, we define $v_p = t_p^{4/7}p^{1/7}$ and set

$$R_1 = \max_{(a,p)=1}\left|\frac{1}{t_p}\sum_{\substack{d\mid t_p\\ d\ge Lv_p}}\sum_{x=1}^{t_p}\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(c(s_n-x))\mathbf{e}_p(a\lambda^x)\right|, \tag{5.1}$$

$$R_2 = \max_{(a,p)=1}\left|\frac{1}{t_p}\sum_{\substack{d\mid t_p\\ d< Lv_p}}\sum_{x=1}^{t_p}\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(c(s_n-x))\mathbf{e}_p(a\lambda^x)\right|. \tag{5.2}$$

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

Then $\max_{(a,p)=1}|\sigma_p(a)|\le R_1+R_2$. In particular,

$$\sum_{p\in\mathcal{E}}\frac{1}{\tau(p-1)}\max_{(a,p)=1}|\sigma_p(a)|^2\le\sum_{p\in\mathcal{E}}\frac{R_1^2}{\tau(p-1)}+\sum_{p\in\mathcal{E}}\frac{R_2^2}{\tau(p-1)}. \tag{5.3}$$

Our aim is to estimate the sums on the right hand side of (5.3).

To estimate R_1, we divide the interval of summation over x to progressions of the form $y+zt_p/d,\ 1\le y\le t_p/d,\ 1\le z\le d$. Then

$$R_1=\max_{(a,p)=1}\Big|\frac{1}{t_p}\sum_{\substack{d|t_p\\ d\ge Lv_p}}\sum_{y=1}^{t_p/d}\sum_{z=1}^{d}\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(c(s_n-y))\mathbf{e}_p(a\lambda^y\lambda^{zt_p/d})\Big|,$$

whence

$$R_1\ll\frac{1}{t_p}\sum_{\substack{d|t_p\\ d\ge Lv_p}}\sum_{y=1}^{t_p/d}\Big|\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(c(s_n-y))\Big|\max_{(a,p)=1}\Big|\sum_{z=1}^{d}\mathbf{e}_p(a\lambda^y\lambda^{zt_p/d})\Big|.$$

The sum over z is estimated by Lemma 4.2. Since $\lambda^{t_p/d}$ is an element of multiplicative order d, we derive the following from Lemma 4.2:

$$\max_{(a,p)=1}\Big|\sum_{z=1}^{d}\mathbf{e}_p(a\lambda^y\lambda^{zt_p/d})\Big|\ll p^{1/8}d^{5/8}.$$

Therefore,

$$R_1\ll\sum_{\substack{d|t_p\\ d\ge Lv_p}}p^{1/8}d^{5/8}R_3, \tag{5.4}$$

where

$$R_3=\frac{1}{t_p}\sum_{y=1}^{t_p/d}\Big|\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(c(s_n-y))\Big|.$$

Next, applying the Cauchy inequality we obtain

$$R_3^2\ll\frac{1}{dt_p}\sum_{y=1}^{t_p/d}\Big|\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(c(s_n-y))\Big|^2=$$

$$\frac{1}{dt_p}\sum_{y=1}^{t_p/d}\sum_{\substack{c_1\le t_p/d\\ (c_1,t_p/d)=1}}\sum_{\substack{c_2\le t_p/d\\ (c_2,t_p/d)=1}}\sum_{n_1\le T}\sum_{n_2\le T}\gamma_{n_1}\overline{\gamma}_{n_2}\mathbf{e}_{t_p/d}(c_1(s_{n_1}-y)-c_2(s_{n_2}-y)).$$

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

Observe that

$$\sum_{y=1}^{t_p/d} \mathbf{e}_{t_p/d}(-c_1 y + c_2 y) = \begin{cases} t_p/d, & \text{if } c_1 \equiv c_2 \pmod{t_p/d}, \\ 0, & \text{if } c_1 \not\equiv c_2 \pmod{t_p/d}. \end{cases}$$

Hence,

$$R_3^2 \ll \frac{1}{d^2} \sum_{\substack{c \le t_p/d \\ (c, t_p/d)=1}} \sum_{n_1 \le T} \sum_{n_2 \le T} \gamma_{n_1} \overline{\gamma}_{n_2} \mathbf{e}_{t_p/d}(c(s_{n_1} - s_{n_2})).$$

Estimating trivially the sums over c, n_1, and n_2 we obtain $R_3^2 \ll \frac{t_p}{d^3} T^2$. Substituting this in (5.4), we derive that

$$R_1^2 \ll \tau(p-1) T^2 \sum_{\substack{d \mid t_p \\ d \ge L v_p}} \frac{p^{1/4} t_p}{d^{7/4}}.$$

Since $v_p = t_p^{4/7} p^{1/7}$, we have

$$R_1^2 \ll \tau(p-1)^2 T^2 \frac{p^{1/4} t_p}{(L v_p)^{7/4}} = \tau(p-1)^2 T^2 L^{-7/4},$$

whence

$$\frac{R_1^2}{\tau(p-1)} \ll \tau(p-1) T^2 L^{-7/4}.$$

Application of the Titchmarsh estimate (3.2) yields

$$\sum_{p \in \mathcal{E}} \frac{R_1^2}{\tau(p-1)} \ll X T^2 L^{-7/4}. \tag{5.5}$$

Now we proceed to treat R_2. From (5.2) we have

$$R_2 \le \frac{1}{t_p} \sum_{\substack{d \mid t_p \\ d < L v_p}} \sum_{x=1}^{t_p} \Bigg| \sum_{\substack{c \le t_p/d \\ (c, t_p/d)=1}} \sum_{n \le T} \gamma_n \mathbf{e}_{t_p/d}(c(s_n - x)) \Bigg|.$$

We apply the Cauchy inequality to the sums over d and x and then obtain

$$R_2^2 \ll \frac{\tau(p-1)}{t_p} \sum_{\substack{d \mid t_p \\ d < L v_p}} \sum_{x=1}^{t_p} \Bigg| \sum_{\substack{c \le t_p/d \\ (c, t_p/d)=1}} \sum_{n \le T} \gamma_n \mathbf{e}_{t_p/d}(c(s_n - x)) \Bigg|^2,$$

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

whence

$$\frac{R_2^2}{\tau(p-1)} \ll$$

$$\frac{1}{t_p}\sum_{\substack{d\mid t_p\\ d<Lv_p}}\sum_{x=1}^{t_p}\sum_{\substack{c_1\le t_p/d\\ (c_1,t_p/d)=1}}\sum_{\substack{c_2\le t_p/d\\ (c_2,t_p/d)=1}}\sum_{n_1\le T}\sum_{n_2\le T}\gamma_{n_1}\overline{\gamma}_{n_2}\mathbf{e}_{t_p/d}(c_1(s_{n_1}-x)-c_2(s_{n_2}-x)).$$

The summation over x guarantees that $c_1=c_2$. Therefore,

$$\frac{R_2^2}{\tau(p-1)} \ll \sum_{\substack{d\mid t_p\\ d<Lv_p}}\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\sum_{n_1\le T}\sum_{n_2\le T}\gamma_{n_1}\overline{\gamma}_{n_2}\mathbf{e}_{t_p/d}(c(s_{n_1}-s_{n_2})),$$

whence

$$\frac{R_2^2}{\tau(p-1)} \ll \sum_{\substack{d\mid t_p\\ d<Lv_p}}\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\Big|\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(cs_n)\Big|^2.$$

Summing up both sides of this bound over $p\in\mathcal{E}$, we obtain

$$\sum_{p\in\mathcal{E}}\frac{R_2^2}{\tau(p-1)} \ll \sum_{p\in\mathcal{E}}\sum_{\substack{d\mid t_p\\ d<Lv_p}}\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\Big|\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(cs_n)\Big|^2.$$

We divide the interval $(\Delta, X]$ into disjoint subintervals $(X_j, X_{j+1}]$, where

$$X_1=\Delta,\quad X_{j+1}=\min\{2X_j, X\}.$$

Denote by $\mathcal{E}_j$ the subset of $\mathcal{E}$ such that $t_p\in(X_j,X_{j+1}]$ for any $p\in\mathcal{E}_j$. Next, define

$$V_j=2X_j^{4/7}X^{1/7}$$

and observe that V_j does not depend on p, and $V_j\ge v_p$ for any $p\in\mathcal{E}_j$. Thus,

$$\sum_{p\in\mathcal{E}}\frac{R_2^2}{\tau(p-1)} \ll \sum_j\sum_{p\in\mathcal{E}_j}\sum_{\substack{d\mid t_p\\ d<LV_j}}\sum_{\substack{c\le t_p/d\\ (c,t_p/d)=1}}\Big|\sum_{n\le T}\gamma_n\mathbf{e}_{t_p/d}(cs_n)\Big|^2.$$

We remember that $j\ll\log X$, $2^jX_1\ll X$ and $\Delta\le X_j<X_{j+1}\le 2X_j\le 2X$. Note that for different primes p, $p\in\mathcal{E}_j$, the corresponding values of t_p do not have to be different. For a given $r\in(X_j,X_{j+1}]$ denote by $s(r)$ the number of all primes p, $p\in\mathcal{E}_j$, for which $t_p=r$. Since $p-1\equiv 0 \pmod r$, we have $s(r)\le X/r\le X/X_j$. Therefore,

$$\sum_{p\in\mathcal{E}}\frac{R_2^2}{\tau(p-1)} \ll \sum_j\frac{X}{X_j}\sum_{r\in(X_j,X_{j+1}]}\sum_{\substack{d\mid r\\ d<LV_j}}\sum_{\substack{c\le r/d\\ (c,r/d)=1}}\Big|\sum_{n\le T}\gamma_n\mathbf{e}_{r/d}(cs_n)\Big|^2.$$

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

Changing the order of summation over r and d we deduce

$$\sum_{p\in\mathcal{E}}\frac{R_2^2}{\tau(p-1)} \ll \sum_j \frac{X}{X_j}\sum_{d<LV_j} F_j(d), \tag{5.6}$$

where

$$\begin{aligned} F_j(d) &= \sum_{\substack{r\in(X_j,X_{j+1}]\\ r\equiv 0 \pmod d}} \sum_{\substack{1\le c\le r/d\\ (c,r/d)=1}} \Big|\sum_{n\le T}\gamma_n \mathbf{e}_{r/d}(cs_n)\Big|^2 \\ &= \sum_{k\in(X_jd^{-1},X_{j+1}d^{-1}]} \sum_{\substack{1\le c\le k\\ (c,k)=1}} \Big|\sum_{n\le T}\gamma_n \mathbf{e}_k(cs_n)\Big|^2. \end{aligned}$$

To estimate $F_j(d)$ we apply the large sieve inequality given in Lemma 4.1. Then

$$F_j(d) \ll (X_j^2d^{-2}+s_T)T.$$

Inserting this bound into (5.6), we obtain

$$\sum_{p\in\mathcal{E}}\frac{R_2^2}{\tau(p-1)} \ll \sum_j \frac{X}{X_j}\sum_{d<LV_j} (X_j^2d^{-2}+s_T)T,$$

whence

$$\sum_{p\in\mathcal{E}}\frac{R_2^2}{\tau(p-1)} \ll \sum_j X(X_j+s_TV_jLX_j^{-1})T.$$

Since $V_j = 2X_j^{4/7}X^{1/7}$, we have

$$\sum_{p\in\mathcal{E}}\frac{R_2^2}{\tau(p-1)} \ll XT\Big(\sum_j X_j + s_TLX^{1/7}\sum_j X_j^{-3/7}\Big).$$

Finally, from the definition of X_j we know that

$$\sum_j X_j \ll X, \qquad \sum_j X_j^{-3/7} \ll \Delta^{-3/7}.$$

Therefore,

$$\sum_{p\in\mathcal{E}}\frac{R_2^2}{\tau(p-1)} \ll XT(X+s_TX^{1/7}\Delta^{-3/7}L). \tag{5.7}$$

Theorem 3.1 now follows from (5.3), (5.5), and (5.7). ∎

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

6 Proof of Theorem 3.3

For $K \le 10$ the estimate of Theorem 3.3 is trivial. Therefore, we will suppose that $K > 10$.

Set $M = [T/K]$. Without loss of generality we may assume that for $n \ge 1$,

$$\gamma_{T+n} = 0, \quad s_{T+n} = s_T + n.$$

Applying the shifting argument we obtain

$$\Big|\sum_{n=1}^{T_p} \gamma_n \mathbf{e}_p(a\lambda^{s_n})\Big|^2 \ll \frac{1}{(M+1)^2}\Big|\sum_{n=1}^{T_p}\sum_{r=0}^{M} \gamma_{n+r}\mathbf{e}_p(a\lambda^{s_{n+r}})\Big|^2 + \frac{T^2}{K^2}. \tag{6.1}$$

Further, we have

$$\sum_{n=1}^{T_p}\sum_{r=0}^{M} \gamma_{n+r}\mathbf{e}_p(a\lambda^{s_{n+r}}) = \frac{1}{2T+1}\sum_{b=-T}^{T}\sum_{m=1}^{2T}\sum_{r=0}^{M}\sum_{n=1}^{T_p} \gamma_m e^{2\pi i \frac{b(n+r-m)}{2T+1}}\mathbf{e}_p(a\lambda^{s_m}). \tag{6.2}$$

By the Cauchy inequality,

$$\Big(\sum_{0<|b|\le T}\Big|\sum_{n=1}^{T_p}\sum_{r=0}^{M} e^{2\pi i\frac{b(n+r)}{2T+1}}\Big|\Big|\sum_{m=1}^{2T}\gamma_m e^{2\pi i\frac{bm}{2T+1}}\mathbf{e}_p(a\lambda^{s_m})\Big|\Big)^2 \ll$$

$$\Big(\sum_{0<|b|\le T}\Big|\sum_{n=1}^{T_p}\sum_{r=0}^{M} e^{2\pi i\frac{b(n+r)}{2T+1}}\Big|\Big)\times$$

$$\Big(\sum_{0<|b|\le T}\Big|\sum_{n=1}^{T_p}\sum_{r=0}^{M} e^{2\pi i\frac{b(n+r)}{2T+1}}\Big|\Big|\sum_{m=1}^{T}\gamma_m e^{2\pi i\frac{bm}{2T+1}}\mathbf{e}_p(a\lambda^{s_m})\Big|^2\Big).$$

Hence, using

$$\Big|\sum_{n=1}^{T_p} e^{2\pi i\frac{bn}{2T+1}}\Big| \ll \frac{T}{|b|},$$

we obtain the bound

$$\Big(\sum_{0<|b|\le T}\Big|\sum_{n=1}^{T_p}\sum_{r=0}^{M} e^{2\pi i\frac{b(n+r)}{2T+1}}\Big|\Big|\sum_{m=1}^{2T}\gamma_m e^{2\pi i\frac{bm}{2T+1}}\mathbf{e}_p(a\lambda^{s_m})\Big|\Big)^2 \ll$$

$$T^2\Big(\sum_{0<|b|\le T}\frac{|S(b)|}{|b|}\Big)\Big(\sum_{b=1}^{T}\frac{|S(b)|}{|b|}\Big|\sum_{m=1}^{T}\gamma_m e^{2\pi i\frac{bm}{2T+1}}\mathbf{e}_p(a\lambda^{s_m})\Big|^2\Big),$$

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

where

$$S(b) = \sum_{r=0}^{M} e^{2\pi i \frac{br}{2T+1}}. \tag{6.3}$$

Combining this with (6.1) and (6.2), we deduce

$$\Big|\sum_{n=1}^{T_p} \gamma_n \mathbf{e}_p(a\lambda^{s_n})\Big|^2 \ll \frac{1}{(M+1)^2}\Big(\sum_{0<|b|\le T} \frac{|S(b)|}{|b|}\Big) \Big(\sum_{0<|b|\le T} \frac{|S(b)|}{|b|}\Big|\sum_{m=1}^{T} \gamma_m e^{2\pi i \frac{bm}{2T+1}} \mathbf{e}_p(a\lambda^{s_m})\Big|^2\Big) + \Big|\sum_{m=1}^{T} \gamma_m \mathbf{e}_p(a\lambda^{s_m})\Big|^2 + \frac{T^2}{K^2}.$$

Now we take the maximum over a, $(a,p)=1$, and observe that the maximum of sums is not greater than the sum of maximums. We then divide the estimate by $\tau(p-1)$ and perform the summation over $p \in \mathcal{E}_1$. This yields

$$\sum_{p\in\mathcal{E}_1} \frac{1}{\tau(p-1)} \max_{(a,p)=1}\Big|\sum_{n=1}^{T_p} \gamma_n \mathbf{e}_p(a\lambda^{s_n})\Big|^2 \ll \frac{1}{(M+1)^2}\Big(\sum_{0<|b|\le T} \frac{|S(b)|}{|b|}\Big) \times \Big(\sum_{0<|b|\le T} \frac{|S(b)|}{|b|} \sum_{p\in\mathcal{E}_1} \frac{1}{\tau(p-1)} \max_{(a,p)=1}\Big|\sum_{m=1}^{T} \gamma_m e^{2\pi i \frac{bm}{2T+1}} \mathbf{e}_p(a\lambda^{s_m})\Big|^2\Big) + \sum_{p\in\mathcal{E}_1} \frac{1}{\tau(p-1)} \max_{(a,p)=1}\Big|\sum_{m=1}^{T} \gamma_m \mathbf{e}_p(a\lambda^{s_m})\Big|^2 + \frac{T^2}{K^2} \sum_{p\in\mathcal{E}_1} \frac{1}{\tau(p-1)}.$$

For each b, we apply Theorem 3.1 with γ_n substituted by $\gamma_n e^{2\pi i \frac{bn}{2T+1}}$ to the sum

$$\sum_{p\in\mathcal{E}_1} \frac{1}{\tau(p-1)} \max_{(a,p)=1}\Big|\sum_{m=1}^{T} \gamma_m e^{2\pi i \frac{bm}{2T+1}} \mathbf{e}_p(a\lambda^{s_m})\Big|^2.$$

Thus,

$$\sum_{p\in\mathcal{E}_1} \frac{1}{\tau(p-1)} \max_{(a,p)=1}\Big|\sum_{n=1}^{T_p} \gamma_n \mathbf{e}_p(a\lambda^{s_n})\Big|^2 \ll \Big(\frac{1}{(M+1)^2}\Big(\sum_{b=1}^{T} \frac{|S(b)|}{b}\Big)^2 + 1\Big) \Big(X + s_T X^{1/7}\Delta^{-3/7}L + TL^{-7/4}\Big) XT + \frac{T^2}{K^2} \sum_{p\in\mathcal{E}_1} \frac{1}{\tau(p-1)}.$$

Now it remains to prove that

$$\sum_{b=1}^{T} \frac{|S(b)|}{b} \ll (M+1)\log K.$$

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

To this end, choose $\ell = [\log K]$ and use the Holder inequality to obtain

$$\sum_{b=1}^{T}\frac{|S(b)|}{b} \le \Big(\sum_{b=1}^{2T+1}\frac{1}{b^{2\ell/(2\ell-1)}}\Big)^{1-1/2\ell}\Big(\sum_{b=1}^{2T+1}|S(b)|^{2\ell}\Big)^{1/2\ell}. \tag{6.4}$$

Next, we have

$$\sum_{b=1}^{2T+1}\frac{1}{b^{2\ell/(2\ell-1)}} \ll \int_1^{\infty} x^{-1-(2\ell-1)^{-1}}dx = 2\ell - 1 \ll \log K. \tag{6.5}$$

Besides, from the definition of $S(b)$, see (6.3), it follows

$$\sum_{b=1}^{2T+1}|S(b)|^{2\ell} = (2T+1)J, \tag{6.6}$$

where J denotes the number of solutions to the congruence

$$\sum_{i=1}^{\ell}x_i \equiv \sum_{i=1}^{\ell}y_i \pmod{(2T+1)}, \qquad 0 \le x_i, y_j \le M.$$

Since $M < T$, then the trivial estimate gives $J \le (M+1)^{2\ell-1}$. Besides, $T < K(M+1)$. Therefore,

$$\sum_{b=1}^{2T+1}|S(b)|^{2\ell} \ll K(M+1)^{2\ell},$$

whence, in view of (6.4)–(6.6), we conclude that

$$\sum_{b=1}^{T}\frac{|S(b)|}{b} \ll (\log K)(M+1)K^{1/(2\ell)} \ll (M+1)\log K. \qquad \blacksquare$$

7 Exponent Pairs for Gauss Sums

We remark that if in Lemma 4.2 we have the bound

$$\max_{(a,p)=1}\Big|\sum_{z=1}^{t}\mathbf{e}_p(a\theta^z)\Big| \ll p^{\alpha}t^{\beta} \tag{7.1}$$

with $0 \le \alpha, \beta \le 1$, then the right hand side of the estimate of Theorem 3.1 can be substituted by

$$(X + s_T X^{\frac{2\alpha}{3-2\beta}}\Delta^{-\frac{2-2\beta}{3-2\beta}}L + TL^{-3+2\beta})XT.$$

In particular, Corollary 3.2 holds for the sequence s_n satisfying

$$s_T \le T^{1+\frac{1-2\alpha-\beta}{3-2\beta}+o(1)}.$$

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press

Define $\mathcal{K}$ to be the set of all ordered pairs $\{\alpha, \beta\}$, $0 \le \alpha, \beta \le 1$, satisfying property (7.1). Konyagin [14] has proved that the set $\mathcal{K}$ contains the pairs $\{\alpha_n, \beta_n\}$ and $\{\alpha'_n, \beta'_n\}$ defined as

$$\alpha_n = \frac{1}{2n^2}, \quad \beta_n = 1 - \frac{2}{n^2} + \frac{1}{2^{n-1}n^2},$$
$$\alpha'_n = \frac{1}{2n(n+1)}, \quad \beta'_n = 1 - \frac{2}{n(n+1)} + \frac{3}{2^{n+1}n(n+1)}$$

for any positive integer n. Next we define the function $f\colon \mathcal{K} \to \mathbb{R}$ by

$$f(x, y) = 1 + \frac{1 - 2x - y}{3 - 2y}.$$

The problem is to find the biggest possible value of $f(x, y)$. The result of this paper corresponds to the pair $\{\alpha_2, \beta_2\}$ (which is due to Heath-Brown and Konyagin). Other pairs give less precise bounds. Next, we note that $\mathcal{K}$ is a convex set. That is, if

$$\{\alpha, \beta\} \in \mathcal{K}, \quad \{\alpha', \beta'\} \in \mathcal{K},$$

then for any x, $0 \le x \le 1$,

$$\{x\alpha + (1-x)\alpha', x\beta + (1-x)\beta'\} \in \mathcal{K}.$$

However, this property applied to any two given pairs, in particular to the pairs due to Konyagin, is not sufficient to get further improvements in our problem. It would be very interesting, similar to the set of exponent pairs, to carry out a method which would provide the nontrivial properties of $\mathcal{K}$. The truth of the conjecture of Montgomery, Vaughan, and Wooley [15] would imply $\{\varepsilon, 1/2 + \varepsilon\} \in \mathcal{K}$, which can be considered an analogy of the exponent pair hypothesis for Gauss sums.

Finally, we remark that the method we have applied leads to the following generalization of our main result.

Theorem 7.1 *For any $L > 0$, any pair $\{\alpha, \beta\} \in \mathcal{K}$ and any complex coefficients δ_n, $1 \le n \le T$, the following bound holds:*

$$\sum_{p \in \mathcal{E}} \frac{1}{\tau(p-1)} \max_{(a,p)=1} \Big| \sum_{n \le T} \delta_n \mathbf{e}_p(a\lambda^{s_n}) \Big|^2 \ll$$
$$X(X + s_T X^{\frac{2\alpha}{3-2\beta}} \Delta^{-\frac{2-2\beta}{3-2\beta}} L) \sum_{n \le T} |\delta_n|^2 + XL^{-3+2\beta} \Big(\sum_{n \le T} |\delta_n| \Big)^2,$$

where the implied constant depends only on the pair $\{\alpha, \beta\}$.

Acknowledgment The author is thankful to the referee for useful suggestions.

References

[1] W. D. Banks, A. Conflitti, J. B. Friedlander, and I. E. Shparlinski, *Exponential sums over Mersenne numbers.* Compos. Math. **140**(2004), no. 1, 15–30.

[2] W. D. Banks, M. Z. Garaev, F. Luca and I. E. Shparlinski, *Uniform distribution of fractional parts related to pseudoprimes.* Canad. J. Math., to appear.

[3] J. Bourgain, *Estimates on exponential sums related to the Diffie-Hellman distributions.* Geom. Funct. Anal. **15**(2005), no. 1, 1–34.

[4] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order.* J. London Math. Soc. (2) **73**(2006), no. 2, 380–398.

[5] J. Bourgain and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order.* C. R. Math. Acad. Sci. Paris **337**(2003), no. 2, 75–80.

[6] H. Davenport, *Multiplicative number theory.* Graduate Texts in Mathematics 74, Springer-Verlag, New York, 2000.

[7] M. Drmota and R. Tichy, *Sequences, discrepancies and applications.* Lecture Notes in Mathematics 1651, Springer-Verlag, Berlin, 1997.

[8] P. Erdős and M. R. Murty, *On the order of a* (mod p). In: Number theory, CRM Proc. Lecture Notes 19, American Mathematical Society, Providence, RI, 1999, pp. 87–97.

[9] K. Ford, *The distribution of integers with a divisor in a given interval.* Annals of Math. **168**(2008), no. 2, 367–433.

[10] M. Z. Garaev and I. E. Shparlinski, *The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes.* Int. Math. Res. Not. **39**(2005), no. 39, 2391–2408.

[11] H. Halberstam and H. E. Richert, *Sieve methods.* London Mathematical Society Monographs 4, Academic Press, London-New York, 1974.

[12] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum.* Q. J. Math. **51**(2000), no. 2, 221–235.

[13] K.-H. Indlekofer and N. M. Timofeev, *Divisors of shifted primes.* Publ. Math. Debrecen **60**(2002), no. 3-4, 307–345.

[14] S. V. Konyagin, *Bounds of exponential sums over subgroups and Gauss sums.* In: IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part III (Russian) Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002, pp. 86–114 (in Russian).

[15] H. L. Montgomery, R. C. Vaughan, and T. D. Wooley, *Some remarks on Gauss sums associated with kth powers.* Math. Proc. Cambridge Philos. Soc. **118**(1995), no. 1, 21–33.

[16] K. Prachar, *Primzahlverteilung.* Springer-Verlag, Berlin, 1957.

Instituto de Matemáticas, Universidad Nacional Aútonoma de México, Campus Morelia, Ap. Postal 61-3 (Xangari), C.P. 58089, Morelia, Michoacán, México
e-mail: garaev@matmor.unam.mx

https://doi.org/10.4153/CJM-2009-017-3 Published online by Cambridge University Press