Mathematika 58 (2012) 11–20
doi:10.1112/S0025579311002117

ON THE CONSECUTIVE POWERS OF A PRIMITIVE ROOT: GAPS AND EXPONENTIAL SUMS

SERGEI V. KONYAGIN AND IGOR E. SHPARLINSKI

Abstract. For a primitive root g modulo a prime $p \geq 1$ we obtain upper bounds on the gaps between the residues modulo p of the N consecutive powers ag^n, $n = 1, \ldots, N$, which is uniform over all integers a with $\gcd(a, p) = 1$.

§1. *Introduction.* For a prime p we denote by $\mathbb{F}_p$ the finite field of p elements.

Given a primitive root $g \in \mathbb{F}_p^*$ and an integer $N \geq 1$ we denote by $H_{g,p}(N)$ the largest gaps between the residues modulo p of the N consecutive powers ag^n, $n = 1, \ldots, N$, (taken over all $a \in \mathbb{F}_p^*$). That is, denoting by $\mathcal{G}_{g,p}(N) \subseteq \mathbb{F}_p$ the set of residues of $g, \ldots, g^N$ modulo p, we have

$$H_{g,p}(N) = \max\{H : \exists a \in \mathbb{F}_p^*, \exists u \in \mathbb{F}_p \text{ such that } \{u+1, \ldots, u+H\} \cap a \cdot \mathcal{G}_{g,p}(N) = \emptyset\}.$$

In the case where $N = t$ is the multiplicative order of g modulo an integer $m \geq 2$, non-trivial bounds on the similar quantity have been obtained in [4, 5]; see also [1, 3, 12] for some applications.

One can immediately estimate $H_{g,p}(N)$ directly via the bound of Bourgain and Garaev [2, Corollary 1.2] on exponential sums

$$S_{g,p}(\lambda, N) = \sum_{n=1}^{N} \mathbf{e}_p(\lambda g^n),$$

where

$$\mathbf{e}_p(z) = \exp(2\pi \mathrm{i} z/p).$$

It particular, by [2, Corollary 1.2] we have

$$\max_{\gcd(\lambda,p)=1} |S_{g,p}(\lambda, N)| \leq N^{215/217+o(1)}, \tag{1}$$

for

$$p^{1/2} < N < p, \tag{2}$$

as $p \to \infty$.

We start with an observation that one can get a better estimate by slightly modifying the argument of the proof of [2, Corollary 1.2].

Received 23 January 2011, published online 8 November 2011.
MSC (2000): 11A07 (primary), 11B05, 11B50, 11T23 (secondary).

THEOREM 1. *For any primitive root $g \in \mathbb{F}_p$ and an integer N the following bound holds:*

$$\max_{\gcd(\lambda,p)=1} |S_{g,p}(\lambda, N)| \le \begin{cases} p^{1/8+o(1)} N^{71/96} & \text{if } N \le p^{1/2}, \\ p^{23/96+o(1)} N^{49/96} & \text{if } p^{1/2} < N < p, \end{cases}$$

as $p \to \infty$.

In particular, in the range (2) we improve (1) as

$$\max_{\gcd(\lambda,p)=1} |S_{g,p}(\lambda, N)| \le N^{95/96+o(1)}.$$

We now immediately obtain from Theorem 1 that, for any $u \in \mathbb{F}_p$ and $a \in \mathbb{F}_p^*$, under the condition (2) we have

$$\#(\{u+1, \ldots, u+H\} \cap a \cdot \mathcal{G}_{g,p}(N)) = \frac{NH}{p} + O(p^{23/96+o(1)} N^{49/96}).$$

Thus

$$H_{g,p}(N) \le p^{119/96+o(1)} N^{-47/96} \tag{3}$$

for all N in the range (2). Using some other bounds, such as the bound of Korobov [9]

$$\max_{\gcd(a,p)=1} \left| \sum_{n=1}^{N} \mathbf{e}_p(ag^n) \right| = O(p^{1/2} \log p),$$

one can improve the bound (3) in some subintervals of (2).

Here we use the methods of [4, 8] to get a stronger bound on $H_{g,p}(N)$. Although our approach (as well as results which are based on the direct use of bounds of exponential sums) hold in wider generality we always consider the interval (2), and also always assume that g is a primitive root.

THEOREM 2. *Let $\nu \ge 1$ be a fixed integer. Then for any primitive root $g \in \mathbb{F}_p$ and any N satisfying (2) the following bound holds:*

$$\begin{aligned} H_{g,p}(N) \le\ & N^{-47/72+(2\nu+1)/6\nu(\nu+1)+o(1)} p^{95/72-1/6(\nu+1)} \\ & + N^{-47/96+1/4\nu+o(1)} p^{119/96-1/4\nu} \end{aligned}$$

as $p \to \infty$.

To compare the bound of Theorem 2 with (3) we consider the most interesting case of $N = \lceil p^{1/2} \rceil$. From Theorem 2 we derive

$$H_{g,p}(\lceil p^{1/2} \rceil) \le p^{143/144+1/12\nu(\nu+1)+o(1)} + p^{191/192-1/8\nu+o(1)},$$

which with $\nu = 72$ implies

$$H_{g,p}(\lceil p^{1/2} \rceil) \le p^{62635/63072+o(1)} = p^{0.9930714\ldots},$$

while by (3) it implies

$$H_{g,p}(\lceil p^{1/2} \rceil) \le p^{191/192+o(1)} = p^{0.9947916\ldots}.$$

Finally, we also mention that several more questions about the distribution of small powers of primitive roots have been considered in [6, 10, 11, 13]; see also [8, Ch. 15].

Throughout the paper, any implied constants in the symbols O and $\ll$ may occasionally depend, where obvious, on some integer parameter $\nu \ge 1$ and some real positive parameter ε, and are absolute otherwise. We recall that the notations $U \ll V$ and $U = O(V)$ are both equivalent to the statement that $|U| \le cV$ holds with some constant $c > 0$.

§2. *Preliminaries.* Here we establish an analogue of [8, Lemma 7.1], which gives a link between $H_{g,p}(N)$ and $S_{g,p}(\lambda, N)$.

In fact we present this link in a very general form which applies to many other sets besides $\mathcal{G}_{g,p}(N)$.

Given two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$ and $\lambda \in \mathbb{F}_p$ we denote by $I_p(\mathcal{A}, \mathcal{B})$ the largest gaps between the residues modulo p of products ab, $a \in \mathcal{A}$, $b \in \mathcal{B}$. That is,

$$I_p(\mathcal{A}, \mathcal{B}) = \max\{H : \exists u \in \mathbb{F}_p \text{ such that } \{u+1, \dots, u+H\} \cap \mathcal{AB} = \emptyset\},$$

where, as usual, $\mathcal{AB} = \{ab : a \in \mathcal{A}, b \in \mathcal{B}\}$.

Furthermore, let $Q_p(\lambda; \mathcal{A}, L)$ be the number of solutions to the congruence

$$\lambda \equiv ra \pmod p, \quad 1 \le |r| \le L, a \in \mathcal{A}.$$

We also put

$$S_p(\lambda, \mathcal{B}) = \sum_{b \in \mathcal{B}} \mathbf{e}_p(\lambda b),$$

LEMMA 3. *Assume that for $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$ and some positive integer $L \le p/2$ we have*

$$\sum_{\lambda \in \mathbb{F}_p} Q_p(\lambda; \mathcal{A}, L)|S_p(\lambda, \mathcal{B})| \le 0.5AB,$$

where

$$A = \#\mathcal{A} \quad \text{and} \quad B = \#\mathcal{B}.$$

Then, as $p \to \infty$,

$$I_p(\mathcal{A}, \mathcal{B}) \le p^{1+o(1)} L^{-1}.$$

Proof. Let us fix some $\varepsilon > 0$. We put

$$s = \lceil 0.5(1 + \varepsilon^{-1}) \rceil \quad \text{and} \quad Z = \lceil p^{1+\varepsilon} L^{-1} \rceil.$$

Obviously it is enough to show that for a sufficiently large p and any integer U the congruence,

$$\begin{aligned} ab \equiv U + x_1 + \dots + x_s - y_1 - \dots - y_s \pmod p, \\ a \in \mathcal{A}, b \in \mathcal{B}, \quad 0 \le x_1, y_1, \dots, x_s, y_s < Z, \end{aligned} \tag{4}$$

is solvable. Indeed, in this case we have $I_p(\mathcal{A}, \mathcal{B}) \le 2s(Z-1)$, and since $\varepsilon > 0$ is arbitrary the result follows.

For the number J of solutions to the congruence (4) one easily sees from the identity

$$\frac{1}{p}\sum_{r=-(p-1)/2}^{(p-1)/2}\mathbf{e}_p(rz)=\begin{cases}1 & \text{if } z\equiv 0 \pmod p,\\ 0 & \text{otherwise,}\end{cases}$$

which holds for any $z\in\mathbb{Z}$, that

$$\begin{aligned}J &= \sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{0\le x_1,y_1,\ldots,x_s,y_s<Z}\\ &\quad\times\frac{1}{p}\sum_{r=-(p-1)/2}^{(p-1)/2}\mathbf{e}_p(r(ab-U-x_1-\cdots-x_s+y_1+\cdots+y_s))\\ &= \frac{1}{p}\sum_{r=-(p-1)/2}^{(p-1)/2}\mathbf{e}_p(-rU)\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\mathbf{e}_p(rab)\\ &\quad\times\sum_{0\le x_1,y_1,\ldots,x_s,y_s<Z}\mathbf{e}_p(-r(x_1+\cdots+x_s-y_1-\cdots-y_s))\\ &= \frac{1}{p}\sum_{r=-(p-1)/2}^{(p-1)/2}\mathbf{e}_p(-rU)\left|\sum_{0\le x<Z}\mathbf{e}_p(rx)\right|^{2s}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\mathbf{e}_p(rab).\end{aligned}$$

Separating the term $ABZ^{2s}p^{-1}$ corresponding to $r=0$, and separating the remaining sum into two parts corresponding to $1\le|r|\le L$ and $L<|r|\le p/2$ we see that

$$J\ge ABZ^{2s}p^{-1}-\sigma_1p^{-1}-\sigma_2p^{-1}, \tag{5}$$

where

$$\sigma_1=\sum_{1\le|r|\le L}\left|\sum_{0\le x<Z}\mathbf{e}_p(rx)\right|^{2s}\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\mathbf{e}_p(rab)\right|,$$

$$\sigma_2=\sum_{L<|r|\le p/2}\left|\sum_{0\le x<Z}\mathbf{e}_p(rx)\right|^{2s}\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\mathbf{e}_p(rab)\right|.$$

For $1\le|r|\le L$ we use the trivial estimate

$$\left|\sum_{0\le x<Z}\mathbf{e}_p(rx)\right|\le Z$$

and derive

$$\begin{aligned}\sigma_1 &\le Z^{2s}\sum_{1\le|r|\le L}\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\mathbf{e}_p(rab)\right|\\ &\le Z^{2s}\sum_{1\le|r|\le L}\sum_{a\in\mathcal{A}}\left|\sum_{b\in\mathcal{B}}\mathbf{e}_p(rab)\right|\\ &= Z^{2s}\sum_{\lambda\in\mathbb{F}_p}Q_p(\lambda;\mathcal{A},L)|S_p(\lambda,\mathcal{B})|.\end{aligned}$$

Therefore, by the conditions of the lemma, we have

$$\sigma_1 \le 0.5ABZ^{2s}. \tag{6}$$

If $L < |r| \le p/2$ then we use the bound

$$\left|\sum_{0\le x<Z} \mathbf{e}_p(rx)\right| \ll \frac{p}{|r|};$$

see [7, Bound (8.6)]. From the trivial bound

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} \mathbf{e}_p(rab)\right| \le AB,$$

recalling the choice of Z, we obtain

$$\sigma_2 \ll \sum_{L<|r|\le p/2}\left(\frac{p}{|r|}\right)^{2s} AB \ll AB\frac{p^{2s}}{L^{2s-1}} \le AB\frac{Z^{2s}L}{p^{2s\varepsilon}} \ll AB\frac{Z^{2s}L}{p^{1+\varepsilon}}$$

as $2s\varepsilon > 1+\varepsilon$ for the above choice of s. In particular,

$$\sigma_2 \ll ABZ^{2s}p^{-\varepsilon}. \tag{7}$$

Substituting (6) and (7) into (5), we obtain

$$J \ge \tfrac{1}{2}ABZ^{2s}p^{-1} + O(ABZ^{2s}p^{-1-\varepsilon}).$$

Thus $J > 0$ provided that p is large enough and the result follows. □

Now, for a primitive root $g \in \mathbb{F}_p$, an integer M and $\lambda \in \mathbb{F}_p$ we denote by $R_{g,p}(\lambda; M, L)$ the number of solutions to the congruence

$$\lambda \equiv rg^n \pmod p, \quad 1 \le |r| \le L, n = 1, \dots, M.$$

That is, $R_{g,p}(\lambda; M, L)$ is equal to the number of non-zero elements of the set $\lambda g^{-M-1}\mathcal{G}_{g,p}(M)$. Then we derive the following corollary from Lemma 3.

COROLLARY 4. *Assume that, for a primitive root $g \in \mathbb{F}_p$ and some positive integer $L \le p/2$ for any $a \in \mathbb{F}_p^*$, we have*

$$\sum_{\lambda\in\mathbb{F}_p} R_{g,p}(\lambda; M, L)|S_{g,p}(a\lambda, M)| \le 0.5M^2,$$

where

$$M = \lfloor N/2 \rfloor.$$

Then, as $p \to \infty$,

$$H_{g,p}(N) \le p^{1+o(1)}L^{-1}.$$

Obviously, we have

$$\sum_{\lambda\in\mathbb{F}_p} R_{g,p}(\lambda; M, L) = 2ML. \tag{8}$$

Furthermore, for a positive integer $L < p$ we denote by $W_{g,p}(M, L)$ the number of solutions $(n, r, s) \in \mathbb{Z}^3$ to the congruence

$$sg^n \equiv r \pmod p, \quad 1 \le n \le M, |r|, |s| \le L.$$

This essentially counts the number of rational numbers of height at most L which are congruent modulo p to some element of $\mathcal{G}_{g,p}(M)$. Then we also have

$$\sum_{\lambda \in \mathbb{F}_p} R_{g,p}(\lambda; M, L)^2 \le 2MW_{g,p}(M, L). \tag{9}$$

Now, using the Hölder inequality. we see that for any α with $1/4 \le \alpha \le 1/2$, we have

$$\begin{aligned}
&\sum_{\lambda \in \mathbb{F}_p} R_{g,p}(\lambda; M, L)|S_{g,p}(a\lambda, M)| \\
&\quad \le \left(\sum_{\lambda \in \mathbb{F}_p} R_{g,p}(\lambda; M, L)\right)^{1-2\alpha} \left(\sum_{\lambda \in \mathbb{F}_p} R_{g,p}(\lambda; M, L)^2\right)^{\alpha} \\
&\qquad \times \left(\sum_{\lambda \in \mathbb{F}_p} |S_{g,p}(a\lambda, M)|^2\right)^{2\alpha-1/2} \left(\sum_{\lambda \in \mathbb{F}_p} |S_{g,p}(a\lambda, M)|^4\right)^{1/2-\alpha}.
\end{aligned}$$

Therefore, as in [8, Ch. 7] using (8), we derive that

$$\begin{aligned}
&\sum_{\lambda \in \mathbb{F}_p} R_{g,p}(\lambda; M, L)|S_{g,p}(a\lambda, M)| \\
&\quad \le M^{1-\alpha} L^{1-2\alpha} W_{g,p}(M, L)^{\alpha} \\
&\qquad \times \left(\sum_{\lambda \in \mathbb{F}_p} |S_{g,p}(a\lambda, M)|^2\right)^{2\alpha-1/2} \left(\sum_{\lambda \in \mathbb{F}_p} |S_{g,p}(a\lambda, M)|^4\right)^{1/2-\alpha}.
\end{aligned} \tag{10}$$

Thus, following the approach of [8, Ch. 7] we now need to estimate $W_{g,p}(M, L)$ and the average values of the sums $S_{g,p}(a\lambda, M)$.

§3. *Average values of exponential sums.* First we record the following estimate, which is essentially a form of the Parseval identity:

$$\sum_{\lambda \in \mathbb{F}_p} |S_{g,p}(\lambda, M)|^2 = pM. \tag{11}$$

Furthermore, by [2, Theorem 1.4] we have the following lemma.

LEMMA 5. *Let $g \in \mathbb{F}_p$ be a primitive root. Then for a positive integer $M < p$ we have*

$$\sum_{\lambda \in \mathbb{F}_p} |S_{g,p}(\lambda, M)|^4 \ll pM^{3-1/24+o(1)}(1 + (M^2/p)^{1/24}).$$

So substituting (11) and the bound of Lemma 5 we obtain that for $1/4 \le \alpha \le 1/2$

$$\sum_{\lambda \in \mathbb{F}_p} R_{g,p}(\lambda; M, L)|S_{g,p}(a\lambda, M)| \ll M^{1-\alpha} L^{1-2\alpha} W_{g,p}(M, L)^{\alpha} \times (pM)^{2\alpha-1/2}(pM^{3-1/24+o(1)}(1 + (M^2/p)^{1/24}))^{1/2-\alpha}.$$

Therefore,

$$\sum_{\lambda \in \mathbb{F}_p} R_{g,p}(\lambda; M, L)|S_{g,p}(a\lambda, M)| \le M^{1/2+\alpha+71(1-2\alpha)/48+o(1)} L^{1-2\alpha} p^{\alpha} \times W_{g,p}(M, L)^{\alpha}(1 + (M^2/p)^{1/24})^{1/2-\alpha}. \tag{12}$$

So in order to apply Corollary 4 it now remains to estimate $W_{g,p}(M, L)$.

§4. *Rational fractions of small height in sets with small product sets.* Our treatment of $W_{g,p}(M, L)$ is based on the results of [4], in which, as in § 2, we present our results in a form more general that we actually need for our specific applications.

For a set $\mathcal{A} \subseteq \mathbb{F}_p$, we consider the set

$$\mathcal{V}_p(\mathcal{A}, L) = \{a \in \mathcal{A} : as \equiv r \pmod p \text{ for some } r, s \in \mathbb{Z} \text{ with } |r|, |s| \le L\}.$$

We say that $\mathcal{A}$ is a set with a small product set if for any integer $\nu \ge 1$ we have

$$\#\mathcal{A}^{(\nu)} \le \#\mathcal{A} p^{o(1)} \tag{13}$$

as $p \to \infty$, where $\mathcal{A}^{(\nu)}$ denotes the ν-fold product set

$$\mathcal{A}^{(\nu)} = \{a_1 \cdots a_\nu : a_1, \dots, a_\nu \in \mathcal{A}\}.$$

We have the following estimate.

LEMMA 6. *Let $\nu \ge 1$ be a fixed integer. Then for any set $\mathcal{A} \subseteq \mathbb{F}_p$ with a small product set and any positive integer $L < p$, the following bounds hold as $p \to \infty$.*

(i) *If $L^{2\nu} < p/2$ then*

$$\#\mathcal{V}_p(\mathcal{A}, L) \le (\#\mathcal{A})^{1/\nu} p^{o(1)}.$$

(ii) *If $L^{2\nu} \ge p/2$ then*

$$\#\mathcal{V}_p(\mathcal{A}, L) \le \left(\frac{\#\mathcal{A}}{p}\right)^{1/\nu} L^{2+o(1)}.$$

Proof. The proof follows the proof of [4, Lemma 4] literally with the only change being that (13) replaces the inequality

$$\mathcal{V}_p(\mathcal{G}, L)^{(\nu)} \le t,$$

where $\mathcal{G}$ is a multiplicative subgroup of $\mathbb{F}_p^*$ of order t used in the proof of [4, Lemma 4]. □

Now, we immediately obtain from Lemma 6 an analogue of [4, Lemma 5] and then consecutively of [4, Lemma 6].

LEMMA 7. *Let $\nu \ge 1$ be a fixed integer. Then for any set $\mathcal{A} \subseteq \mathbb{F}_p$ with a small product set and any positive integer L with $L^{2\nu} \le p < L^{2(\nu+1)}$, the following bound holds:*

$$\#\mathcal{V}_p(\mathcal{A}, L) \le LT^{(2\nu+1)/2\nu(\nu+1)} p^{-1/2(\nu+1)+o(1)},$$

as $p \to \infty$, where

$$T = \max\{\#\mathcal{A}, p^{1/2}\}.$$

LEMMA 8. *Let $\nu \ge 1$ be a fixed integer. Then for any set $\mathcal{A} \subseteq \mathbb{F}_p$ with a small product set and any positive integer $L < p$, the following bound holds:*

$$\#\mathcal{V}_p(\mathcal{A}, L) \le LT^{(2\nu+1)/2\nu(\nu+1)} p^{-1/2(\nu+1)+o(1)} + L^2 T^{1/\nu} p^{-1/\nu+o(1)},$$

as $p \to \infty$, where

$$T = \max\{\#\mathcal{A}, p^{1/2}\}.$$

Furthermore, for a set $\mathcal{A} \subseteq \mathbb{F}_p$ and a positive integer $L < p$ we denote by $U_p(\mathcal{A}, L)$ the number of solutions $(n, r, s) \in \mathbb{Z}^3$ to the congruence

$$as \equiv r \pmod p, \quad a \in \mathcal{A}, |r|, |s| \le L.$$

Now, repeating the arguments of the proof of [4, Theorem 1] (in a much simplified form as we work modulo a prime number rather than an arbitrary positive integer as in [4]), we derive the following lemma.

LEMMA 9. *Let $\nu \ge 1$ be a fixed integer. Then for any set $\mathcal{A} \subseteq \mathbb{F}_p$ with a small product set and any positive integer $L < p^{1/2}$, the following bound holds:*

$$U_p(\mathcal{A}, L) \le LT^{(2\nu+1)/2\nu(\nu+1)} p^{-1/2(\nu+1)+o(1)} + L^2 T^{1/\nu} p^{-1/\nu+o(1)},$$

as $p \to \infty$, where

$$T = \max\{\#\mathcal{A}, p^{1/2}\}.$$

COROLLARY 10. *Let $\nu \ge 1$ be a fixed integer. Then for any primitive root $g \in \mathbb{F}_p$ and any positive integers $L < p^{1/2}$ and $M < p$, the following bound holds:*

$$W_{g,p}(M, L) \le LT^{(2\nu+1)/2\nu(\nu+1)} p^{-1/2(\nu+1)+o(1)} + L^2 T^{1/\nu} p^{-1/\nu+o(1)},$$

as $p \to \infty$, where

$$T = \max\{M, p^{1/2}\}.$$

Remark 11. Note that in the formulation of [4, Theorem 1] the condition $h < p^{1/2}$ (essential for the proof given there) is missing. However, it is shown in [5] how to get the same result without this condition. Thus it is very likely that Lemma 9 and Corollary 10 also hold for any $L < p$.

§5. *Proof of Theorem 1.* For an integer $N \ge 1$, we define

$$\sigma_{g,p}(N) = \max_{1 \le K \le N} \max_{\gcd(\lambda, p)=1} |S_{g,p}(\lambda, K)|.$$

It is easy to see that for any integer K we have

$$\left| S_{g,p}(\lambda, N) - \frac{1}{K} \sum_{k=1}^{K} \sum_{n=1}^{N} \mathbf{e}_p(\lambda g^{k+n}) \right| \le 2\sigma_{g,p}(K).$$

Now, using [2, Theorem 1.4, Lemma 7.1], as in the proof of [2, Corollary 1.2] we obtain for $1 \le K \le N \ll p^{1/2}$ that

$$\left| \frac{1}{K} \sum_{k=1}^{K} \sum_{n=1}^{N} \mathbf{e}_p(\lambda g^{k+n}) \right| \le p^{1/8+o(1)} K^{73/192} N^{169/192}.$$

Thus, for $K = \lfloor N/3 \rfloor$ we immediately derive

$$\sigma_{g,p}(N) \le \sigma_{g,p}(\lfloor N/3 \rfloor) + p^{1/8+o(1)} N^{71/96}$$

which gives

$$\max_{\gcd(\lambda, p)=1} |S_{g,p}(\lambda, N)| \le p^{1/8+o(1)} N^{71/96} \tag{14}$$

in the range $N \le p^{1/2}$.

In the range $N \gg p^{1/2}$ we use the Hölder inequality

$$\left| \sum_{k=1}^{K} \sum_{n=1}^{N} \mathbf{e}_p(\lambda g^{k+n}) \right|^4 \le K^3 \sum_{k=1}^{K} \left| \sum_{n=1}^{N} \mathbf{e}_p(\lambda g^{k+n}) \right|^4,$$

and, by Lemma 5, we obtain

$$\left| \sum_{k=1}^{K} \sum_{n=1}^{N} \mathbf{e}_p(\lambda g^{k+n}) \right| \le p^{23/96+o(1)} K^{3/4} N^{73/96}.$$

Thus, for $K = \lfloor N/3 \rfloor$ we derive

$$\sigma_{g,p}(N) \le \sigma_{g,p}(\lfloor N/3 \rfloor) + p^{23/96+o(1)} N^{49/96},$$

and we conclude the proof.

§6. *Proof of Theorem 2.* Using (12) with $\alpha = 1/4$ and applying Corollary 10, we see that for $M \gg p^{1/2}$ we have

$$\begin{aligned} &\sum_{\lambda \in \mathbb{F}_p} R_{g,p}(\lambda; M, L) |S_{g,p}(a\lambda, M)| \\ &\quad \le L^{1/2} M^{145/96+o(1)} p^{23/96} \\ &\qquad \times (L^{1/4} M^{(2\nu+1)/8\nu(\nu+1)} p^{-1/8(\nu+1)} + L^{1/2} M^{1/4\nu} p^{-1/4\nu}). \end{aligned} \tag{15}$$

We now fix some $\varepsilon > 0$ and put

$$L = \min\{M^{47/72-(2\nu+1)/6\nu(\nu+1)+\varepsilon} p^{-23/72+1/6(\nu+1)}, \\ M^{47/96-1/4\nu+\varepsilon} p^{-23/96+1/4\nu}\}.$$

Recalling Corollary 4 and taking into account that $\varepsilon > 0$ is arbitrary, we conclude the proof.

Acknowledgement. The research of S. V. K. was supported in part by Grant N. 11-01-00329 from the Russian Fund of Basic Researches and that of I. E. S. by ARC grant DP1092835.

References

1. J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, On the divisibility of Fermat quotients. *Michigan Math. J.* **59** (2010), 313–328.
2. J. Bourgain and M. Z. Garaev, On a variant of sum–product estimates and explicit exponential sum bounds in prime fields. *Math. Proc. Cambridge Philos. Soc.* **146** (2008), 1–21.
3. J. Bourgain, S. Konyagin, C. Pomerance and I. E. Shparlinski, On the smallest pseudopower. *Acta Arith.* **140** (2009), 43–55.
4. J. Bourgain, S. V. Konyagin and I. E. Shparlinski, Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm. *Int. Math. Res. Not. IMRN* **2008** (2008), 1–29, Article ID rnn090.
5. J. Bourgain, S. V. Konyagin and I. E. Shparlinski, Corrigenda to: Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm. *Int. Math. Res. Not. IMRN* **2009** (2009), 3146–3147.
6. C. Cobeli, S. Gonek and A. Zaharescu, On the distribution of small powers of a primitive root. *J. Number Theory* **88** (2001), 49–58.
7. H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society (Providence, RI, 2004).
8. S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and Their Applications*, Cambridge University Press (Cambridge, 1999).
9. N. M. Korobov, On the distribution of digits in periodic fractions. *Mat. Sb.* **89** (1972), 654–670 (in Russian).
10. H. L. Montgomery, Distribution of small powers of a primitive root. In *Advances in Number Theory*, Clarendon Press (Oxford, 1993), 137–149.
11. Z. Rudnick and A. Zaharescu, The distribution of spacings between small powers of a primitive root. *Israel J. Math.* **120** (2000), 271–287.
12. I. E. Shparlinski, On the value set of Fermat quotients. *Proc. Amer. Math. Soc.* (to appear).
13. M. Vâjâitu and A. Zaharescu, Differences between powers of a primitive root. *Int. J. Math. Math. Sci.* **29** (2002), 325–331.

Sergei V. Konyagin,
Steklov Mathematical Institute,
8 Gubkin Street, Moscow, 119991,
Russia
E-mail: konyagin23@gmail.com

Igor E. Shparlinski,
Department of Computing,
Macquarie University,
Sydney, NSW 2109,
Australia
E-mail: igor.shparlinski@mq.edu.au

Search Results

Mathematika

Title Details | Table of Contents

Related Titles

- Alternative Media Edition (1)

Lists

Marked Titles (0)

Search History

0025-5793 - (1)

Basic Description

Title	Mathematika: a journal of pure and applied mathematics
ISSN	0025-5793
Publisher	London Mathematical Society
Country	United Kingdom
Status	Active
Start Year	1954
Frequency	Semi-annually
Language of Text	Text in: English
Refereed	Yes
Abstracted / Indexed	Yes
Serial Type	Journal
Content Type	Academic / Scholarly
Format	Print
Website	http://journals.cambridge.org/action/displayJournal?jid=MTK
Description	Contains pure and applied mathematical articles.

Save to List Email Download Print Corrections Expand All Collapse All