ACTA ARITHMETICA
140.1 (2009)

On the smallest pseudopower

by

Jean Bourgain (Princeton, NJ), Sergei V. Konyagin (Moscow),
Carl Pomerance (Hanover, NH) and Igor E. Shparlinski (Sydney)

1. Introduction. Let g be a fixed integer with $|g| \geq 2$. Following E. Bach, R. Lukes, J. Shallit and H. C. Williams [1], we say that an integer $n > 0$ is an *x-pseudopower to base g* if n is not a power of g over the integers but is a power of g modulo all primes $p \leq x$, that is, if for all primes $p \leq x$ there exists an integer $e_p \geq 0$ such that $n \equiv g^{e_p} \pmod p$.

Denote by $q_g(x)$ the least x-pseudopower to base g.

A well-known result of A. Schinzel [8] asserts that if f and $g > 0$ are integers such that $f \neq g^k$ for all integers $k \geq 0$, then for infinitely many primes p the congruence $g^k \equiv f \pmod p$ does not have solutions in nonnegative integers k. Therefore,

$$q_g(x) \to \infty \quad \text{as } x \to \infty.$$

E. Bach, R. Lukes, J. Shallit and H. C. Williams [1] have shown that if the Riemann Hypothesis holds for Dedekind zeta functions, then there is a constant $A_g > 0$ such that

$$q_g(x) \geq \exp(A_g\sqrt{x}/(\log x)^2).$$

On the other hand, if

$$M_x = \prod_{p \leq x} p \tag{1}$$

is the product of all primes $p \leq x$, then $q_g(x) \leq 2M_x + 1$ when $x \geq 2$. Since, by the prime number theorem, $M_x = \exp(x + o(x))$, we have

$$q_g(x) \leq \exp((1 + o(1))x) \quad \text{as } x \to \infty. \tag{2}$$

Supported by numerical data, a heuristic argument is given in [1] suggesting that $q_g(x)$ for fixed g is about $\exp(c_g x/\log x)$, where $c_g > 0$. In [7], towards this conjecture, the upper bound

2010 *Mathematics Subject Classification*: 11A07, 11L07.
Key words and phrases: pseudopowers, exponential sums, multiplicative subgroups of residue rings.

DOI: 10.4064/aa140-1-3

$$q_g(x) \le \exp\left(c_g \frac{x \log\log x}{\log x}\right)$$

is proved conditionally under the Extended Riemann Hypothesis.

In [5], combining some bounds of exponential sums with new results about the average behaviour of the multiplicative order of g modulo prime numbers, the bound (2) has been improved as

$$q_g(x) \le \exp(0.88715x)$$

for x sufficiently large and $|g| \le x$. Here we obtain a further improvement.

THEOREM 1. *For all sufficiently large numbers x and all integers g with $1 < |g| \le x$, we have*

$$q_g(x) \le \exp(0.86092x).$$

The result is based on a combination of the approach of [5] with some new estimates on the distribution of multiplicative subgroups in residue rings, which in turn are based on the results and ideas from [2].

We remark that [5] and [7] give some results showing some level of uniform distribution for x-pseudopowers to base g, unconditionally and under the Extended Riemann Hypothesis, respectively. Unfortunately, it seems that our approach here does not imply results on uniform distribution; it remains an open problem to improve the estimates of [5] and [7].

2. Preliminaries. For an integer m we use $\mathbb{Z}_m$ to denote the residue ring modulo m and we also use $\mathbb{Z}_m^*$ to denote the group of units of $\mathbb{Z}_m$.

Let $\mathcal{G}$ be a multiplicative subgroup of $\mathbb{Z}_m^*$ of order t. We denote by $H_m(\mathcal{G})$ the largest gap between the elements of $\mathcal{G}$, that is,

$$H_m(\mathcal{G}) = \max\{H : \exists u \in \mathbb{Z}_m \text{ such that } u + j \notin \mathcal{G},\ j = 1, \ldots, H\}.$$

For a prime p with $\gcd(g,p) = 1$, we denote by $\mathcal{G}_{g,p}$ the subgroup of $\mathbb{Z}_p^*$ generated by powers of g modulo p, that is,

$$\mathcal{G}_{g,p} = \{n \in \mathbb{Z}_p : n \equiv g^k \pmod p \text{ for some nonnegative } k \in \mathbb{Z}\}.$$

Clearly, if $\gcd(g,p) = 1$ then $\mathcal{G}_{g,p}$ is a subgroup of $\mathbb{Z}_p^*$. Finally, if $p \mid g$, then we define $\mathcal{G}_{g,p} = \{1\}$.

We consider the subgroup of $\mathbb{Z}_{M_x}^*$ defined by

$$\mathcal{G}_g(x) = \{n \in [0, M_x) : n \in \mathcal{G}_{g,p} \text{ for all primes } p \le x\}. \tag{3}$$

Since we are assuming that $|g| \le x$, we note that $\mathcal{G}_g(x)$ consists of both the x-pseudopowers to base g in $[0, M_x)$ that are coprime to M_x and the number 1. Thus, the interval $[2, H_{M_x}(\mathcal{G}_g(x)) + 2]$ contains at least one x-pseudopower to the base g and we deduce that

$$q_g(x) \le H_{M_x}(\mathcal{G}_g(x)) + 2. \tag{4}$$

Therefore we concentrate on getting an upper bound on $H_{M_x}(\mathcal{G}_g(x))$.

3. Gaps between elements of multiplicative subgroups of residue rings and exponential sums. We need an analogue of [6, Lemma 7.1] which relates $H_m(\mathcal{G})$ with certain exponential sums.

Given a subgroup $\mathcal{G}$ of $\mathbb{Z}_m^*$, we denote by $M_\lambda(m,\mathcal{G};h)$ the number of solutions to the congruence

$$\lambda \equiv aw \pmod m, \qquad 1 \le |a| \le h,\ w \in \mathcal{G}.$$

Essentially, $M_\lambda(m,\mathcal{G};h)$ is the number of nonzero elements of the set $\lambda\mathcal{G}$ that lie in the interval $[-h,h]$. (Note that λ need not be coprime to m, so that the translated subgroup $\lambda\mathcal{G}$ need not be a coset in $\mathbb{Z}_m^*$.)

Also, we put

$$\mathbf{e}_m(z) = \exp(2\pi i z/m)$$

and define exponential sums

$$S_\lambda(m,\mathcal{G}) = \sum_{v\in\mathcal{G}} \mathbf{e}_m(\lambda v).$$

Lemma 2. *Assume that $\mathcal{G}$ is of order t and that for some positive integer $h \le m/2$ we have*

$$\sum_{\lambda\in\mathbb{Z}_m} M_\lambda(m,\mathcal{G};h)|S_\lambda(m,\mathcal{G})| \le 0.5t^2.$$

Then, as $m\to\infty$,

$$H_m(\mathcal{G}) \le m^{1+o(1)}h^{-1}.$$

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

$$s = \lceil 0.5(1+\varepsilon^{-1})\rceil, \qquad Z = \lceil m^{1+\varepsilon}h^{-1}\rceil.$$

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

$$v \equiv U + x_1 + \cdots + x_s - y_1 - \cdots - y_s \pmod m, \qquad v\in\mathcal{G},\ 0 \le x_1, y_1, \ldots, x_s, y_s < Z, \tag{5}$$

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

For the number Q of solutions to the congruence (5) one easily sees from the identity

$$\frac{1}{m}\sum_{-(m-1)/2\le a\le m/2} \mathbf{e}_m(az) = \begin{cases} 1 & \text{if } z \equiv 0 \pmod m,\\ 0 & \text{otherwise,}\end{cases}$$

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

$$\begin{aligned} Q &= \sum_{v\in\mathcal{G}} \sum_{0\le x_1,y_1,\dots,x_s,y_s<Z} \frac{1}{m} \\ &\quad \times \sum_{-(m-1)/2\le a\le m/2} \mathbf{e}_m(a(v-U-x_1-\cdots-x_s+y_1+\cdots+y_s)) \\ &= \frac{1}{m} \sum_{-(m-1)/2\le a\le m/2} \mathbf{e}_m(-aU)\sum_{v\in\mathcal{G}}\mathbf{e}_m(av) \\ &\quad \times \sum_{0\le x_1,y_1,\dots,x_s,y_s<Z} \mathbf{e}_m(-a(x_1+\cdots+x_s-y_1-\cdots-y_s)) \\ &= \frac{1}{m} \sum_{-(m-1)/2\le a\le m/2} \mathbf{e}_m(-aU)\Big|\sum_{0\le x<Z}\mathbf{e}_m(ax)\Big|^{2s}\sum_{v\in\mathcal{G}}\mathbf{e}_m(av). \end{aligned}$$

Therefore

$$Q \ge tZ^{2s}m^{-1} - \sigma_1 m^{-1} - \sigma_2 m^{-1}, \tag{6}$$

where

$$\begin{aligned} \sigma_1 &= \sum_{1\le|a|\le h}\Big|\sum_{0\le x<Z}\mathbf{e}_m(ax)\Big|^{2s}\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_m(av)\Big|, \\ \sigma_2 &= \sum_{h<|a|\le m/2}\Big|\sum_{0\le x<Z}\mathbf{e}_m(ax)\Big|^{2s}\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_m(av)\Big|. \end{aligned}$$

For $1 \le |a| \le h$ we use the trivial estimate

$$\Big|\sum_{0\le x<Z}\mathbf{e}_m(ax)\Big| \le Z$$

and derive

$$\begin{aligned} \sigma_1 &\le Z^{2s}\sum_{1\le|a|\le h}\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_m(av)\Big| = \frac{Z^{2s}}{\#\mathcal{G}}\sum_{1\le|a|\le h}\sum_{w\in\mathcal{G}}\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_m(awv)\Big| \\ &= \frac{Z^{2s}}{\#\mathcal{G}}\sum_{\lambda\in\mathbb{Z}_m} M_\lambda(m,\mathcal{G};h)|S_\lambda(m,\mathcal{G})|. \end{aligned}$$

Therefore, by the conditions of the lemma, we have

$$\sigma_1 \le 0.5tZ^{2s}. \tag{7}$$

If $h < |a| \le m/2$ then we use the bound

$$\Big|\sum_{0\le x<Z}\mathbf{e}_m(ax)\Big| \ll \frac{m}{|a|}$$

(see [4, bound (8.6)]). From the trivial bound

$$\Big|\sum_{v\in\mathcal{G}} \mathbf{e}_m(av)\Big| \le t,$$

recalling the choice of Z, we obtain

$$\sigma_2 \ll \sum_{h<|a|\le m/2} \left(\frac{m}{|a|}\right)^{2s} t \ll t\,\frac{m^{2s}}{h^{2s-1}} \le t\,\frac{Z^{2s}h}{m^{2s\varepsilon}} \ll t\,\frac{Z^{2s}h}{m^{1+\varepsilon}}$$

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

$$\sigma_2 \ll tZ^{2s}m^{-\varepsilon}. \tag{8}$$

Substituting (7) and (8) in (6), we obtain

$$Q \ge 0.5tZ^{2s}m^{-1} + O(tZ^{2s}m^{-1-\varepsilon}).$$

Thus $Q>0$ provided that m is large enough, and the result follows. ■

4. Further preparations. Now, for each $d\,|\,m$, we collect together the terms in the sum in Lemma 2 with $\gcd(\lambda,m)=d$.

In particular, let $\mathcal{G}_d$ be the homomorphic image of $\mathcal{G}$ in $\mathbb{Z}_{m/d}^*$. It is easy to verify that every element of $\mathcal{G}$ is mapped to

$$\#\{w\in\mathcal{G} : w\equiv 1 \pmod{m/d}\} = \frac{\#\mathcal{G}}{\#\mathcal{G}_d}$$

elements of $\mathcal{G}_d$. Thus,

$$\begin{aligned}\sum_{\lambda\in\mathbb{Z}_m} M_\lambda(m,\mathcal{G};h)|S_\lambda(m,\mathcal{G})| &= \sum_{d|m}\ \sum_{\substack{\lambda\in\mathbb{Z}_m\\ \gcd(\lambda,m)=d}} M_\lambda(m,\mathcal{G};h)|S_\lambda(m,\mathcal{G})| \\ &= \sum_{d|m}\left(\frac{\#\mathcal{G}}{\#\mathcal{G}_d}\right)^2 \sum_{\lambda\in\mathbb{Z}_{m/d}^*} M_\lambda(m/d,\mathcal{G}_d;h/d)|S_\lambda(m/d,\mathcal{G}_d)|.\end{aligned} \tag{9}$$

We remark that by the Hölder inequality

$$\begin{aligned}&\sum_{\lambda\in\mathbb{Z}_{m/d}^*} M_\lambda(m/d,\mathcal{G}_d;h/d)|S_\lambda(m/d,\mathcal{G}_d)| \\ &\quad= \sum_{\lambda\in\mathbb{Z}_{m/d}^*} M_\lambda(m/d,\mathcal{G}_d;h/d)^{1/2}(M_\lambda(m/d,\mathcal{G}_d;h/d)^2)^{1/4}(|S_\lambda(m/d,\mathcal{G}_d)|^4)^{1/4} \\ &\quad\le \Big(\sum_{\lambda\in\mathbb{Z}_{m/d}^*} M_\lambda(m/d,\mathcal{G}_d;h/d)\Big)^{1/2}\Big(\sum_{\lambda\in\mathbb{Z}_{m/d}^*} M_\lambda(m/d,\mathcal{G}_d;h/d)^2\Big)^{1/4} \\ &\qquad\times\Big(\sum_{\lambda\in\mathbb{Z}_{m/d}^*} |S_\lambda(m/d,\mathcal{G}_d)|^4\Big)^{1/4}.\end{aligned}$$

Clearly,

$$\sum_{\lambda\in\mathbb{Z}_{m/d}^*} M_\lambda(m/d,\mathcal{G}_d;h/d) \le \sum_{\lambda\in\mathbb{Z}_{m/d}} M_\lambda(m/d,\mathcal{G}_d;h/d) \le 2h\#\mathcal{G}_d/d.$$

Given a multiplicative subgroup $\mathcal{H}\subseteq\mathbb{Z}_n^*$ in the residue ring modulo a positive integer n, and a positive integer h, we define

$$V(n,\mathcal{H};h) = \#\{(u_1,u_2,v) : u_1,u_2\in[-h,h],\ \gcd(u_1u_2,n)=1,\ v\in\mathcal{H},\ u_1v\equiv u_2 \pmod n\}. \tag{10}$$

We have

$$\begin{aligned}\sum_{\lambda\in\mathbb{Z}_{m/d}^*} & M_\lambda(m/d,\mathcal{G}_d;h/d)^2 \\ &\le \sum_{\lambda\in\mathbb{Z}_{m/d}^*} \#\{u_1,u_2\in[-h/d,h/d] : u_1,u_2\in\lambda\mathcal{G}_d\}\\ &= \#\{(u_1,u_2,v_1,v_2) : u_1,u_2\in[-h/d,h/d],\ \gcd(u_1u_2,m/d)=1,\\ &\qquad v_1,v_2\in\mathcal{G}_d,\ u_1v_1\equiv u_2v_2 \pmod{m/d}\}\\ &= \#\mathcal{G}_dV(m/d,\mathcal{G}_d;h/d).\end{aligned}$$

Therefore,

$$\sum_{\lambda\in\mathbb{Z}_{m/d}^*} M_\lambda(m/d,\mathcal{G}_d;h/d)|S_\lambda(m/d,\mathcal{G}_d)| \le 2^{1/2}h^{1/2}d^{-1/2}(\#\mathcal{G}_d)^{3/4}V(m/d,\mathcal{G}_d;h/d)^{1/4}W_4(m/d,\mathcal{G}_d)^{1/4}, \tag{11}$$

where

$$W_4(m/d,\mathcal{G}_d) = \sum_{\lambda\in\mathbb{Z}_{m/d}^*} |S_\lambda(m/d,\mathcal{G}_d)|^4.$$

For $V(m/d,\mathcal{G}_d;h/d)$ we use the bound which is readily available from [2].

For the fourth moment $W_4(m/d,\mathcal{G}_d)$ such general purpose bounds are not available. However, in the case of our interest, that is, for the modulus $m = M_x$ (given by (1)) and the subgroup $\mathcal{G}_g(x)$ (given by (3)), we obtain such a bound using some results from [3] and [5]. Substituting these estimates in (11) enables us to show that the condition of Lemma 2 is satisfied for a sufficiently large h, which in turn leads to the desired estimate on $H_m(\mathcal{G})$.

5. Bound on $V(n,\mathcal{G};h)$. We recall the following result of [2, Lemma 4], which gives the desired estimate on $V(n,\mathcal{H};h)$, defined by (10) for an arbitrary modulus $n\ge 1$ and a subgroup $\mathcal{H}\subseteq\mathbb{Z}_n^*$.

LEMMA 3. *Let $\nu\ge 1$ be a fixed integer and let $n\to\infty$. Assume that $\mathcal{H}$ is a multiplicative subgroup of $\mathbb{Z}_n^*$. Then for any positive number $h\le n$, we* *have*

$$V(n,\mathcal{H},h) \le hT^{\frac{2\nu+1}{2\nu(\nu+1)}} n^{-\frac{1}{2(\nu+1)}+o(1)} + h^2T^{1/\nu}n^{-1/\nu+o(1)}$$

as $n \to \infty$, *where*

$$T = \max\{\#\mathcal{H}, n^{1/2}\}.$$

6. Bounds on the fourth moment of exponential sums. For $d \mid M_x$, we consider the homomorphic image of $\mathcal{G}_g(x)$ in $\mathbb{Z}^*_{M_x/d}$, which we denote by $\mathcal{G}_g(d;x)$ (this slightly deviates from our previous notation $\mathcal{G}_g(x)_d$, which for typographical reasons, we prefer to avoid).

As in [5] we remark that by the Chinese remainder theorem we have

$$S_\lambda(M_x/d, \mathcal{G}_g(d;x)) = \sum_{v\in\mathcal{G}_g(d;x)} \mathbf{e}_m(\lambda v) = \prod_{\substack{p\le x\\ \gcd(p,d)=1}} \sum_{v\in\mathcal{G}_{g,p}} \mathbf{e}_p(\lambda_p v), \tag{12}$$

where $\lambda_p \in \mathbb{Z}_p$ is determined by the condition

$$\lambda_p(M_x/p) \equiv \lambda \pmod{M_x}.$$

We also remark that when λ runs through $\mathbb{Z}_{M_x/d}$, the corresponding vector $(\lambda_p)_{p\le x,\, p\nmid d}$ runs through the Cartesian product

$$\mathcal{U}_x(d) = \prod_{\substack{p\le x\\ \gcd(p,d)=1}} \mathbb{Z}_p^*.$$

Thus, using (12), we obtain

$$\begin{aligned} W_4(M_x/d, \mathcal{G}_g(d;x)) &= \sum_{\lambda\in\mathbb{Z}^*_{M_x/d}} |S_\lambda(M_x/d, \mathcal{G}_g(d;x))|^4 \\ &= \sum_{(\lambda_p)_{p\le x,\, \gcd(p,d)=1}\in\mathcal{U}_x(d)} \prod_{\substack{p\le x\\ \gcd(p,d)=1}} \Big|\sum_{v\in\mathcal{G}_{g,p}} \mathbf{e}_p(\lambda_p v)\Big|^4. \end{aligned}$$

Therefore

$$W_4(M_x/d, \mathcal{G}_g(d;x)) = \prod_{\substack{p\le x\\ \gcd(p,d)=1}} \sum_{\lambda_p\in\mathbb{Z}_p^*} \Big|\sum_{v\in\mathcal{G}_{g,p}} \mathbf{e}_p(\lambda_p v)\Big|^4. \tag{13}$$

We now recall the bound of [3, Lemma 3] on the fourth moment of exponential sums over multiplicative subgroups in a residue ring modulo a prime (see also [6, Lemma 3.3]).

Lemma 4. *For any prime* p *and subgroup* $\mathcal{G}$ *of* $\mathbb{Z}_p^*$ *of order* $\#\mathcal{G} = t < p^{2/3}$, *the following bound holds*:

$$\sum_{\lambda\in\mathbb{Z}_p^*} \Big|\sum_{v\in\mathcal{G}} \mathbf{e}_p(\lambda v)\Big|^4 \ll pt^{5/2}.$$

Proof. It is enough to note that by the orthogonality of exponential functions

$$\sum_{\lambda\in\mathbb{Z}_p^*}\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_p(\lambda v)\Big|^4 \le \sum_{\lambda\in\mathbb{Z}_p}\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_p(\lambda v)\Big|^4$$
$$= p\#\{v_1+v_2=v_3+v_4 : v_1,v_2,v_3,v_4\in\mathcal{G}\},$$

and then apply the bound of [3, Lemma 3]. ■

For groups of order $\#\mathcal{G}=t>p^{2/3}$ we use a different bound which relies on some classical estimates.

LEMMA 5. *For any prime p and subgroup $\mathcal{G}$ of $\mathbb{Z}_p^*$ of order $\#\mathcal{G}=t\ge p^{2/3}$, the following bound holds*:

$$\sum_{\lambda\in\mathbb{Z}_p^*}\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_p(\lambda v)\Big|^4 \le p^2 t.$$

Proof. We recall the well-known estimate

$$\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_p(\lambda v)\Big| \le p^{1/2}$$

for any t and $\lambda\in\mathbb{Z}_p^*$ (see [6, Theorem 3.4]). Therefore

$$\sum_{\lambda\in\mathbb{Z}_p^*}\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_p(\lambda v)\Big|^4 \le p\sum_{\lambda\in\mathbb{Z}_p}\Big|\sum_{v\in\mathcal{G}}\mathbf{e}_p(\lambda v)\Big|^2 = p\sum_{\lambda\in\mathbb{Z}_p}\sum_{v_1,v_2\in\mathcal{G}}\mathbf{e}_p(\lambda(v_1-v_2)) = p^2 t,$$

as after the change of the order of summation, the sum over λ vanishes if $v_1\ne v_2$ and is equal to p otherwise. ■

For a prime $p\nmid g$ we denote by $t_{g,p}=\#\mathcal{G}_{g,p}$ the multiplicative order of g modulo p. We also put $t_{g,p}=1$ for $p\,|\,g$. In particular,

$$\#\mathcal{G}_g(d;x) = \prod_{\substack{p\le x\\ \gcd(p,d)=1}} t_{g,p}.$$

We also put

$$Q_g(d;x) = \prod_{\substack{p\le x\\ \gcd(p,d)=1\\ t_{g,p}\ge p^{2/3}}} (t_{g,p}p^{-2/3}).$$

We are now ready to obtain the desired estimate of $W_4(M_x,\mathcal{G}_g(x))$.

LEMMA 6. *We have*

$$W_4(M_x/d,\mathcal{G}_g(d;x)) \ll \frac{M_x}{d}\,(\#\mathcal{G}_g(d;x))^{5/2}Q_g(d;x)^{-3/2}.$$

Proof. Substituting the bound of Lemmas 4 and 5 in (13), we see that

$$W_4(M_x/d, \mathcal{G}_g(d;x)) \ll \prod_{\substack{p \le x \\ \gcd(p,d)=1 \\ t_{g,p} < p^{2/3}}} (p t_{g,p}^{5/2}) \prod_{\substack{p \le x \\ \gcd(p,d)=1 \\ t_{g,p} \ge p^{2/3}}} (p^2 t_{g,p})$$

$$= \prod_{\substack{p \le x \\ \gcd(p,d)=1}} (p t_{g,p}^{5/2}) \prod_{\substack{p \le x \\ \gcd(p,d)=1 \\ t_{g,p} \ge p^{2/3}}} (p t_{g,p}^{-3/2}),$$

which implies the desired estimate. ∎

7. Bounds on multiplicative orders. We recall the following two estimates, which are [5, Theorem 1] and [5, Lemma 9], respectively.

LEMMA 7. *For x sufficiently large, we have*

$$\#\mathcal{G}_g(x) \ge \exp(0.58045x)$$

uniformly for $1 < |g| \le x$.

Let

$$Q_g(x) = \prod_{\substack{p \le x \\ t_{g,p} \ge p^{2/3}}} (t_{g,p} p^{-2/3}).$$

LEMMA 8. *For x sufficiently large, we have*

$$Q_g(x) \ge \exp(0.000217x)$$

uniformly for $1 < |g| \le x$.

8. Concluding the proof of Theorem 1. We now define

$$T_g(d;x) = \max\{\#\mathcal{G}_g(d;x), (M_x/d)^{1/2}\}.$$

Using Lemmas 3 and 6 together with (11), we obtain

$$\sum_{\lambda \in \mathbb{Z}^*_{M_x/d}} M_\lambda(M_x/d, \mathcal{G}_d; h/d) |S_\lambda(M_x/d, \mathcal{G}_d)|$$

$$\ll h^{1/2} d^{-1/2} (\#\mathcal{G}_g(d;x))^{3/4}$$

$$\times \left(h T_g(d;x)^{\frac{2\nu+1}{2\nu(\nu+1)}} \left(\frac{M_x}{d}\right)^{-\frac{1}{2(\nu+1)} + o(1)} + h^2 T_g(d;x)^{1/\nu} \left(\frac{M_x}{d}\right)^{-1/\nu + o(1)} \right)^{1/4}$$

$$\times \left(\frac{M_x}{d} (\#\mathcal{G}_g(d;x))^{5/2} Q_g(d;x)^{-3/2} \right)^{1/4}$$

$$\ll h^{1/2}(\#\mathcal{G}_g(d;x))^{11/8}M_x^{1/4}d^{-3/4}Q_g(d;x)^{-3/8}$$
$$\times\left(hT_g(d;x)^{\frac{2\nu+1}{2\nu(\nu+1)}}\left(\frac{M_x}{d}\right)^{-\frac{1}{2(\nu+1)}+o(1)}+h^2T_g(d;x)^{1/\nu}\left(\frac{M_x}{d}\right)^{-1/\nu+o(1)}\right)^{1/4}.$$

Recalling (9), we now derive

$$\sum_{\lambda\in\mathbb{Z}_{M_x}}M_\lambda(M_x,\mathcal{G};h)|S_\lambda(M_x,\mathcal{G})|\le(\#\mathcal{G}_g(x))^2\sum_{d\mid M_x}(I_g(d;x)+J_g(d;x)),\tag{14}$$

where

$$I_g(d;x)=h^{3/4}(\#\mathcal{G}_g(d;x))^{-5/8}Q_g(d;x)^{-3/8}T_g(d;x)^{\frac{2\nu+1}{8\nu(\nu+1)}}\times M_x^{\frac{2\nu+1}{8(\nu+1)}+o(1)}d^{-\frac{6\nu+5}{8(\nu+1)}},$$
$$J_g(d;x)=h(\#\mathcal{G}_g(d;x))^{-5/8}Q_g(d;x)^{-3/8}T_g(d;x)^{\frac{1}{4\nu}}M_x^{\frac{\nu-1}{4\nu}+o(1)}d^{-\frac{3\nu-1}{4\nu}}.$$

Therefore, using $T_g(d;x)\le\#\mathcal{G}_g(d;x)+(M_x/d)^{1/2}$, we have

$$I_g(d;x)\le A_g(d;x)+B_g(d;x),\qquad J_g(d;x)\le C_g(d;x)+D_g(d;x),\tag{15}$$

where

$$A_g(d;x)=h^{3/4}(\#\mathcal{G}_g(d;x))^{-\frac{5\nu^2+3\nu-1}{8\nu(\nu+1)}}Q_g(d;x)^{-3/8}M_x^{\frac{2\nu+1}{8(\nu+1)}+o(1)}d^{-\frac{6\nu+5}{8(\nu+1)}},$$
$$B_g(d;x)=h^{3/4}(\#\mathcal{G}_g(d;x))^{-5/8}Q_g(d;x)^{-3/8}M_x^{\frac{(2\nu+1)^2}{16\nu(\nu+1)}+o(1)}d^{-\frac{12\nu^2+12\nu+1}{16\nu(\nu+1)}},$$
$$C_g(d;x)=h(\#\mathcal{G}_g(d;x))^{-\frac{5\nu-2}{8\nu}}Q_g(d;x)^{-3/8}M_x^{\frac{\nu-1}{4\nu}+o(1)}d^{-\frac{3\nu-1}{4\nu}},$$
$$D_g(d;x)=h(\#\mathcal{G}_g(d;x))^{-5/8}Q_g(d;x)^{-3/8}M_x^{\frac{2\nu-1}{8\nu}+o(1)}d^{-\frac{6\nu-1}{8\nu}}.$$

We note that

$$\#\mathcal{G}_g(d;x)\ge\#\mathcal{G}_g(x)/d,$$

and also that

$$Q_g(d;x)=Q_g(x)\prod_{\substack{p\mid d\\ t_{g,p}\ge p^{2/3}}}(t_{g,p}p^{-2/3})^{-1}\ge Q_g(x)/d^{1/3}.\tag{16}$$

Therefore,

$$A_g(d;x)\le h^{3/4}(\#\mathcal{G}_g(x))^{-\frac{5\nu^2+3\nu-1}{8\nu(\nu+1)}}Q_g(x)^{-3/8}M_x^{\frac{2\nu+1}{8(\nu+1)}+o(1)}d^{-\frac{1}{8\nu}},$$
$$B_g(d;x)\le h^{3/4}(\#\mathcal{G}_g(x))^{-5/8}Q_g(x)^{-3/8}M_x^{\frac{(2\nu+1)^2}{16\nu(\nu+1)}+o(1)}d^{-\frac{1}{16\nu(\nu+1)}},$$
$$C_g(d;x)\le h(\#\mathcal{G}_g(x))^{-\frac{5\nu-2}{8\nu}}Q_g(x)^{-3/8}M_x^{\frac{\nu-1}{4\nu}+o(1)},$$
$$D_g(d;x)\le h(\#\mathcal{G}_g(x))^{-5/8}Q_g(x)^{-3/8}M_x^{\frac{2\nu-1}{8\nu}+o(1)}d^{\frac{1}{8\nu}}.$$

Notice that all exponents of d in the above estimates on $A_g(d;x)$, $B_g(d;x)$ and $C_g(d;x)$ are nonpositive. Thus, since

$$\sum_{d|M_x} 1 = 2^{\pi(x)} = M_x^{o(1)},$$

in the summation over d in these three expressions, the term with $d = 1$ dominates. We obtain

$$\sum_{d|M_x} A_g(d;x) \le h^{3/4}(\#\mathcal{G}_g(x))^{-\frac{5\nu^2+3\nu-1}{8\nu(\nu+1)}} Q_g(x)^{-3/8} M_x^{\frac{2\nu+1}{8(\nu+1)}+o(1)},$$

$$\sum_{d|M_x} B_g(d;x) \le h^{3/4}(\#\mathcal{G}_g(x))^{-5/8} Q_g(x)^{-3/8} M_x^{\frac{(2\nu+1)^2}{16\nu(\nu+1)}+o(1)},$$

$$\sum_{d|M_x} C_g(d;x) \le h(\#\mathcal{G}_g(x))^{-\frac{5\nu-2}{8\nu}} Q_g(x)^{-3/8} M_x^{\frac{\nu-1}{4\nu}+o(1)}.$$

Unfortunately, the exponent of d in $D_g(d;x)$ is negative. However, if instead of (16) we use the trivial bound

$$Q_g(d,x) \ge 1$$

we derive the alternative estimate

$$\begin{aligned} D_g(d;x) &\le h(\#\mathcal{G}_g(d;x))^{-5/8} M_x^{\frac{2\nu-1}{8\nu}+o(1)} d^{-\frac{6\nu-1}{8\nu}} \\ &\le h(\#\mathcal{G}_g(x))^{-5/8} M_x^{\frac{2\nu-1}{8\nu}+o(1)} d^{-\frac{\nu-1}{8\nu}}, \end{aligned}$$

which we use for large values of d (namely for $d \ge Q_g(x)^3$). Thus,

$$\begin{aligned} \sum_{d|M_x} D_g(d;x) = & \sum_{\substack{d|M_x \\ d<Q_g(x)^3}} D_g(d;x) + \sum_{\substack{d|M_x \\ d\ge Q_g(x)^3}} D_g(d;x) \\ \ll & \sum_{\substack{d|M_x \\ d<Q_g(x)^3}} h(\#\mathcal{G}_g(x))^{-5/8} Q_g(x)^{-3/8} M_x^{\frac{2\nu-1}{8\nu}+o(1)} d^{\frac{1}{8\nu}} \\ & + \sum_{\substack{d|M_x \\ d\ge Q_g(x)^3}} h(\#\mathcal{G}_g(x))^{-5/8} M_x^{\frac{2\nu-1}{8\nu}+o(1)} d^{-\frac{\nu-1}{8\nu}} \\ = & \; h(\#\mathcal{G}_g(x))^{-5/8} Q_g(x)^{-\frac{3(\nu-1)}{8\nu}} M_x^{\frac{2\nu-1}{8\nu}+o(1)}. \end{aligned}$$

We now choose

$$\nu = 4.$$

Then, using Lemmas 7 and 8, one verifies that

$$\sum_{d|M_x} A_g(d;x) = o(1) \quad \text{for } h \le M_x^{0.140283},$$
$$\sum_{d|M_x} B_g(d;x) = o(1) \quad \text{for } h \le M_x^{0.146316},$$
$$\sum_{d|M_x} C_g(d;x) = o(1) \quad \text{for } h \le M_x^{0.139084},$$
$$\sum_{d|M_x} D_g(d;x) = o(1) \quad \text{for } h \le M_x^{0.144092}.$$

We now select

$$h = \lfloor M_x^{0.139084} \rfloor$$

(that is, the largest admissible value for which all of the above hold). Using Lemma 2, we see from the bounds (14) and (15) that the result of Theorem 1 follows. ∎

Acknowledgments. S.V.K. gratefully acknowledges support from Russian Foundation for Basic Research grant 08-01-00208 and Program Supporting Leading Scientific Schools grant NSh-3233.2008.1. C.P. gratefully acknowledges support from NSF grants DMS-0401422 and DMS-0703850. I.E.S. gratefully acknowledges support from ARC grant DP0556431.

References

[1] E. Bach, R. Lukes, J. Shallit and H. C. Williams, *Results and estimates on pseudopowers*, Math. Comp. 65 (1996), 1737–1747.

[2] 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. Notices 2008, art. ID rnn090, 29 pp. (corrigendum: ibid. 2009, no. 16, 3146–3147).

[3] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Quart. J. Math. 51 (2000), 221–235.

[4] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.

[5] S. V. Konyagin, C. Pomerance and I. E. Shparlinski, *On the distribution of pseudopowers*, Canad. J. Math., to appear.

[6] S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and Their Applications*, Cambridge Univ. Press, Cambridge, 1999.

[7] C. Pomerance and I. E. Shparlinski, *On pseudosquares and pseudopowers*, in: Combinatorial Number Theory, Proc. Integers Conf. 2007, Walter de Gruyter, Berlin, 2009, 171–184.

[8] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, Acta Arith. 17 (1970), 161–168.

Institute for Advanced Study
Princeton, NJ 08540, U.S.A.
E-mail: bourgain@ias.edu

Department of Mathematics
Dartmouth College
Hanover, NH 03755-3551, U.S.A.
E-mail: carlp@gauss.dartmouth.edu

Department of Mechanics and Mathematics
Moscow State University
Moscow, 119992, Russia
E-mail: konyagin@ok.ru

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

Received on 27.11.2008 (5872)