On the smallest simultaneous power nonresidue modulo a prime

K. Ford, M. Z. Garaev and S. V. Konyagin

Abstract

Let p be a prime and $p_1, \dots, p_r$ be distinct prime divisors of $p-1$. We prove that the smallest positive integer n which is a simultaneous $p_1, \dots, p_r$-power nonresidue modulo p satisfies

$$n < p^{1/4 - c_r + o(1)} \quad (p \to \infty)$$

for some positive c_r satisfying $c_r = e^{-(1+o(1))r}$ $(r \to \infty)$.

Mathematical Subject Classification: 11A15, 11A07, 11N29

Keywords: simultaneous power nonresidues; primitive roots; sieve methods; well-spaced divisors

1 Introduction

Let $n(p)$ be the smallest positive quadratic nonresidue modulo p and $g(p)$ be the smallest positive primitive root modulo p. The problem of upper bound estimates for $n(p)$ and $g(p)$ starts from the early works of Vinogradov. It is believed that $n(p) = p^{o(1)}$ and $g(p) = p^{o(1)}$ as $p \to \infty$. Vinogradov [14, 15] proved that

$$n(p) \ll p^{\frac{1}{2\sqrt{e}}} (\log p)^2, \qquad g(p) < \frac{2^{k+1}(p-1)p^{\frac{1}{2}}}{\phi(p-1)},$$

where k is the number of distinct prime divisors of $p-1$. Hua [9] improved Vinogradov's result to $g(p) < 2^{k+1}p^{1/2}$ and then Erdős and Shapiro [6] refined it to $g(p) \ll k^C p^{\frac{1}{2}}$, where C is an absolute constant. These bounds were improved by Burgess [1, 2] to

$$n(p) < p^{\frac{1}{4\sqrt{e}}+o(1)}, \qquad g(p) < p^{\frac{1}{4}+o(1)} \qquad (p \to \infty).$$

The Burgess bounds remains essentially the best known up to date, in a sense that it is not even known that $n(p) \ll p^{1/4\sqrt{e}}$ or that $g(p) \ll p^{1/4}$.

If one allows a small exceptional set of primes, then better estimates may be obtained. Using his "large sieve", Linnik [12] proved that for any $\varepsilon > 0$, there are only $O_\varepsilon(\log\log x)$ primes $p \leqslant x$ for which $n(p) > p^\varepsilon$. The sharpest to date results for $g(p)$ (which also hold for the least *prime* primitive root modulo p) are due to Martin [13], who proved that for any $\varepsilon > 0$, there is a $C > 0$ so that $g(p) = O((\log p)^C)$ with at most $O(x^\varepsilon)$ exceptions $p \leqslant x$. All of these type of results are "purely existential", in that one cannot say for which specific primes p the bounds hold (say, in terms of the factorization of $p-1$).

From elementary considerations it follows that an integer g is a primitive root modulo p if and only if for any prime divisor $q|p-1$ the number g is a q-th power nonresidue modulo p. Thus, if $p_1, \ldots, p_k$ are all the distinct prime divisors of $p-1$, then $g(p)$ is the smallest positive simultaneous $p_1, \ldots, p_k$-th power nonresidue modulo p. In the present paper we prove the following result.

Theorem 1. *Let p be a prime number and $p_1, \ldots, p_r$ be distinct prime divisors of $p-1$. Then the smallest positive integer n which is a simultaneous $p_1, \ldots, p_r$-th power nonresidue modulo p satisfies*

$$n < p^{1/4-c_r} e^{C(\log r)^{1/2}(\log p)^{1/2}}$$

where $C > 0$ is an absolute constant and $c_r = e^{-(1+o(1))r}$ as $r \to \infty$.

The novelty of the result is given by the factor p^{-c_r}. We observe that for $c_r < (\log p)^{-1/2}$ (in particular, for $r \geqslant (0.5+\varepsilon)\log\log p$ and $p \geqslant p(\varepsilon)$) this factor is dominated by the exponential factor.

The following corollaries directly follow from Theorem 1.

Corollary 1. *Let p be a prime number and $p_1, \ldots, p_r$ be distinct prime divisors of $p-1$, where r is fixed. Then the smallest positive integer n which is a simultaneous $p_1, \ldots, p_r$-th power nonresidue modulo p satisfies*

$$n < p^{1/4-c_r+o(1)} \quad (p \to \infty).$$

From our earlier discussion, the upper bound given in Theorem 1 holds also for $g(p)$ whenever $p-1$ has r distinct prime factors.

Corollary 2. *For any $\varepsilon > 0$, if $p-1$ has at most $(0.5-\varepsilon)\log\log p$ distinct prime divisors, then $g(p) = o(p^{1/4})$ as $p \to \infty$.*

The counting function of primes satisfying the hypothesis of Corollary 2 is $x(\log x)^{-3/2+(\log 2)/2-O(\varepsilon)}$ (the upper bound follows from e.g., [4, Inequality (5)]; the lower bound can be obtained using sieve methods).

Remark 1. *The focus of our arguments is to establish bounds which are uniform in r. We have made no attempt to optimize the value of c_r for small r, and leave this as a problem for further study.*

Our proof of Theorem 1 proceeds in three main steps. The first is a standard application of character sums to show that a large proportion of integers $n < p^{1/4+o(1)}$ are simultaneous $p_1, \ldots, p_r$-th power nonresidue modulo p. Next, we show that if such a number n has many divisors ($r2^r$ divisors suffice), then for some pair $d < d'$ of these divisors, the smaller number $n' = dn/d'$ is also a simultaneous $p_1, \ldots, p_r$-th power nonresidue modulo p. This procedure is most efficient when the ratios d'/d are uniformly large. In the third step we show that integers possessing many well-spaced divisors are sufficiently dense, so that there must be one such number in the set guaranteed by first step (with an appropriate quantification of "well-spaced" and "dense").

2 Character sums and distribution of power nonresidues

We begin by recalling the well-known character sum estimate of Burgess [2, 3].

Lemma 1. *If p is a prime and χ is a non-principal character modulo p and if H and m are arbitrary positive integers, then*

$$\Big|\sum_{n=N+1}^{N+H} \chi(n)\Big| \ll H^{1-1/m} p^{(m+1)/4m^2} (\log p)^{1/m}$$

for any integer N, where the implied constant is absolute.

See the proof in [11], (12.58). In the remark after the proof the authors announce that the factor $(\log p)^{1/m}$ can be replaced by $(\log p)^{1/(2m)}$, but this is not important for us.

Lemma 2. *Let p be a prime number and $p_1, \ldots, p_r$ be distinct prime divisors of $p-1$. The number J of integers $n \leqslant H$ which are simultaneous $p_1, \ldots, p_r$-th power nonresidues modulo p satisfies*

$$J \geqslant \frac{H}{8} \prod_{i=1}^{r} \Big(1 - \frac{1}{p_i}\Big) + O\Big(r^9 H^{1-1/m} p^{(m+1)/4m^2} (\log p)^{1/m}\Big),$$

where the constant implied in the "O"-symbol is absolute.

Proof. We follow the method of [5]. Let C be a sufficiently large constant, to be chosen later. Assuming that $p_1 < \cdots < p_r$, we choose the largest $s \leqslant r$ so that $p_s \leqslant Cr^2$ (if $p_1 > Cr^2$, then set $s = 0$). Let J_1 be the number of integers $n \leqslant H$ which are simultaneous $p_1, \ldots, p_s$-th power nonresidues modulo p. For $j > s$, let $J_{2,j}$ be the number of integers $n \leqslant H$ which are p_j-th power residues modulo p. Clearly,

$$J \geqslant J_1 - \sum_{j=s+1}^{r} J_{2,j}. \tag{2.1}$$

Let g be a primitive root of p and let χ_0 be the principal Dirichlet character modulo p. We will denote by χ a generic Dirichlet character modulo p. By orthogonality, for $(x, p) = 1$ we have

$$\frac{1}{d} \sum_{\chi^d = \chi_0} \chi(x) = \begin{cases} 1, & \text{if } \operatorname{ind}_g x \equiv 0 \pmod{d}, \\ 0, & \text{if } \operatorname{ind}_g x \not\equiv 0 \pmod{d}. \end{cases}$$

A number n is a p_i-power residue modulo p if and only if $p_i | \operatorname{ind}_g n$. Hence,

$$J_1 = \sum_{\substack{n \leqslant H \\ \gcd(\operatorname{ind}_g n, p_1 \ldots p_s) = 1}} 1 = \sum_{d | p_1 \ldots p_s} \mu(d) \sum_{\substack{n \leqslant H \\ d | \operatorname{ind}_g n}} 1$$

and for $j = s+1, \ldots, r$ we have

$$J_{2,j} = \sum_{\substack{n \leqslant H \\ p_j | \operatorname{ind}_g n}} 1. \tag{2.2}$$

We denote
$$R = H^{1-1/m} p^{(m+1)/4m^2} (\log p)^{1/m}.$$
Using Lemma 1 for $\chi \neq \chi_0$, we get for any d that
$$\sum_{\substack{n \leqslant H \\ d \mid \operatorname{ind}_g n}} 1 = \frac{1}{d} \sum_{\chi^d = \chi_0} \sum_{n \leqslant H} \chi(n) = \frac{H}{d} + O(R). \tag{2.3}$$

To estimate J_1 we use a lower bound sieve as in [5] combining with (2.3). Brun's sieve [8, Theorem 2.1 and the following Remark 2] suffices. Here the "sieve dimension" is $\kappa = 1$. Taking $\lambda = \frac{1}{4}$, $b = 1$, $z = Cr^2$ and $L = O(R)$ in [8, Theorem 2.1 and the following Remark 2], we get that
$$\begin{aligned} J_1 &\geqslant H \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \left(1 - 2\frac{\lambda^{2b} e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} + O\left(\frac{1}{\log z}\right)\right) - O(z^{4.1} R) \\ &\geqslant 0.13 H \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) - O(r^9 R) \end{aligned}$$
if C is large enough.

By (2.2) and (2.3),
$$\sum_{j=s+1}^{r} J_{2,j} = H \sum_{j=s+1}^{r} \frac{1}{p_j} + O(rR) \leqslant \frac{H}{Cr} + O(rR),$$
since $p_j > Cr^2$ for all $j \geqslant s+1$. Taking into account
$$\prod_{i=1}^{s} \Bigl(1 - \frac{1}{p_i}\Bigr) \geqslant \prod_{i=1}^{r} \Bigl(1 - \frac{1}{p_i}\Bigr) \geqslant \frac{1}{r+1} \geqslant \frac{1}{2r}$$
and assuming that $C \geqslant 400$, we get
$$J_1 - \sum_{j=s+1}^{r} J_{2,j} \geqslant \frac{H}{8} \prod_{i=1}^{r} \Bigl(1 - \frac{1}{p_i}\Bigr) + O(r^9 R).$$
Using (2.1) we complete the proof of the lemma. $\square$

3 Reduction of simultaneous nonresidues

The aim of this section is to show that if a positive integer n which is a simultaneous $p_1, \dots, p_r$-th power nonresidue modulo p has many divisors then it is possible to construct $n' < n$ which is also a simultaneous $p_1, \dots, p_r$-th power nonresidue modulo p.

Lemma 3. *Let q be a prime, $u \in \mathbb{R}$, $u > 1$ and $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod q$. Assume that*

$$a_1, a_2, \dots, a_t \tag{3.1}$$

is a sequence of $t \geqslant 2uq/(q-1)$ integers (not necessarily distinct). Then for some $\ell \in \mathbb{N}$, $\ell \geqslant u$ and indices $i_1 < i_2 < \dots < i_\ell$ we have that

$$a_{i_v} - a_{i_w} \not\equiv a \pmod q \quad (1 \leqslant v, w \leqslant \ell).$$

Proof. From the pigeon-hole principle, there is a residue class $h \pmod q$ containing at most t/q elements from the sequence (3.1). For $1 \leqslant j \leqslant q-1$, let

$$Q_j = \{1 \leqslant i \leqslant t : \, a_i \equiv h + ja \pmod q\}.$$

Then

$$\Big|\bigcup_{j=1}^{q-1} Q_j\Big| \geqslant t - \frac{t}{q} = \frac{(q-1)t}{q}.$$

Let

$$A = \bigcup_{\substack{1 \leqslant j \leqslant q-1 \\ 2 \mid j}} Q_j, \quad B = \bigcup_{\substack{1 \leqslant j \leqslant q-1 \\ 2 \nmid j}} Q_j$$

Clearly, the sets A and B have no solutions to $x - y \equiv a \pmod q$. Since

$$\max\{|A|, |B|\} \geqslant \frac{1}{2}\Big|\bigcup_{j=1}^{q-1} Q_j\Big| \geqslant \frac{(q-1)t}{2q} \geqslant u,$$

the result follows. $\square$

Remark 2. *For $q = 2$ it is enough to require $t \geqslant 2u$. Indeed, we can choose a large subsequence of $a_1, a_2, \dots, a_t$ of the same parity.*

Corollary 3. *Let $p_1, p_2, \dots, p_r$ be prime numbers, and*

$$\mathbf{b} = (b_1, b_2, \dots, b_r) \in \mathbb{F}_{p_1}^* \times \mathbb{F}_{p_2}^* \times \dots \times \mathbb{F}_{p_r}^*.$$

Let

$$t > 2^r \prod_{i:p_i>2} \frac{p_i}{p_i - 1}$$

and

$$\mathbf{a}_1,\ \mathbf{a}_2\ \dots, \mathbf{a}_t$$

be a sequence of t elements from $\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \dots \times \mathbb{F}_{p_r}$. Then for some $i < j$ we have that

$$\mathbf{a}_j - \mathbf{a}_i \in (\mathbb{F}_{p_1} \setminus \{b_1\}) \times (\mathbb{F}_{p_2} \setminus \{b_2\}) \times \dots \times (\mathbb{F}_{p_r} \setminus \{b_r\})\,.$$

Corollary 3 follows from r applications of Lemma 3 and taking into account Remark 2.

Corollary 4. *Let p be a prime number and suppose $p_1, \dots, p_r$ are distinct prime divisors of $p-1$. Let n be a simultaneous $p_1, \dots, p_r$-th power nonresidue modulo p and $d_1 < \dots < d_t$ be some divisors of n where*

$$t > 2^r \prod_{p_i>2} \frac{p_i}{p_i - 1}.$$

Then there exists i, j such that $1 \leqslant i < j \leqslant t$ and the number $n' = nd_i/d_j$ is also a simultaneous $p_1, \dots, p_r$-th power nonresidue modulo p.

Proof. Let g be a primitive root modulo p. To each number x we associate the vector

$$(s_1, s_2, \dots, s_r) \in \mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \dots \times \mathbb{F}_{p_r},$$

so that for $1 \leqslant i \leqslant r$, $x \equiv g^{p_i k_i + s_i} \pmod p$ where $0 \leqslant s_i < p_i$

Let the vector $(b_1, b_2, \dots, b_r)$ correspond to n and the vectors $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_t$ correspond to $d_1, \dots, d_t$, respectively. Apply Corollary 3 and select the indices $i < j$ such that

$$\mathbf{a}_j - \mathbf{a}_i \in (\mathbb{F}_{p_1} \setminus \{b_1\}) \times (\mathbb{F}_{p_2} \setminus \{b_2\}) \times \dots \times (\mathbb{F}_{p_r} \setminus \{b_r\})$$

Then $n' = nd_i/d_j$ is a simultaneous $p_1, p_2, \dots, p_r$-power nonresidue modulo p. □

Remark 3. *We note that if $p_1, p_2, \dots, p_r$ are distinct primes, then*

$$r > \prod_{p_i>2} \frac{p_i}{p_i - 1}. \tag{3.2}$$

Hence, in Corollaries 3 and 4 one can take $t = 2^r r$.

4 Integers with well-spaced divisors

Let $P^-(n)$ and $P^+(n)$ denote the smallest and largest prime factor of n, respectively, let $\omega(n)$ be the number of distinct prime factors of n, and let $\tau(n)$ be the number of positive divisors of n.

Lemma 4. *For each fixed constant $c > 1/\log 2 = 1.442\ldots$, there is $\eta = \eta(c) > 0$ such that the following holds. Uniformly for integers t, $2 \leqslant t \leqslant (\log x)^{1/c}$, all but $O_c(x/t^\eta)$ integers $n \leqslant x$ have t divisors $d_1 < d_2 < \cdots < d_t$ such that $d_{j+1}/d_j > x^{1/t^c}$ for all $1 \leqslant j \leqslant t-1$.*

Proof. We may assume that $t \geqslant 10$. Take

$$\varepsilon = \frac{c - 1/\log 2}{4}, \qquad \alpha = 1/\log 2 + \varepsilon.$$

Write each $n \leqslant x$ in the form abd where $P^-(d) > x^{1/\log t}$, $P^+(a) \leqslant x^{1/(t^\alpha \log t)}$ and all prime factors of b lie in $(x^{1/(t^\alpha \log t)}, x^{1/\log t}]$. We divide n into several categories. Let $k_0 = \lceil \frac{\log 2t}{\log 2} \rceil$. Let S_0 be the set of $n \leqslant x$ with either $d = 1$ or with b not squarefree. Let S_1 be the set of n with $d > 1$, b squarefree and $\omega(b) < k_0$. We denote $\alpha_j = j\varepsilon$ for $1 \leqslant j \leqslant J-1 := [\alpha/\varepsilon]$, $\alpha_J = \alpha$, $a_j = x^{1/(t^{\alpha_j} \log t)}$ for $j = 1, \ldots, J$. Let S_2 be the set of n with $d > 1$, b squarefree and the number of primes from the interval $(a_j, x^{1/\log t}]$ dividing n is less than $k_j := (\alpha_j - \varepsilon)\log t$ for some $j = 1, \ldots, J-1$. Let S_3 be the set of the remaining integers n.

We first show that S_0, S_1, and S_2 are small. By standard counts for smooth numbers,

$$|S_0| \leqslant \Psi(x, x^{1/\log t}) + \sum_{p > x^{1/(t^\alpha \log t)}} \frac{x}{p^2} \ll \frac{x}{t} + \frac{x}{x^{1/(t^\alpha \log t)}} \ll \frac{x}{t}.$$

Next, by the results of Halász [7] on the number of integers with a prescribed number of prime factors from a given set (see also Theorem 08 of [10]), we have

$$
\begin{aligned}
|S_1| &\ll \sum_{k<k_0} x e^{-E}\frac{E^k}{k!}, \qquad E = \sum_{x^{1/(t^\alpha \log t)}<p\leqslant x^{1/\log t}} \frac{1}{p} = \alpha \log t + O(1) \\
&\ll x t^{-\alpha} \sum_{k<k_0} \frac{(\alpha \log t)^k}{k!} \\
&\ll x(t^\alpha)^{-(\beta\log\beta-\beta+1)}, \quad \beta = \frac{1}{\alpha\log 2} = \frac{1}{1+\varepsilon\log 2} < 1 \\
&\ll x/t^\delta
\end{aligned}
$$

for some $\delta > 0$ which depends on ε.

For any $j = 1, \ldots, J-1$ we denote by $S_{2,j}$ the set of $n \leqslant x$ with less than k_j prime divisors from $(a_j, x^{1/\log t}]$. We have

$$
|S_{2,j}| \ll \sum_{k<k_j} x e^{-E_j}\frac{E_j^k}{k!},
$$

where

$$
E_j = \sum_{x^{1/(t^{\alpha_j}\log t)}<p\leqslant x^{1/\log t}} \frac{1}{p} = \alpha_j \log t + O(1).
$$

Arguing as before we get

$$
|S_{2,j}| \ll x/t^{\delta'}
$$

for some $\delta' > 0$ which depends on ε.

Notice that for $n \in S_3$, $\tau(b) = 2^{\omega(b)} \geqslant 2^{k_0} \geqslant 2t$. Next, let S_4 be the set of $n \in S_3$ for which b does *not* have t well-spaced divisors in the sense of the lemma. Since $d > 1$ for such n, given such a *bad* value of b, using a standard sieve bound the number of choices for the pair (a, d) is bounded above by

$$
\sum_a |\{d \leqslant x/ab : P^-(d) > x^{1/\log t}\}| \ll \sum_a \frac{x/ab}{\log(x^{1/\log t})} \ll \frac{x}{bt^\alpha}.
$$

Hence,

$$
|S_4| \ll \sum_{\text{bad } b} \frac{x}{bt^\alpha} \tag{4.1}
$$

A number b which is bad has many pairs of *neighbor divisors*. To be precise, let $\sigma = t^{-c}\log x$ and define

$$
W^*(b;\sigma) = |\{(d', d'') : d'|b, d''|b, d' \neq d'', |\log(d'/d'')| \leqslant \sigma\}|.
$$

Let $d_1 < \cdots < d_{\tau(b)}$ be the divisors of b. We construct the subsequence $D_1 < \cdots < D_r$ of this sequence:

$$D_1 = 1, \quad D_i = \min\{d_j : d_j > x^{t^{-c}} D_{i-1}\} \, (i > 1).$$

The process is terminated if D_i does not exist. Let $D_{r+1} = +\infty$. The set $\{d_1, \ldots, d_{\tau(b)}\}$ is divided into r subsets $\mathcal{D}_i$, $i = 1, \ldots, r$, where

$$\mathcal{D}_i = \{d_j : D_i \leqslant d_j < D_{i+1}\}.$$

We see that (d', d'') is counted in $W^*(b; \sigma)$ if $d', d'' \in \mathcal{D}_i$ for some i and $d' \neq d''$. Hence,

$$W^*(b; \sigma) \geqslant \sum_{i=1}^{r} |\mathcal{D}_i|(|\mathcal{D}_i| - 1) = \sum_{i=1}^{r} |\mathcal{D}_i|^2 - \tau(b).$$

Since $\tau(b) \geqslant 2t$ and $r \leqslant t$, we get by the Cauchy-Schwartz inequality that

$$\tau(b)^2 = \left(\sum_{i=1}^{r} |\mathcal{D}_i| \right)^2 \leqslant t \left(\sum_{i=1}^{r} |\mathcal{D}_i|^2 \right) \leqslant t(W^*(b; \sigma) + \tau(b)) \leqslant tW^*(b; \sigma) + \frac{1}{2}\tau(b)^2.$$

Therefore,

$$\sum_{\text{bad } b} \frac{1}{b} \leqslant \sum_{\text{all } b} \frac{2W^*(b; \sigma)t}{b\tau(b)^2}, \tag{4.2}$$

each sum being over squarefree integers whose prime factors lie in $(x^{1/(t^{\alpha} \log t)}, x^{1/\log t}]$.

In the latter sum, fix $k = \omega(b)$, write $b = p_1 \cdots p_k$, where the p_i are primes, and $p_1 < \cdots < p_k$. Then $W^*(p_1 \cdots p_k; \sigma)$ counts the number of pairs $Y, Z \subset \{1, \ldots, k\}$ with $Y \neq Z$ and

$$\left| \sum_{i \in Y} \log p_i - \sum_{i \in Z} \log p_i \right| \leqslant \sigma. \tag{4.3}$$

Fix Y, Z, and let I be the maximum element of the symmetric difference $(Y \cup Z) - (Y \cap Z)$. We fix I and count the number of $p_1, \ldots, p_k$ satisfying (4.3). We further partition the solutions, according to the condition $a_j < p_I \leqslant a_{j-1}$, for $j = 1, \ldots, J$. Fix the value of j. If all the p_i are fixed except for p_I, then (4.3) implies that p_I lies in some interval of the form $[U, Ue^{2\sigma}]$. As $p_I > x^{1/t^{\alpha_j} \log t}$ as well, and $\alpha > c$, we have (putting $U_j = \max(U, x^{1/t^{\alpha_j} \log t})$)

$$\sum_{p_I} \frac{1}{p_I} \ll \log \left(1 + \frac{2\sigma}{\log U_j} \right) \ll \frac{\sigma}{\log U_j} \ll t^{\alpha_j - c} \log t.$$

Hence, for each fixed k, j, Y and Z,

$$\begin{aligned}\sum_{x^{1/t^{\alpha}\log t}<p_1<\ldots<p_k\leqslant x^{1/\log t}} \frac{1}{p_1\cdots p_k} &\ll \frac{t^{\alpha_j-c}(\log t)}{(k-1)!}\Big(\sum_{x^{1/t^{\alpha}\log t}<p\leqslant x^{1/\log t}} \frac{1}{p}\Big)^{k-1} \\ &\ll \frac{t^{\alpha_j-c}(\log t)(\alpha\log t+O(1))^{k-1}}{(k-1)!}.\end{aligned} \tag{4.4}$$

Now we estimate the number $N(I,j)$ of choices for the pair Y,Z for fixed I and j. Since $p_I\leqslant a_{j-1}$, the condition $n\in S_3$ implies $I\leqslant k-k_{j-1}$. For any $i\leqslant I$ there are at most four possibilities: $i\in Y\cap Z$, $i\in Y\setminus Z$, $i\in Z\setminus Y$, $i\notin Y\cup Z$. For $i>I$ there are two possibilities: $i\in Y\cap Z$ and $i\notin Y\cup Z$. Therefore,

$$N(I,j)\leqslant 4^I2^{k-I}\leqslant 4^k2^{-k_{j-1}}\leqslant 4^kt^{-\alpha_j\log 2+2\varepsilon\log 2}. \tag{4.5}$$

It follows from (4.4) and (4.5) that

$$\sum_{\omega(b)=k}\frac{W^*(b;\sigma)t}{b\tau(b)^2}\ll \sum_{j=1}^{J} t^{1+(1-\log 2)\alpha_j+2\varepsilon-c}\sum_{k}\frac{(\alpha\log t+O(1))^{k-1}}{(k-1)!}.$$

Taking into account that $\alpha_j\leqslant\alpha$ and summing on j,k we get

$$\sum_{b}\frac{W^*(b;\sigma)t}{b\tau(b)^2}\ll t^{1+2\varepsilon+(2-\log 2)\alpha-c}.$$

Thus, by (4.1) and (4.2),

$$|S_4|\ll\frac{x}{t^{c-(1-\log 2)\alpha-2\varepsilon-1}}=\frac{x}{t^{c-1/\log 2-\varepsilon(3-\log 2)}}\ll\frac{x}{t^{\varepsilon}}.$$

Therefore, there are $x-O(x/t^{\min(\delta,\delta',\varepsilon)})$ numbers $n\leqslant x$ for which b does have t well-spaced divisors. $\square$

Remark 4. *Lemma 4 is best possible in the sense that the conclusion does not hold for $c<1/\log 2$. In fact, for any $c<1/\log 2$, the number of integers $n\leqslant x$ that* do *have t divisors $d_1,\ldots,d_t$ with $d_{j+1}/d_j>n^{1/t^c}$ for all j is $O_c(x/t^{\eta})$ for some $\eta>0$ which depends on c.*

Proof. It is well-known that if t is large, $c < 1/\log 2$ and ε small enough, then a typical integer n has $r \sim (c+\varepsilon)\log t$ prime factors $p_1, \dots, p_r$ in $[n^{1/t^{c+\varepsilon}}, n]$. This can be seen, e.g. by the theorem of Halász used in the estimation of $|S_1|$. In fact, the number of exceptional $n \leqslant x$ is $O_c(x/t^\eta)$. Thus, a typical n has about $2^{(c+\varepsilon)\log t} = t^{(c+\varepsilon)\log 2} < t$ divisors composed of such primes. Also, for most of these n, $n/(p_1 \cdots p_r) < n^{1/(2t^c)}$; by Theorem 07 of [10], the number of exceptions $n \leqslant x$ is $O(x \exp\{-c_1 t^\varepsilon\})$ for some $c_1 > 0$. Suppose that such an n has t well-spaced divisors $d_1, \dots, d_t$ with $d_{j+1}/d_j > n^{1/t^c}$ for all j. By the pigeon-hole principle, two of these divisors share the same set of prime factors from $\{p_1, \dots, p_r\}$, hence their ratio is less than $n^{1/(2t^c)}$, a contradiction. □

5 Proof of Theorem 1

We rewrite the assertion of Lemma 2 as

$$J \geqslant \frac{H}{8}\prod_{i=1}^{r}\Big(1-\frac{1}{p_i}\Big) - R', \quad R' = (5r)^{C''} H^{1-1/m} p^{(m+1)/4m^2} (\log p)^{1/m} \tag{5.1}$$

for some constant C''. Let $\mathcal{N}$ denotes the set of $n \in [1, H]$ which are simultaneous $p_1, \dots, p_r$-th power nonresidue modulo p, where

$$H = p^{1/4} e^{(C''+3)(\log p)^{1/2}(\log(5r))^{1/2}} \log p.$$

Assume that p is sufficiently large, and take

$$m = \lfloor (\log p)^{1/2} (\log(5r))^{-1/2} \rfloor.$$

Notice that $m \gg (\log p)^{1/2} (\log\log p)^{-1/2} \to \infty$ as $p \to \infty$. Since

$$R' = H(Hp^{-1/4}/\log p)^{-1/m} p^{1/(4m^2)} (5r)^{C''},$$

we have

$$(Hp^{-1/4}/\log p)^{-1/m} \leqslant (5r)^{-C''-3}$$

and

$$p^{1/(4m^2)} \leqslant 5r.$$

Consequently,

$$R' \leqslant H(5r)^{-2}.$$

By (5.1) and (3.2),

$$J \geqslant (0.12r^{-1} - (5r)^{-2})H \geqslant 0.08H/r.$$

So, we see that

$$|\mathcal{N}| \geqslant 0.08H/r. \tag{5.2}$$

We consider the case

$$r < 0.6 \log\log p \tag{5.3}$$

first. We will apply Lemma 4 with $x = H$, fixed $c \in (1/\log 2, 1.5]$, and with $t = Kr2^r$, where K is a sufficiently large constant depending on c. By (5.2), the exceptional set in Lemma 4 is smaller than $|\mathcal{N}|$ provided that K is large enough. The condition $2 \leqslant t \leqslant (\log x)^{1/c}$ is satisfied due to the restriction on r and c. By Lemma 4, for some $n \in \mathcal{N}$, there are well-separated divisors $d_1 < \cdots < d_t$ of n, satisfying $d_{i+1}/d_i > n^{1/t^c}$ for each i. Now we are in position to apply Corollary 4 and we see that there is an $n' \leqslant np^{-t^{-c}/4}$ such that n' is a simultaneous $p_1, \ldots, p_r$-th power nonresidue modulo p. Noting that $t^{-c}/4 = \exp\{-r(c\log 2 + o(1))\}$ and that c may be taken arbitrarily close to $1/\log 2$, we complete the proof.

If (5.3) does not hold, then, as we have mentioned in Section 1, the factor p^{-c_r} in the statement of the theorem is dominated by the second factor, and the claim follows from the fact that $\mathcal{N} \neq \emptyset$.

6 Acknowledgements

The first author is supported in part by National Science Foundation grants DMS-1201442 and DMS-1501982. The third author is supported by grant RFBR 14-01-00332.

References

[1] D. A. Burgess, 'The distribution of quadratic residues and non-residues', *Mathematika*, **4** (1957), 106–112.

[2] D. A. Burgess, 'On character sums and primitive roots', *Proc. London Math. Soc.*, **12** (1962), 179–192.

[3] D. A. Burgess, ‘On character sums and L-series. II.’, *Proc. London Math. Soc.*, **13** (1963), 524–536.

[4] P. Erdős, ‘On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function’, *Quart. J. Math. Oxford Ser.*, **6** (1935), 205–213.

[5] P. Erdős, ‘On the least primitive root of a prime’, *Bull. London Math. Soc.*, **55** (1945), 131–132.

[6] P. Erdős, H. N. Shapiro, ‘On the least primitive root of a prime’, *Pacific J. Math.,* **7** (1957), 861–865.

[7] G. Halász, ‘Remarks to my paper: "On the distribution of additive and the mean values of multiplicative arithmetic functions"’, *Acta Math. Acad. Sci. Hungar.*, **23** (1972), 425–432.

[8] H. Halberstam, H.-E. Richert, *Sieve methods*, Academic Press, 1974.

[9] L.-K. Hua, ‘On the least primitive root of a prime’, *Bull. Amer. Math. Soc.,* **48** (1942), 726–730.

[10] R. R. Hall, G. Tenenbaum, *Divisors,* Cambridge Tracts in mathematics vol. **90**, 1988.

[11] H. Iwaniec, E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, Rhode Island, 2004.

[12] Yu. V. Linnik, ‘A remark on the least quadratic non-residue’, (Russian) *C. R. (Doklady) Acad. Sci. URSS (N.S.)*, **36** (1942), 119–120.

[13] G. Martin, ‘The least prime primitive root and the shifted sieve’, *Acta Arith.*, **80** (1997), no. 3, 277–288.

[14] I. M. Vinogradov, ‘On the distribution of quadratic residues and non-residues’, (in Russian), *Journal of the Physico-Mathematical Society of Perm*, 1919.

[15] I. M. Vinogradov, ‘On the least primitive root’, (Russian), *Doklady Akad. Nauk SSSR*, **1** (1930), 7–11.

Address of the authors:

K. Ford, Department of Mathematics, 1409 West Green Street, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA.
E-mail address: ford@math.uiuc.edu

M. Z. Garaev, Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México.
Email address: garaev@matmor.unam.mx

S. V. Konyagin, Steklov Mathematical Institute, 8 Gubkin Street, Moscow, 119991, Russia.
Email address: konyagin@mi.ras.ru