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 \( p_1, \ldots, p_r \) be distinct prime divisors of \( p - 1 \). We prove that the smallest positive integer \( n \) which is a simultaneous \( p_1, \ldots, p_r \)-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

\[
n(p) \ll p^{1/(2k\sqrt{\pi})} (\log p)^2, \quad g(p) < \frac{2^{k+1}(p - 1)p^{1/2}}{\phi(p - 1)},
\]

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 \( g(p) \ll k^C p^{1/4} \), where \( C \) is an absolute constant. These bounds were improved by Burgess \([1, 2]\) to

\[
n(p) < p^{1/4 + o(1)}, \quad g(p) < p^{1/4 + o(1)} \quad (p \to \infty).
\]

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 \( p \leq x \) 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 \( p \leq x \). 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 \( q \mid p - 1 \) 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 \( c_r = e^{-r(1 + o(1))} \) 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 \( r \geq 0.5 + \varepsilon \) log log \( p \) and \( p \geq p(\varepsilon) \)) 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 $\chi$ is a non-principal character modulo $p$ and if $H$ and $m$ are arbitrary positive integers, then

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

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 \(n \leq H\) which are simultaneous \(p_1, \ldots, p_r\)-th power nonresidues modulo \(p\) satisfies

\[
J \geq 0.12H \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) + O \left(r^{13} H^{1-1/m} p^{(m+1)/4m^2} (\log p)^{1/m}\right),
\]

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 \(s \leq r\) so that \(p_s \leq Cr^2\) (if \(p_1 > Cr^2\), then set \(s = 0\)). Let \(J_1\) be the number of integers \(n \leq H\) 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 \(n \leq H\) which are \(p_j\)-th power residues modulo \(p\). Clearly,

\[
J \geq J_1 - \sum_{j=s+1}^r J_{2,j}. \quad (2.1)
\]

Let \(g\) be a primitive root of \(p\) and let \(\chi_0\) be the principal Dirichlet character modulo \(p\). We will denote by \(\chi\) a generic Dirichlet character modulo \(p\). By orthogonality, for \((x, p) = 1\) we have

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

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

\[
J_1 = \sum_{\substack{n \leq H \\ \gcd(\text{ind}_g n, p_1 \cdots p_s) = 1}} 1 = \sum_{d | p_1 \cdots p_s} \mu(d) \sum_{\substack{n \leq H \\ d | \text{ind}_g n}} 1
\]

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

\[
J_{2,j} = \sum_{\substack{n \leq H \\ p_j | \text{ind}_g n}} 1. \quad (2.2)
\]
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
\[
\sum_{n \leq H \atop d | \text{ind}_s n} 1 = \frac{1}{d} \sum_{\chi \neq \chi_0} \sum_{n \leq H} \chi(n) = \frac{H}{d} + O(R). \tag{2.3}
\]
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 \( \lambda = \frac{1}{4} \), \( b = 1 \), \( z = C r^2 \) and \( L = O(R) \) in [8, Theorem 2.1 and the following Remark 2], we get that
\[
J_1 \geq H \prod_{i=1}^{s} \left( 1 - \frac{1}{p_i} \right) \left( 1 - 2 \lambda^{2b} e^{2\lambda} + O \left( \frac{1}{\log z} \right) \right) - O(z^{4.1} R)
\]
\[
\geq 0.13 H \prod_{i=1}^{s} \left( 1 - \frac{1}{p_i} \right) - O(r^{13} R)
\]
if \( C \) is large enough.

By (2.2) and (2.3),
\[
\sum_{j=s+1}^{r} J_{2,j} = H \sum_{j=s+1}^{r} \frac{1}{p_j} + O(r R) \leq \frac{H}{C r} + O(r R),
\]
since \( p_j > C r^2 \) for all \( j \geq s + 1 \). Invoking (3.3) and assuming that \( C \geq 100 \), we get
\[
J_1 - \sum_{j=s+1}^{r} J_{2,j} \geq 0.12 H \prod_{i=1}^{s} \left( 1 - \frac{1}{p_i} \right) + O(r^{13} R).
\]
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 \( p_1, \ldots, p_r \)-th power nonresidue modulo \( p \) has many divisors then it is possible to construct \( n' < n \) which is also a simultaneous \( p_1, \ldots, p_r \)-th power nonresidue modulo \( p \).
Lemma 3. Let $a$ be a non-zero real number, $\ell \in \mathbb{N}$ and
\[ a_1, a_2, \ldots, a_{2\ell-1} \] be any sequence of $2\ell - 1$ real numbers (not necessarily distinct). Then for some indices $i_1 < i_2 < \ldots < i_\ell$ we have that $a_{i_s} - a_{i_t} \neq a$ for all $1 \leq s, t \leq \ell$.

Proof. We may assume that $a > 0$. Define an equivalence relation on the numbers $i$ by setting $i \sim j$ if $a_i - a_j = ka$ for some integer $k$. Let $S_1, \ldots, S_m$ be the different (nonempty) equivalence classes. Clearly $a_i - a_j = a$ is only possible for $i, j$ within a given equivalence class. Let $b_r$ be the smallest element of $S_r$, for each $r = 1, \ldots, m$. Divide each $S_r$ into two subclasses,
\[ S_r^{(0)} = \{ i \in S_r : a_i - a_{b_r} = ka \text{ for some even integer } k \}, \]
\[ S_r^{(1)} = \{ i \in S_r : a_i - a_{b_r} = ka \text{ for some odd integer } k \}. \]

Obviously $a_i - a_j = a$ is impossible within each subclass $S_r^{(0)}, S_r^{(1)}$. For $1 \leq r \leq m$, define $\varepsilon_r = 0$ if $|S_r^{(0)}| \geq |S_r^{(1)}|$, and $\varepsilon_r = 1$ otherwise, and let $B = \bigcup_{r=1}^{m} S_r^{(\varepsilon_r)}$. Then $|B| \geq \ell$, and $a_i - a_j \neq a$ for $i, j \in B$. Any set $\{i_1, \ldots, i_\ell\} \subset B$ then satisfies the requirements of the lemma. \qed

Remark 2. The conclusion of Lemma 3 is best possible, as may be seen by taking $a_i = ai$ for $1 \leq i \leq 2\ell - 1$; in any set of $\ell + 1$ elements $a_i$ there are two with difference $a$.

Lemma 4. Let $q$ be a prime, $u \in \mathbb{R}$, $u > 1$ and $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{q}$. Assume that
\[ a_1, a_2, \ldots, a_t \] is a sequence of $t \geq 2uq/(q-1)$ integers (not necessarily distinct). Then for some $\ell \in \mathbb{N}$, $\ell \geq u$ and indices $i_1 < i_2 < \ldots < i_\ell$ we have that
\[ a_{i_v} - a_{i_w} \not\equiv a \pmod{q} \quad (1 \leq v, w \leq \ell). \]

Proof. We can assume that $a = 1$. Define $\ell = \lfloor u \rfloor$. From the pigeon-hole principle, there is a residue class $h \pmod{q}$ containing at most $t/q$ elements from the sequence (3.2). Since
\[ \left\lfloor \frac{t - \ell}{q} \right\rfloor = \left\lfloor \frac{t(q-1)}{q} \right\rfloor \geq \left\lfloor 2u \right\rfloor \geq 2\ell - 1, \]
after rearranging (3.2) we may assume that

\[ a_s \not\equiv h \pmod{q} \quad (s = 1, 2, \ldots, 2\ell - 1). \]

Define \( c_s \in \{1, 2, \ldots, q - 1\} \) by

\[ c_s \equiv a_s - h \pmod{q}. \]

By Lemma 3, there is a subsequence \( c_{i_1}, \ldots, c_{i_\ell} \) such that

\[ c_{i_v} - c_{i_w} \not\equiv 1 \quad (1 \leq v, w \leq \ell). \]

Since \( 1 \leq c_i \leq q - 1 \) this implies that

\[ c_{i_v} - c_{i_w} \not\equiv 1 \pmod{q} \quad (1 \leq v, w \leq \ell) \]

and thus

\[ a_{i_v} - a_{i_w} \not\equiv 1 \pmod{q} \quad (1 \leq v, w \leq \ell). \]

**Remark 3.** For \( q = 2 \) it is enough to require \( t \geq 2u \). Indeed, we can choose a large subsequence of \( a_1, a_2, \ldots, a_t \) of the same parity.

**Corollary 3.** Let \( p_1, p_2, \ldots, p_r \) be prime numbers, and

\[ b = (b_1, b_2, \ldots, b_r) \in \mathbb{F}_{p_1}^* \times \mathbb{F}_{p_2}^* \times \cdots \times \mathbb{F}_{p_r}^*. \]

Let

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

and

\[ a_1, a_2, \ldots, a_t \]

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

\[ a_j - a_i \in (\mathbb{F}_{p_1} \setminus \{b_1\}) \times (\mathbb{F}_{p_2} \setminus \{b_2\}) \times \cdots \times (\mathbb{F}_{p_r} \setminus \{b_r\}). \]

Corollary 3 follows from \( r \) applications of Lemma 4 and taking into account Remark 3.
Corollary 4. Let $p$ be a prime number and suppose $p_1, \ldots, p_r$ are distinct prime divisors of $p-1$. Let $n$ be a simultaneous $p_1, \ldots, p_r$-th power nonresidue modulo $p$ and $d_1 < \cdots < d_t$ 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 $1 \leq i < j \leq t$ and the number $n' = nd_i/d_j$ is also a simultaneous $p_1, \ldots, p_r$-th power nonresidue modulo $p$.

Proof. Let $g$ be a primitive root modulo $p$. To each number $x$ we associate the vector $(u_1, u_2, \ldots, u_r) \in \mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \cdots \times \mathbb{F}_{p_r}$, so that for $1 \leq i \leq r$, $x \equiv g^{u_i} \mod p$ where $0 \leq s_i < p_i$

Let the vector $(b_1, b_2, \ldots, b_r)$ correspond to $n$ and the vectors $a_1, a_2, \ldots, a_t$ correspond to $d_1, \ldots, d_t$, respectively. Apply Corollary 3 and select the indices $i < j$ such that

$$a_j - a_i \in \left( \mathbb{F}_{p_1} \setminus \{b_1\} \right) \times \left( \mathbb{F}_{p_2} \setminus \{b_2\} \right) \times \cdots \times \left( \mathbb{F}_{p_r} \setminus \{b_r\} \right)$$

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

Remark 4. We note that if $p_1, p_2, \ldots, p_r$ are distinct primes, then

$$r > \prod_{p_i > 2} \frac{p_i}{p_i - 1}. \tag{3.3}$$

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 5. 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 $t$, $2 \leq t \leq (\log x)^{1/c}$, all but $O_c(x/t^\eta)$ integers $n \leq x$ have $t$ divisors $d_1 < d_2 < \cdots < d_t$ such that $d_{j+1}/d_j > x^{1/c}$ for all $1 \leq j \leq t - 1$. 

8
Proof. We may assume that $t \geq 10$. Take
\[ \varepsilon = \frac{c - 1}{4 \log 2}, \quad \alpha = \frac{1}{\log 2} + \varepsilon. \]

Write each $n \leq x$ in the form $abd$ where $P^-(d) > x^{1/\log t}$, $P^+(a) \leq x^{1/(\alpha t^\log t)}$ 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 $k_0 = \lceil \frac{\log 2 t}{\log 2} \rceil$. Let $S_0$ be the set of $n \leq x$ 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 $1 \leq j \leq J - 1 := \lceil \alpha/\varepsilon \rceil$, $\alpha_j = \alpha$, $a_j = x^{1/(t^\alpha \log t)}$ 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,
\[ |S_0| \leq \Psi(x, x^{1/\log t}) + \sum_{p > x^{1/(t^\alpha \log t)}} \frac{x}{p^2} \ll \frac{x}{t} + \frac{x}{x^{1/(t^\alpha \log t)}} \ll \frac{x}{t}. \]

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
\[ |S_1| \ll \sum_{k < k_0} xe^{-E_j \frac{E_j^k}{k!}}, \quad E = \sum_{x^{1/(t^\alpha \log t)} \leq p < x^{1/\log t}} \frac{1}{p} = \alpha \log t + O(1) \]
\[ \ll xt^{-\alpha} \sum_{k < k_0} \frac{(\alpha \log t)^k}{k!} \]
\[ \ll x(t^\alpha)^{-((\beta \log \beta - \beta + 1)}}, \quad \beta = \frac{1}{\alpha \log 2} = \frac{1}{1 + \varepsilon \log 2} < 1 \]
\[ \ll x/t^\delta \]
for some $\delta > 0$ which depends on $\varepsilon$.

For any $j = 1, \ldots, J - 1$ we denote by $S_{2,j}$ the set of $n \leq x$ with less than $k_j$ prime divisors from $(a_j, x^{1/\log t}]$. We have
\[ |S_{2,j}| \ll \sum_{k < k_j} xe^{-E_j \frac{E_j^k}{k!}}, \]
where
\[ E_j = \sum_{x^{1/(t^u_j \log t)} < p < x^{1/ \log t}} \frac{1}{p} = \alpha_j \log t + O(1). \]

Arguing as before we get
\[ |S_{2,j}| \ll x/t^\delta' \]
for some \( \delta' > 0 \) which depends on \( \varepsilon \).

Notice that for \( n \in S_3 \), \( \tau(b) = 2^{\omega(b)} \geq 2^{k_0} \geq 2t \). 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 \emph{bad} value of \( b \), using a standard sieve bound the number of choices for the pair \((a,d)\) is bounded above by
\[ \sum_{a} |\{d \leq x/ab : P^-(d) > x^{1/\log t}\}| \ll \sum_{a} \frac{x/ab}{\log(x^{1/\log t})} \ll \frac{x}{bt^\alpha}. \]

Hence,
\[ |S_4| \ll \sum_{\text{bad } b} \frac{x}{bt^\alpha} \quad (4.1) \]

A number \( b \) which is bad has many pairs of \emph{neighbor divisors}. To be precise, let \( \sigma = t^{-c \log x} \) and define
\[ W^*(b; \sigma) = |\{(d',d'') : d'|b, d''|b, d' \neq d'', |\log(d'/d'')| \leq \sigma\}|. \]

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 \( D_i \), \( i = 1, \ldots, r \), where
\[ D_i = \{d_j : D_i \leq d_j < D_{i+1}\}. \]

We see that \((d',d'')\) is counted in \( W^*(b; \sigma) \) if \( d',d'' \in D_i \) for some \( i \) and \( d' \neq d'' \). Hence,
\[ W^*(b; \sigma) \geq \sum_{i=1}^{r} |D_i|(|D_i| - 1) = \sum_{i=1}^{r} |D_i|^2 - \tau(b). \]
Since \( \tau(b) \geq 2t \) and \( r \leq t \), we get by the Cauchy-Schwartz inequality that

\[
\tau(b)^2 = \left( \sum_{i=1}^{r} |D_i| \right)^2 \leq t \left( \sum_{i=1}^{r} |D_i|^2 \right) \leq t(W^*(b; \sigma) + \tau(b)) \leq tW^*(b; \sigma) + \frac{1}{2} \tau(b)^2.
\]

Therefore,

\[
\sum_{\text{bad } b} \frac{1}{b} \leq \sum_{\text{all } b} \frac{2W^*(b; \sigma)t}{b\tau(b)^2},
\]

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

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

\[
\left| \sum_{i \in Y} \log p_i - \sum_{i \in Z} \log p_i \right| \leq \sigma.
\]

(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 \( a_j < p_I \leq a_{j-1} \), 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 \([U, Uc^{2\sigma}]\). As \( p_I > x^{1/\alpha_j \log t} \) as well, and \( \alpha > c \), we have (putting \( U_j = \max(U, x^{1/\alpha_j \log t}) \))

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

Hence, for each fixed \( k, j, Y \) and \( Z \),

\[
\sum_{x^{1/\alpha_j \log t} < p_1 \cdots p_k \leq x^{1/\log t}} \frac{1}{p_1 \cdots p_k} \ll \frac{t^{\alpha_j - c} (\log t)}{(k-1)!} \sum_{x^{1/\alpha_j \log t} < p \leq x^{1/\log t}} \frac{1}{p^{k-1}} \ll \frac{t^{\alpha_j - c} (\log t) (\alpha \log t + O(1))^{k-1}}{(k-1)!}.
\]

(4.4)

Now we estimate the number \( N(I, j) \) of choices for the pair \( Y, Z \) for fixed \( I \) and \( j \). Since \( p_I \leq a_{j-1} \), the condition \( n \in S_3 \) implies \( I \leq k - k_{j-1} \). For any \( i \leq I \) 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,

\[
N(I, j) \leq 4^I 2^{k-I} \leq 4^k 2^{-k_j-1} \leq 4^{k_I - \alpha_j \log 2 + 2 \varepsilon \log 2}.
\] (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 \( \alpha_j \leq \alpha \) 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),

\[
|S_4| \ll \frac{x}{t \varepsilon}.
\]

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

**Remark 5.** Lemma 5 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 \( n \leq x \) that do have \( t \) divisors \( d_1, \ldots, d_t \) with \( d_{j+1}/d_j < n^{1/t^c} \) for all \( j \) is \( O(x/t^n) \) for some \( \eta > 0 \) which depends on \( c \).

**Proof.** It is well-known that if \( t \) is large, \( c < 1/\log 2 \) and \( \varepsilon \) small enough, then a typical integer \( n \) has \( r \sim (c + \varepsilon) \log t \) prime factors \( p_1, \ldots, p_r \) 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 \( n \leq x \) is \( O_c(x/t^n) \). 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 \( n \leq x \) is \( O(x \exp\{-c_1 t^c\}) \) for some \( c_1 > 0 \). Suppose that such an \( n \) has \( t \) well-spaced divisors \( d_1, \ldots, d_t \) with \( d_{j+1}/d_j < n^{1/t} \) for all \( j \). By the pigeon-hole principle, two of these divisors share the same set of prime factors from \( \{p_1, \ldots, p_r\} \), 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

\[ J \geq 0.12H \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) - R', \quad R' = (5r)^{C''} H^{1-1/m} p^{(m+1)/4m^2} (\log p)^{1/m} \tag{5.1} \]

for some constant \( C'' \). Let \( \mathcal{N} \) denotes the set of \( n \in [1, H] \) which are simultaneous \( p_1, \ldots, p_r \)-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

\[ (Hp^{-1/4}/\log p)^{-1/m} \leq (5r)^{-C''-3} \]

and

\[ p^{1/(4m^2)} \leq 5r. \]

Consequently,

\[ R' \leq H(5r)^{-2}. \]

By (5.1) and (3.3),

\[ J \geq (0.12r^{-1} - (5r)^{-2})H \geq 0.08H/r. \]

So, we see that

\[ |\mathcal{N}| \geq 0.08H/r. \tag{5.2} \]

We consider the case

\[ r < 0.6 \log \log p \tag{5.3} \]

first. We will apply Lemma 5 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 5 is smaller than \( |\mathcal{N}| \) provided that \( K \) is large enough. The condition \( 2 \leq t \leq (\log x)^{1/c} \) is satisfied due to the restriction
on \( r \) and \( c \). By Lemma 5, 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 \( n' \leq np^{-t^c/4} \) 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 and grant Leading Scientific Schools N 3082.2014.1.

References


the mean values of multiplicative arithmetic functions”’, Acta Math.


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


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