JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Kevin FORD, Mikhail R. GABDULLIN et Andrew GRANVILLE

Primes with small primitive roots

Tome 38, nº 1 (2026), p. 71-89.

https://doi.org/10.5802/jtnb.1355

CENTRE MERSENNE

Le Journal de Théorie des Nombres de Bordeaux *est membre du*
Centre Mersenne pour l'édition scientifique ouverte
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **38** (2026), 71–89

Primes with small primitive roots

par Kevin FORD, Mikhail R. GABDULLIN et Andrew GRANVILLE

Résumé. Supposons que la fonction $\delta(p)$ tend vers zéro arbitrairement lentement quand $p \to \infty$. Nous présentons un ensemble explicite $\mathcal{S}$ de nombres premiers p, défini en termes de fonctions simples des facteurs premiers de $p-1$, pour lequel la racine primitive la plus petite de p est $\leqslant p^{1/4-\delta(p)}$ pour tout $p \in \mathcal{S}$, où $\#\{p \leqslant x : p \in \mathcal{S}\} \sim \pi(x)$ quand $x \to \infty$.

Abstract. Let $\delta(p)$ tend to zero arbitrarily slowly as $p \to \infty$. We exhibit an explicit set $\mathcal{S}$ of primes p, defined in terms of simple functions of the prime factors of $p-1$, for which the least primitive root of p is $\leqslant p^{1/4-\delta(p)}$ for all $p \in \mathcal{S}$, where $\#\{p \leqslant x : p \in \mathcal{S}\} \sim \pi(x)$ as $x \to \infty$.

1. Introduction

In his masterwork *Disquisitiones Arithmeticae*, C. F. Gauss showed that every prime p has a primitive root (that is, a generator of $(\mathbb{Z}/p\mathbb{Z})^*$), and in fact has $\phi(p-1)$ primitive roots, where ϕ is Euler's totient function. These have applications to cryptography and pseudo-random number generation [4, Ch. 8], where an efficient algorithm for finding a primitive root is needed. In particular, it is of great interest to find upper bounds on $g(p)$, the least primitive root modulo p. It is believed that $g(p) = p^{o(1)}$ as $p \to \infty$, and this is considered as a notoriously difficult problem (which is known to be true under the Generalized Riemann Hypothesis, see [1, 19, 24]). The first unconditional upper bounds for $g(p)$ were obtained by Vinogradov [21, 23], Hua [12], and Erdős and Shapiro [6]. The current best estimate is due to Wang [24], who established in 1959 that

$$g(p) \ll p^{1/4+\varepsilon} \tag{1.1}$$

for every fixed $\varepsilon > 0$. A key ingredient in the proof is the character sum bound of Burgess [2].

Manuscrit reçu le 7 octobre 2024, révisé le 23 mars 2025, accepté le 25 avril 2025.
2020 *Mathematics Subject Classification.* 11A07, 11A15, 11A41.
The first author was partially supported by National Science Foundation grants DMS-1501982, DMS-1802139 and DMS-2301264. A.G. is partially supported by the Conseil de recherches en sciences naturelles et en génie du Canada.

On the other hand, if one allows a small exceptional set of primes, much better estimates are known. It was shown by Burgess and Elliott [3] that

$$\frac{1}{\pi(x)}\sum_{p\leqslant x} g(p) \ll (\log x)^2(\log\log x)^4,$$

which implies that for any $\varepsilon>0$, most primes p satisfy $g(p)\ll(\log p)^{2+\varepsilon}$. One can even get such a statement with a tiny exceptional set of primes. Martin [16] proved that for any $\varepsilon>0$ there is a $C\ll 1/\varepsilon$ so that

$$g(p)=O\Big((\log p)^C\Big)$$

with at most $O(x^\varepsilon)$ exceptions $p\leqslant x$. This is in the spirit of Linnik's famous theorem [15], which states that the least quadratic non-residue $n(p)$ modulo p satisfies $n(p)\leqslant p^\varepsilon$ for allbut $O_\varepsilon(\log\log x)$ primes $p\leqslant x$. All such statements are "purely existential", in that one cannot say for which specific primes p the bounds hold (say, in terms of the factorization of $p-1$). This motivates the search for explicit conditions on primes p under which (1.1) can be refined. A first such result appears in [8], where the first author, together with Garaev and Konyagin, proved that for each $r\geqslant 2$, there is a positive c_r so that $g(p)<p^{1/4-c_r}$ for all large p with $p-1$ having r distinct prime factors. Moreover, in [8] it is also shown that

$$g(p)=o(p^{1/4}),\quad p\to\infty$$

whenever $p-1$ has at most $(0.5-\varepsilon)\log\log p$ prime divisors, for any fixed $\varepsilon>0$. As noted in [8], the set of such primes has counting function about $x(\log x)^{-3/2+(\log 2)/2-O(\varepsilon)}$ and thus (since $-3/2+(\log 2)/2=-1.153\ldots<-1$) has relative density zero in the set of all primes. In fact, as was shown by Erdős [5], for most primes p, $p-1$ has close to $\log\log p$ prime factors.

Using different ideas, Sartori [18] showed that for every fixed $\varepsilon>0$ there exists $y=y(\varepsilon)$ such that

$$g(p)\ll p^{\frac{1}{4\sqrt{e}}+\varepsilon}$$

provided that

- all prime divisors of $(p-1)$ except 2 are greater than y;
- for any divisor d of $p-1$ the bound $J(d)\leqslant 10\omega(d)$ holds (here $J(d)$ is Jacobsthal's function; see Section 3 for its definition);
- one has
$$\sum_{\substack{q|p-1\\ q>2\text{ prime}}}\frac{\log\log q}{\log q}\leqslant\varepsilon/20.$$

It is proved in [18] that the set of primes enjoying the above three properties has positive relative density (which depends on ε). This bound for $g(p)$ matches, up to an ε in the exponent, the best known upper bound for the least quadratic non-residue modulo p, due to Burgess [2]; note that a primitive root modulo p is necessarily a quadratic non-residue. In fact, a number b is a primitive root of p if and only if it is a q-th power non-residue modulo p for all primes $q|(p-1)$. Comparing this with [8], we see that the bounds in [8] are sensitive to the *number* of prime factors of $p-1$, whereas the methods of [18] are sensitive primarily to the *size* of the odd prime factors of $p-1$.

In this paper we find an explicit set of almost all (that is, of relative density 1) primes p for which $g(p) = o(p^{1/4})$.

Theorem 1. *There is an absolute constant $\xi > 0$ such that the following holds. For any given large x and for $\delta \in [(\log x)^{-1/2}, \xi]$, we have*

$$g(p) \leqslant p^{1/4-\delta}$$

whenever $p \in (\sqrt{x}, x]$ is a prime for which the following two conditions hold:

(i) *One has*

$$\sum_{j \leqslant \log(1/\delta)} \frac{1}{q_j} \leqslant \xi \log\log\log(1/\delta);$$

(ii) *There exists $1 \leqslant r \leqslant \frac{1}{3}\log(1/\delta)$ such that*

$$\sum_{j>r} \frac{j^3 \log\log q_j}{\log q_j} \leqslant e^{-r-\sqrt{r \log\log\log(1/\delta)}},$$

where $2 = q_1 < q_2 < \cdots < q_{\omega(p-1)}$ are the prime divisors of $p-1$.

All but $O\Big(\exp\{-(\log\log(1/\delta))^{1/4}\}\pi(x)\Big)$ primes $p \in (\sqrt{x}, x]$ satisfy (i) *and* (ii)*.*

We now give a rough explanation why primes failing (i) or (ii) are rare. By standard results from the "anatomy of integers", a typical shifted prime $p-1 \leqslant x$ has multiplicative structure similar to that of a typical integer $n \leqslant x$, specifically there are close to $\log\log t$ prime factors below t, uniformly in $2 \leqslant t \leqslant x$; see, e.g., [7]. In particular, for typical primes p, $\sum_j 1/q_j$ is bounded. Moreover, $\log\log q_j$ is about j and thus the sum on the left side of (ii) is about e^{-r} for most r. However, for reasons stemming from the law of the iterated logarithm from probability theory, typically there will be some values of r for which the sum is roughly $\leqslant e^{-r-\sqrt{2r\log\log r}}$. Thus, if δ is sufficiently small, we expect (ii) to hold with high likelihood.

One of the key ingredients of the proof of Theorem 1 is the following refinement of the main result from [8].

Theorem 2. *The smallest positive integer n which is a simultaneous $p_1, \ldots, p_r$-power nonresidue modulo p, where $p_1, \ldots, p_r$ are distinct prime* *divisors of* $p-1$*, satisfies*

$$n < p^{1/4-\beta(r,\Phi)} \exp\Big(C(\log p)^{1/2}(\log(2r))^{1/2}\Big),$$

where

$$\beta(r,\Phi) = \exp\Big(-r - C'\sqrt{r\max(1,\log\Phi)}\Big), \quad \Phi := \frac{p_1\cdots p_r}{\phi(p_1\cdots p_r)}$$

and C, C' *are positive, absolute constants.*

From Theorem 2, we shall deduce the following.

Theorem 3. *For a given prime* p *let* $2 = q_1 < q_2 < \cdots < q_{\omega(p-1)}$ *be the prime divisors of* $p-1$*. For any integer* r *in the range* $1 \leqslant r \leqslant \omega(p-1)$ *we have*

$$g(p) \leqslant p^{1/4-\alpha(p,r)}$$

with

$$\alpha(p,r) = \beta(r,\Phi) - C''\left(\frac{(\log(2r))^{1/2}}{(\log p)^{1/2}} + \sum_{j>r}\frac{j^3\log\log q_j}{\log q_j}\right)$$

$$\text{and } \Phi := \frac{q_1\cdots q_r}{\phi(q_1\cdots q_r)}$$

where $\beta(r,\Phi)$ *is defined in Theorem 2 and* C'' *is a positive absolute constant.*

We first prove Theorem 2 in Section 2 by refining the argument from [8]. In Section 3 we deduce Theorem 3 from Theorem 2 using an argument which is optimized for large prime factors of $p-1$. Section 4 is devoted to estimating the number of primes $\leqslant x$ failing (i) or (ii) in Theorem 1, and finally Theorem 1 is proved in Section 5.

1.1. Notation. With $p \geqslant 3$ fixed, we denote the distinct prime factors of $p-1$ as $q_1, \ldots, q_{\omega(p-1)}$, where $q_1 = 2 < q_2 < \cdots < q_{\omega(p-1)}$. For prime $q|(p-1)$, let $\mathcal{R}_q$ be the set of q-th power residues modulo p, and let $\mathcal{N}_q$ denote the set of q-th power nonresidues modulo p, both considered as subsets of $\{1,2,\ldots,p-1\}$. We let $P^+(n)$ be the largest prime factor of a positive integer n, with $P^+(1)$ defined to be zero, and $P^-(n)$ the smallest prime factor of n, with $P^-(1) = \infty$. We denote $\phi(n)$ for Euler's totient function, $\omega(n)$ for the number of distinct prime factors of n, and $\omega(n,a,b)$ for the number of distinct prime factors of n in the interval $(a,b]$. We denote $\mathbb{P}$ for probability and $\mathbb{E}$ for probabilistic expectation. We also use the notation $\log_k x$ for the k-th iterate of the logarithm and $\exp_k x$ for the k-th iterate of the exponential function. Constants implied by the big-O and $\ll$-symbols are absolute, that is, they are independent of any parameter unless explicitly stated, e.g. with a subscript to the O or $\ll$ symbol.

2. Proof of Theorem 2

We follow the argument from [8] with some technical modifications. First of all, we need to find explicit dependence on δ in the cornerstone Lemma 4.1 of [8]. In [8], the dependence on δ of the big-O bound is unspecified, but it can be shown to be $O(1/\delta)$. Such a bound, however, is fatal to our argument and we need to refine the proof of Lemma 4.1 in [8] to show a better dependence on δ.

Lemma 2.1. *Fix $\delta \in (0, \frac{1}{100}]$ and let $c = \frac{1}{\log 2} + \delta$. If x is large enough, and t is a large enough integer with $t \leqslant (\log x)^{1/c}$ then all but $O(xt^{-\delta^2/210})$ integers $n \leqslant x$ have t divisors $d_1 < d_2 < \cdots < d_t$ for which $d_{j+1}/d_j > x^{1/t^c}$ for all $1 \leqslant j \leqslant t-1$.*

Proof. Let $\varepsilon = \delta/2$, so that $c = \frac{1}{\log 2} + 2\varepsilon$. We may assume that $\varepsilon \geqslant (100 \log t)^{-1/2}$, since t is "large enough" by the hypothesis. Let $\alpha = \frac{1}{\log 2} + \varepsilon$. We write each $n \leqslant x$ in the form $n = abd$, where

$$P^-(d) > x^{1/\log t}, \quad P^+(a) \leqslant x^{1/(t^\alpha \log t)},$$

and all prime divisors of b lie in

$$(x^{1/(t^\alpha \log t)}, x^{1/\log t}].$$

Let $J = \lceil \alpha/\varepsilon \rceil$, and define

$$\begin{aligned} \alpha_j &= j\varepsilon \quad (0 \leqslant j \leqslant J-1), \quad \alpha_J = \alpha, \\ A_j &= x^{1/(t^{\alpha_j} \log t)} \quad (0 \leqslant j \leqslant J), \\ \gamma_j &= \frac{J-j}{3J} \quad (1 \leqslant j \leqslant J-1), \quad \gamma_0 = 1. \end{aligned}$$

Now we consider the set S of $n \leqslant x$ which obey the conditions

(i′) $d > 1$ and b is squarefree;

(ii′) $\omega(b) \geqslant k' := \lceil \frac{\log 2t}{\log 2} \rceil$;

(iii′) for each $j = 1, \ldots, J-1$, the number of primes from $(A_j, x^{1/\log t}]$ dividing n is at least $k_j = (1-\gamma_j)\alpha_j \log t$.

We begin by showing that all but a small set of integers $n \leqslant x$ belong to S, by bounding the number of exceptions to (i′), (ii′) and (iii′), respectively.

(i′). If $d = 1$ then n is $x^{1/\log t}$-smooth. If b is not squarefree then n is divisible by p^2 for some prime $p > x^{1/(t^\alpha \log t)}$. Therefore, by Corollary 1.3 in [11], there are at most

$$O\Big(\frac{x}{t}\Big) + \sum_{p > x^{1/(t^\alpha \log t)}} \frac{x}{p^2} \ll \frac{x}{t} + \frac{x}{x^{1/(t^\alpha \log t)}}$$

integers $n \leqslant x$ violating (i′). We have $t < x^{1/(t^\alpha \log t)}$, since $t^\alpha (\log t)^2 < t^c \leqslant \log x$ by the hypothesis, and so the number of $n \leqslant x$ violating (i′) is $\ll x/t$.

(ii′). For each $k < k'$, the number of $n \leqslant x$ with $\omega(b) = k$ is $O(xe^{-E}E^k/k!)$, where

$$E := \sum_{x^{1/(t^\alpha \log t)} < p \leqslant x^{1/\log t}} \frac{1}{p}.$$

This is a consequence of a theorem of Halász [9] (see also Theorems 08 and 09 of [10]). Mertens theorems imply that $E = \alpha \log t + O(1)$. Therefore, the number of $n \leqslant x$ for which (ii′) fails is

$$\ll \sum_{k<k'} xe^{-E}\frac{E^k}{k!} \ll xt^{-\alpha} \sum_{k<k'} \frac{(\alpha \log t)^k}{k!} \leqslant x(t^{-\alpha})^{Q(\kappa)},$$

where $Q(z) = z \log z - z + 1$ and

$$\kappa = \frac{k'}{\alpha \log t} = \frac{1}{\alpha \log 2} + O\left(\frac{1}{\log t}\right) = \frac{1}{1+\varepsilon \log 2} + O\left(\frac{1}{\log t}\right) \leqslant 1 - \frac{2}{3}\varepsilon$$

since t is sufficiently large in terms of ε (recall that $\varepsilon \geqslant (100 \log t)^{-1/2}$). Since $Q(1+\lambda) \geqslant \frac{1}{3}\lambda^2$ for $|\lambda| \leqslant \frac{1}{2}$, we see that the number of $n \leqslant x$ violating (ii′) is at most

$$\ll xt^{-\frac{1}{3}\alpha(1-\kappa)^2} \ll xt^{-\frac{1}{5}\varepsilon^2}.$$

(iii′). Now fix some j with $1 \leqslant j \leqslant J-1$ and let U_j be the set of $n \leqslant x$ which have fewer than k_j prime divisors in $(A_j, x^{1/\log t}]$. Arguing similarly, we define

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

and then (since $k_j \leqslant \alpha_j \log t$)

$$\begin{aligned}|U_j| &\ll \sum_{k<k_j} xe^{-E_j}\frac{E_j^k}{k!} \ll xt^{-\alpha_j} \sum_{k<k_j} \frac{(\alpha_j \log t + O(1))^k}{k!} \\ &\ll xt^{-\alpha_j} \sum_{k<k_j} \frac{(\alpha_j \log t)^k}{k!} \ll x(t^{-\alpha_j})^{Q(1-\gamma_j)} \ll xt^{-\alpha_j\gamma_j^2/3} = xt^{-j\varepsilon\gamma_j^2/3}.\end{aligned}$$

Recalling the definitions of γ_j and J, we obtain that the number of $n \leqslant x$ for which (iii′) fails is at most

$$x \sum_{j=1}^{J-1} t^{-(j\varepsilon)((J-j)/J)^2/27} \leqslant x \sum_{j=1}^{J-1} t^{-(J-j)j^2\varepsilon^3/(27\alpha^2)}; \tag{2.1}$$

here we used that $J \geqslant \alpha/\varepsilon$ and made the substitution $j \mapsto J - j$. The summands on the right side of (2.1) with $j \leqslant J/4$ have total at most

$$\sum_{1 \leqslant j \leqslant J/4} t^{-j^2\varepsilon^2/(36\alpha)} \leqslant \frac{t^{-\varepsilon^2/(36\alpha)}}{1 - t^{-\varepsilon^2/(36\alpha)}} \leqslant 2t^{-\varepsilon^2/(36\alpha)}.$$

The summand on the right side of (2.1) with $j > J/4$ have total at most

$$\sum_{J/4 < j \leqslant J-1} t^{-(J-j)\varepsilon/432} \ll t^{-\varepsilon/432}.$$

By combining the above estimates and using the lower bound for ε, we see that all but

$$\ll x\Big(t^{-\frac{1}{5}\varepsilon^2} + t^{-\varepsilon^2/(36\alpha)} + t^{-\varepsilon/432}\Big) \ll xt^{-\varepsilon^2/52.5} = xt^{-\delta^2/210} \tag{2.2}$$

numbers $n \leqslant x$ belong to S.

Now let S' be the set of $n \in S$ for which b does not have t divisors $d_1 < d_2 < \cdots < d_t$ satisfying $d_{j+1}/d_j > x^{1/t^c}$ for $1 \leqslant j \leqslant t-1$. Since $d > 1$ for such n, given such a bad value of b, using a standard sieve bound for counts of integers without small prime factors ([20], Theorem III.6.4), the number of choices for the pair (a, d) is bounded above by (here $P := x^{1/(t^\alpha \log t)}$)

$$\begin{aligned}\sum_{P^+(a) \leqslant P} \#\{1 < d \leqslant x/ab : P^-(d) > x^{1/\log t}\} &\ll \sum_{P^+(a) \leqslant P} \frac{x/ab}{\log(x^{1/\log t})} \\ &\ll \frac{x \log t}{b \log x} \sum_{P^+(a) \leqslant P} \frac{1}{a} \ll \frac{x}{bt^\alpha}.\end{aligned}$$

Hence,

$$|S'| \ll \sum_{\text{bad } b} \frac{x}{bt^\alpha}. \tag{2.3}$$

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

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

Recall that for bad b we have $\tau(b) \geqslant 2t$ by (ii′). By the argument leading to (4.2) of [8],

$$\sum_{\text{bad } b} \frac{1}{b} \leqslant \sum_{\text{all } b} \frac{2W^*(b;\sigma)t}{b\tau(b)^2}, \tag{2.4}$$

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

In the sum on the right side of (2.4), 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 $Y, Z \subseteq \{1, \dots, k\}$ with $Y \neq Z$ and

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

Fix Y and Z, and let I be the maximum element of the symmetric difference $(Y \cup Z) \setminus (Y \cap Z)$. We fix I and further partition the solutions according to the condition $A_j < p_I \leqslant A_{j-1}$, where $1 \leqslant j \leqslant J$. Fix the value of j. By the argument leading to [8, (4.4)],

$$\sum_{x^{1/t^{\alpha}\log t} < p_1 < \cdots < p_k \leqslant x^{1/\log t}} \frac{1}{p_1 \dots p_k} \ll \frac{t^{\alpha_j - c}(\log t)(\alpha \log t + O(1))^{k-1}}{(k-1)!}.$$

Since $n \in S$, $I \leqslant k - k_{j-1}$; to cover the $j = 1$ case we define $k_0 = 0$. Therefore, by [8, (4.5)], the number $N(I, j)$ of choices for the pair Y, Z for fixed I and j satisfies

$$N(I, j) \leqslant 4^I 2^{k-I} \leqslant 4^k 2^{-k_{j-1}} \leqslant 4^k t^{-(1-\gamma_{j-1})\alpha_{j-1} \log 2}.$$

The above bounds, the bound $\alpha_j \leqslant \alpha_{j-1} + \varepsilon$ and the fact that $\log t \ll t^{0.001\varepsilon}$ imply

$$\begin{aligned} \sum_b \frac{W^*(b;\sigma)t}{b\tau(b)^2} &\ll \sum_{j=1}^{J} t^{1+\alpha_j - c - (1-\gamma_{j-1})\alpha_{j-1}\ \log 2 + 0.001\varepsilon} \sum_k \frac{(\alpha \log t + O(1))^{k-1}}{(k-1)!} \\ &\ll t^{1+\alpha-c+0.7\varepsilon} \sum_{j=1}^{J} t^{(1-\log 2+\gamma_{j-1}\log 2)\alpha_j}. \end{aligned} \tag{2.5}$$

Now since $\alpha_j = \alpha_{J-1} - (J-j-1)\varepsilon \leqslant \alpha - (J-j-1)\varepsilon$, we have

$$\alpha_j(1 - \log 2) \leqslant \frac{1}{\log 2} - 1 - (J-j-2)(1-\log 2)\varepsilon.$$

Also, $\alpha_j \gamma_{j-1} \leqslant \frac{1}{3}(J-j+1)\varepsilon$, and hence, recalling that $c = \frac{1}{\log 2} + 2\varepsilon$,

$$(1 - \log 2 + \gamma_{j-1}\log 2)\alpha_j \leqslant c - 1 - 2\varepsilon - 0.07(J-j)\varepsilon + 0.85\varepsilon.$$

Summing over j and recalling that $t^{\varepsilon} \geqslant \exp\{\frac{1}{10}\sqrt{\log t}\}$, we get from (2.5) that

$$\sum_b \frac{W^*(b;\sigma)t}{b\tau(b)^2} \ll t^{\alpha - 0.4\varepsilon}.$$

Thus, by (2.3) and (2.4), we have

$$|S'| \ll x t^{-0.4\varepsilon} = x t^{-0.2\delta}.$$

Recalling (2.2), we see that there are $O(xt^{-\delta^2/210})$ numbers $n \leqslant x$ for which b does have t well-spaced divisors, and the claim follows. $\square$

Next, we quote the following combinatorial lemma from [8].

Lemma 2.2 ([8, Corollary 3.4])**.** *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 $d_1 < \cdots < d_t$ 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 $1 \leqslant i < j \leqslant t$ and the number $n' = nd_i/d_j$ is also a simultaneous $p_1, \dots, p_r$-th power nonresidue modulo p.

The next statement follows from [8, Lemma 2.2 and (5.1)], and it is a consequence of Burgess' bound for character sums.

Lemma 2.3. *Let p be a prime number and let $p_1, \dots, p_r$ be distinct prime factors of $p-1$. Let also H and m be arbitrary positive integers. Then the number of integers $n \leqslant H$ which are in $\mathcal{N}_{p_1} \cap \cdots \cap \mathcal{N}_{p_r}$ is at least*

$$\frac{H}{8} \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) - (5r)^{C'''} H^{1-1/m} p^{(m+1)/4m^2} (\log p)^{1/m},$$

where $C''' > 0$ is an absolute constant.

Now we are ready to prove Theorem 2. Let p be large enough. We choose

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

and

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

By an identical calculation to that in Section 5 of [8], the subtracted term in Lemma 2.3 is at most $H(5r)^{-2}$. Let

$$\Phi := \frac{p_1 \cdots p_r}{\phi(p_1 \cdots p_r)} = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)^{-1}.$$

Crudely,

$$\Phi^{-1} \geqslant \prod_{k=2}^{r+1} \left(1 - \frac{1}{k}\right) = \frac{1}{r+1}, \tag{2.6}$$

it follows from Lemma 2.3 that the set $\mathcal{K}$ of $n \in [1, H]$ which are in $\mathcal{N}_{p_1} \cap \cdots \cap \mathcal{N}_{p_r}$ satisfies

$$|\mathcal{K}| \geqslant 0.04 H \Phi^{-1}.$$

Let $r < 0.6 \log_2 p$. We apply Lemma 2.1 with $x = H$, $c = 1/\log 2 + \delta$ with $\delta \in (0, \frac{1}{100}]$ chosen later, and $t = \max(t_0, \lfloor 2^r \Phi \rfloor + 1)$ for some large enough constant t_0. Since $r \leqslant 0.6\log_2 x$, $t \leqslant \Phi(\log x)^{0.6}+1 \leqslant (\log x)^{1/c}$ if x is large enough. Then, for some absolute $C>0$, all but

$$CHt^{-\delta^2/210}$$

integers $n \leqslant H$ have t well-spaced divisors $d_1 < \cdots < d_t$ with $d_{j+1}/d_j > x^{t^{-c}}$ for each $j<t$. We take

$$\delta = \min\left(\frac{1}{100}, \frac{c_3\max(1,\log\Phi)^{1/2}}{r^{1/2}}\right),$$

with c_3 chosen large enough. We claim that

$$CHt^{-\delta^2/210} < 0.02H\Phi^{-1} \tag{2.7}$$

if t_0 is large enough. Indeed, if $\delta = \frac{1}{100}$, then by (2.6), r is bounded, and (2.7) holds for large t_0. If $\delta < \frac{1}{100}$ then

$$CHt^{-\delta^2/210} \leqslant CH\exp\left\{-\frac{c_3^2}{210}(\log 2)\max(1,\log\Phi)\right\},$$

and so (2.7) holds for large enough c_3.

We thus see that there is a simultaneous $p_1,\dots,p_r$-th power nonresidue $n \leqslant H$ which has t well-spaced divisors in the sense of Lemma 2.1. By Lemma 2.2, for some $1 \leqslant i < j \leqslant t$ the number nd_i/d_j is also a simultaneous $p_1,\dots,p_r$-th power nonresidue, and

$$\frac{nd_i}{d_j} \leqslant H^{1-t^{-c}} \leqslant Hp^{-t^{-c}/4}.$$

Since $c = 1/\log 2 + \delta$, we get

$$\begin{aligned} t^{-c}/4 &= \exp\{-cr\log 2 + O(1+\log\Phi)\} \\ &\geqslant \exp\Big\{-(r + c_3'(r\max(1,\log\Phi))^{1/2})\Big\}, \end{aligned}$$

for a sufficiently large constant c_3', upon recalling (2.6). The claim follows.

It remains to note that for $r \geqslant 0.6\log_2 p$ the fact that $\mathcal{K}$ is nonempty implies that the least simultaneous $p_1,\dots,p_r$-th power nonresidue modulo p is $\leqslant H$, and this is good enough since $\beta(r,\Phi) \leqslant (\log p)^{-0.6}$. This concludes the proof of Theorem 2.

3. Proof of Theorem 3

The following lemma is based on the work in Section 3 of [18]. Jacobsthal's function $J(m)$ is defined to be the smallest integer J such that any set of J consecutive integers contains one which is coprime to m.

Lemma 3.1. *Let p be a prime and let $Q_0, Q_1, \dots, Q_k$ be disjoint subsets of the prime factors of $p-1$. For $i = 0, 1, \dots, k$, let $m_i = \prod_{q \in Q_i} q$ and suppose that n_i is an integer such that*

(a) *$n_i \in \mathcal{N}_q$ for all primes $q \in Q_i$;*
(b) *$n_i \in \mathcal{R}_q$ for all primes $q \in Q_0 \cup \dots \cup Q_{i-1}$.*

Then there exist integers a_i with $0 \leqslant a_i < J(m_i)$, $i = 1, \dots, k$, such that

$$n_0 n_1^{a_1} n_2^{a_2} \dots n_k^{a_k} \in \mathcal{N}_q \quad \text{for all primes } q \in Q_0 \cup \dots \cup Q_k.$$

Proof. We induct on $k \geqslant 0$. The claim is trivial for $k = 0$. Now fix k and suppose the claim is true when k is replaced by $k-1$. Let $Q_0, \dots, Q_k, n_0, \dots, n_k$ be as in the lemma, in particular satisfying (a) and (b). By the induction hypothesis, there are non-negative integers $a_1, \dots, a_{k-1}$ with $a_i < J(m_i)$ for all i, and so that $N := n_0 n_1^{a_1} \dots n_{k-1}^{a_{k-1}}$ is in $\mathcal{N}_q$ for all primes $q \in Q_0 \cup \dots \cup Q_{k-1}$. By (b), $n_k \in \mathcal{R}_q$ for all primes $q \in Q_0 \cup \dots \cup Q_{k-1}$. Therefore for any $a \geqslant 0$, $N n_k^a \in \mathcal{N}_q$ for all primes $q \in Q_0 \cup \dots \cup Q_{k-1}$. It remains to find a such that $N n_k^a \in \mathcal{N}_q$ for all primes $q \in Q_k$. Let g be a primitive root mod p and $N \equiv g^u \pmod{p}$, $n_k \equiv g^v \pmod{p}$; then

$$N n_k^a \equiv g^{u+av} \pmod{p}.$$

Since $n_k \in \mathcal{N}_q$ for all primes $q \in Q_k$, we have $(v, m_k) = 1$. Let w be an integer for which $wv \equiv 1 \pmod{m_k}$. By the definition of Jacobsthal's function, there exists an integer a_k in the range $0 \leqslant a_k \leqslant J(m_k) - 1$ such that $(uw + a_k, m_k) = 1$, and so $(u + a_k v, m_k) = 1$ as $u + a_k v \equiv v(uw + a_k) \pmod{m_k}$. But then

$$N n_k^{a_k} \equiv g^{u+a_k v} \pmod{p},$$

and thus $N n_k^{a_k} \in \mathcal{N}_q$ for all primes $q \in Q_k$, as desired. □

The next incorporates an idea dating back to work of Vinogradov [22].

Lemma 3.2. *Let p be a large prime and $M \geqslant 3$ be a divisor of $p-1$, and suppose that every integer less than Y is an M-th power residue mod p. Then*

$$Y \leqslant p^{O\left(\frac{\log\log M}{\log M}\right)}.$$

Proof. There are exactly $\frac{p-1}{M}$ numbers up to $p-1$ which are M-th power residues. On the other hand, the assumption implies that any number $n \leqslant p-1$ with $P^+(n) \leqslant Y-1$ is a M-th power residue modulo p. By standard counts of "smooth numbers" (e.g., [11, Theorem 1.2]), the number of such n is at least $(p-1)e^{-O(u \log u)}$, where $u = \frac{\log(p-1)}{\log(Y-1)}$, uniformly in $p \geqslant 3$ and $1 < Y < p$. Thus, $\log M \ll u \log u$, so $u \gg \frac{\log M}{\log\log M}$ and the claim follows. □

Proof of Theorem 3. If $r = \omega(p-1)$ then the claim follows immediately from Theorem 2. Now assume that $1 \leqslant r \leqslant \omega(p-1)-1$. For each prime $q|(p-1)$, let t_q be the least element of $\mathcal{N}_q$, and write the set $\{t_q : q|(p-1)\}$ as $\{s_0, \dots, s_\ell\}$, where $s_0 > s_1 > \cdots > s_\ell$ and let

$$\mathcal{V}_i = \{q|(p-1) : t_q = s_i\} \qquad (0 \leqslant i \leqslant \ell).$$

Since s_i is the least element of $\mathcal{N}_q$ for all $q \in \mathcal{V}_i$, we see that if $j > i$ then $s_j \in \mathcal{R}_q$ for all $q \in \mathcal{V}_i$.

Consider an integer r satisfying $1 \leqslant r \leqslant \omega(p-1)-1$, and define h as the smallest integer satisfying $r < |\mathcal{V}_0| + \cdots + |\mathcal{V}_h|$. Thus, if $h \geqslant 1$ then $r \geqslant |\mathcal{V}_0| + \cdots + |\mathcal{V}_{h-1}|$. We apply Lemma 3.1 with $Q_0 = \mathcal{V}_0 \cup \cdots \cup \mathcal{V}_{h-1}$, $Q_i = \mathcal{V}_{h+i-1}$ for $1 \leqslant i \leqslant \ell-h+1$, $n_i = s_{i+h-1}$ for $1 \leqslant i \leqslant \ell-h+1$, and with n_0 the least integer in $\mathcal{N}_q$ for all $q \in Q_0$. If $h \geqslant 1$ the Q_0 is nonempty and

$$n_0 \geqslant s_0 \geqslant s_{h-1} > s_h = n_1 > \cdots > s_\ell = n_{\ell-h+1},$$

thus the hypotheses of Lemma 3.1 hold. If $h = 0$, then Q_0 is empty and we take $n_0 = 1$ and the hypotheses of Lemma 3.1 also hold. Consequently, writing $m_i = \prod_{q \in Q_i} q$ for each i,

$$g(p) \leqslant n_0 \prod_{i=1}^{\ell-h+1} n_i^{J(m_i)-1}. \tag{3.1}$$

We apply Theorem 2 with r replaced by $r' = |Q_0|$, $\{p_1, \dots, p_{r'}\} = Q_0$ and Φ replaced by $\Phi' = q_1 \cdots q_{r'}/\phi(q_1 \cdots q_{r'})$. Since $r' \leqslant r$ and $\Phi' \leqslant \Phi = q_1 \cdots q_r/\phi(q_1 \cdots q_r)$,

$$\begin{aligned} n_0 &\leqslant p^{1/4-\beta(r',\Phi')} e^{C(\log p)^{1/2}(\log(2r'))^{1/2}} \\ &\leqslant p^{1/4-\beta(r,\Phi)} e^{C(\log p)^{1/2}(\log(2r))^{1/2}}. \end{aligned} \tag{3.2}$$

As in Lemma 3.1, let

$$M_i = m_0 \cdots m_i \ \ (0 \leqslant i \leqslant \ell-h+1).$$

For each $i \geqslant 1$, any $n < n_i$ is a M_i-th power residue modulo p, so by Lemma 3.2,

$$n_i \leqslant p^{O\left(\frac{\log\log M_i}{\log M_i}\right)}. \tag{3.3}$$

Here we also used that $\omega(M_i) > r$ so $M_i \geqslant 6$. By Iwaniec's theorem [14],

$$J(m) \ll (\omega(m)\log(\omega(m)+1))^2 \ll (\omega(m))^3$$

for all positive integers m. Together with (3.1), (3.2) and (3.3), we have

$$\begin{aligned} &g(p) \leqslant p^{\theta(p)}, \quad \text{where} \\ &\theta(p) = \frac{1}{4} - \beta(r,\Phi) + O\left(\frac{(\log(2r))^{1/2}}{(\log p)^{1/2}} + \sum_{i=1}^{\ell-h+1} \frac{(\omega(m_i))^3 \log\log M_i}{\log M_i}\right). \end{aligned} \tag{3.4}$$

Recall that $\omega(M_1) > r$. Thus, for each i we have

$$\frac{\omega(m_i)^3 \log\log M_i}{\log M_i} \ll \sum_{\max(r,\omega(M_{i-1}))<j\leqslant\omega(M_i)} \frac{j^3 \log\log q_j}{\log q_j}.$$

Inserting this into (3.4) completes the proof of Theorem 3. □

4. Estimate for the number of exceptional primes

In this section we bound the number of primes below x failing either condition (i) or condition (ii) in Theorem 1.

4.1. Large values of $1/q_1 + \cdots + 1/q_r$.

Lemma 4.1. *Fix $\xi > 0$. Uniformly for real R with $3 \leqslant R \leqslant \log_2 x$, the number of primes $p \leqslant x$ such that $\sum_{i\leqslant R} 1/q_i \geqslant \xi \log_2 R$ is $O_\xi(\pi(x)/\exp_2\{(\log R)^{\xi/6}\})$.*

Proof. We may assume that R is sufficiently large as a function of ξ. Suppose that $p \leqslant x$ and $1/q_1 + \cdots + 1/q_R \geqslant \xi \log_2 R$. Let $\mathcal{J}$ be the set of integers j with $(\log R)^{\xi/3} < 2^j \leqslant \log R$, and for $j \in \mathcal{J}$ let I_j denote the interval $(\exp(2^j), \exp(2^{j+1})]$. Note that $|\mathcal{J}| \leqslant (1/\log 2)\log_2 R + O(1)$. For some $j \in \mathcal{J}$, at least $t_j := \lceil(\xi/3)\exp(2^j)\rceil$ of the q_i lie in I_j, for otherwise

$$\begin{aligned}\sum_{i\leqslant R}\frac{1}{q_i} &\leqslant \sum_{\log q_i \leqslant 2(\log R)^{\xi/3}} \frac{1}{q_i} + \sum_{\substack{i\leqslant R\\ q_i>R}} \frac{1}{q_i} + \sum_{j\in\mathcal{J}}\sum_{i:q_i\in I_j}\frac{1}{q_i}\\ &\leqslant \frac{\xi\log_2 R}{3} + O(1) + \frac{\xi}{3}|\mathcal{J}| < \xi \log_2 R\end{aligned}$$

if R is large enough. For $j \in \mathcal{J}$, $\exp\{R\cdot 2^{j+1}\} \leqslant R^{2R} \leqslant \exp\{(\log_2 x)^2\}$, and also the sum of $\frac{1}{p'-1}$ over all primes $p' \in I_j$ is $\leqslant 1$ for large enough R. Thus by the Brun–Titchmarsh theorem, the number of primes $p \leqslant x$ with at least t_j of the q_i in I_j is at most

$$\begin{aligned}&\ll \sum_{k=t_j}^{\lfloor R\rfloor} \sum_{\substack{p_1<\cdots<p_k\\ p_i\in I_j\ \forall i}} \frac{\pi(x)}{(p_1-1)\cdots(p_k-1)}\\ &\leqslant \pi(x)\sum_{k=t_j}^{\lfloor R\rfloor}\frac{1}{k!}\left(\sum_{p'\in I_j}\frac{1}{p'-1}\right)^k \ll \frac{\pi(x)}{t_j!}.\end{aligned}$$

As $t_j \geqslant \exp_2(j/2)$ for large j, the total number of such primes is $\ll \pi(x)/\exp_3(j_0/2)$, with $j_0 = \min\mathcal{J}$. Since $j_0 \geqslant (\xi/3)\log_2 R$, the lemma follows. □

4.2. Applying the law of the iterated logarithm for shifted primes.

Theorem 4. *Fix $\varepsilon \in (0,1]$. Uniformly for $1 \leqslant \eta \leqslant (\frac{1}{2}+\varepsilon)^{-1}\log_4 x$, there are at most $O_\varepsilon\big(\pi(x)/\exp_2(0.8\eta\varepsilon)+\pi(x)/\exp_2(\eta/4)\big)$ primes $p \leqslant x$ for which there is no integer r with $1 \leqslant r \leqslant \exp_2\big((\frac{1}{2}+\varepsilon)\eta\big)$ and*

$$\sum_{j>r} \frac{j^3 \log_2 q_j}{\log q_j} \leqslant e^{-r-\sqrt{\eta r}}.$$

The same proof gives a similar statement with the exponent 3 replaced by any fixed constant, but we do not need this here.

We need standard bounds on the tails of the Poisson distribution, e.g. Norton [17, Lemmas (4.1) and (4.6)].

Lemma 4.2. *Let Y be Poisson with parameter $\lambda \geqslant 1$ and $1 \leqslant \alpha \leqslant \lambda^{1/6}$. Then*

(a) $\mathbb{P}(Y \leqslant \lambda - \alpha\sqrt{\lambda}) \gg \alpha^{-1}e^{-\frac{1}{2}\alpha^2}$;
(b) $\mathbb{P}(Y \geqslant \lambda + \alpha\sqrt{\lambda}) \ll e^{-\frac{1}{2}\alpha^2}$.

Proof of Theorem 4. We first relate the quantity in question to a purely probabilistic calculation using [7], and then use ideas from the law of the iterated logarithm in probability theory to complete the proof. WLOG suppose $\eta \geqslant \eta_0(\varepsilon)$, a sufficiently large constant depending only on ε. For each integer j let $t_j = \exp(e^j)$, and let

$$D = \lfloor \eta/2 \rfloor + 1, \quad J = \Big\lfloor \log_2(x^{1/\log_2 x}) \Big\rfloor = \lfloor \log_2 x - \log_3 x \rfloor.$$

For a randomly selected prime $p \leqslant x$, let $W_j = \omega(p-1, t_j, t_{j+1})$ and $W_{a,b} = W_a + \cdots + W_{b-1} = \omega(p-1, t_a, t_b)$, where j, a, b are non-negative integers. It is expected by the Kubilius model, and proved in [7], that W_j is approximately Poisson with parameter λ_j, where

$$\lambda_j = \sum_{t_j < q \leqslant t_{j+1}} \frac{1}{q-1}.$$

The prime number theorem with strong error term (cf. Theorem 12.2 in [13]) gives

$$\lambda_j = 1 + O\big(\exp\{-e^{j/2}\}\big). \tag{4.1}$$

For each $D \leqslant j \leqslant J$, let Z_j be a Poisson random variable with parameter λ_j, with $Z_D, \ldots, Z_J$ mutually independent, and let $Y_D, \ldots, Y_J$ be mutually independent Poisson random variables each with parameter 1. Then we expect that $(W_D, \ldots, W_J)$ has distribution close to $(Y_D, \ldots, Y_J)$. It is convenient to describe the quality of the approximation using the total variation distance $d_{TV}(X,Y)$ between two random variables living on the same discrete space Ω:

$$d_{TV}(X,Y) := \sup_{A\subset\Omega} \big|\mathbb{P}(X\in A) - \mathbb{P}(Y\in A)\big|.$$

Since $t_{J+1} \leqslant x^{e/\log_2 x}$ and $t_D < \log_2 x$, applying Theorem 2 of [7] with $\alpha = 1/2$ and $u = (1/e)\log_2 x$, together with (4.1), gives

$$d_{TV}\big((W_D,\dots,W_J),(Z_D,\dots,Z_J)\big) \ll \frac{1}{t_D} + \frac{1}{\log x} + u^{-\alpha u} \ll \exp\{-e^{\eta/2}\}.$$

Using (4.1), an easy calculation, e.g. [7, Lemmas 2.2 and 2.3], gives

$$d_{TV}\big((Y_D,\dots,Y_J),(Z_D,\dots,Z_J)\big) \ll \sum_{j\geqslant D} \exp\{-e^{j/2}\} \ll \exp\{-e^{\eta/4}\}.$$

Therefore, by the triangle inequality,

$$d_{TV}\big((W_D,\dots,W_J),(Y_D,\dots,Y_J)\big) \ll \exp\{-e^{\eta/4}\}. \tag{4.2}$$

For integers a,b with $D\leqslant a<b\leqslant J$ let $Y_{a,b} = Y_a+\dots+Y_{b-1}$, so that $Y_{a,b}$ is a Poisson variable with parameter $b-a$, and for disjoint intervals $[a_1,b_1-1],\dots,[a_r,b_r-1]$ the variables $Y_{a_1,b_1},\dots,Y_{a_r,b_r}$ are mutually independent. Let

$$K_1 = \big\lfloor e^{\eta/2}\big\rfloor, \qquad K_2 = \lfloor (2\eta)^{-1} e^{(\frac12+\varepsilon)\eta}\rfloor.$$

In particular, since $\varepsilon\leqslant 1$ and $(\frac12+\varepsilon)\eta \leqslant \log_4 x$, we have

$$K_2! \leqslant K_2^{K_2} \leqslant \exp\big\{(3/4)\cdot e^{(\frac12+\varepsilon)\eta}\big\} \leqslant (\log_2 x)^{3/4} \leqslant J.$$

For $K_1\leqslant k\leqslant K_2-1$ consider the events

$$\begin{aligned}
E_k &: \ W_{k!,(k+1)!} \leqslant k\cdot k! - (1+\varepsilon/10)\sqrt{\eta k\cdot k!},\\
\mathcal{E}_k &: \ Y_{k!,(k+1)!} \leqslant k\cdot k! - (1+\varepsilon/10)\sqrt{\eta k\cdot k!},\\
F_k &: \ W_{D,k!} \leqslant k! - D + e^{\eta/6}\sqrt{\eta(k!-D)},\\
\mathcal{F}_k &: \ Y_{D,k!} \leqslant k! - D + e^{\eta/6}\sqrt{\eta(k!-D)}.
\end{aligned}$$

By (4.2), the events E_k and F_k corresponding to random primes $p\leqslant x$ are close, respectively, to $\mathcal{E}_k$ and $\mathcal{F}_k$.

Consider four more events:

$$\begin{aligned}
A &: \ \text{for some } k\in[K_1,K_2-1], E_k\wedge F_k,\\
\mathcal{A} &: \ \text{for some } k\in[K_1,K_2-1], \mathcal{E}_k\wedge \mathcal{F}_k,\\
B &: \ W_j\leqslant j \text{ for all } j\geqslant K_1!,\\
\mathcal{B} &: \ Y_j\leqslant j \text{ for all } j\geqslant K_1!.
\end{aligned}$$

By (4.2),

$$\mathbb{P}(A\wedge B) = \mathbb{P}(\mathcal{A}\wedge\mathcal{B}) + O\big(\exp\{-e^{\eta/4}\}\big). \tag{4.3}$$

We will show later that $\mathcal{A} \wedge \mathcal{B}$ holds with high probability, and hence so does $A \wedge B$.

Assume for now that A and B both hold. Then, for some k in the range $K_1 \leqslant k \leqslant K_2 - 1$, we have E_k and F_k. Then

$$\begin{aligned} W_{D,(k+1)!} &\leqslant k \cdot k! - (1+\varepsilon/10)\sqrt{\eta k \cdot k!} + k! + e^{\eta/6}\sqrt{\eta k!} \\ &= (k+1)! - \sqrt{\eta(k+1)!}\left((1+\varepsilon/10)\sqrt{\frac{k}{k+1}} - e^{\eta/6}(k+1)^{-1/2}\right) \\ &\leqslant (k+1)! - (1+\varepsilon/20)\sqrt{\eta(k+1)!} \end{aligned}$$

as long as $\eta_0(\varepsilon)$ is large enough, and recalling that $k+1 \geqslant e^{\eta/2}$. Since

$$\omega(p-1, 1, t_D) \leqslant t_D \leqslant \exp_2(\eta/2+1) < (\varepsilon/100)\sqrt{\eta(k+1)!},$$

we have

$$r := \omega(p-1, t_{(k+1)!}) \leqslant (k+1)! - (1+\varepsilon/30)\sqrt{\eta(k+1)!}. \tag{4.4}$$

In particular,

$$r \leqslant K_2! \leqslant \exp\Big\{(3/4)e^{(\frac{1}{2}+\varepsilon)\eta}\Big\} \leqslant \exp_2\Big\{(\tfrac{1}{2}+\varepsilon)\eta\Big\}. \tag{4.5}$$

Then

$$\sum_{\substack{i>r \\ q_i \leqslant t_{J+1}}} \frac{i^3 \log_2 q_i}{\log q_i} = \sum_{j=(k+1)!}^{J} \sum_{t_j < q_i \leqslant t_{j+1}} \frac{i^3 \log_2 q_i}{\log q_i}.$$

For $j \geqslant (k+1)!$ and $t_j < q_i \leqslant t_{j+1}$, event B implies that

$$i \leqslant r + \sum_{\ell=(k+1)!}^{j} \ell \leqslant \sum_{\ell=1}^{j} \ell \leqslant j^2.$$

Since $\frac{\log_2 z}{\log z}$ is decreasing for $z \geqslant e^e = t_1$, $\frac{\log_2 q_i}{\log q_i} \leqslant je^{-j}$. Since W_j holds, (4.4) implies that

$$\begin{aligned} \sum_{\substack{i>r \\ q_i \leqslant t_{J+1}}} \frac{i^3 \log_2 q_i}{\log q_i} &\leqslant \sum_{j=(k+1)!}^{J} \frac{j^8}{e^j} \leqslant 2((k+1)!)^8 e^{-(k+1)!} \\ &\leqslant e^{-r-(1+\varepsilon/30)\sqrt{\eta(k+1)!}+O(k\log k)} \\ &\leqslant e^{-r-(1+\varepsilon/40)\sqrt{\eta(k+1)!}}. \end{aligned}$$

Since $\omega(p-1, t_{J+1}) \leqslant J^2$ and

$$\omega(p-1, t_{J+1}, x) \leqslant \frac{\log x}{\log t_{J+1}} \leqslant \log_2 x,$$

we have $\omega(p-1) \ll (\log_2 x)^2$. By (4.5), $r \leqslant K_2! \leqslant (\log_2 x)^{3/4}$ and hence

$$\sum_{q_i > t_{J+1}} \frac{i^3 \log_2 q_i}{\log q_i} \ll \big(\omega(p-1)\big)^3 \omega(p-1, t_{J+1}, x) J e^{-J}$$
$$\ll \frac{(\log_2 x)^9}{\log x} \ll e^{-r-2\sqrt{\eta(k+1)!}}.$$

It follows that

$$\sum_{i>r} \frac{i^3 \log_2 q_i}{\log q_i} \leqslant e^{-r-\sqrt{\eta(k+1)!}} \leqslant e^{-r-\sqrt{\eta r}},$$

as desired.

It remains to bound the probability that $\mathcal{A} \wedge \mathcal{B}$ holds. By Lemma 4.2 (b), $\mathbb{P}(\overline{\mathcal{F}_k}) \ll e^{-\frac{1}{2}e^{\eta/3}}$, and thus the probability that $\mathcal{F}_k$ fails for some $k \in [K_1, K_2-1]$ is $\leqslant \exp\{-e^{0.3\eta}\}$ for large enough $\eta_0(\varepsilon)$. By Lemma 4.2 (a),

$$\mathbb{P}(\mathcal{E}_k) \gg \eta^{-1/2} e^{-\frac{1}{2}(1+\varepsilon/10)^2\eta},$$

and so if $\eta_0(\varepsilon)$ is large enough then $\mathbb{P}(\mathcal{E}_k) \geqslant e^{-\frac{1}{2}(1+\varepsilon/4)\eta}$. By independence, the probability that none of the events $\mathcal{E}_k$ hold is at most

$$\Big(1 - e^{-\frac{1}{2}(1+\varepsilon/4)\eta}\Big)^{K_2-K_1} \leqslant \exp\Big\{-e^{-\frac{1}{2}(1+\varepsilon/4)\eta}(K_2-K_1)\Big\}$$
$$\leqslant \exp\Big\{-e^{0.8\eta\varepsilon}\Big\}.$$

Thus,

$$\mathbb{P}(\mathcal{A}) \geqslant 1 - \exp\Big\{-e^{0.3\eta}\Big\} - \exp\Big\{-e^{0.8\eta\varepsilon}\Big\}.$$

Since $\mathbb{P}(Y_j > j) = \sum_{k>j} 1/k! \leqslant 1/j!$,

$$\mathbb{P}(\overline{\mathcal{B}}) \leqslant \sum_{j \geqslant K_1!} \frac{1}{j!} \leqslant \frac{2}{(K_1!)!} \leqslant \frac{1}{\exp_2 K_1} \leqslant \frac{1}{\exp_3(\eta/3)}.$$

Therefore,

$$\mathbb{P}(\mathcal{A} \wedge \mathcal{B}) \geqslant 1 - \frac{1}{\exp_2(0.8\eta\varepsilon)} - \frac{1}{\exp_2(\eta/4)}.$$

Combining this last estimate with (4.3) completes the proof. □

5. Proof of Theorem 1

We may assume that $\xi > 0$ is small enough, so that $1/\delta$ and x are large enough. Assume that estimates (i) and (ii) in Theorem 1 hold with some $r \leqslant \frac{1}{3}\log(1/\delta)$. Let $\eta = \log_3(1/\delta)$. To prove the first claim $g(p) \leqslant p^{1/4-\delta}$, by Theorem 3 it suffices to show that $\alpha(p, r) \geqslant \delta$. We first note that $\log \Phi \leqslant 2(1/q_1 + \cdots + 1/q_r) \leqslant 2\xi\eta$. If ξ is chosen so that

$$C'\sqrt{2\xi} \leqslant \tfrac{1}{2}, \qquad C'' \leqslant \tfrac{1}{2} e^{\frac{1}{2}\sqrt{\log_3(1/\xi)}},$$

then $C'' \leqslant \frac{1}{2}e^{\frac{1}{2}\sqrt{r\eta}}$, and by (i) and (ii),

$$\alpha(p,r) \geqslant e^{-r-\frac{1}{2}\sqrt{r\eta}} - C''\bigg(\Big(\frac{\log(2r)}{\log p}\Big)^{1/2} + e^{-r-\sqrt{r\eta}}\bigg)$$
$$\geqslant \tfrac{1}{2}\, e^{-r-\frac{1}{2}\sqrt{r\eta}} - C''\Big(\frac{\log(2r)}{\log p}\Big)^{1/2}.$$

By assumption, $r \leqslant \frac{1}{3}\log(1/\delta) \leqslant \frac{1}{6}\log_2 x$, and thus (recall that $p > \sqrt{x}$)

$$C''\Big(\frac{\log(2r)}{\log p}\Big)^{1/2} \leqslant C''\Big(\frac{\log_2 x}{\log x}\Big)^{1/2} \leqslant \frac{1}{(\log x)^{1/3}}.$$

Since x is sufficiently large and $\delta \geqslant (\log x)^{-1/2}$ is sufficiently small, we conclude that

$$\alpha(p,r) \geqslant 0.5e^{-0.4\log(1/\delta)} - (\log x)^{-1/3} \geqslant \delta.$$

We now bound the number of primes $p \leqslant x$ failing (i) or (ii) in Theorem 1. Let $R = \log(1/\delta)$, so that by assumption $R \leqslant \frac{1}{2}\log_2 x$. By Lemma 4.1, the number of primes $p \leqslant x$ failing (i) is

$$\ll \frac{\pi(x)}{\exp_2\{(\log_2(1/\delta))^{\xi/6}\}},$$

which is much smaller than the bound given in Theorem 1.

Take $\varepsilon = 0.49$. We have $\eta \leqslant \log_4 x$ and $\frac{1}{3}\log(1/\delta) \geqslant \exp_2((\frac{1}{2}+\varepsilon)\eta)$ for small enough δ. Theorem 4 then implies that the number of primes $p \leqslant x$ failing (ii) is

$$\ll \frac{\pi(x)}{\exp_2(\eta/4)} = \frac{\pi(x)}{\exp\{(\log_2(1/\delta))^{1/4}\}}.$$

This completes the proof of Theorem 1.

References

[1] N. C. Ankeny, "The least quadratic non-residue", *Ann. Math.* **55** (1952), p. 65-72.

[2] D. A. Burgess, "The distribution of quadratic residues and non-residues", *Mathematika* **4** (1957), p. 106-112.

[3] D. A. Burgess & P. D. T. A. Elliott, "The average of the least primitive root", *Mathematika* **15** (1968), no. 1, p. 39-50.

[4] R. Crandell & C. Pomerance, *Prime Numbers: a Computational Perspective*, 2nd ed., Springer, 2005, xvi+597 pages.

[5] P. Erdős, "On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function", *Q. J. Math.* **6** (1935), p. 205-213.

[6] P. Erdős & H. N. Shapiro, "On the least primitive root of a prime", *Mathematics* **7** (1957), p. 861-865.

[7] K. Ford, "Poisson Approximation of Prime Divisors of Shifted Primes", *Int. Math. Res. Not.* **2025** (2025), no. 7, article no. rnaf079 (16 pages).

[8] K. Ford, M. Garaev & S. Konyagin, "On the smallest simultaneous power nonresidue modulo a prime", *Forum Math.* **29** (2017), no. 2, p. 347-355.

[9] G. Halasz, "Remarks to my paper: "On the distribution of additive and the mean values of multiplicative arithmetic functions"", *Acta Math. Acad. Sci. Hung.* **23** (1972), p. 425-432.

[10] R. R. Hall & G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, 1988, xvi+167 pages.

[11] A. Hildebrand & G. Tenenbaum, "Integers without large prime factors", *J. Théor. Nombres Bordeaux* **5** (1993), no. 2, p. 411-484.

[12] L.-K. Hua, "On the least primitive root of a prime", *Bull. Am. Math. Soc.* **48** (1942), p. 726-730.

[13] A. Ivić, *The Riemann zeta-function. Theory and Applications*, Theory and applications, John Wiley & Sons, 1985, xvi+517 pages.

[14] H. Iwaniec, "On the problem of Jacobsthal", *Demonstr. Math.* **11** (1978), p. 225-231.

[15] Y. V. Linnik, "A remark on the least quadratic non-residue", *C. R. (Dokl.) Acad. Sci. URSS, n. Ser.* **36** (1942), p. 119-120.

[16] G. Martin, "The least prime primitive root and the shifted sieve", *Acta Arith.* **80** (1997), no. 3, p. 277-288.

[17] K. K. Norton, "On the number of restricted prime factors of an integer. I", *Ill. J. Math.* **20** (1976), no. 4, p. 681-705.

[18] A. Sartori, "Least primitive root and simultaneous power non-residues", *J. Number Theory* **204** (2019), p. 246-263.

[19] V. Shoup, "Searching for primitive roots in finite fields", *Math. Comput.* **58** (1992), p. 369-380, extended abstract in the Proceedings of the 22nd ACM Symposium on Theory of Computation (STOC), pp. 546–554, 1990.

[20] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, 3rd expanded ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, 2015, translated from the 2008 French edition by Patrick D. F. Ion., xxiv+629 pages.

[21] I. M. Vinogradov, "On the distribution of quadratic residues and nonresidues", *J. Phys.-Math. Soc. Perm* (1919).

[22] ———, "On the bound of the least non-residue of nth powers", *Trans. Am. Math. Soc.* **29** (1927), p. 218-226.

[23] ———, "On the least primitive root", *C. R. Acad. Sci. URSS* **1930** (1930), p. 7-11.

[24] Y. Wang, "A note on the least primitive root of a prime", *Sci. Record, New Ser.* **3** (1959), p. 174-179.

Kevin Ford
Department of mathematics, 1409 West Green Street,
University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA
E-mail: ford126@illinois.edu

Mikhail R. Gabdullin
Department of mathematics, 1409 West Green Street,
University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA
E-mail: mikhailg@illinois.edu
and
Steklov Mathematical Institute,
Gubkina str., 8, Moscow, 119991, Russia
E-mail: mikhail.gabdullin@gmail.com

Andrew Granville
Département de Mathématiques et Statistique, Université de Montréal,
CP 6128 succ Centre-Ville, Montréal, QC H3C 3J7, Canada
E-mail: andrew.granville@umontreal.ca