THE MAXIMAL ORDER OF THE SHIFTED-PRIME DIVISOR FUNCTION

KAI (STEVE) FAN AND PAUL POLLACK

Dedicated to the 80^{th} Birthdays of Melvyn Nathanson and Carl Pomerance

ABSTRACT. For each positive integer n, we denote by $\omega^*(n)$ the number of shifted-prime divisors $p-1$ of n, i.e.,

$$\omega^*(n) := \sum_{p-1|n} 1.$$

First introduced by Prachar in 1955, this function has interesting applications in primality testing and bears a strong connection with counting Carmichael numbers. Prachar showed that for a certain constant $c_0 > 0$,

$$\omega^*(n) > \exp\left(c_0 \frac{\log n}{(\log\log n)^2}\right)$$

for infinitely many n. This result was later improved by Adleman, Pomerance and Rumely, who established an inequality of the same shape with $(\log\log n)^2$ replaced by $\log\log n$. Assuming the Generalized Riemann Hypothesis for Dirichlet L-functions, Prachar also proved the stronger inequality

$$\omega^*(n) > \exp\left(\left(\frac{1}{2}\log 2 + o(1)\right)\frac{\log n}{\log\log n}\right)$$

for infinitely many n. By refining the arguments of Prachar and of Adleman, Pomerance and Rumely, we improve on their results by establishing

$$\omega^*(n) > \exp\left(0.6736 \log 2 \cdot \frac{\log n}{\log\log n}\right) \text{ (unconditionally)},$$

$$\omega^*(n) > \exp\left(\left(\log\left(\frac{1+\sqrt{5}}{2}\right) + o(1)\right)\frac{\log n}{\log\log n}\right) \text{ (under GRH)},$$

for infinitely many n.

1. INTRODUCTION

For each $n \in \mathbb{N}$, let $\omega^*(n)$ count the number of shifted primes of the form $p-1$ dividing n, that is,

$$\omega^*(n) := \sum_{p-1|n} 1.$$

This function has found interesting applications in primality testing [1] and is closely related to counting Carmichael numbers [2]. It is easy to see that $\omega^*(n) \geq 1$ with equality if and only if n is odd. On the other hand, the function ω^* can attain fairly large values infinitely often. Indeed, Prachar, who initiated the study of ω^* in his influential work [16], showed that there is some absolute constant $c_1 > 0$ such that

$$\omega^*(n) > \exp\left(c_1 \frac{\log n}{(\log\log n)^2}\right) \tag{1.1}$$

for infinitely many n. Assuming the Generalized Riemann Hypothesis for Dirichlet L-functions (GRH), he was able to save a $\log\log n$ factor and provide a lower bound for c_1. More precisely, he

proved that GRH implies the inequality

$$\omega^*(n) > \exp\left(\left(\frac{1}{2}\log 2 + o(1)\right)\frac{\log n}{\log\log n}\right) \tag{1.2}$$

for infinitely many n. Nearly three decades later, Adleman, Pomerance and Rumely [1] improved Prachar's unconditional lower bound (1.1) to

$$\omega^*(n) > \exp\left(c_2\frac{\log n}{\log\log n}\right), \tag{1.3}$$

along a sequence of n tending to infinity, where $c_2 > 0$ is some absolute constant. This lower bound has the same shape as Prachar's GRH-conditional lower bound (1.2), up to the constant factor. They also conjectured that the constant $\frac{1}{2}\log 2$ in (1.2) can in fact be upgraded to $\log 2$. It is worth noting that the conjectured constant $\log 2$ would be best possible, since

$$\omega^*(n) \le \tau(n) \le \exp\left((\log 2 + o(1))\frac{\log n}{\log\log n}\right)$$

for sufficiently large n [9, Theorem 317], where $\tau(n)$ denotes the number of positive divisors of n. Interestingly, this conjecture, if true, would imply that the Carmichael function $\lambda(n)$, which may be defined as the exponent of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, satisfies

$$\liminf_{n\to\infty}\frac{\log\lambda(n)}{(\log\log n)\log\log\log n} = \frac{1}{\log 2},$$

an observation first made by Erdős, Pomerance, and Schmutz [5].

The study of ω^* was recently revived by Murty and Murty [14]. For each $k \in \mathbb{N}$, we define the kth moment of ω^* by

$$M_k(x) := \frac{1}{x}\sum_{n\le x}\omega^*(n)^k.$$

These moments encode useful information about the distribution of ω^*. A quick application of Mertens' theorem [9, Theorem 427] yields $M_1(x) = \log\log x + O(1)$. In the same paper [16], Prachar showed that $M_2(x) \ll (\log x)^2$. In their recent work [14], Murty and Murty [14] proved the estimate $(\log\log x)^3 \ll M_2(x) \ll \log x$ and conjectured the asymptotic formula $M_2(x) \sim C_2\log x$ with some constant $C_2 > 0$. Two years later, Ding [4] achieved the order matching lower bound $M_2(x) \gg \log x$. More recently, Pomerance and the first author [7] established the estimate $M_3(x) \asymp (\log x)^4$ and made the more general conjecture that for each $k \ge 2$ there exists a constant $C_k > 0$ such that $M_k(x) \sim C_k(\log x)^{2^k-k-1}$. Based on a heuristic argument, the first author [6] also conjectured that $C_2 = \zeta(2)^2\zeta(3)/\zeta(6)$, where ζ is the Riemann zeta-function. Despite the fact that no asymptotic formula is currently known even for a single value of $k \ge 2$, quite recently Gabdullin [8] pinned down the correct order of magnitude for $M_k(x)$, showing that $M_k(x) \asymp (\log x)^{2^k-k-1}$ for every fixed $k \ge 2$.

The main objective of this paper is to furnish explicit values for the constant c_2 appearing in (1.3). Perhaps a bit surprisingly, we are able to obtain unconditionally a numerical value for c_2 which is slightly larger than $\frac{2}{3}\log 2$, hence surpassing the constant $\frac{1}{2}\log 2$ in Prachar's GRH-conditional lower bound (1.2). Under GRH, our argument yields a numerical value for c_2 which exceeds $(\log 2)^2$. The following theorem provides a precise statement of our results.

Theorem 1.1. *There exist infinitely many n such that*

$$\omega^*(n) > \exp\left(0.6736 \log 2 \cdot \frac{\log n}{\log\log n}\right). \tag{1.4}$$

Moreover, if GRH is true, then we have

$$\omega^*(n) > \exp\left(\left(\log\left(\frac{1+\sqrt{5}}{2}\right) + o(1)\right)\frac{\log n}{\log\log n}\right) \tag{1.5}$$

for infinitely many n.

2. An overview of Prachar's argument

We first outline Prachar's simple proof of (1.2) upon which our proof of Theorem 1.1 is built. In what follows, the letter p always denotes a prime. We write $\pi(x)$ for the number of primes $p \le x$, and let $\pi(x; d, a)$ count the number of primes $p \le x$ with $p \equiv a \pmod d$.

Suppose that x is sufficiently large. Let $\epsilon \in (0,1)$ be arbitrary, and put

$$k = \prod_{p \le (1-\epsilon)\log x} p = x^{1-\epsilon+o(1)}.^{\dagger} \tag{2.1}$$

Under GRH we have [13, Corollary 13.8]

$$\pi(x; d, 1) = \frac{\mathrm{Li}(x)}{\varphi(d)} + O\left(\sqrt{x}\log x\right) \gg \frac{x}{\varphi(d)\log x}$$

uniformly for all positive integers $d \le \sqrt{k}$, where

$$\mathrm{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t}.$$

For each $1 \le d \le \sqrt{k}$ dividing k, denote by A_d the number of pairs (m, p), where $m \in \mathbb{N}$ and p is prime, such that $m, p \le x$,

$$p \equiv 1 \pmod d \quad \text{and} \quad \gcd(m, k) = \frac{k}{d}. \tag{2.2}$$

Let A record the total number of pairs (m, p) with $m, p \le x$ satisfying the congruence $m(p-1) \equiv 0 \pmod k$. Every pair counted by A_d, for some $d \mid k, d \le \sqrt{k}$, is counted by A. Moreover, an individual pair is counted by A_d for at most one d. Since the number of choices for p is clearly $\pi(x; d, 1)$, and since the count of m is at least $\lfloor x/k \rfloor \varphi(d)$, we have

$$A_d \ge \pi(x; d, 1)\left\lfloor \frac{x}{k} \right\rfloor \varphi(d) \gg \frac{x^2}{k \log x},$$

[†]In fact, Prachar [16] took

$$k = \prod_{p \le (1/2-\epsilon)\log x} p.$$

However, this appears to be a misstep: This choice of k only yields the smaller constant $\frac{1}{4}\log 2$ rather than $\frac{1}{2}\log 2$ asserted in [16] and (1.2).

from which it follows that

$$A \geq \sum_{\substack{d \leq \sqrt{k} \\ d|k}} A_d \gg \frac{x^2}{k \log x} \sum_{\substack{d \leq \sqrt{k} \\ d|k}} 1 \geq \frac{\tau(k) x^2}{2k \log x}.$$

On the other hand, each pair (m, p) counted by A yields a positive integer $n = m(p-1) \leq x^2$ divisible by k. Thus,

$$A \leq \sum_{\substack{n \leq x^2 \\ k|n}} \#\{(m,p) \colon m, p \leq x \text{ and } n = m(p-1)\}.$$

Combining the above upper and lower bounds for A, we deduce that there exists some large $n \leq x^2$ which is divisible by k and admits

$$\gg \frac{\tau(k) x^2/(k \log x)}{x^2/k} = \frac{\tau(k)}{\log x} = \frac{2^{\pi((1-\epsilon)\log x)}}{\log x} > \exp\left((\log 2 - 2\epsilon) \frac{\log x}{\log\log x} \right)$$

representations of the form $n = m(p-1)$. For this particular n, we have

$$\omega^*(n) \geq \exp\left((\log 2 - 2\epsilon) \frac{\log x}{\log\log x} \right) > \exp\left(\left(\frac{1}{2} \log 2 - 2\epsilon \right) \frac{\log n}{\log\log n} \right),$$

as desired.

In the argument outlined above, the representations $n = m(p-1)$ counted by A_d all have $m, p \leq x$ and $d \leq \sqrt{k}$, with k defined by (2.1). In the next section, we shall prove Theorem 1.1 by adjusting the choices for k, d, m, p. We use insights from the theory of anatomy of integers to maximize the total number of representations $n = m(p-1)$ counted by A.

3. Refining Prachar's argument: Proof of Theorem 1.1

We start by proving the GRH-conditional inequality (1.5). Suppose that x is sufficiently large. Put

$$\epsilon := (\log\log x)^{-1/2} \quad \text{and} \quad u := \frac{3+\sqrt{5}}{4}, \tag{3.1}$$

and set

$$\begin{aligned} k &:= \prod_{p \leq (u-\epsilon)\log x} p \\ &= x^{u-\epsilon} \exp\left(O\left(\frac{\log x}{\log\log x} \right) \right). \end{aligned}$$

We will show momentarily that there is a set $\mathcal{D}$ of divisors of k, where each $d \in \mathcal{D}$ obeys the estimate

$$d = x^{\frac{1}{2}-\epsilon} \exp\left(O\left(\frac{\log x}{(\log\log x)^2} \right) \right), \tag{3.2}$$

and where, with $X := x^{\frac{1}{2}+u}$,

$$\#\mathcal{D} \geq \exp\left(\left(\log\left(\frac{1+\sqrt{5}}{2} \right) + o(1) \right) \frac{\log X}{\log\log X} \right). \tag{3.3}$$

Let us see now how this claim implies (1.5).

For each $d \in \mathcal{D}$, let A_d denote the number of pairs (m,p) with $m \le y_d := x^u/d$ and $p \le x$, satisfying the same conditions described in (2.2). By inclusion-exclusion, the number of choices for m is

$$\sum_{\substack{m' \le y_d/(k/d) \\ (m',d)=1}} 1 = \frac{\varphi(d)}{d} \cdot \frac{y_d}{k/d} + O(\tau(d)) \gg \frac{\varphi(d)}{d} \cdot \frac{x^u}{k},$$

since $\tau(d) \le \exp\left(O\left(\frac{\log x}{\log\log x}\right)\right)$, and

$$\frac{\varphi(d)}{d} \cdot \frac{y_d}{k/d} = \frac{\varphi(d)}{d} \cdot \frac{x^u}{k} \gg \exp\left(\frac{\log x}{2(\log\log x)^{1/2}}\right).$$

Our estimate (3.2) for d, along with the choice of ϵ in (3.1), implies that $d \le x^{1/2}/(\log x)^3$ (say), so that

$$\pi(x;d,1) = \frac{\mathrm{Li}(x)}{\varphi(d)} + O\left(\sqrt{x}\log x\right) \gg \frac{x}{\varphi(d)\log x}.$$

It follows that for all $d \in \mathcal{D}$,

$$A_d \gg \pi(x;d,1)\frac{\varphi(d)}{d} \cdot \frac{x^u}{k} \gg \frac{x^{u+1}}{kd\log x} = \frac{x^{u+\frac{1}{2}+\epsilon}}{k\log x} \exp\left(O\left(\frac{\log x}{(\log\log x)^2}\right)\right). \tag{3.4}$$

Therefore,

$$\sum_{d\in\mathcal{D}} A_d \gg \#\mathcal{D}\, \frac{x^{u+\frac{1}{2}+\epsilon}}{k\log x} \exp\left(O\left(\frac{\log x}{(\log\log x)^2}\right)\right). \tag{3.5}$$

On the other hand, if (m,p) is counted by some A_d, then $m(p-1)$ is a multiple of k and

$$m(p-1) \le \left(\max_{d\in\mathcal{D}} y_d\right)x = x^{u+\frac{1}{2}+\epsilon} \exp\left(O\left(\frac{\log x}{(\log\log x)^2}\right)\right). \tag{3.6}$$

Reasoning as in §2, we conclude upon comparing (3.5) and (3.6) that there is a large multiple n of k, not exceeding the final expression in (3.6), with

$$\omega^*(n) \ge \frac{\#\mathcal{D}}{\log x} \exp\left(O\left(\frac{\log x}{(\log\log x)^2}\right)\right).$$

Substituting the lower bound (3.3) for $\#\mathcal{D}$ gives

$$\begin{aligned}\omega^*(n) &\ge \exp\left(\left(\log\left(\frac{1+\sqrt{5}}{2}\right) + o(1)\right)\frac{\log X}{\log\log X}\right) \\ &\ge \exp\left(\left(\log\left(\frac{1+\sqrt{5}}{2}\right) + o(1)\right)\frac{\log n}{\log\log n}\right),\end{aligned}$$

where we use in the second line that $n \le X^{1+o(1)}$.

To show the existence of the set $\mathcal{D}$, we employ the probabilistic method. Let

$$L = (u-\epsilon)\log x \quad \text{and} \quad R = \pi(L).$$

Furthermore, set

$$\rho = \frac{\frac{1}{2}-\epsilon}{u-\epsilon}.$$

We introduce i.i.d. Bernoulli random variables v_r, for each prime $r \le L$, where every v_r takes the value 1 with probability ρ. Then

$$d \coloneqq \prod_{r \le L} r^{v_r}$$

is a random divisor of k. We proceed to study the distribution of d.

It is straightforward to compute the expectation and variance of the random variable $\log d = \sum_{r \le L} v_r \log r$: We have

$$\mathbb{E}[\log d] = \sum_{r \le L} \mathbb{E}[v_r \log r] = \rho \sum_{r \le L} \log r = \left(\frac{1}{2} - \epsilon\right) \log x + O(L/(\log L)^3),$$

$$\mathbb{V}[\log d] = \sum_{r \le L} \mathbb{V}[v_r \log r] = \rho(1-\rho) \sum_{r \le L} (\log r)^2 \ll \sum_{r \le L} (\log r)^2 \ll L \log L.$$

This latter estimate implies, via Chebyshev's inequality, that $|\log d - \mathbb{E}[\log d]| > L^{2/3}$ with probability $O(L^{-1/3} \log L) = o(1)$. Thus, with probability $1 + o(1)$,

$$\begin{aligned} \left|\log d - \left(\frac{1}{2} - \epsilon\right) \log x\right| &\le |\log d - \mathbb{E}[\log d]| + \left|\mathbb{E}[\log d] - \left(\frac{1}{2} - \epsilon\right) \log x\right| \\ &\le L^{2/3} + L/(\log L)^2 < 2L/(\log L)^2. \end{aligned} \tag{3.7}$$

Let $\mathcal{D}$ be the set of divisors d of k for which $|\log d - (\frac{1}{2} - \epsilon) \log x| < 2L/(\log L)^2$. For each $d \in \mathcal{D}$, the desired estimate (3.2) holds, and we have just seen that $\mathbb{P}(d \in \mathcal{D}) = 1 + o(1)$, as $x \to \infty$. We proceed to translate this probability bound into a lower bound on $\#\mathcal{D}$. In fact, we will obtain the claimed lower bound (3.3) for a certain convenient subset of $\mathcal{D}$.

The mean and variance of $\Omega(d) = \sum_{r \le L} v_r$ satisfy $\mathbb{E}[\Omega(d)] = \rho R$, $\mathbb{V}[\Omega(d)] \ll R$. So if we let $\mathcal{E}$ denote the set of $d \mid k$ with $|\Omega(d) - \rho R| > R^{2/3}$, then $\mathbb{P}(d \in \mathcal{E}) = o(1)$ by another application of Chebyshev's inequality. We put $\mathcal{D}' \coloneqq \mathcal{D} \setminus \mathcal{E}$ and observe that

$$\mathbb{P}(d \in \mathcal{D}') \ge \mathbb{P}(d \in \mathcal{D}) - \mathbb{P}(d \in \mathcal{E}) = 1 + o(1).$$

If $d \in \mathcal{D}'$, then $v_r = 1$ for $\rho R + O(R^{2/3})$ primes $r \le L$, while $v_r = 0$ for $(1-\rho)R + O(R^{2/3})$ primes $r \le L$. Hence, each $d \in \mathcal{D}'$ carries a probability mass of

$$\rho^{\rho R} (1-\rho)^{(1-\rho)R} \exp(O(R^{2/3})).$$

In order for the probability masses corresponding to $d \in \mathcal{D}'$ to sum to $1 + o(1)$, it must be that

$$\#\mathcal{D} \ge \#\mathcal{D}' \ge \rho^{-\rho R} (1-\rho)^{-(1-\rho)R} \exp(O(R^{2/3})). \tag{3.8}$$

Since $R = (1 + o(1)) u \frac{\log x}{\log \log x}$ while $\rho = \frac{1}{2u} + o(1)$, we have

$$\rho^{-\rho R} (1-\rho)^{-(1-\rho)R} \exp(O(R^{2/3})) = \exp((C + o(1)) \log x / \log \log x), \tag{3.9}$$

where

$$\begin{aligned} C &= \frac{1}{2}\log(2u) + \left(u - \frac{1}{2}\right)\log\frac{2u}{2u-1} \\ &= \left(u + \frac{1}{2}\right)\log\frac{2u}{2u-1} + \left(\log\sqrt{2u} - \log\frac{2u}{2u-1}\right) \\ &= \left(u + \frac{1}{2}\right)\log\frac{1+\sqrt{5}}{2}, \end{aligned}$$

noting for the last line that $\frac{2u}{2u-1} = \frac{1+\sqrt{5}}{2} = \sqrt{2u}$. Finally, since $X = x^{\frac{1}{2}+u}$,

$$\left(u + \frac{1}{2}\right)\frac{\log x}{\log\log x} = (1+o(1))\frac{\log X}{\log\log X}. \tag{3.10}$$

The lower bound (3.3) on $\#\mathcal{D}$ follows from (3.8), (3.9) and (3.10).

The unconditional inequality (1.4) follows in a similar fashion, using the following result of Harman (see [11, Theorem 1.2]) as a proxy for the GRH.

Proposition 3.1. *There is an absolute constant $\delta > 0$ making the following true.*

For each $\eta > 0$, there are constants $K \geq 2$ and $c > 0$ such that the following holds. Suppose

$$K < d < x^{0.4736}, \quad \text{and} \quad p \mid d \Rightarrow p < d^{\delta}.$$

Furthermore, assume that for every $f \mid d$ and primitive character $\chi \bmod f$,

$$L(s,\chi) \neq 0 \quad \text{for} \quad \mathrm{Re}(s) > 1 - \frac{1}{(\log d)^{3/4}},\ |\mathrm{Im}(s)| \leq \exp(\eta(\log d)^{3/4}). \tag{3.11}$$

Then for every a with $\gcd(a,d) = 1$, we have

$$\pi(x;d,a) \geq \frac{cx}{\varphi(d)\log x}.$$

Put

$$\epsilon \coloneqq (\log\log x)^{-1/2} \quad \text{and} \quad \theta \coloneqq 0.4736,$$

and define $u \approx 1.2694$ to be the unique point at which the function

$$f_\theta(t) := \frac{1}{t+1-\theta}\left(\theta\log\frac{t}{\theta} - (t-\theta)\log\left(1-\frac{\theta}{t}\right)\right) = \frac{t\log t - (t-\theta)\log(t-\theta) - \theta\log\theta}{t+1-\theta} \tag{3.12}$$

attains its global maximum $f_\theta(u) \approx 0.4669$ on $[\theta,\infty)$.

Below, we describe how Proposition 3.1 can be used to find a positive integer $k \mid \prod_{p \leq (u-\epsilon)\log x} p$, along with a set $\mathcal{D}$ of divisors of k, where each $d \in \mathcal{D}$ has the property that

$$\pi(x;d,1) \gg \frac{x}{\varphi(d)\log x}. \tag{3.13}$$

Furthermore, $\mathcal{D}$ will be selected in such a way that each $d \in \mathcal{D}$ obeys the estimate

$$d = x^{\theta-\epsilon}\exp\left(O\left(\frac{\log x}{(\log\log x)^2}\right)\right), \tag{3.14}$$

and such that

$$\#\mathcal{D} \geq \exp\left((C' + o(1))\,\frac{\log x}{\log\log x}\right) = \exp\left((f_\theta(u) + o(1))\,\frac{\log Y}{\log\log Y}\right), \tag{3.15}$$

with

$$Y \coloneqq x^{u+1-\theta}, \quad \text{and} \quad C' \coloneqq \theta \log\frac{u}{\theta} - (u-\theta)\log\left(1 - \frac{\theta}{u}\right) = (u+1-\theta) f_\theta(u).$$

After k and $\mathcal{D}$ have been located, the rest of the argument can be carried out as before. For each $d \in \mathcal{D}$, let A_d denote the number of pairs (m,p) with $m \leq y_d = x^u/d$ and $p \leq x$, satisfying the conditions in (2.2). Then we have

$$A_d \gg \pi(x;d,1)\frac{\varphi(d)}{d} \cdot \frac{x^u}{k} \gg \frac{x^{u+1}}{kd\log x} = \frac{x^{u+1-\theta+\epsilon}}{k\log x}\exp\left(O\left(\frac{\log x}{(\log\log x)^2}\right)\right),$$

and

$$\sum_{d\in\mathcal{D}} A_d \gg \frac{x^{u+1-\theta+\epsilon}}{k\log x}\exp\left((f_\theta(u)+o(1))\,\frac{\log Y}{\log\log Y}\right).$$

Each pair (m,p) counted by some A_d corresponds to a multiple $m(p-1)$ of k for which

$$m(p-1) \leq x^{u+1-\theta+\epsilon}\exp\left(O\left(\frac{\log x}{(\log\log x)^2}\right)\right).$$

Comparing the last two displays, we conclude that there is an $n \leq x^{u+1-\theta+o(1)}$ with

$$\omega^*(n) \geq \exp\left((f_\theta(u)+o(1))\,\frac{\log Y}{\log\log Y}\right) \geq \exp\left((f_\theta(u)+o(1))\,\frac{\log n}{\log\log n}\right).$$

As $f_\theta(u)/\log 2 = 0.67365\ldots > 0.6736$, the estimate (1.4) follows.

To produce k and $\mathcal{D}$, we borrow ideas and results from [10, pp. 647–648]. Let

$$W \coloneqq \left(\frac{2}{5}\log x\right)^{3/4}.$$

As on p. 647 of [10], for some absolute constant $\eta > 0$, there is at most one primitive character $\chi_1 \bmod f_1$ of conductor

$$f_1 < V \coloneqq \exp(\eta(\log x)^{3/4})$$

for which $L(s,\chi_1)$ has a zero ρ with

$$\mathrm{Re}(\rho) > 1 - \frac{1}{W}, \quad |\mathrm{Im}(\rho)| \leq V. \tag{3.16}$$

(This follows from the results on exceptional zeros appearing on pp. 93–95 of [3].) We will apply Proposition 3.1 with this η. Note that if $x^{0.4} < d < x^\theta$, in order for (3.11) to fail, $L(s,\chi)$ must have a zero ρ belonging to the region (3.16).

If the primitive character $\chi_1 \bmod f_1$ of the last paragraph exists, we let p_1 be a prime factor of f_1. Otherwise, we let $p_1 = 1$. Let $L = (u-\epsilon)\log x$ and $R = \pi(L)$ (as before), and set

$$\rho = \frac{\theta - \epsilon}{u - \epsilon}.$$

We take

$$k = \prod_{\substack{p \le L \\ p \ne p_1}} p = x^{u-\epsilon} \exp\left(O\left(\frac{\log x}{\log\log x}\right)\right),$$

and we let $d = \prod_{r|k} r^{v_r}$, where the v_r are i.i.d. Bernoulli random variables with each $\mathbb{P}(v_r = 1) = \rho$.

By our earlier arguments, a random d satisfies both

$$|\log d - (\theta - \epsilon)\log x| < L^{2/3} \tag{3.17}$$

and

$$|\Omega(d) - \rho R| < R^{2/3} \tag{3.18}$$

with probability $1 + o(1)$. (The possibly missing prime p_1 has a negligible effect.) Let $\mathcal{D}_0$ be the set of divisors d of k satisfying (3.17) and (3.18). We proceed to remove from $\mathcal{D}_0$ those d for which there is a primitive character $\chi \bmod f$, $f \mid d$, where (3.11) fails. Since $\gcd(d, p_1) = 1$, in these cases we necessarily have $f \ge V$. Furthermore, $L(s, \chi)$ has a zero in the region (3.16).

Zero density estimates (e.g., [12, Theorem 1] suffices here) show that there are no more than $\exp(O((\log x)^{1/4}))$ primitive characters $\chi \bmod f$, $f \le x$, having a zero in the region (3.16). (Compare with pp. 647–648 of [10].) From that set of characters, throw away those of conductors smaller than V, and collect their remaining conductors in a set $\mathcal{F}$. Then each d to be removed from $\mathcal{D}_0$ is divisible by some $f \in \mathcal{F}$.

We fix $f \in \mathcal{F}$ and examine the probability that $f \mid d$. If $f \nmid k$, then $\mathbb{P}(f \mid d) = 0$. Otherwise, $\mathbb{P}(f \mid d) = \rho^{\omega(f)}$, where $\omega(f)$ denotes the number of distinct prime factors of f. Since

$$V \le f \le (u \log x)^{\omega(f)},$$

we have

$$\omega(f) \ge \frac{\log V}{\log(u \log x)} = \frac{\eta(\log x)^{3/4}}{\log(u \log x)}.$$

Thus (for large x),

$$\mathbb{P}(f \mid d) = \rho^{\omega(f)} < \exp(-(\log x)^{7/10}).$$

Hence,

$$\mathbb{P}(f \mid d \text{ for some } f \in \mathcal{F}) \le \#\mathcal{F} \exp(-(\log x)^{7/10}) = o(1),$$

recalling for the last equality that $\#\mathcal{F} \le \exp(O((\log x)^{1/4}))$.

Therefore, after removing all $d \in \mathcal{D}_0$ divisible by an $f \in \mathcal{F}$, we are left with a set $\mathcal{D}$ of divisors of k for which $\mathbb{P}(d \in \mathcal{D}) = 1 + o(1)$. We see from (3.17) that each $d \in \mathcal{D}$ satisfies (3.14). Furthermore, invoking (3.18) and repeating the argument leading to (3.3), we arrive at (3.15). Finally, Proposition 3.1 furnishes the desired lower bound (3.13) on $\pi(x; d, 1)$ for all $d \in \mathcal{D}$.

4. Concluding remarks

We have seen that a key, common ingredient in Prachar's argument and the proof of Theorem 1.1 is an inequality of the form

$$\pi(x; d, 1) \gg \frac{x}{\varphi(d)\log x} \tag{4.1}$$

for $d \mid k$, where k is essentially the product of all primes $p \le \theta \log x$ with some $\theta \in (0,1)$. The proof of Theorem 1.1 reveals that if (4.1) holds for some fixed $\theta \in (0,1)$, then we have

$$\omega^*(n) \ge \exp\left(\left(\max_{t\ge\theta} f_\theta(t) + o(1)\right)\frac{\log n}{\log\log n}\right)$$

for infinitely many n, where $f_\theta(t)$ is defined as in (3.12). In particular, the conjecture of Adleman, Pomerance and Rumely [1] mentioned in the introduction, that

$$\omega^*(n) \ge \exp\left((\log 2 + o(1))\frac{\log n}{\log\log n}\right) \tag{4.2}$$

for infinitely many n, would follow if (4.1) holds for any fixed $\theta \in (0,1)$ (since, for instance, $\max_{t\ge\theta} f_\theta(t) \ge f_\theta(2\theta) = \frac{2\theta}{\theta+1}\log 2$). As [2, Theorem 2.1] shows, the lower bound (4.1) is intimately related to zero densities for Dirichlet L-functions. An implication of this is that our inequality (1.5) still holds under the Density Hypothesis which is weaker than GRH.

Note that in Prachar's argument, if we sum A_d over all divisors d of k instead, we would have

$$\sum_{d\mid k} A_d \gg \frac{x}{k}\sum_{d\mid k}\varphi(d)\pi(x;d,1) = \frac{x}{k}\sum_{p\le x}\sum_{\substack{d\mid k\\ d\mid p-1}}\varphi(d) = \frac{x}{k}\sum_{p\le x}\gcd(p-1,k).$$

The last sum hints at the connection between the maximal order of ω^* and the distribution of smooth shifted primes $p-1$. Given $y \ge 1$, we say that $n \in \mathbb{N}$ is *y-smooth* if $P^+(n) \le y$, where $P^+(n)$ denotes the greatest prime factor of n, with the convention that $P^+(1) = 1$. In other words, y-smooth numbers are precisely those integers with no prime factors exceeding y. For $x \ge y \ge 1$, we define the counting functions

$$\Psi(x,y) := \#\left\{n \le x\colon P^+(n) \le y\right\},$$
$$\pi(x,y) := \#\left\{p \le x\colon P^+(p-1) \le y\right\}.$$

In contrast to $\Psi(x,y)$ whose asymptotic behavior is rather well-understood (see for instance [17, Chapter III.5]), the function $\pi(x,y)$ has remained elusive. Nevertheless, it is widely believed that smooth shifted primes have the same asymptotic density relative to shifted primes as smooth integers do relative to integers. Indeed, Pomerance [15] has conjectured that if $x \ge y \ge 1$, then

$$\frac{\pi(x,y)}{\pi(x)} \sim \frac{\Psi(x,y)}{x} \tag{4.3}$$

as $y \to \infty$. We conclude our paper with a demonstration that the Adleman–Pomerance–Rumely conjecture (4.2) is an easy consequence of Pomerance's conjecture (4.3).

Assume (4.3). Fix $v > 0$ and set $y = v\log x$ with x sufficiently large. The number of pairs (m,p), with $m, p \le x$, $P^+(m) \le y$, and $P^+(p-1) \le y$, is $\Psi(x,y)\pi(x,y)$. Since each $n = (m-1)p \le x^2$ is y-smooth, and since the number of y-smooth numbers up to x^2 is precisely given by $\Psi(x^2,y)$, we deduce from (4.3) that there is some large y-smooth number $n \le x^2$ with at least

$$\frac{\Psi(x,y)\pi(x,y)}{\Psi(x^2,y)} \sim \frac{\Psi(x,y)^2}{\Psi(x^2,y)}\cdot\frac{\pi(x)}{x} \sim \frac{\Psi(x,y)^2}{\Psi(x^2,y)}\cdot\frac{1}{\log x} \tag{4.4}$$

representations as $n = m(p-1)$. By [17, Theorem III.5.2], we have

$$\begin{aligned}\log \Psi(x,y) &= \left(1 + O\left(\frac{1}{\log\log x}\right)\right) \frac{\log x}{\log y} \int_0^1 \log\left(1 + \frac{y}{t\log x}\right) \mathrm{dt} \\ &= \left(1 + O\left(\frac{1}{\log\log x}\right)\right) \frac{\log x}{\log\log x} \int_0^1 \log\left(1 + \frac{v}{t}\right) \mathrm{dt},\end{aligned}$$

and analogously,

$$\log \Psi(x^2,y) = \left(1 + O\left(\frac{1}{\log\log x}\right)\right) \frac{2\log x}{\log\log x} \int_0^1 \log\left(1 + \frac{v}{2t}\right) \mathrm{dt}.$$

Since $\log(1+z) \geq z/(1+z)$ for all $z > -1$, it follows that

$$\begin{aligned}\log \frac{\Psi(x,y)^2}{\Psi(x^2,y)} &= \left(\log 2 + \int_0^1 \log\left(1 - \frac{t}{2t+v}\right) \mathrm{dt} + O\left(\frac{1}{\log\log x}\right)\right) \frac{2\log x}{\log\log x} \\ &\geq \left(\log 2 - \int_0^1 \frac{t}{t+v}\,\mathrm{dt} + O\left(\frac{1}{\log\log x}\right)\right) \frac{2\log x}{\log\log x} \\ &\geq \left(\log 2 - \frac{1}{1+v} + O\left(\frac{1}{\log\log x}\right)\right) \frac{2\log x}{\log\log x}.\end{aligned}$$

Inserting this in (4.4), we find that this particular n has at least

$$\begin{aligned}\frac{\Psi(x,y)\pi(x,y)}{\Psi(x^2,y)} &\gg \exp\left(\left(\log 2 - \frac{1}{1+v} + O\left(\frac{1}{\log\log x}\right)\right) \frac{2\log x}{\log\log x}\right) \\ &\geq \exp\left(\left(\log 2 - \frac{1}{v}\right) \frac{\log n}{\log\log n}\right)\end{aligned}$$

representations as $n = m(p-1)$. Since $v > 0$ is arbitrary, this verifies our claim that (4.2) follows from (4.3).

References

[1] L. M. Adleman, C. Pomerance, and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. **117** (1983), 173–206.

[2] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), 703–722.

[3] H. Davenport, *Multiplicative number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York-Berlin, 1980. Revised by Hugh L. Montgomery.

[4] Y. Ding, *On a conjecture of M. R. Murty and V. K. Murty*, Canad. Math. Bull. **66** (2023), 679–681.

[5] P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael's lambda function*, Acta Arith. **58** (1991), 363–385.

[6] K. (S.) Fan, *The shifted prime-divisor function over shifted primes*, Ramanujan J. **66** (2025), 1–46.

[7] K. (S.) Fan and C. Pomerance, *Shifted-prime divisors*, preprint (2024). arXiv:2401.10427. To appear in a Springer volume dedicated to Helmut Maier on his 70th birthday and edited by J. Friedlander, C. Pomerance, and M. Rassias.

[8] M. R. Gabdullin, *Moments of the shifted prime divisor function*, preprint (2025). arXiv:2505.24050.

[9] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University Press, Oxford, 2008. Revised by D. R. Heath-Brown and J. H. Silverman.

[10] G. Harman, *On the number of Carmichael numbers up to x*, Bull. London Math. Soc. **37** (2005), 641–650.

[11] ———, *Watt's mean value theorem and Carmichael numbers*, Int. J. Number Theory **4** (2008), 241–248.

[12] H. L. Montgomery, *Zeros of L-functions*, Invent. Math. **8** (1969), 346–354.

[13] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2006.

[14] M. R. Murty and V. K. Murty, *A variant of the Hardy–Ramanujan theorem*, Hardy–Ramanujan J. **44** (2021), 32–40.
[15] C. Pomerance, *Popular values of Euler's function*, Mathematika **27** (1980), 84–89.
[16] K. Prachar, *Über die Anzahl der Teiler einer natürlichen Zahl, welche die form $p-1$ haben*, Monatsh. Math. **59** (1955), 91–97.
[17] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, 3rd ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015.

Department of Mathematics, University of Georgia, Athens, GA 30602

Email address: Steve.Fan@uga.edu

Email address: pollack@uga.edu