SMALL VALUES OF CARMICHAEL'S λ-FUNCTION

PAUL POLLACK

ABSTRACT. Let $\lambda(n)$ be the exponent of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^{\times}$, and set $L(x,y) = \#\{n \le x : \lambda(n) \le y\}$. We prove an upper bound for $\log \frac{L(x,y)}{x}$ valid for $\exp((\log_2 x)^{1+\varepsilon}) \le y \le x/\exp((\log_2 x)^{1+\varepsilon})$. Our bound is asymptotically sharp under a plausible hypothesis on powersmooth shifted primes. As an application, we obtain a new upper bound on the count of odd $n \le x$ for which the order of 2 modulo n is appreciably smaller than $x^{1/2}$.

1. INTRODUCTION

Every student passing through a course in elementary number theory learns about Euler's theorem, according to which $a^{\phi(n)} \equiv 1 \pmod{n}$ for all integers a with $\gcd(a,n) = 1$. Let $\lambda(n)$ denote the least positive integer that can take the place of $\phi(n)$ in this result — in other words, the exponent of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^{\times}$. It was already known to Gauss that $\lambda(n) = \mathrm{lcm}_{p^k \| n}[\lambda(p^k)]$, where $\lambda(p^k) = p^{k-1}(p-1)$ if p is odd or $k \le 2$, and $\lambda(2^k) = 2^{k-2}$ for every $k \ge 3$ (see Articles 82–92 of *Disquisitiones Arithmeticae* [11]). But R. D. Carmichael [3], working a century later, was the first to study properties of $\lambda(n)$ as an *arithmetic function*; accordingly, one typically refers to $\lambda(n)$ as Carmichael's lambda-function.

Determining the maximal order of $\lambda(n)$ is trivial: Clearly, $\lambda(n) \le \phi(n) \le n-1$ for all integers $n > 1$, with $\lambda(n) = n-1$ whenever n is prime. The average, minimal, and typical (normal) orders are considerably more interesting; these were investigated by Erdős, Pomerance, and Schmutz in [9]. Concerning the typical size of $\lambda(n)$, those authors prove the existence of an explicit constant $A \approx 0.227$ for which

$$\lambda(n) = n(\log n)^{-\log_3 n - A + o(1)} \tag{1.1}$$

as n tends to infinity through a set of asymptotic density 1. (Here and below, $\log_k$ is the kth iterate of the natural logarithm.) As for the minimal order of $\lambda(n)$, they show that for a certain constant $C > 0$ and infinitely many n,

$$\lambda(n) \le (\log n)^{C \log_3 n},$$

while on the other hand,

$$\lambda(n) \ge (\log n)^{(\frac{1}{\log 2} + o(1)) \log_3 n} \tag{1.2}$$

whenever n tends to infinity.

In this paper, we study the distribution of "intermediate" values of $\lambda(n)$, meaning values of $\lambda(n)$ lying between the scales suggested by its typical and minimal orders. Let

$$L(x,y) = \#\{n \le x : \lambda(n) \le y\}.$$

2020 *Mathematics Subject Classification.* Primary 11N64; Secondary 11K65, 11N37.

Constraint	$y = y(x)$	**Upper bound for** $L(x,y)$**, as** $x \to \infty$
$\alpha \in K \subseteq (0,1)$ (compact subset K)	$x^{1-\alpha}$	$x \exp\left(-(\alpha + o(1))\frac{\log x \log_3 x}{\log_2 x}\right)$
	$\exp((\log x)^\alpha)$	$x \exp\left(-(\frac{1}{\alpha} + o(1))\frac{\log x \log_3 x}{\log_2 x}\right)$
	$x/\exp((\log x)^\alpha)$	$x \exp\left(-(\frac{1}{\alpha} + o(1))\frac{(\log x)^\alpha \log_3 x}{\log_2 x}\right)$
$\beta \in K \subseteq (1,\infty)$ (compact subset K)	$\exp((\log_2 x)^\beta)$	$x^{1-\frac{1}{\beta}+o(1)}$

Table 1. A few instances of Theorem 1.1.

As long as y and x/y are both "reasonably large", we obtain an upper bound for $\log \frac{L(x,y)}{x}$ that we expect to be asymptotically sharp. To state our results precisely, it is convenient to let

$$\mathscr{L}(x,y) = \exp\left(\frac{\log x \log_3 x}{\log_2 y}\right), \quad \text{setting} \quad \mathscr{L}(x) := \mathscr{L}(x,x) = \exp\left(\frac{\log x \log_3 x}{\log_2 x}\right).$$

Theorem 1.1. *Fix $\varepsilon > 0$. Suppose that in the domain $x, y \geq 100$, we have both*

$$y \geq \exp((\log_2 x)^{1+\varepsilon}) \tag{1.3}$$

and

$$y \leq x/\exp((\log_2 x)^{1+\varepsilon}). \tag{1.4}$$

Then, as $x \to \infty$,

$$\frac{1}{x}L(x,y) \leq \begin{cases} \mathscr{L}(x/y)^{-1+o(1)} & \text{if } y \geq \mathscr{L}(x)^2, \\ \mathscr{L}(x,y)^{-1+o(1)} & \text{otherwise.} \end{cases}$$

Furthermore, under a plausible hypothesis on powersmooth shifted primes (Hypothesis U *below*), *equality holds in both cases.*

Some examples of Theorem 1.1 are recorded in Table 1.

While $L(x,y)$ does not seem to have been studied previously in the literature, a closely related quantity appears in Theorem 5 of [10], by Friedlander, Pomerance, and Shparlinski. It is shown there that for all large x and y with $y \geq \exp((\log_2 x)^3)$,

$$\#\{n \leq x : \lambda(n) \leq ny^{-1}\} \leq x\exp(-0.69(\log y \log\log y)^{1/3}). \tag{1.5}$$

We can improve this by our methods. Note that the left-hand side of (1.5) is majorized by $L(x, xy^{-1})$. We show in Proposition 7.1 that $L(x, xy^{-1}) \leq x\mathscr{L}(y)^{-1+o(1)}$ whenever $x \to \infty$ and $\exp((\log_2 x)^{1+\varepsilon}) \leq y \leq x/100$.

The quoted normal order theorem of Erdős–Pomerance–Schmutz implies that asymptotically 100% of $n \leq x$ have $\lambda(n) < x\exp(-(1+o(1))\log_2 x \log_3 x)$. So one cannot hope to obtain a nontrivial upper bound on $L(x,y)$ unless y is a bit smaller than $\approx x/\exp(\log_2 x \log_3 x)$. This makes our assumption (1.4) seem fairly natural. Similarly, (1.2) shows that the only way one can have

$\lambda(n) \leq \exp(\log_2 x \log_3 x)$ is if n itself is very small (e.g., we must have $n < \exp((\log x)^{0.7})$). This motivates assuming a condition such as (1.3).

We now explain the hypothesis under which the upper bounds in Theorem 1.1 are sharp. Let $P^+(n)$ (respectively, $P^*(n)$) denote the largest prime (resp., prime power) dividing n, setting $P^+(1) = P^*(1) = 1$. We say n is y-smooth (resp., y-powersmooth) if $P^+(n) \leq y$ (resp., $P^*(n) \leq y$). The count of y-smooth (resp., y-powersmooth) $n \leq x$ is denoted $\Psi(x, y)$ (resp., $\Psi^*(x, y)$).

Fix $\varepsilon > 0$. It is known that whenever x, y, and $u := \frac{\log x}{\log y}$ tend to infinity, with $y \geq (\log x)^{1+\varepsilon}$,

$$x \exp(-(1 + o(1))u \log u) \leq \Psi^*(x, y) \leq \Psi(x, y) \leq x \exp(-(1 + o(1))u \log u).$$

That $\Psi(x, y) = x \exp(-(1 + o(1))u \log u)$ throughout this range is a consequence of work of de Bruijn [4, 6] and Erdős–Canfield–Pomerance [2]. To deduce the claimed lower bound on $\Psi^*(x, y)$, one can then appeal to work of Naimi [17], which gives that the count of *squarefree* smooth $n \leq x$ is within a factor of $\exp(o(u \log u))$ of $\Psi(x, y)$ in this regime of x and y.

Let $\Pi^*(x, y)$ denote the corresponding count of powersmooth shifted primes $p - 1$; that is,

$$\Pi^*(x, y) := \#\{p \leq x : P^*(p - 1) \leq y\}.$$

The heuristic principle that shifted primes behave like random integers of the same size (up to local considerations) suggests that $\Psi^*(x, y)/x \approx \Pi^*(x, y)/\pi(x)$ in a wide range of x and y. We will prove lower bounds matching the upper bounds of Theorem 1.1 conditional on the following precise form of this hypothesis.

Hypothesis U. *Fix $\varepsilon > 0$. Whenever x, y, and $u := \frac{\log x}{\log y}$ tend to infinity with $y \geq (\log x)^{1+\varepsilon}$, we have*

$$\Pi^*(x, y) = \pi(x) \exp(-(1 + o(1))u \log u).$$

(The "U" is taken from "ultrafriable," a term sometimes preferred over "powersmooth".) Conjectures of a similar sort were introduced by Pomerance (e.g., [21–24]) to study pseudoprimes and the value-distribution of Euler's totient function; see also [1, 18, 19]. The upper bound implicit in Hypothesis U is known (it follows, for instance, from the results quoted above on $\Psi(x, y)$ together with Theorem 1 of [25]). Unfortunately, our applications require *lower* bounds on $\Pi^*(x, y)$.

By definition, $\lambda(n)$ is the maximal possible order of an element of $(\mathbb{Z}/n\mathbb{Z})^\times$. Thus, for every odd integer n, the order $l(n)$ (say) of 2 modulo n divides $\lambda(n)$. It is natural to ask whether our results have any implications for the distribution of small values of $l(n)$.[1]

It is known that all but $o(x)$ odd integers $n \leq x$ satisfy $l(n) > x^{1/2}$. Furthermore, $\frac{1}{2}$ marks the boundary of our current knowledge: We do not know the same result if the exponent $\frac{1}{2}$ is replaced by a larger constant. (But see Theorem 1 of [13] for an improvement of $\frac{1}{2}$ by "an arbitrary $o(1)$," as well as a discussion of what is known under the Generalized Riemann Hypothesis.) The following corollary to Theorem 1.1 gives a strong upper bound on solutions to $l(n) \leq x^\beta$ once β dips appreciably below $\frac{1}{2}$.

Corollary 1.2. *Fix $\delta > 0$. For all x sufficiently large in terms of δ,*

$$\#\{\text{odd } n \leq x : l(n) \leq x^\beta\} \leq x/\mathscr{L}(x)^{\frac{1}{2}-\beta-\delta}$$

---

[1] With minor changes, everything we do for $l(n)$ carries over with 2 replaced by an arbitrary fixed $b \notin \{0, \pm 1\}$, where of course we now impose the condition $\gcd(n, b) = 1$.

uniformly in $\beta \geq 0$.

Corollary 1.2 becomes trivial when $\beta \geq \frac{1}{2}$. At the endpoint $\beta = \frac{1}{2}$, we have no nontrivial estimates of comparable strength. In fact, at present we cannot prove that there are $O(x/(\log x)^2)$ *primes* $p \leq x$ with $l(p) \leq x^{1/2}$ — even permitting ourselves the luxury of assuming the Generalized Riemann Hypothesis!

Notwithstanding our current ignorance, it seems likely the "correct" version of Corollary 1.2 has $1-\beta$ in place of $\frac{1}{2}-\beta$ in the exponent of $\mathscr{L}(x)$. (See the remark concluding §8.) Conditional on Hypothesis U, this would be best possible in the following sense: small modifications to the proof of Theorem 1.1 show that, for fixed $\beta \in (0,1)$ and $x \to \infty$, there are at least $x/\mathscr{L}(x)^{1-\beta+o(1)}$ odd integers $n \leq x$ with $\lambda(n) \leq x^{\beta}$. All such n have $l(n) \leq x^{\beta}$ automatically.

Notation. Most of our notation is familiar. For instance, $\omega(n) = \sum_{p \mid n} 1$ and $\Omega(n) = \sum_{p^k \| n} k$, where here and below, p always denotes a prime. Perhaps a little less standard are $P^+(n)$ for the largest prime factor of n (with $P^+(1) = 1$) and $P^-(n)$ for the least prime factor of n (with $P^-(1) = \infty$). We write $\mathrm{rad}(n)$ for the radical of n, meaning the largest squarefree divisor of n.

2. Overview

We will give separate arguments for the rigorous upper bounds and conditional lower bounds, in each of the two ranges of y:

- (Upper bound for small y) In §3, we establish that $L(x,y) \leq x\mathscr{L}(x,y)^{-1+o(1)}$ when $\exp((\log_2 x)^{1+\varepsilon}) \leq y \leq x^{1/\log_2 x}$ and $x \to \infty$ (Proposition 3.2).
- (Lower bound for small y) In §4, we assume Hypothesis U and show, in Proposition 4.1, that $L(x,y) \geq x\mathscr{L}(x,y)^{-1+o(1)}$ whenever $x \geq y \geq \exp((\log_2 x)^{1+\varepsilon})$ and $x \to \infty$.
- (Lower bound for large y) In §5, we assume Hypothesis U and show, in Proposition 5.1, that $L(x,y) \geq x\mathscr{L}(x/y)^{-1+o(1)}$ when $y \geq \mathscr{L}(x)^2$ and $x/y \to \infty$.
- (Upper bound for large y) In §§6–7, we show that $L(x,y) \leq x\mathscr{L}(x/y)^{-1+o(1)}$ whenever $x \to \infty$ and $100 \leq y \leq x/\exp((\log_2 x)^{1+\varepsilon})$ (Proposition 7.1).

The attentive reader will notice that together these results *almost* cover all of the assertions of Theorem 1.1. However, if $x^{1/\log_2 x} < y < \mathscr{L}(x)^2$, we are claiming in Theorem 1.1 that $L(x,y) \leq x\mathscr{L}(x,y)^{-1+o(1)}$, while this range is not included in Proposition 3.2. In fact, this is no problem at all: For these values of y, we have $\log \mathscr{L}(x,y) \sim \log \mathscr{L}(x) \sim \log \mathscr{L}(x/y)$, and so our "upper bound for large y" (Proposition 7.1) furnishes the desired upper bound.

The first three bulleted components will come to us by adapting arguments of Erdős and Pomerance, originally applied to study (related, but different) questions concerning the λ and ϕ-functions.

The chief novelty of the paper is the proof of the upper bound for large y. (The cases when $x/y = \exp((\log_2 x)^{O(1)})$ require particularly delicate arguments.) This requires revisiting and reworking methods from [19] and its sequel paper [20], used to investigate popular subsets for Euler's ϕ-function and large values of the factorization counting function. Preliminary results are collected in §6, after which the proof of Proposition 7.1 is detailed in §7. It seems plausible that some of the new results of §6 will find other applications.

Corollary 1.2 is proved in §8. The strategy there is inspired by the proof of Theorem 1 in [13].

3. UPPER BOUND FOR SMALL y

The following consequence of the prime number theorem appears, in stronger form, as [15, Lemma 7.4].

Lemma 3.1. *Let $0 < c < 1$, and let T be a positive real number for which $T^{1-c} \geq \exp(4)$. Then*

$$\sum_{p \leq T} \frac{1}{p^c} \ll \frac{T^{1-c}}{\log(T^{1-c})} + \log\frac{1}{1-c},$$

where the implied constant is absolute.

Proposition 3.2. *Fix $\varepsilon > 0$. If $x, y \to \infty$ with*

$$\exp((\log_2 x)^{1+\varepsilon}) \leq y \leq x^{1/\log_2 x},$$

then

$$L(x,y) \leq x \exp\left(-(1+o(1))\frac{\log x \log_3 x}{\log_2 y}\right). \tag{3.1}$$

Proof. We give a pointwise upper bound. Put $\ell(x,m) = \#\{n \leq x : \lambda(n) = m\}$, so that $L(x,y) = \sum_{m \leq y} \ell(x,m)$. We will show that $\ell(x,m)$ is bounded above by the expression on the right of (3.1), uniformly for positive integers $m \leq y$. This suffices to prove the proposition. Indeed,

$$\log y \ll \frac{\log x}{\log_2 x}, \quad \text{while} \quad \frac{\log x \log_3 x}{\log_2 y} \gg \frac{\log x \log_3 x}{\log_2 x}.$$

Hence, $y = \exp(o(\log x \log_3 x / \log_2 y))$, and

$$\begin{aligned} L(x,y) &\leq y \max_{m \leq y} \ell(x,m) \\ &= x \exp\left(-(1+o(1))\frac{\log x \log_3 x}{\log_2 y}\right), \end{aligned}$$

as desired.

To bound $\ell(x,m)$, we lean on an idea of Pomerance (see the proof of [23, Lemma 5.2]). If $\lambda(n) = m$, then $p - 1 \mid m$ for each prime $p \mid n$. Hence, for every $c > 0$, we have (Rankin's trick)

$$\ell(x,m) \leq x^c \sum_{\substack{n \leq x \\ p \mid n \Rightarrow p-1 \mid m}} n^{-c} \leq x^c \prod_{p\colon p-1 \mid m} \left(1 + \frac{1}{p^c} + \frac{1}{p^{2c}} + \dots\right).$$

Below, we will select a value of $c \gg 1$. (Here we mean that c is bounded below by a positive constant depending only on ε.) Assuming this lower bound on c for the time being, $1/p^c + 1/p^{2c} + \dots \leq p^{-c}(1 - 1/2^c)^{-1} \ll p^{-c}$, so that

$$\prod_{p\colon p-1 \mid m} \left(1 + \frac{1}{p^c} + \frac{1}{p^{2c}} + \dots\right) \leq \exp\left(\sum_{p\colon p-1 \mid m} \frac{1}{p^c} + \frac{1}{p^{2c}} + \dots\right) \leq \exp\left(O\left(\sum_{p\colon p-1 \mid m} \frac{1}{p^c}\right)\right).$$

Furthermore,

$$\sum_{p\colon p-1 \mid m} \frac{1}{p^c} \leq \sum_{p\colon p-1 \mid m} \frac{1}{(p-1)^c} \leq \sum_{d \mid m} \frac{1}{d^c} \leq \prod_{p \mid m} \left(1 + \frac{1}{p^c} + \frac{1}{p^{2c}} + \dots\right) \leq \exp\left(O\left(\sum_{p \mid m} \frac{1}{p^c}\right)\right).$$

Collecting estimates, we see that for certain constants $C_1, C_2 > 0$ (depending only on ε),

$$\ell(x,m) \le x^c \exp\left(C_1 \exp\left(C_2 \sum_{p \mid m} \frac{1}{p^c}\right)\right). \tag{3.2}$$

The sum over primes p dividing m is bounded above by the corresponding sum over the first $\omega(m)$ primes, which (as $m \le y$) is in turn bounded above by the sum over the primes not exceeding $2\log y$ (once y is large enough). This can be estimated by Lemma 3.1. We choose c so that $(2\log y)^{1-c} = \log_2 x$, i.e.,

$$c = 1 - \frac{\log_3 x}{\log(2\log y)}.$$

Then

$$\sum_{p \mid m} \frac{1}{p^c} \ll \frac{(2\log y)^{1-c}}{\log((2\log y)^{1-c})} + \log\frac{1}{1-c} \ll \frac{\log_2 x}{\log_3 x}.$$

Recalling that $y \ge \exp((\log_2 x)^{1+\varepsilon})$, we have that $c > \varepsilon(1+\varepsilon)^{-1}$, vindicating our previous assumption that $c \gg 1$. Plugging this choice of c into (3.2) gives that

$$\begin{aligned}\ell(x,m) &\le x \exp\left(-\frac{\log x \log_3 x}{\log(2\log y)}\right) \exp\left(O((\log x)^{o(1)})\right)\\ &= x \exp\left(-(1+o(1))\frac{\log x \log_3 x}{\log_2 y}\right),\end{aligned}$$

as needed. ☐

4. Lower bound for small y

Proposition 4.1. *Assume Hypothesis U. Fix $\varepsilon > 0$. If $x, y \to \infty$ with*

$$x \ge y \ge \exp((\log_2 x)^{1+\varepsilon}),$$

then

$$L(x,y) \ge x \exp\left(-(1+o(1))\frac{\log x \log_3 x}{\log_2 y}\right). \tag{4.1}$$

Remark. It will emerge in the proof that the lower bound (4.1) holds even if we restrict $L(x,y)$ to include only n all of whose prime factors are bounded above by $\exp((\log_2 x)^2)$. This observation will be useful momentarily.

Proof. We can (and will) assume that $0 < \varepsilon < 1$. We follow the arguments of Erdős [7] and Pomerance [21, 23] used to construct "popular" values of Euler's ϕ-function. Put

$$X := \exp(\log_2 x \log_2 y), \quad Y := \frac{1}{2}\log y, \quad k := \left\lfloor \frac{\log x}{\log X} \right\rfloor.$$

We let S be the set of squarefree numbers n constructed as products of k distinct primes from the set

$$\mathcal{P} := \{p \le X : P^*(p-1) \le Y\}.$$

If $n \in S$, then $n \le X^k \le x$. Furthermore, for large x, y,

$$\lambda(n) = \operatorname*{lcm}_{p \mid n}[p-1] \le \operatorname{lcm}[1, 2, \dots, \lfloor Y \rfloor] < \exp(2Y) = y.$$

Therefore, it suffices to bound $\#S$ from below by the expression on the right-hand side of (4.1).

Putting $U := \frac{\log X}{\log Y}$, we have that $U = (1+o(1)) \log_2 x$. Moreover, for large x and y, we have $Y/(\log Y)^2 = \frac{1}{2}\log y/(\log(\frac{1}{2}\log y))^2 > (\log_2 x)^{1+\frac{1}{2}\varepsilon}$, so that

$$Y > (\log_2 x)^{1+\frac{1}{2}\varepsilon}(\log Y)^2 > (\log_2 x \log_2 y)^{1+\frac{1}{2}\varepsilon} = (\log X)^{1+\frac{1}{2}\varepsilon}.$$

Therefore, we may apply Hypothesis U to deduce that

$$\begin{aligned}\#\mathcal{P} &= \pi(X)\exp\left(-(1+o(1))U\log U\right)\\ &= X\exp(-(1+o(1))\log_2 x\log_3 x). \qquad (4.2)\end{aligned}$$

We proceed to estimate $\#S = \binom{\#\mathcal{P}}{k}$. By assumption, $\log_2 y \geq (1+\varepsilon)\log_3 x$, so that $X \geq \exp((1+\varepsilon)\log_2 x\log_3 x)$. Thus, for large x, y,

$$\#\mathcal{P} > \exp\left(\frac{\varepsilon}{2}\log_2 x\log_3 x\right) > \log x > k,$$

and so in estimating $\#S$ we may invoke the inequality $\binom{A}{B} \geq \left(\frac{A}{B}\right)^B$, valid for all pairs of integers $A \geq B \geq 1$. Referring back to the definition of k, we see that

$$k^k = \exp\left(k\log k\right) \leq \exp\left(\frac{\log x}{\log X}\log_2 x\right) = \exp\left(\frac{\log x}{\log_2 y}\right) = \exp\left(o\left(\frac{\log x\log_3 x}{\log_2 y}\right)\right).$$

Furthermore, the estimate (4.2) for $\#\mathcal{P}$ implies that

$$\begin{aligned}(\#\mathcal{P})^k &= X^k\exp(-(1+o(1))k\log_2 x\log_3 x)\\ &\geq \frac{x}{X}\exp\left(-(1+o(1))\frac{\log x\log_3 x}{\log_2 y}\right)\\ &= x\exp\left(-(1+o(1))\frac{\log x\log_3 x}{\log_2 y}\right).\end{aligned}$$

We conclude that $\#S \geq (\#\mathcal{P})^k/k^k = x\exp(-(1+o(1))\log x\log_3 x/\log_2 y)$, as claimed. ☐

5. Lower bound for large y

Proposition 5.1. *Assume Hypothesis U. Whenever $x, y \to \infty$ with*

$$y \geq \mathscr{L}(x)^2 \quad \textit{and} \quad \frac{x}{y} \to \infty,$$

we have

$$L(x,y) \geq x/\mathscr{L}(x/y)^{1+o(1)}.$$

(Here $o(1)$ means a quantity tending to 0 as $x/y \to \infty$, under the assumption that $y \geq \mathscr{L}(x)^2$.)

Proof. Below, we say that a statement holds "eventually" if it holds whenever x/y is sufficiently large, subject to $y \geq \mathscr{L}(x)^2$ (and $x, y \geq 100$). Put

$$A := \frac{y}{\mathscr{L}(x/y)}, \quad B := \frac{x}{y}\mathscr{L}(x/y).$$

Let S be the collection of all ordered pairs (a,b), where

$$a \leq A \quad \text{with} \quad P^-(a) > \exp((\log_2 B)^2), \qquad (5.1)$$

and

$$b \le B \quad \text{with} \quad P^+(b) \le \exp((\log_2 B)^2) \text{ and } \lambda(b) \le \mathscr{L}(x/y). \tag{5.2}$$

If $n = ab$ for some $(a,b) \in S$, then $n \le x$ and

$$\lambda(n) = \lambda(ab) \le a\lambda(b) \le A \cdot \mathscr{L}(x/y) = y.$$

The restrictions on $P^-(a)$ and $P^+(b)$ guarantee that the map $(a,b) \mapsto ab$ is one-to-one. So the proposition will be proved if we show that $\#S \ge x/\mathscr{L}(x/y)^{1+o(1)}$.

Our assumption that $y \ge \mathscr{L}(x)^2$ implies that, eventually,

$$\frac{y}{\mathscr{L}(x/y)} > \mathscr{L}(x/y), \quad \text{which in turn yields that} \quad \exp((\log_2 B)^2) = \left(\frac{y}{\mathscr{L}(x/y)}\right)^{o(1)}.$$

It now follows from Brun's sieve that the number of a satisfying (5.1) is $\gg A/(\log_2 B)^2$. Hence, the number of choices for a is at least $A \cdot \mathscr{L}(x/y)^{o(1)}$. On the other hand, by Proposition 4.1 and the remark following, the number of choices of b is at least $B \cdot \mathscr{L}(x/y)^{-1+o(1)}$ (keeping in mind that $B = (x/y)^{1+o(1)}$). Hence, $\#S \ge AB \cdot \mathscr{L}(x/y)^{-1+o(1)} = x\mathscr{L}(x/y)^{-1+o(1)}$, as desired. ☐

6. UPPER BOUND FOR LARGE y: PREPARATION

In this section, we collect several preliminary results needed to treat this range of y. We begin with a crude form of a result of de Bruijn.

Lemma 6.1. *For each fixed $\delta > 0$ and all large x, we have $\sum_{n \le x} 1/\mathrm{rad}(n) < x^\delta$.*

Remark. According to Theorem 1 of de Bruijn's paper [5], we in fact have $\sum_{n\le x} 1/\mathrm{rad}(n) = \exp((1+o(1))\sqrt{\frac{8\log x}{\log\log x}})$, as $x \to \infty$.

Proof. Observe that for all $x \ge 1$,

$$\sum_{n \le x} \mathrm{rad}(n)^{-1} \le x^{\delta/2} \sum_{n \ge 1} \mathrm{rad}(n)^{-1} n^{-\delta/2} = x^{\delta/2} \prod_p (1 + p^{-1-\frac{1}{2}\delta} + p^{-1-\delta} + p^{-1-\frac{3}{2}\delta} + \dots) \ll x^{\delta/2}. \quad \square$$

6.1. **Factorizations and compositions.** By a factorization, we mean a finite multiset of integers all at least 2. We denote the factorization consisting of the integers $d_1, \dots, d_k$ as $\langle d_1, \dots, d_k \rangle$, and we say that $\langle d_1, \dots, d_k \rangle$ is a factorization of the integer $d_1 \cdots d_k$. We let $f(n)$ denote the number of factorizations of the positive integer n (where, by convention, $f(1) = 1$). For example, the factorizations of 18 are

$$\langle 18 \rangle, \quad \langle 2, 9 \rangle, \quad \langle 3, 6 \rangle, \quad \langle 2, 3, 3 \rangle,$$

and so $f(18) = 4$. (What we call a factorization is sometimes referred to as a multiplicative partition.)

The following proposition is the main result of [20] and appears as that paper's Theorem 1.1. (With the ϕ-preimage counting function $\#\phi^{-1}(n)$ in place of $f(n)$, this appears earlier as the main theorem of [19].)

Proposition 6.2. *Fix $\delta > 0$ and $\beta \in (0,1)$. There is an $x_0 = x_0(\delta,\beta)$ for which the following holds. If $x > x_0$ and $S \subseteq [1,x]$ is a set of integers with $\#S \le x^{1-\beta}$, then*

$$\sum_{n\in S} f(n) \le x/\mathscr{L}(x)^{\beta-\delta}. \tag{6.1}$$

We require a variant of Proposition 6.2 with some uniformity in β, with factorizations replaced by "multiplicative compositions with not too many parts."

By a multiplicative composition of n, we mean a finite sequence of integers, all at least 2, whose product is n. (This is sometimes called an ordered factorization.) We let $g(n)$ denote the total number of multiplicative compositions of n, setting $g(1) = 1$, and we let $g_w(n)$ denote the number of multiplicative compositions of n into w parts. (We define $g_0(1) = 1$ and $g_0(n) = 0$ for $n > 1$.) For example, the multiplicative compositions of 18 are

$$[18], \quad [2,9], \quad [9,2], \quad [3,6], \quad [6,3], \quad [2,3,3], \quad [3,2,3], \quad [3,3,2],$$

so that $g_1(18) = 1, g_2(18) = 4, g_3(18) = 3$, and $g(18) = 8$. It will be useful to note that, trivially, $g_w(n) \le \tau_w(n)$ where τ_w is the w-fold divisor function.

Let $x \ge 100$. We say that the integer w belongs to the critical range (with respect to x) if

$$1 \le w \le \frac{\log x}{(\log_2 x)^2}(\log_3 x)^2. \tag{K}$$

Proposition 6.3. *Fix $\delta > 0$. There is an $x_0 = x_0(\delta)$ for which the following holds. If $x > x_0$, $\beta \in [\frac{1}{1000}, 1]$, and $S \subseteq [1,x]$ is a set of integers with $\#S \le x^{1-\beta}$, then*

$$\sum_{n\in S} g_w(n) \le x/\mathscr{L}(x)^{\beta-\delta}$$

for all integers w belonging to the critical range.

Here $\frac{1}{1000}$ was chosen for definiteness; it may be replaced with any fixed positive real number.

We prove Proposition 6.3 by modifying the method used to establish [20, Theorem 1.1]. The following two lemmas are analogues of [20, Lemma 2.1, Lemma 2.2]. Below, $\Omega_{>z}(n) := \sum_{p^e \| n,\ p>z} e$.

Lemma 6.4. *Let*

$$z = \exp((\log_2 x)^{1/2}).$$

Fix any $\eta \in (0,1)$, and let

$$A = (\log_2 x)^{1-\eta}.$$

As $x \to \infty$,

$$\sum_{n\le x} A^{\Omega_{>z}(n)} g_w(n) \le x\mathscr{L}(x)^{o(1)},$$

where the decay of the $o(1)$ term to 0 is uniform for w in the critical range.

Proof. We once again apply Rankin's trick. For any choice of $c > 1$,

$$\sum_{n\le x} A^{\Omega_{>z}(n)} g_w(n) \le x^c \sum_{n\ge1} \frac{A^{\Omega_{>z}(n)} g_w(n)}{n^c} = x^c \left(\sum_{d\ge2} \frac{A^{\Omega_{>z}(d)}}{d^c}\right)^w.$$

This exact sum on d appears already in the proof of Lemma 2.1 of [20], where it is shown that

$$\sum_{d\ge 2}\frac{A^{\Omega_{>z}(d)}}{d^c} \ll \log z + \frac{\Gamma(A)}{(c-1)^A},$$

uniformly for $c \in (1,2)$.

We now select c in order that

$$c-1 = \frac{Aw}{\log x}.$$

Let

$$W = \frac{\log x}{(\log_2 x)^2}(\log_3 x)^2 \tag{6.2}$$

be the upper limit of the critical range (K). (Note that $1 < c \le 1 + \frac{AW}{\log x} < 2$ for all large x.) Then

$$x^c = x\exp(Aw) \le x\exp(AW) = x\mathscr{L}(x)^{o(1)}.$$

Furthermore, for a certain large positive constant C_4,

$$\begin{aligned}\left(\sum_{d\ge 2}\frac{A^{\Omega_{>z}(d)}}{d^c}\right)^w &\le C_4^w\left(\log z + \frac{\Gamma(A)}{(c-1)^A}\right)^w\\ &\le (2C_4)^w\left((\log z)^w + \frac{\Gamma(A)^w}{(c-1)^{Aw}}\right).\end{aligned}$$

Here we have

$$\begin{aligned}(2C_4)^w &\le \exp(O(W)) = \mathscr{L}(x)^{o(1)},\\ (\log z)^w &\le \exp(O(W\log_3 x)) = \mathscr{L}(x)^{o(1)},\\ \Gamma(A)^w &\le \exp(O(AW\log A)) = \mathscr{L}(x)^{o(1)},\end{aligned}$$

and

$$\begin{aligned}(c-1)^{-Aw} = \left(\frac{\log x}{Aw}\right)^{Aw} &\le \left(\frac{\log x}{AW}\right)^{AW}\\ &\le \exp(O(AW\log_3 x)) = \mathscr{L}(x)^{o(1)}.\end{aligned}$$

(In the first line of the last display, we use that $t \mapsto (\frac{\log x}{t})^t$ is increasing for $t \le \frac{1}{\mathrm{e}}\log x$, while $AW \le \frac{1}{\mathrm{e}}\log x$.) Collecting estimates completes the proof. □

Lemma 6.5. *As $x\to\infty$,*

$$\sum_{n\le x}(3/2)^{\Omega(n)}g_w(n) \le x\mathscr{L}(x)^{o(1)},$$

where the decay of the $o(1)$ term to 0 is uniform for w in the critical range.

Proof. Put $S(T) := \sum_{m\le T}(3/2)^{\Omega(m)}$. Then $S(T) \le \sum_{m\le T}2^{\Omega(m)} \ll T(\log T)^2$ for all $T\ge 2$ (for the last estimate, see [12] or [15, Exercise 15(c), p. 42]). Thus, uniformly for $c\in(1,2)$,

$$\sum_{d\ge 2}\frac{(3/2)^{\Omega(d)}}{d^c} \ll \int_2^\infty \frac{(\log t)^2}{t^c}\,\mathrm{d}t < \int_1^\infty \frac{(\log t)^2}{t^c}\,\mathrm{d}t = \frac{1}{(c-1)^3}\int_0^\infty s^2\mathrm{e}^{-s}\,\mathrm{d}s = \frac{2}{(c-1)^3}.$$

(Here we have made the substitution $t = \mathrm{e}^{s/(c-1)}$.) Therefore, for w in the critical range and $c \in (1,2)$,

$$\sum_{n\le x}(3/2)^{\Omega(n)}g_w(n) \le x^c \sum_{n\ge 1}\frac{(3/2)^{\Omega(n)}g_w(n)}{n^c} = x^c\left(\sum_{d\ge 2}\frac{(3/2)^{\Omega(d)}}{d^c}\right)^w \le x^c C_5^w (c-1)^{-3w},$$

where C_5 is a certain large (positive) absolute constant.

Let W be as in (6.2). We apply the upper bound of the last paragraph with c chosen to satisfy $c - 1 = \frac{3w}{\log x}$. Then $x^c \le x\exp(3W) = x\mathscr{L}(x)^{o(1)}$ and $C_5^w \le C_5^W = \mathscr{L}(x)^{o(1)}$. Furthermore,

$$(c-1)^{-3w} = \left(\frac{\log x}{3w}\right)^{3w} \le \left(\frac{\log x}{3W}\right)^{3W} \le \exp(O(W\log_3 x)) = \mathscr{L}(x)^{o(1)}.$$

Again, collect estimates. □

We can now give the proof of Proposition 6.3.

Proof of Proposition 6.3. We can and will assume $\delta \in (0,1)$. We begin by fixing $\eta := \frac{1}{4}\delta \in (0,1)$; this is the value of η with which we will apply Lemma 6.4.

Let us consider the contribution to $\sum_{n\in S} g_w(n)$ made by n with $\Omega_{>z}(n) > (1-\eta)\beta\frac{\log x}{\log_2 x}$. By Lemma 6.4, for all w in the critical range,

$$A^{(1-\eta)\beta\log x/\log_2 x}\sum_{\substack{n\in S\\ \Omega_{>z}(n)>(1-\eta)\beta\frac{\log x}{\log_2 x}}} g_w(n) \le \sum_{n\le x} A^{\Omega_{>z}(n)}g_w(n) \le x\mathscr{L}(x)^{o(1)}.$$

Here and below, $o(1)$ means an expression that decays to 0 as $x\to\infty$, uniformly in all parameters *except* possibly the fixed quantity δ. Rearranging,

$$\sum_{\substack{n\in S\\ \Omega_{>z}(n)>(1-\eta)\beta\frac{\log x}{\log_2 x}}} g_w(n) \le x\mathscr{L}(x)^{o(1)}\cdot A^{-(1-\eta)\beta\log x/\log_2 x} = x/\mathscr{L}(x)^{(1-\eta)^2\beta+o(1)}.$$

As

$$(1-\eta)^2\beta > \beta - 2\eta\beta = \beta - \frac{1}{2}\delta\beta \ge \beta - \frac{1}{2}\delta, \tag{6.3}$$

it follows that

$$\sum_{\substack{n\in S\\ \Omega_{>z}(n)>(1-\eta)\beta\frac{\log x}{\log_2 x}}} g_w(n) < \frac{1}{2}x/\mathscr{L}(x)^{\beta-\delta}$$

for all large enough x (here and below, "large enough" means "with respect to a threshold depending only on the fixed parameter δ").

Similarly, Lemma 6.5 implies that

$$\sum_{\substack{n\in S\\ \Omega(n)>\log x/(\log_2 x)^{2/3}}} g_w(n) \le x\mathscr{L}(x)^{o(1)}\cdot(2/3)^{\log x/(\log_2 x)^{2/3}},$$

for all w in the critical range. Here the right-hand expression is $o(x/\mathscr{L}(x)^{\beta-\delta})$.

Call the positive integer $n \le x$ admissible if

$$\Omega_{>z}(n) \le (1-\eta)\beta\frac{\log x}{\log_2 x} \quad \text{and} \quad \Omega(n) \le \frac{\log x}{(\log_2 x)^{2/3}}.$$

To finish off the proposition, it is enough to show that (for x large, and w in the critical range) the sum of $g_w(n)$, taken over admissible $n \in S$, is smaller than $\frac{1}{3}x/\mathscr{L}(x)^{\beta-\delta}$. In fact, we will prove that this sum is bounded by the much smaller quantity $x^{1-\frac{1}{2}\beta\eta}$.

Suppose $n \in S$ is admissible, and write $n = n_0 n_1$, where n_0 is z-smooth and every prime factor of n_1 exceeds z. Then $g_w(n) \le \tau_w(n) = \tau_w(n_0)\tau_w(n_1)$. Since n_0 is z-smooth and $\Omega(n) \le \log x/(\log_2 x)^{2/3}$, we have that

$$n_0 \le z^{\Omega(n)} \le \exp(\log x/(\log_2 x)^{1/6}) = x^{o(1)}.$$

Hence (uniformly for w in the critical range),

$$\tau_w(n_0) \le n_0^2 \sum_m \frac{\tau_w(m)}{m^2} = n_0^2 \cdot \zeta(2)^w < 2^w n_0^2 = x^{o(1)}.$$

Furthermore (again for w in the critical range),

$$\tau_w(n_1) \le w^{\Omega(n_1)} = w^{\Omega_{>z}(n)} \le w^{(1-\eta)\beta\log x/\log_2 x} \le x^{(1-\eta)\beta+o(1)}.$$

Recalling that $\#S \le x^{1-\beta}$, we conclude that

$$\sum_{\substack{n\in S\\ n \text{ admissible}}} g_w(n) \le x^{(1-\eta)\beta+o(1)}\#S \le x^{1-\beta\eta+o(1)},$$

which is indeed smaller than $x^{1-\frac{1}{2}\beta\eta}$ for large enough x. ☐

6.2. **Euler's function.** Our proof requires precise estimates for the frequency with which $\phi(n)$ possesses a given divisor d. The next lemma is a refinement, in terms of multiplicative compositions, of [19, Lemma 7] (which was expressed in terms of factorizations).

Let $\mathbf{d} = \langle d_1, \dots, d_k\rangle$ be a factorization with distinct parts $d_1', \dots, d_\ell'$, appearing with respective multiplicities $m_1, \dots, m_\ell$. The symmetry constant of $\mathbf{d}$, denoted $\mathrm{sym}(\mathbf{d})$, is the product $m_1! \cdots m_\ell!$.

Lemma 6.6. *There is an absolute constant $C_\phi > 0$ for which the following holds: Let $x \ge 3$, and let $W > 0$. For each positive integer d, the number of squarefree positive integers $n \le x$ for which*

$$\omega(n) \le W \quad \text{and} \quad d \mid \phi(n)$$

is at most

$$\frac{x}{d}\sum_{0\le w\le W}\frac{(C_\phi(\log_2 x)(\log_2(3d)))^w}{w!}g_w(d).$$

Proof. We may assume that $1 < d \le x$. Let $\mathscr{F}(d)$ denote the set of factorizations of d. If $\mathbf{d} \in \mathscr{F}(d)$, we say that the positive integer n corresponds to $\mathbf{d}$ if, writing $\mathbf{d} = \langle d_1, \dots, d_k\rangle$, there are distinct primes $p_1, \dots, p_k$ dividing n with each $p_i \equiv 1 \pmod{d_i}$.

Suppose n is squarefree and $d \mid \phi(n)$. Write $n = p_1 \cdots p_t$, where the p_i are distinct primes and $t = \omega(n) \le W$. Then $d \mid (p_1-1)\cdots(p_t-1)$. Hence, we can write $d = d_1 \cdots d_t$, where each $d_i \mid p_i - 1$. Reordering, we can assume that $d_i > 1$ precisely for $1 \le i \le w$. This shows: Whenever $d \mid \phi(n)$, the integer $n \le x$ corresponds to some $\mathbf{d} \in \mathscr{F}(d)$ of length at most W (namely, $\mathbf{d} = \langle d_1, \dots, d_w\rangle$).

Now take any $\mathbf{d} \in \mathscr{F}(d)$. Suppose $\mathbf{d}$ has length w, say $\mathbf{d} = \langle d_1, \dots, d_w \rangle$. Let $d'_1, \dots, d'_\ell$ be the distinct parts in $\mathbf{d}$, and let $m_1, \dots, m_\ell$ be their multiplicities (so that $m_1 + \dots + m_\ell = w$). Then the number of $n \le x$ corresponding to $\mathbf{d}$ is bounded above by

$$x \prod_{j=1}^{\ell} \frac{1}{m_j!} \Bigg(\sum_{\substack{p \le x \\ p \equiv 1 \pmod{d'_j}}} \frac{1}{p} \Bigg)^{m_j} \le x \prod_{j=1}^{\ell} \frac{1}{m_j!} \left(\frac{C_\phi (\log_2 x)(\log_2 (3d))}{d'_j} \right)^{m_j}$$

$$= \frac{x (C_\phi (\log_2 x)(\log_2 (3d)))^w}{d \operatorname{sym}(\mathbf{d})}.$$

(We use here that $\sum_{p \le x,\, p \equiv 1 \pmod{d'_j}} 1/p \ll \log_2 x/\phi(d'_j) \ll \log_2 x \log_2(3d'_j)/d'_j$, from the Brun–Titchmarsh inequality and the minimal order of Euler's function.) Letting $\mathbf{d}$ (resp. $\mathbf{D}$) run over all factorizations (resp. compositions) of d of length w,

$$\sum_{\mathbf{d}} \frac{1}{\operatorname{sym}(\mathbf{d})} = \frac{1}{w!} \sum_{\mathbf{d}} \frac{w!}{\operatorname{sym}(\mathbf{d})} = \frac{1}{w!} \sum_{\mathbf{D}} 1 = \frac{g_w(d)}{w!},$$

since each length w factorization $\mathbf{d}$ is induced by $w!/\operatorname{sym}(\mathbf{d})$ compositions $\mathbf{D}$. ("Induced" means "recovered by forgetting order.") Collecting estimates, the number of $n \le x$ corresponding to a length w element of $\mathscr{F}(d)$ is bounded above by

$$\frac{x}{d} g_w(d) \frac{(C_\phi (\log_2 x)(\log_2 (3d)))^w}{w!}.$$

The proof of Lemma 6.6 is completed by summing on nonnegative integers $w \le W$. ☐

7. UPPER BOUND FOR LARGE y: COMPLETION OF THE PROOF

Proposition 7.1. *Fix* $\varepsilon > 0$. *Suppose* $x \to \infty$ *and*

$$100 \le y \le x / \exp((\log_2 x)^{1+\varepsilon}). \tag{7.1}$$

Then

$$L(x, y) \le x \mathscr{L}(x/y)^{-1+o(1)}.$$

Proof. We start by reducing to the squarefree case. Suppose that under the same assumptions on x, y, the count of *squarefree* $n \le x$ with $\lambda(n) \le y$ is at most $x\mathscr{L}(x/y)^{-1+o(1)}$. We take an arbitrary $n \le x$ with $\lambda(n) \le y$ and write $n = n_0 n_1$, where n_0 is squarefull, n_1 is squarefree, and $\gcd(n_0, n_1) = 1$. For the sake of proving Proposition 7.1, we may assume that $n_0 \le \mathscr{L}(x/y)^2$, as only $O(x\mathscr{L}(x/y)^{-1})$ integers up to x are divisible by a squarefull number exceeding $\mathscr{L}(x/y)^2$. For each n_0, we count corresponding squarefree values of $n_1 \le x/n_0$. Certainly $\lambda(n_1) \le \lambda(n_0 n_1) \le y$. Under (7.1), we have that

$$\frac{x}{n_0 y} > \left(\frac{x}{y}\right)^{1/2} > \exp\left(\frac{1}{2} (\log\log x)^{1+\varepsilon}\right) > \exp\left((\log\log x)^{1+\frac{1}{2}\varepsilon}\right) \ge \exp\left((\log\log (x/n_0))^{1+\frac{1}{2}\varepsilon}\right),$$

so that

$$100 \le y \le \frac{x/n_0}{\exp((\log_2 (x/n_0))^{1+\frac{1}{2}\varepsilon})},$$

uniformly in our range of n_0. Thus, applying our squarefree version, the number of n_1 corresponding to a given n_0 is at most $x n_0^{-1} \mathscr{L}(x/n_0 y)^{-1+o(1)} = x n_0^{-1} \mathscr{L}(x/y)^{-1+o(1)}$. Summing on n_0 gives the proposition as originally stated.

We may reduce further to the case when $\lambda(n)$ has the same order of magnitude as y. That is, it suffices to prove the upper bound of the proposition for

$$L^*(x,y) := \#\{\text{squarefree } n \le x : \frac{1}{2}y < \lambda(n) \le y\}.$$

Indeed,

$$\#\{\text{squarefree } n \le x : \lambda(n) \le y\} \le L(x, x^{1/\log_2 x}) + \sum_{\substack{m \ge 0 \\ 2^{-m}y > x^{1/\log_2 x}}} L^*(x, 2^{-m}y),$$

while $L(x, x^{1/\log_2 x}) \le x\mathscr{L}(x)^{-1+o(1)}$ by Proposition 3.2. If we have the L^*-variant of Proposition 7.1, then $L^*(x, 2^{-m}y) \le x\mathscr{L}(x/y)^{-1+o(1)}$, uniformly in these m. We conclude by noting that there are $\ll \log y = \mathscr{L}(x/y)^{o(1)}$ values of m.

The rest of the proof is focused on proving this theorem about $L^*(x,y)$. More precisely, we show the following: Fix $\varepsilon \in (0,1)$ and $\delta \in (0, \frac{1}{10})$. If x is sufficiently large in terms of ε, δ, and x, y satisfy (7.1), then

$$L^*(x,y) \le x\mathscr{L}(x/y)^{12\delta - 1}.$$

Below, all estimates are made under the assumption that x is sufficiently large (and that (7.1) holds). We emphasize that "large" means "in terms of ε and δ" *only*; the largeness thresholds are uniform in all other parameters.

We begin by throwing away all n that do *not* satisfy

$$\omega(n) \le W, \quad \text{where} \quad W := \left\lfloor \frac{10}{\varepsilon} \frac{\log \frac{x}{y} \log_3 \frac{x}{y}}{(\log_2 \frac{x}{y})^2} \right\rfloor. \tag{7.2}$$

By a well-known theorem of Hardy and Ramanujan, the number of n we discard in this way is

$$\ll \frac{x}{\log x} \sum_{w > W} \frac{(\log_2 x + C_3)^{w-1}}{(w-1)!}.$$

(Here C_3 is a certain absolute constant.) As $\log \frac{x}{y} \ge (\log_2 x)^{1+\varepsilon}$, we have that $W \ge (\log_2 x)^{1+\frac{1}{2}\varepsilon}$ and that each term in the right-hand sum on w is at most half the previous. Thus,

$$\frac{x}{\log x} \sum_{w > W} \frac{(\log_2 x + C_3)^{w-1}}{(w-1)!} \le 2\frac{x}{\log x} \frac{(\log_2 x + C_3)^W}{W!} \le x\frac{(2\log_2 x)^W}{W!} \le x\left(\frac{2\mathrm{e}\log_2 x}{W}\right)^W.$$

Continuing, we observe that $W^{1-\frac{1}{4}\varepsilon} \ge 2\mathrm{e}\log_2 x$, and so

$$\left(\frac{2\mathrm{e}\log_2 x}{W}\right)^W = \exp\left(-W \log \frac{W}{2\mathrm{e}\log_2 x}\right) \le \exp\left(-\frac{1}{4}\varepsilon W \log W\right) < \mathscr{L}(x/y)^{-2}.$$

Thus, the number of n removed in this initial step is smaller than $x\mathscr{L}(x/y)^{-1}$.

Next, we place the integers $n \le x$ into dyadic intervals. For each $j \in \mathbb{Z}^+$, let

$$\mathcal{N}_j = (2^{-j}x, 2^{1-j}x].$$

At the cost of excluding $O(x\mathscr{L}(x/y)^{-1})$ values of $n \le x$, we can (and will) assume that $n \in \mathcal{N}_j$ where

$$2^{-j}x > x\mathscr{L}(x/y)^{-1}. \tag{7.3}$$

We continue by sorting the ratios $\frac{\phi(n)}{\lambda(n)}$ dyadically. Suppose $n \in \mathcal{N}_j$ and $\lambda(n) \in (y/2, y]$. Then

$$\frac{\phi(n)}{\lambda(n)} > \frac{\frac{1}{2}n/\log_2 n}{\lambda(n)} > 2^{-1-j}\frac{x}{y\log_2 x},$$

while

$$\frac{\phi(n)}{\lambda(n)} \le \frac{2^{1-j}x}{y/2} = 4 \cdot 2^{-j}\frac{x}{y}.$$

(In the lower bound, we use again the known minimal order of $\phi(n)$.) Put

$$D_j = 2^{-1-j}\frac{x}{y\log_2 x}, \tag{7.4}$$

and for each positive integer k, set

$$\mathcal{D}_{j,k} = (2^{k-1}D_j, 2^k D_j].$$

Then $\frac{\phi(n)}{\lambda(n)} \in \mathcal{D}_{j,k}$ for a positive integer k with

$$2^k D_j \le 8 \cdot 2^{-j}\frac{x}{y}. \tag{7.5}$$

Our strategy will be to bound, for each j satisfying (7.3) and k satisfying (7.5), the number of squarefree $n \in \mathcal{N}_j$ satisfying (7.2) for which $\frac{\phi(n)}{\lambda(n)} \in \mathcal{D}_{j,k}$. The desired estimate for $L^*(x,y)$ will follow upon summing on j and k.

Suppose $d = \frac{\phi(n)}{\lambda(n)}$. The integers $\lambda(n)$ and $\phi(n)$ share the same set of prime divisors. (By the theorems of Cauchy and Lagrange, the exponent of a finite group always has the same set of prime divisors as the order of the group.) Hence,

$$d\,\mathrm{rad}(d) \mid d\,\mathrm{rad}(\phi(n)) = d\,\mathrm{rad}(\lambda(n)) \mid d\lambda(n) = \phi(n).$$

It therefore suffices to bound the number of squarefree $n \in \mathcal{N}_j$ satisfying (7.2) with $\phi(n)$ divisible by $d\,\mathrm{rad}(d)$ for some integer $d \in \mathcal{D}_{j,k}$.

We stratify dyadically one more time. Let $d \in \mathcal{D}_{j,k}$. As $d\,\mathrm{rad}(d) \in [d, d^2]$, there is some $\ell \in \mathbb{Z}^+$ with

$$d\,\mathrm{rad}(d) \in \mathcal{I}_{j,k,\ell} := (2^{\ell-1}\cdot 2^{k-1}D_j, 2^{\ell}\cdot 2^{k-1}D_j],$$

for a value of ℓ with

$$2^{\ell}\cdot 2^{k-1}D_j \le 2\cdot (2^k D_j)^2. \tag{7.6}$$

Letting ℓ run over positive integers satisfying (7.6), we have from Lemma 6.6 and the observation that $d\,\mathrm{rad}(d) \le d^2 \le 2^{2k}D_j^2 < 64(x/y)^2$,

$$\begin{aligned}
&\#\{\text{squarefree } n \in \mathcal{N}_j :\ \omega(n) \le W,\ d\,\mathrm{rad}(d) \mid \phi(n) \text{ for some } d \in \mathcal{D}_{j,k}\}\\
&\qquad \le \sum_{\ell} \sum_{\substack{d\in\mathcal{D}_{j,k}\\ d\,\mathrm{rad}(d)\in\mathcal{I}_{j,k,\ell}}} \#\{n \le 2^{1-j}x : d\,\mathrm{rad}(d) \mid \phi(n)\}\\
&\qquad \le 2^{1-j}x\sum_{\ell} \sum_{\substack{d\in\mathcal{D}_{j,k}\\ d\,\mathrm{rad}(d)\in\mathcal{I}_{j,k,\ell}}} \frac{1}{d\,\mathrm{rad}(d)} \sum_{1\le w\le W} \left(2C_{\phi}(\log_2 x)\left(\log_2\frac{x}{y}\right)\right)^{w} \frac{g_w(d\,\mathrm{rad}(d))}{w!}.
\end{aligned} \tag{7.7}$$

(We start the sum at $w = 1$ rather than $w = 0$ since $d\,\mathrm{rad}(d) > 1$ for our values of d.)

We focus attention on the right-hand inner double sum on d, w. This will be estimated (uniformly in j, k, ℓ) via Proposition 6.3. To ease notation, when convenient below, we suppress subscripts indicating dependence on j, k, ℓ.

The map $d \mapsto d\,\mathrm{rad}(d)$ is injective (on the entire domain of positive integers). We let

$$S = \{d\,\mathrm{rad}(d) : d \in \mathcal{D}_{j,k},\ d\,\mathrm{rad}(d) \in \mathcal{I}_{j,k,\ell}\}.$$

To estimate $\#S$, observe that if $d \in \mathcal{D}_{j,k}$ and $d\,\mathrm{rad}(d) \in \mathcal{I}_{j,k,\ell}$, then

$$\frac{1}{\mathrm{rad}(d)} = \frac{d}{d\,\mathrm{rad}(d)} \geq \frac{2^{k-1}D_j}{2^\ell \cdot 2^{k-1}D_j} = \frac{1}{2^\ell}.$$

As $\sum_{d \in \mathcal{D}_{j,k}} 1/\mathrm{rad}(d) \leq \sum_{d \leq 2^k D_j} 1/\mathrm{rad}(d) \leq (2^k D_j)^\delta$, we conclude from the last display that

$$\#S \leq 2^\ell (2^k D_j)^\delta.$$

To put this in a form to which we can apply Proposition 6.3, let $X = 2^\ell \cdot 2^{k-1} D_j$ and $s = 2^\ell (2^k D_j)^\delta$, so that

$$S \subseteq [1, X] \quad \text{with} \quad \#S \leq s.$$

We define β by the relation

$$s = X^{1-\beta}.$$

From (7.6), we have $2^\ell \leq 4 \cdot 2^k D_j$, and thus

$$\begin{aligned} X &= 2^\ell \cdot 2^{k-1} D_j \\ &\leq 2 \cdot (2^k D_j)^2. \end{aligned} \tag{7.8}$$

Hence, $2^k D_j \geq \frac{1}{2} X^{1/2}$, and

$$s = 2^\ell (2^k D_j)^\delta = \frac{X}{2^{k-1} D_j} (2^k D_j)^\delta = 2X (2^k D_j)^{\delta - 1} \leq 4 X^{\frac{1}{2} + \frac{1}{2}\delta} < X^{0.6},$$

recalling our restriction that $\delta \in (0, \frac{1}{10})$. It follows that $\beta \in [\frac{2}{5}, 1]$.

We now return to estimating the sum over d, w in (7.7). We claim that all $1 \leq w \leq W$ fall into the critical range for the parameter X. To see this, we refer back to (7.3) and (7.4). These give us that

$$X = 2^\ell \cdot 2^{k-1} D_j > D_j = 2^{-j} x \cdot \frac{1}{2y \log_2 x} \geq \frac{1}{2 \log_2 x} \frac{x/y}{\mathscr{L}(x/y)} = (x/y)^{1+o(1)}. \tag{7.9}$$

Thus (see the definition (7.2) of W),

$$W < \frac{11}{\varepsilon} \frac{\log X \log_3 X}{(\log_2 X)^2} < \frac{\log X (\log_3 X)^2}{(\log_2 X)^2}, \tag{7.10}$$

yielding criticality.

Continuing, notice that for all $w \leq W$,

$$\left(\log_2 \frac{x}{y}\right)^w \leq \left(\log_2 \frac{x}{y}\right)^W \leq \exp\left(\frac{10}{\varepsilon} \frac{\log \frac{x}{y} (\log_3 \frac{x}{y})^2}{(\log_2 \frac{x}{y})^2}\right) = \mathscr{L}(x/y)^{\frac{10}{\varepsilon} \frac{\log_3 \frac{x}{y}}{\log_2 \frac{x}{y}}} = \mathscr{L}(x/y)^{o(1)}.$$

Furthermore, as $\mathscr{L}(x/y) \ge \mathscr{L}(\exp((\log_2 x)^{1+\varepsilon})) > \exp((\log_2 x)^{1+\frac{1}{2}\varepsilon})$, we have

$$\frac{(2C_\phi \log_2 x)^w}{w!} \le \sum_{w' \ge 0} \frac{(2C_\phi \log_2 x)^{w'}}{w'!} = \exp(2C_\phi \log_2 x) = (\log x)^{2C_\phi} = \mathscr{L}(x/y)^{o(1)}.$$

Therefore, bearing in mind that every element of $\mathcal{I}_{j,k,\ell}$ exceeds $\frac{1}{2}X$,

$$\begin{aligned}\sum_{\substack{d\in\mathcal{D}_{j,k}\\ d\,\mathrm{rad}(d)\in\mathcal{I}_{j,k,\ell}}} \frac{1}{d\,\mathrm{rad}(d)} \sum_{1\le w\le W} &\frac{\left(2C_\phi(\log_2 x)\left(\log_2 \frac{x}{y}\right)\right)^w}{w!} g_w(d\,\mathrm{rad}(d)) \\ &\le 2X^{-1}\mathscr{L}(x/y)^{o(1)} \sum_{\substack{d\in\mathcal{D}_{j,k}\\ d\,\mathrm{rad}(d)\in\mathcal{I}_{j,k,\ell}}} \sum_{1\le w\le W} g_w(d\,\mathrm{rad}(d)). \qquad (7.11)\end{aligned}$$

Applying Proposition 6.3,

$$\sum_{\substack{d\in\mathcal{D}_{j,k}\\ d\,\mathrm{rad}(d)\in\mathcal{I}_{j,k,\ell}}} \sum_{1\le w\le W} g_w(d\,\mathrm{rad}(d)) = \sum_{1\le w\le W} \sum_{s\in S} g_w(s) \le W\cdot X/\mathscr{L}(X)^{\beta-\delta} \le X/\mathscr{L}(X)^{\beta-2\delta}.$$

Substituting into (7.11), we conclude that the double sum on d, w in (7.7) is bounded above by $\mathscr{L}(X)^{2\delta-\beta}\mathscr{L}(x/y)^{\delta}$ (say).

Let us see how large this last expression is in terms of $\mathscr{L}(x/y)$. Notice that

$$X^\beta = \frac{X}{s} = \frac{2^\ell \cdot 2^{k-1}D_j}{2^\ell (2^k D_j)^\delta} = \frac{1}{2}(2^k D_j)^{1-\delta} > (x/y)^{1-2\delta},$$

using in the last step that $D_j \ge (x/y)^{1+o(1)}$, from (7.9). Hence,

$$\mathscr{L}(X)^\beta = \mathscr{L}(X^\beta)^{1+o(1)} > \mathscr{L}(x/y)^{1-3\delta}.$$

Furthermore, (7.5) and (7.8) yield $X < 128(x/y)^2$, and so

$$\mathscr{L}(X) \le \mathscr{L}(x/y)^{2+o(1)}.$$

Therefore,

$$\begin{aligned}\mathscr{L}(X)^{2\delta-\beta}\mathscr{L}(x/y)^\delta &= \mathscr{L}(X)^{2\delta}\mathscr{L}(X)^{-\beta}\mathscr{L}(x/y)^\delta \\ &\le \mathscr{L}(x/y)^{5\delta}\mathscr{L}(x/y)^{3\delta-1}\mathscr{L}(x/y)^\delta \\ &= \mathscr{L}(x/y)^{9\delta-1}.\end{aligned}$$

Referring back to (7.7), we deduce that for each k and j,

$$\#\{\text{squarefree } n \in \mathcal{N}_j : \omega(n) \le W, d\,\mathrm{rad}(d) \mid \phi(n) \text{ for some } d \in \mathcal{D}_{j,k}\} \le 2^{1-j} x \mathscr{L}(x/y)^{9\delta-1} \sum_{\ell} 1, \qquad (7.12)$$

where the remaining sum is on ℓ satisfying (7.6). There are $\ll \log x = \mathscr{L}(x/y)^{o(1)}$ such values of ℓ, and so the right-hand side of (7.12) is at most $2^{1-j}x\mathscr{L}(x/y)^{10\delta-1}$. It remains to sum on k and j. For each j, there are (crudely) $\ll \log x = \mathscr{L}(x/y)^{o(1)}$ values of k. Summing finally on j, we conclude that the number of n counted in this piece of the argument is at most $x\mathscr{L}(x/y)^{11\delta-1}$. Earlier, we discarded at most $x\mathscr{L}(x/y)^{-1}$ integers n, and so

$$L^*(x,y) \le x\mathscr{L}(x/y)^{11\delta-1} + x\mathscr{L}(x/y)^{-1} \le x\mathscr{L}(x/y)^{12\delta-1},$$

which is what we claimed above. ☐

8. APPLICATION TO MULTIPLICATIVE ORDERS: PROOF OF COROLLARY 1.2

We will need the following clean lower bound on $l(n)$, in terms of $\lambda(n)$ and the orders $l(p)$ for primes p dividing n.

Lemma 8.1. *For all odd natural numbers n,*

$$l(n) \geq \frac{\lambda(n)}{n} \prod_{p \mid n} l(p).$$

Lemma 8.1 is due essentially to Kurlberg and Rudnick [14, §§5.1–5.2]; see [13, Lemma 5] for an explicit statement and a slightly shorter proof.

We also need the following (well-known) lemma.

Lemma 8.2. *Let $\delta \in (0, 1/2)$, and let $\mathcal{P}_\delta = \{\text{odd primes } p : l(p) < p^{\frac{1}{2}-\delta}\}$. Then*

$$\sum_{p \in \mathcal{P}_\delta} \frac{1}{p^{1-\delta}} < \infty.$$

Proof. For each $T \geq 1$, there are at most $T^{1-2\delta}$ primes $p \in \mathcal{P}_\delta \cap [1, T]$. Indeed, any such p has $l(p) \leq T^{\frac{1}{2}-\delta}$, so that $p \mid 2^n - 1$ for some $n \leq T^{\frac{1}{2}-\delta}$. But $2^n - 1$ always has fewer than n distinct prime divisors. Thus, the number of elements of $\mathcal{P}_\delta \cap [1, T]$ is at most $\sum_{n \leq T^{\frac{1}{2}-\delta}} n \leq T^{1-2\delta}$. Now apply partial summation. ☐

Proof of Corollary 1.2. We may (and will) assume that $0 < \delta < \frac{1}{2}$ and that $0 \leq \beta < \frac{1}{2} - \delta$. Below, we let

$$\mathscr{M} = \mathscr{M}(x) := \mathscr{L}(x)^{\log_3 x},$$

noting that $\mathscr{M}$ tends to infinity faster than any power of $\mathscr{L}(x)$ while $\mathscr{M} = x^{o(1)}$ as $x \to \infty$.

Here is the plan of attack. We show that if $n \leq x$ is odd, with $l(n) \leq x^\beta$, then at least one of the following four conditions holds:

(a) $n \leq x/\mathscr{M}$,

(b) n has a squarefull divisor exceeding $\mathscr{M}$,

(c) $\lambda(n) \leq x^{\frac{1}{2}+\beta+\frac{1}{2}\delta}$,

(d) n has a divisor exceeding $\mathscr{M}$ composed entirely of primes $p \in \mathcal{P}_{\delta/4}$ (in the notation of Lemma 8.2).

On the other hand, we prove that the number of $n \leq x$ for which at least one of (a)–(d) holds is bounded above by $x/\mathscr{L}(x)^{\frac{1}{2}-\beta-\delta}$. Corollary 1.2 follows.

First, suppose all of (a)–(d) fail. Write $n = n_{\mathcal{P}} n_s n'$, where $n_{\mathcal{P}}$ is the largest divisor of n composed of primes from $\mathcal{P}_{\delta/4}$, and n_s is the largest squarefull divisor of $n/n_{\mathcal{P}}$. Then n' is squarefree, every prime dividing n' lies outside $\mathcal{P}_{\delta/4}$, and

$$n' = \frac{n}{n_{\mathcal{P}} n_s} > \frac{x/\mathscr{M}}{n_{\mathcal{P}} n_s} \geq x/\mathscr{M}^3.$$

Furthermore, by Lemma 8.1,

$$l(n) \geq \frac{\lambda(n)}{n} \prod_{p \mid n} l(p) \geq x^{-\frac{1}{2}+\beta+\frac{1}{2}\delta} \prod_{p \mid n'} l(p) \geq x^{-\frac{1}{2}+\beta+\frac{1}{2}\delta} n'^{\frac{1}{2}-\frac{1}{4}\delta} \geq x^{-\frac{1}{2}+\beta+\frac{1}{2}\delta} (x/\mathscr{M}^3)^{\frac{1}{2}-\frac{1}{4}\delta} \geq x^{\beta+\frac{1}{8}\delta}.$$

(Here and below, we always assume x is sufficiently large; the notion of "large" may depend on δ but is uniform for $\beta \in [0, \frac{1}{2} - \delta)$.) In particular, we do not have $l(n) \leq x^\beta$.

Next, we show that each of (a)–(d) holds on a set of odd $n \leq x$ of size at most $\frac{1}{4}x/\mathscr{L}(x)^{\frac{1}{2}-\beta-\delta}$. Conditions (a) and (b) hold for $O(x/\mathscr{M})$ and $O(x/\mathscr{M}^{1/2})$ values of $n \leq x$, respectively, which is more than sufficient. Condition (c) is handled directly by Theorem 1.1. Finally, the count of $n \leq x$ for which (d) holds is bounded above by

$$\begin{aligned} x \sum_{\substack{d > \mathscr{M} \\ p \mid d \Rightarrow p \in \mathcal{P}_{\delta/4}}} \frac{1}{d} &\leq x \sum_{p \mid d \Rightarrow p \in \mathcal{P}_{\delta/4}} \frac{1}{d} \left(\frac{d}{\mathscr{M}} \right)^{\frac{1}{4}\delta} \\ &= x \mathscr{M}^{-\frac{1}{4}\delta} \prod_{p \in \mathcal{P}_{\delta/4}} \left(1 + \frac{1}{p^{1-\frac{1}{4}\delta}} + \frac{1}{p^{2(1-\frac{1}{4}\delta)}} + \dots \right) \\ &\ll x \mathscr{M}^{-\frac{1}{4}\delta} \exp \left(\sum_{p \in \mathcal{P}_{\delta/4}} \frac{1}{p^{1-\frac{1}{4}\delta}} \right) \\ &\ll x \mathscr{M}^{-\frac{1}{4}\delta}, \end{aligned}$$

using Lemma 8.2 (with δ replaced by $\frac{1}{4}\delta$) for the last step. Again, this upper bound is tighter than required. This completes the proof. ☐

Remark. It seems plausible that for each fixed $\theta > 0$, the set of primes p with $l(p) < p^{1-\theta}$ is power-saving sparse, in the sense that its counting function is $O(T^{1-\eta})$ for some $\eta = \eta(\theta) > 0$. (For instance, this follows from Erdős's conjecture in [8] that $\#\{p : l(p) = r\} = O_\varepsilon(r^\varepsilon)$. It also follows from the weaker conjecture of Murty and Srinivasan, in the remark following Theorem 4 of [16], that $\sum_{p \leq T} l(p)^{-1} = O_\varepsilon(T^\varepsilon)$.) Under this hypothesis, small modifications of the proof of Corollary 1.2 show that for each fixed $\delta > 0$, and all large x,

$$\#\{\text{odd } n \leq x : l(n) \leq x^\beta\} \leq \frac{x}{\mathscr{L}(x)^{1-\beta-\delta}}$$

uniformly in $\beta \geq 0$.

ACKNOWLEDGEMENTS

I thank Casia Siegel for useful conversations. The simple proof of Lemma 6.1 is taken from a beautiful talk by Jared Lichtman at the 2025 INTEGERS conference.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process

ChatGPT 5.5 was used for editing the manuscript and for pre-submission "refereeing." It also suggested the use of Rankin's trick to handle condition (d) in the proof of Corollary 1.2; this replaces the more cumbersome Hardy–Ramanujanesque approach originally envisioned (cf. pp. 153–154 of [13]). All other mathematical ideas and arguments are to be credited or blamed on the human author and those who trained him.

References

[1] W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Multiplicative structure of values of the Euler function*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, 2004, pp. 29–47.

[2] E. R. Canfield, P. Erdős, and C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, J. Number Theory **17** (1983), 1–28.

[3] R. D. Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), 232–238.

[4] N. G. de Bruijn, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, Nederl. Akad. Wetensch. Proc. Ser. A **54** (1951), 50–60.

[5] ———, *On the number of integers $\leq x$ whose prime factors divide n*, Illinois J. Math. **6** (1962), 137–141.

[6] ———, *On the number of positive integers $\leq x$ and free of prime factors $> y$. II*, Nederl. Akad. Wetensch. Proc. Ser. A **69** (1966), 239–247.

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

[8] ———, *Bemerkungen zu einer Aufgabe in den Elementen*, Arch. Math. (Basel) **27** (1976), 159–163.

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

[10] J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Period of the power generator and small values of Carmichael's function*, Math. Comp. **70** (2001), 1591–1605. Corrigendum in **71** (2002), 1803–1806.

[11] C. F. Gauss, *Disquisitiones arithmeticae*, Yale University Press, New Haven and London, 1966.

[12] E. Grosswald, *The average order of an arithmetic function*, Duke Math. J. **23** (1956), 41–44.

[13] P. Kurlberg and C. Pomerance, *On the periods of the linear congruential and power generators*, Acta Arith. **119** (2005), 149–169.

[14] P. Kurlberg and Z. Rudnick, *On quantum ergodicity for linear maps of the torus*, Comm. Math. Phys. **222** (2001), 201–227.

[15] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[16] M. R. Murty and S. Srinivasan, *Some remarks on Artin's conjecture*, Canad. Math. Bull. **30** (1987), 80–85.

[17] M. Naimi, *Les entiers sans facteurs carré $\leq x$ dont leurs facteurs premiers $\leq y$*, Groupe de travail en théorie analytique et élémentaire des nombres, 1986–1987, 1988, pp. 69–76.

[18] P. Pollack, *How often is Euler's totient a perfect power?*, J. Number Theory **197** (2019), 1–12.

[19] ———, *Popular subsets for Euler's φ-function*, Math. Ann. **374** (2019), 253–271.

[20] ———, *The distribution of numbers with many factorizations*, Math. Z. **299** (2021), 2327–2339.

[21] C. Pomerance, *Popular values of Euler's function*, Mathematika **27** (1980), 84–89.

[22] ———, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.

[23] ———, *Two methods in elementary analytic number theory*, Number theory and applications (Banff, AB, 1988), 1989, pp. 135–161.

[24] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to $25 \cdot 10^9$*, Math. Comp. **35** (1980), 1003–1026.

[25] C. Pomerance and I. E. Shparlinski, *Smooth orders and cryptographic applications*, Algorithmic number theory (Sydney, 2002), 2002, pp. 338–348.

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

Email address: `pollack@uga.edu`