Canad. J. Math. Vol. **59** (1), 2007 pp. 127–147

Smooth Values of the Iterates of the Euler Phi-Function

Youness Lamzouri

Abstract. Let $\phi(n)$ be the Euler phi-function, define $\phi_0(n) = n$ and $\phi_{k+1}(n) = \phi(\phi_k(n))$ for all $k \geq 0$. We will determine an asymptotic formula for the set of integers n less than x for which $\phi_k(n)$ is y-smooth, conditionally on a weak form of the Elliott–Halberstam conjecture.

1 Introduction

Integers without large prime factors, usually called *smooth numbers,* play a central role in several topics of number theory. From multiplicative questions to analytic methods, they have various and wide applications, and understanding their behavior will have important consequences for number theoretic algorithms, which are an important tool in cryptography.

Let $\phi(n)$ be the Euler phi-function, define $\phi_0(n) = n$ and $\phi_{k+1}(n) = \phi(\phi_k(n))$ for all $k \geq 0$. There are several interesting results on the behavior of the functions ϕ_k [5]. It is known that understanding the multiplicative structure of the phi-function and its iterates is in some sense equivalent to studying the behavior of the integers of the form $p - 1$ where p is prime. It is also believed that the distribution of the prime factors of such an integer behaves like that of a random integer, in the following sense. Define

$$\Psi(x, y) = \left|\{n \leq x \colon p|n \implies p \leq y\}\right|,$$
$$\pi(x, y) = \left|\{p \leq x \colon q|p - 1 \implies q \leq y\}\right|.$$

Conjecture 1.1 *Fix $U \geq 1$. If $x^{1/U} \leq y \leq x$ then*

$$\frac{\pi(x, y)}{\pi(x)} \sim \frac{\Psi(x, y)}{x} \quad \text{as } x \to \infty.$$

Assuming this conjecture, one can deduce the behavior of the function $\pi(x, y)$ from the known asymptotic formula

$$\Psi(x, y) \sim x\rho(u) \quad \text{as } x \to \infty \text{ with } x = y^u$$

Received by the editors November 5, 2004; revised January 12, 2005.
AMS subject classification: 11N37, 11B37, 34K05, 45J05.

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

where $\rho(u)$ is the Dickman function, defined as the unique continuous solution of the differential-difference equation $u\rho'(u) = -\rho(u-1)$ for $u \geq 1$, satisfying the initial condition $\rho(u) = 1$ for $0 \leq u \leq 1$.

Now let P be a set of prime numbers and define

$$\Psi(x,P) = \left|\{n \leq x \colon p|n \implies p \in P\}\right|,$$
$$\pi(x,P) = \left|\{p \leq x \colon q|p-1 \implies q \in P\}\right|.$$

One might guess

$$\frac{\pi(x,P)}{\pi(x)} \sim \frac{\Psi(x,P)}{x} \quad \text{as } x \to \infty, \tag{1}$$

under certain conditions on the set P.

Granville [7] has an unpublished argument that Conjecture 1.1 holds for $u = \log(x)/\log(y)$ bounded, assuming the Elliott–Halberstam conjecture which states that:

$$\sum_{q \leq x^{1-\epsilon}} \max_{y \leq x} \max_{(a,q)=1} \left| \pi(y;q,a) - \frac{\pi(y)}{\phi(q)} \right| \ll_{\epsilon,A} \frac{x}{\log(x)^A}.$$

A weak version of this conjecture is the following:

Conjecture 1.2 *Fix $\epsilon > 0$. Then*

$$\sum_{d \leq x^{1-\epsilon}} \left| \pi(x;d,1) - \frac{\pi(x)}{\phi(d)} \right| = o(\pi(x)) \quad \textit{as } x \to \infty.$$

We will prove a version of (1) assuming Conjecture 1.2; specifically, we show the following:

Theorem 1.3 *Assume Conjecture 1.2. If P is a set of primes less than x for which*

$$\sum_{\substack{p \notin P \\ p \leq x}} \frac{1}{p} \ll 1,$$

then

$$\frac{\pi(x,P)}{\pi(x)} \sim \prod_{p \notin P} \Big(1 - \frac{1}{(p-1)^2}\Big) \frac{\Psi(x,P)}{x} \quad \textit{as } x \to \infty.$$

Note that there is an extra factor in Theorem 1.3 compared with (1). To see why we should expect this, let q be some prime; then the probability that a random integer n is divisible by q is $1/q$. Now the probability that a random integer of the form $p-1$ (where p prime) is divisible by q is $1/(q-1)$ (since p is excluded from the class $0 \bmod q$). The differences between the two probabilities are negligible as q increases, however this is not true for small primes q, and thus we need a correction factor (it can be removed in some special cases, see Lemma 2.1).

Define

$$\Phi_k(x, y) = \big|\{n \le x\colon p|\phi_k(n) \implies p \le y\}\big|.$$

Using Theorem 1.3 we get an asymptotic of this function conditionally on Conjecture 1.2.

Theorem 1.4 *Assume Conjecture* 1.2*. Fix* $U > 1$*. If* $y = x^{1/u}$ *where* $1 \le u \le U$*, then*

$$\Phi_k(x, y) \sim x\sigma_k(u) \quad \text{as } x \to \infty$$

where $\sigma_k(u) = 1$ *for* $u \le 1$*, and* $u\sigma_{k+1}(u) = \int_0^u \sigma_{k+1}(u-t)\sigma_k(t)\,dt$ *for* $u \ge 1$*, with* $\sigma_0(u) = \rho(u) = ((e + o(1))/u\log(u))^u$*. Moreover, for all* $k \ge 1$

$$\sigma_k(u) = \Big(\frac{1 + o(1)}{\log_k(u)\log_{k+1}(u)}\Big)^u$$

and

$$\log_k(u) = \log(\log(\log(\cdots\log(u)\cdots))) \quad k \text{ times}.$$

The first step in the proof uses simple combinatorics to approximate the functions $\Phi_k(x, y)$ by $\Psi(x, P_k)$, where P_k are the sets of primes defined iteratively by $P_{k+1} = \{p \le x : q|p-1 \Rightarrow q \in P_k\}$, with $P_0 = \{p \le y\}$.

Proposition 1.5

$$\Phi_k(x, y) = \Psi(x, P_k) + O\Big(\frac{x(\log x)^{2k}}{y}\Big).$$

From the fact that $|P_k| = \pi(x, P_{k-1})$, the next step in proving Theorem 1.4 is to establish a relation between $|P|$ and $\Psi(x, P)$ for any given set of primes P. This was done by Granville and Soundararajan [8] while studying mean values of multiplicative functions. They proved the following proposition:

Proposition 1.6 ([8, Proposition 1]) *Let* f *be a multiplicative function with* $|f(n)| \le 1$ *for all* n*, and* $f(n) = 1$ *for* $n \le y$*. Let* $\theta(x) = \sum_{p\le x}\log(p)$*, and define*

$$\chi(u) := \frac{1}{\theta(y^u)}\sum_{p\le y^u} f(p)\log(p).$$

Then $\chi(t)$ *is a measurable function with* $\chi(t) = 1$ *for all* $t \le 1$*. Let* σ *be the corresponding unique solution to the equation:*

$$u\sigma(u) = \int_0^u \sigma(u-t)\chi(t)\,dt \quad \text{for } u > 1 \tag{2}$$

subject to the initial condition $\sigma(u) = 1$ *for* $0 \le u \le 1$*. Then*

$$\frac{1}{y^u}\sum_{n\le y^u} f(n) = \sigma(u) + O\Big(\frac{u}{\log(y)}\Big).$$

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

From this result and by partial summation we can deduce

Corollary 1.7 *Fix $U > 1$. Let P be a set of primes less than x such that $P_0 \subseteq P$, and f be a completely multiplicative function such that $f(p) = 1$ if $p \in P$ and 0 otherwise (so that $f(n) = 1$ for all $n \leq y$). For $1 \leq u \leq U$, define*

$$\chi(u) := \frac{1}{\pi(y^u)} \sum_{\substack{p \in P \\ p \leq y^u}} 1,$$

then

$$\Psi(y^u, P) = \sum_{n \leq x} f(n) \sim y^u \sigma(u)$$

where σ is the corresponding solution to (2).

It remains to study (2), a delay integral equation, and to try to estimate the solution σ where χ is a certain measurable function. In several interesting cases $\chi(u)$ decays like $(\{1 + o(1)\}/h(u))^u$ where h is positive and non-decreasing. We prove the following:

Theorem 1.8 *Let χ be a real measurable function for which $\chi(t) = 1$ for $0 \leq t \leq 1$, and $0 \leq \chi(t) \leq 1$ for $t > 1$. Moreover suppose that*

(i) *$\int_T^\infty \chi(t)\,dt = 0$ for some constant T. We define $T = \min\{t : \int_T^\infty \chi(t)\,dt = 0\}$ to avoid redundancy, and suppose that $T > 1$.*

(ii) *$\chi(t) = (\{1+o(1)\}/h(t))^t$ where $h(t)$ is non-decreasing and $h(t) \to \infty$ as $t \to \infty$.*

Let σ be the corresponding solution to (2). Then

$$\sigma(u) = \exp\Big((-\xi(u) + o(1))u + \int_1^\infty \frac{\chi(v)e^{\xi(u)v}}{v}\,dv \Big),$$

where $\xi(u)$ is the unique solution to $u = \int_1^\infty \chi(v)e^{\xi(u)v}\,dv$.

Moreover, we can get explicit asymptotics in a number of interesting cases:

Proposition 1.9 *Let χ be a real measurable function with $\chi(t) = 1$ for $0 \leq t \leq 1$ and $0 \leq \chi(t) \leq 1$ for $t > 1$. Suppose that $\int_T^\infty \chi(t)\,dt = 0$ for some constant T. We define $T = \min\{t : \int_T^\infty \chi(t)\,dt = 0\}$ to avoid redundancy, and suppose that $T > 1$. Then $\xi(u) = \frac{\log(u)}{T}(1 + o(1))$, and*

$$\sigma(u) = \exp\Big(-\frac{u\log(u)}{T}(1 + o(1)) \Big).$$

Proposition 1.10 *Let χ be a real measurable function with $\chi(t) = 1$ for $0 \leq t \leq 1$, and $0 \leq \chi(t) \leq 1$ for $t > 1$. Suppose that $\chi(u) = \big(\{1 + o(1)\}/h(u)\big)^u$ where h satisfies the following conditions:*

(i) *h is positive and non-decreasing with $h(u) \to \infty$ as $u \to \infty$;*

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

(ii) *h is continuously differentiable and $uh'(u)/h(u) \to n$ as $u \to \infty$ for some $0 \leq n < \infty$.*

We distinguish two cases: (a) $0 < n < \infty$*;* (b) $n = 0$*. Then*

$$\sigma(u) = \Big(\frac{1 + o(1)}{h(\zeta \log(u))}\Big)^u,$$

where $\zeta = e/n$ in case (a) *and $\zeta = 1$ in case* (b).

The distinction between cases (a) and (b) in Proposition 1.10 justifies the appearance of the constant e only in the asymptotic of σ_o in Theorem 1.4.

2 Proof of Theorem 1.4

Lemma 2.1 *Assume Conjecture* 1.2*. Fix $U \geq 1$. Suppose that P is a set of primes less than x for which $\{p \leq y\} \subseteq P$, where $y = x^{1/u}$ and $1 \leq u \leq U$. Then*

$$\frac{\pi(x, P)}{\pi(x)} \sim \frac{\Psi(x, P)}{x} \quad \text{as } x \to \infty.$$

Proof We have that

$$\sum_{\substack{p \notin P \\ p \leq x}} \frac{1}{p} \leq \sum_{y < p \leq x} \frac{1}{p} \ll \log\Big(\frac{\log(x)}{\log(y)}\Big) = \log(u) \ll 1$$

and, since $1 - t \geq e^{-2t}$ for $0 \leq t \leq 1/2$, then

$$1 \geq \prod_{p \notin P}\Big(1 - \frac{1}{(p-1)^2}\Big) \geq \prod_{p > y}\Big(1 - \frac{1}{(p-1)^2}\Big) \geq \exp\Big(-2\sum_{p > y}\frac{1}{(p-1)^2}\Big)$$
$$= 1 + o(1).$$

The result follows by Theorem 1.3. ∎

Proof of Theorem 1.4 First note that the sets P_k for $k \geq 0$ satisfy the conditions of Lemma 2.1. Now $\Psi(x, P_0) = \Psi(x, y) \sim \rho(u)x$ as $x \to \infty$. We use induction on k: suppose that $\Psi(x, P_k) \sim \sigma_k(u)x$ as $x \to \infty$ for some smooth function $\sigma_k(u)$. Then by Lemma 2.1

$$\frac{|P_{k+1}|}{\pi(x)} = \frac{\pi(x, P_k)}{\pi(x)} \sim \frac{\Psi(x, P_k)}{x} \sim \sigma_k(u) \quad \text{as } x \to \infty.$$

Now by Corollary 1.7 we have

$$\Psi(x, P_{k+1}) \sim \sigma_{k+1}(u)x \quad \text{as } x \to \infty,$$

where $\sigma_{k+1}(u)$ is the corresponding solution to (2) with $\chi(u) = \sigma_k(u)$. Noting that $\sigma_0(u) = \rho(u) = ((e + o(1))/u\log(u))^u$ and using Proposition 1.10, we deduce that

$$\sigma_k(u) = \Big(\frac{1 + o(1)}{\log_k(u)\log_{k+1}(u)}\Big)^u$$

by induction. Thus, using Proposition 1.5, the Theorem follows. ∎

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

3 Proof of Theorem 1.3

Lemma 3.1 *If P is a set of primes $\le x$, then*

$$\sum_{\substack{p\notin P\\ p\le x}} \frac{1}{p} \ll 1 \iff \prod_{p\in P}\Big(1-\frac{1}{p}\Big) \asymp \frac{1}{\log(x)}.$$

Proof The result follows since

$$\prod_{p\in P}\Big(1-\frac{1}{p}\Big) = \prod_{\substack{p\notin P\\ p\le x}}\Big(1-\frac{1}{p}\Big)^{-1}\prod_{p\le x}\Big(1-\frac{1}{p}\Big) \asymp \exp\Big(O\Big(\sum_{\substack{p\notin P\\ p\le x}}\frac{1}{p}\Big)\Big)\frac{1}{\log(x)}$$

by Mertens' theorem. ■

Lemma 3.2 *Let m, d be positive integers such that $d|m$, then we have*

$$\sum_{\substack{r\le x\\ d|r|m}} \frac{\mu(r)}{r} = \mu(d) \sum_{\substack{n\ge 1\\ d|n\\ p|n\Rightarrow p|d}} \frac{1}{n} \sum_{\substack{r\le x/n\\ r|m}} \frac{\mu(r)}{r}.$$

Proof The result is trivial if $\mu(d) = 0$ or $d = 1$. We fix m and do a double induction on $d \ge 1$ and $x \ge 1$. Now

$$\begin{aligned} S_d(x) := \sum_{\substack{r\le x\\ d|r|m}} \frac{\mu(r)}{r} &= \sum_{\substack{n\le x/d\\ n|\frac{m}{d}}} \frac{\mu(dn)}{dn} = \frac{\mu(d)}{d} \sum_{\substack{n\le x/d\\ n|m\\ (n,d)=1}} \frac{\mu(n)}{n} = \frac{\mu(d)}{d} \sum_{\substack{n\le x/d\\ n|m}} \frac{\mu(n)}{n} \sum_{\substack{a|n\\ a|d}} \mu(a) \\ &= \frac{\mu(d)}{d} \sum_{a|d} \mu(a) \sum_{\substack{n\le x/d\\ a|n|m}} \frac{\mu(n)}{n} = \frac{\mu(d)}{d} \sum_{a|d} \mu(a) S_a(x/d). \end{aligned}$$

Now each $a \le d$ and $x/d < x$, so by induction

$$\begin{aligned} S_d(x) &= \frac{\mu(d)}{d} \sum_{a|d} \mu(a)^2 \sum_{\substack{n\ge 1\\ a|n\\ p|n\Rightarrow p|a}} \frac{1}{n} \sum_{\substack{r\le x/nd\\ r|m}} \frac{\mu(r)}{r} \\ &= \frac{\mu(d)}{d} \sum_{\substack{n\ge 1\\ p|n\Rightarrow p|d}} \frac{1}{n} \sum_{\substack{r\le x/nd\\ r|m}} \frac{\mu(r)}{r} \sum_{\substack{a|d\\ a|n\\ p|n\Rightarrow p|a}} \mu(a)^2. \end{aligned}$$

Now if we write $n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ with each $b_j \ge 1$, then $p|n \Rightarrow p|d$ implies that $p_1 p_2 \cdots p_k | d$. Moreover if a satisfies $a|d$, $a|n$, $p|n \Rightarrow p|a$, and a is a squarefree, then

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

a must be $p_1 p_2 \cdots p_k$, which implies

$$\sum_{\substack{a|d\\ a|n\\ p|n\Rightarrow p|a}} \mu(a)^2 = 1.$$

Then, writing $l = nd$, we have

$$S_d(x) = \mu(d) \sum_{\substack{l\geq 1\\ d|l\\ p|l\Rightarrow p|d}} \frac{1}{l} \sum_{\substack{r\leq x/l\\ r|m}} \frac{\mu(r)}{r},$$

as desired. ■

Lemma 3.3 *For any positive integer k we have*

$$\sum_{\substack{n\geq 1\\ k|n\\ p|n\Rightarrow p|k}} \frac{\log(n)}{n} = \frac{1}{\phi(k)}\Big(\sum_{p|k} \frac{\log(p)}{p-1} + \log(k)\Big) \asymp \frac{\log(k)}{\phi(k)}.$$

Proof Writing $n = kd$ we have

$$\sum_{\substack{n\geq 1\\ k|n\\ p|n\Rightarrow p|k}} \frac{\log(n)}{n} = \sum_{\substack{d\geq 1\\ p|d\Rightarrow p|k}} \frac{\log(d)+\log(k)}{dk} = \frac{1}{k} \sum_{\substack{d\geq 1\\ p|d\Rightarrow p|k}} \frac{\log(d)}{d} + \frac{\log(k)}{\phi(k)}.$$

Now if $p_1, p_2, \ldots, p_n$ are the prime factors of k then

$$\begin{aligned}
\sum_{\substack{d\geq 1\\ p|d\Rightarrow p|k}} \frac{\log(d)}{d} &= \sum_{\substack{a_i\geq 0\\ 1\leq i\leq n}} \frac{a_1\log(p_1) + a_2\log(p_2) + \cdots + a_n\log(p_n)}{p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}} \\
&= \sum_{i=1}^{n} \Big(\sum_{a_i\geq 0} \frac{a_i \log(p_i)}{p_i^{a_i}}\Big) \Big(\prod_{\substack{1\leq j\leq n\\ j\neq i}} \Big(\sum_{a_j\geq 0} \frac{1}{p_j^{a_j}}\Big)\Big) \\
&= \sum_{i=1}^{n} \frac{\log(p_i)}{p_i\big(1-\frac{1}{p_i}\big)^2} \prod_{\substack{1\leq j\leq n\\ j\neq i}} \Big(1 - \frac{1}{p_j}\Big)^{-1} \\
&= \frac{k}{\phi(k)} \sum_{p|k} \frac{\log(p)}{p-1},
\end{aligned}$$

which gives the result. ■

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

We state a classical result of sieve theory which is used throughout the proof:

Lemma 3.4 (Brun's Sieve) *Let A be a set of positive integers contained in $[1, N]$. Suppose that for each prime $p \le N$, A is excluded from $\omega(p)$ residue classes $\bmod p$, where ω is a multiplicative function and $\omega(p) \ll 1$. Then*

$$|A| \ll N \prod_{p \le N} \left(1 - \frac{\omega(p)}{p}\right).$$

Proof of Theorem 1 Let $\epsilon > 0$, $P^* = \{p \le x\} \setminus P$, and $m = \prod_{p \in P^*} p$. Then we have

$$\begin{aligned}(3)\quad \pi(x,P) &= \sum_{\substack{p \le x \\ q|p-1 \Rightarrow q \in P}} 1 = \sum_{\substack{p \le x \\ (p-1,m)=1}} 1 = \sum_{p \le x} \sum_{d|(m,p-1)} \mu(d) = \sum_{d|m} \mu(d) \sum_{\substack{p \le x \\ d|p-1}} 1 \\ &= \sum_{d|m} \mu(d) \pi(x; d, 1).\end{aligned}$$

Now by a similar argument we have

$$(4)\qquad \Psi(x,P) = \sum_{\substack{d \le x \\ d|m}} \mu(d) \left[\frac{x}{d}\right].$$

By (3) and assuming Conjecture 1.2 we have

$$(5)\qquad \pi(x,P) = \left(\sum_{\substack{d \le x^{1-\epsilon} \\ d|m}} \frac{\mu(d)}{\phi(d)}\right) \pi(x) + O\left(\sum_{\substack{x^{1-\epsilon} < d \le x \\ d|m}} \pi(x; d, 1)\right) + o(\pi(x)).$$

From (4), Lemmas 3.1 and 3.4 we deduce

$$(6)\qquad \left|\Psi(x,P) - x \sum_{\substack{d \le x \\ d|m}} \frac{\mu(d)}{d}\right| \le \sum_{\substack{d \le x \\ d|m}} 1 \le \sum_{\substack{d \le x \\ p|d \Rightarrow p \notin P}} 1 \ll x \prod_{p \in P} \left(1 - \frac{1}{p}\right) \ll \frac{x}{\log(x)}.$$

Also by Lemmas 3.1 and 3.4 we have

$$\begin{aligned}(7)\quad \sum_{\substack{x^{1-\epsilon} < d \le x \\ d|m}} \frac{1}{d} &\le \sum_{\substack{x^{1-\epsilon} < d \le x \\ p|d \Rightarrow p \in P^*}} \frac{1}{d} = \int_{x^{1-\epsilon}}^{x} \frac{d\Psi(t,P^*)}{t} \le \frac{\Psi(x,P^*)}{x} + \int_{x^{1-\epsilon}}^{x} \frac{\Psi(t,P^*)}{t^2}\, dt \\ &\ll \prod_{p \in P} \left(1 - \frac{1}{p}\right) \left(1 + \int_{x^{1-\epsilon}}^{x} \frac{dt}{t}\right) \ll \prod_{p \in P} \left(1 - \frac{1}{p}\right) \epsilon \log(x) \ll \epsilon.\end{aligned}$$

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

Then from (5), (6) and (7) we deduce

$$\text{(8)}\qquad \Big|\frac{\pi(x,P)}{\pi(x)} - \prod_{p\notin P}\Big(1-\frac{1}{(p-1)^2}\Big)\frac{\Psi(x,P)}{x}\Big| \le \Big|\sum_{\substack{d\le x^{1-\epsilon}\\ d|m}}\frac{\mu(d)}{\phi(d)} - \sum_{\substack{d\le x^{1-\epsilon}\\ d|m}}\frac{\mu(d)}{d}\prod_{p\notin P}\Big(1-\frac{1}{(p-1)^2}\Big)\Big| + o(1) + O(\epsilon) + O\Big(\sum_{\substack{x^{1-\epsilon}<d\le x\\ d|m}}\frac{\pi(x;d,1)}{\pi(x)}\Big).$$

Now by Lemmas 3.1, 3.4 and the fact that $\sum_{r\le x}\frac{1}{\phi(r)} \ll \log(x)$, we get

$$\text{(9)}\qquad \sum_{\substack{x^{1-\epsilon}<d\le x\\ d|m}}\pi(x;d,1) = \sum_{r\le x^{\epsilon}}\sum_{\substack{x^{1-\epsilon}<d\le x/r\\ p|d\Rightarrow p\notin P\\ dr+1\,\mathrm{prime}}} 1 \ll \sum_{r\le x^{\epsilon}}\frac{x}{r}\prod_{p\in P}\Big(1-\frac{1}{p}\Big)\prod_{\substack{p\le x\\ p\nmid r}}\Big(1-\frac{1}{p}\Big) \ll \frac{x}{\log(x)^2}\sum_{r\le x^{\epsilon}}\frac{1}{\phi(r)} \ll \epsilon\frac{x}{\log(x)}.$$

And from Lemma 3.2 we have

$$\text{(10)}\qquad \sum_{\substack{d\le x^{1-\epsilon}\\ d|m}}\frac{\mu(d)}{\phi(d)} = \sum_{\substack{d\le x^{1-\epsilon}\\ d|m}}\frac{\mu(d)}{d}\sum_{k|d}\frac{\mu(k)^2}{\phi(k)}$$
$$= \sum_{k|m}\frac{\mu(k)^2}{\phi(k)}\sum_{\substack{d\le x^{1-\epsilon}\\ k|d|m}}\frac{\mu(d)}{d} = \sum_{k|m}\frac{\mu(k)}{\phi(k)}\sum_{\substack{n\ge 1\\ k|n\\ p|n\Rightarrow p|k}}\frac{1}{n}\sum_{\substack{r\le x^{1-\epsilon}/n\\ r|m}}\frac{\mu(r)}{r}$$
$$= \sum_{k|m}\frac{\mu(k)}{\phi(k)}\sum_{\substack{n\ge 1\\ k|n\\ p|n\Rightarrow p|k}}\frac{1}{n}\sum_{\substack{r\le x^{1-\epsilon}\\ r|m}}\frac{\mu(r)}{r} - \sum_{k|m}\frac{\mu(k)}{\phi(k)}\sum_{\substack{n\ge 1\\ k|n\\ p|n\Rightarrow p|k}}\frac{1}{n}\sum_{\substack{x^{1-\epsilon}/n<r\le x^{1-\epsilon}\\ r|m}}\frac{\mu(r)}{r}.$$

The first term in the right-hand side of (10) is equal to:

$$\text{(11)}\qquad \sum_{\substack{r\le x^{1-\epsilon}\\ r|m}}\frac{\mu(r)}{r}\sum_{k|m}\frac{\mu(k)}{k\phi(k)}\prod_{p|k}\Big(1-\frac{1}{p}\Big)^{-1} = \sum_{\substack{r\le x^{1-\epsilon}\\ r|m}}\frac{\mu(r)}{r}\prod_{p|m}\Big(1-\frac{1}{(p-1)^2}\Big).$$

By integration by parts and using Lemma 3.4 we have

$$\Big|\sum_{\substack{x^{1-\epsilon}/n<r\leq x^{1-\epsilon}\\ r|m}}\frac{\mu(r)}{r}\Big|\leq\sum_{\substack{x^{1-\epsilon}/n<r\leq x^{1-\epsilon}\\ r|m}}\frac{1}{r}\leq\int_{x^{1-\epsilon}/n}^{x^{1-\epsilon}}\frac{d\Psi(t,P^*)}{t}$$
$$\ll\prod_{p\in P}\Big(1-\frac{1}{p}\Big)\Big(1+\int_{x^{1-\epsilon}/n}^{x^{1-\epsilon}}\frac{dt}{t}\Big)\ll\frac{\log(n)}{\log(x)}.$$

Then, by Lemma 3.3

$$\sum_{k|m}\frac{\mu(k)}{\phi(k)}\sum_{\substack{n\geq1\\ k|n\\ p|n\Rightarrow p|k}}\frac{1}{n}\sum_{\substack{x^{1-\epsilon}/n<r\leq x^{1-\epsilon}\\ r|m}}\frac{\mu(r)}{r}\ll\sum_{k|m}\frac{\mu(k)}{\phi(k)}\sum_{\substack{n\geq1\\ k|n\\ p|n\Rightarrow p|k}}\frac{\log(n)}{n\log(x)}\tag{12}$$
$$\ll\frac{1}{\log(x)}\sum_{k|m}\frac{\mu(k)\log(k)}{\phi(k)^2}\ll\frac{1}{\log(x)}.$$

Thus combining (8), (9), (10), (11) and (12) gives the result, letting $\epsilon\to0$. ■

4 Proof of Proposition 1.5

Lemma 4.1 *$P_0=\{p\leq y\}\subseteq P_1\subseteq P_2\subseteq\cdots\subseteq P_k\subseteq\cdots$, where*

$$P_{k+1}=\{\text{primes } q\leq x: p|q-1\implies p\in P_k\}.$$

Proof If $p\in P_0$ then $p\leq y$ and so $p-1\leq y$, which implies $q|p-1\Rightarrow q\leq y$. This means that $p\in P_1$. Now using a simple induction argument: if $p\in P_k$ then $q|p-1\Rightarrow q\in P_{k-1}\subseteq P_k$, and so $p\in P_{k+1}$. ■

Lemma 4.2 *Let r be a positive integer. Then*

$$R(r,k,x):=\sum_{\substack{y<r<q_1<\cdots<q_k\leq x\\ r|q_1-1,q_1|q_2-1,\dots,q_{k-1}|q_k-1}}\frac{1}{q_k}\leq\frac{(\log x+1)^k}{r}.$$

We deduce that

$$S(r,k,x):=\sum_{\substack{y<r<q_1<\cdots<q_k\leq n\leq x\\ r|q_1-1,q_1|q_2-1,\dots,q_{k-1}|q_k-1,q_k|n}}1\leq\frac{x(\log x+1)^k}{r}.$$

Proof Writing $q_k-1=mq_{k-1}$ we have

$$R(r,k,x)\leq\sum_{m\leq\frac{x}{r}}\frac{1}{m}R(r,k-1,x)\leq R(r,k-1,x)(\log x+1),$$

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

and

$$R(r,1,x) \le \sum_{m \le \frac{x}{r}} \frac{1}{mr} \le \frac{\log x + 1}{r},$$

then by induction

$$R(r,k,x) \le \frac{(\log x + 1)^k}{r}.$$

The second inequality follows since

$$S(r,k,x) \le \sum_{\substack{y<r<q_1<\cdots<q_k\le x \\ r|q_1-1, q_1|q_2-1,\ldots,q_{k-1}|q_k-1}} \frac{x}{q_k} = xR(r,k,x). \qquad \blacksquare$$

Lemma 4.3 *Define*

$$S_k(x,y) = \{n \le x : \textit{there is a prime } p > y \textit{ such that } p^2 | \phi_k(n)\}.$$

Then

$$|\Psi(x,P_k) - \Phi_k(x,y)| \le \sum_{i=0}^{k-1} |S_i(x,y)|.$$

Proof Let $A_k(x) = \{n \le x : p|n \Rightarrow p \in P_k\}$. If $n \in A_{k+1}(x)$ and $\phi(n) \notin A_k(x)$, then there is a prime p which divides $\phi(n)$ and $p \notin P_k$. Now $n \in A_{k+1}(x)$ so every prime factor of $q-1$, where $q|n$, is in P_k, which implies that $p^2|n$. This gives

$$A_{k+1}(x) \setminus \{n \le x : \phi(n) \in A_k(x)\}$$
$$= \{n \le x : n \in A_{k+1}(x), \exists \text{ a prime } p \in P_{k+1} \setminus P_k, p^2|n\}.$$

Then by Lemma 4.1

$$\begin{aligned} 0 &\le \Psi(x,P_k) - \Phi_k(x,y) = |A_k(x)| - |\{n \le x : \phi_k(n) \in A_0(x)\}| \\ &= \sum_{i=0}^{k-1} |\{n \le x : \phi_i(n) \in A_{k-i}(x)\}| - |\{n \le x : \phi_{i+1}(n) \in A_{k-i-1}(x)\}| \\ &= \sum_{i=0}^{k-1} |\{n \le x : \phi_i(n) \in A_{k-i}(x), \text{ there is a prime } p \in P_{k-i} \setminus P_{k-i-1}, p^2|\phi_i(n)\}| \\ &\le \sum_{i=0}^{k-1} |S_i(x,y)|. \end{aligned} \qquad \blacksquare$$

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

Proof of Proposition 1.5 Note that if $q|(\phi(n), n)$ for some prime q, then $q^2|n$. Define

$$S_k^*(x,y) = S_k(x,y) \setminus \bigcup_{i=0}^{k-1} S_i(x,y).$$

If $n \in S_k^*(x,y)$ and $q^2|\phi_j(n)$ for some $0 \le j \le k-1$, then $q \le y$ (by definition); also there exists some prime p satisfying $p^2|\phi_k(n)$ with $p > y$, which implies $p^2 \nmid \phi_{k-1}(n)$. Thus we have two cases:

(i) There exists a prime $q_1|\phi_{k-1}(n)$ such that $p^2|q_1 - 1$.
(ii) There are two primes $q_1|\phi_{k-1}(n)$ and $Q_1|\phi_{k-1}(n)$ such that $p|q_1 - 1$ and $p|Q_1 - 1$.

In the first case $q_1|\phi_{k-1}(n) = \phi(\phi_{k-2}(n))$, $p|q_1 - 1$, so that $q_1 > y$, which implies that $q_1^2 \nmid \phi_{k-2}(n)$, so that there exists a prime $q_2|\phi_{k-2}(n)$ such that $q_1|q_2 - 1$ and $q_2 > q_1 > p > y$. By a simple induction, there exist primes $y < p < q_1 < q_2 < \cdots < q_k$ for which $p^2|q_1 - 1, q_1|q_2 - 1, \dots, q_{k-1}|q_k - 1, q_k|n$.

We deduce that the total number of possibilities for this case is:

$$S_1 = \sum_{\substack{y<p<q_1<\cdots<q_k\le n\le x\\ p^2|q_1-1,q_1|q_2-1,\dots,q_{k-1}|q_k-1,q_k|n}} 1 = \sum_{y<p<\sqrt{x}} S(p^2,k,x) \le x(\log x+1)^k \sum_{p>y}\frac{1}{p^2}$$
$$\ll \frac{x(\log x)^k}{y}$$

by Lemma 4.2.

Now, following an analogous argument we find (for the second case) that there exist primes $p, q_1, q_2, \dots, q_k, Q_1, Q_2, \dots, Q_k$ such that $p|q_1 - 1, q_1|q_2 - 1, \dots, q_{k-1}|q_k - 1, q_k|n$ and $p|Q_1 - 1, Q_1|Q_2 - 1, \dots, Q_{k-1}|Q_k - 1, Q_k|n$; we shall have two cases again:

(a) $q_i \ne Q_i$ for all $1 \le i \le k$.
(b) There exists i such that $q_i = Q_i$; so let $j = \min\{1 \le i \le k : q_i = Q_i\}$.

For case (a) the total number of possibilities is:

$$S_2 = \sum_{\substack{y<p<q_1<\cdots<q_k\le n\le x\\ p<Q_1<\cdots<Q_k\le n\le x\\ p|q_1-1,q_1|q_2-1,\dots,q_{k-1}|q_k-1,q_k|n\\ p|Q_1-1,Q_1|Q_2-1,\dots,Q_{k-1}|Q_k-1,Q_k|n}} 1 \le \sum_{\substack{y<p<q_1<\cdots<q_k\le x\\ p<Q_1<\cdots<Q_k\le x\\ p|q_1-1,q_1|q_2-1,\dots,q_{k-1}|q_k-1\\ p|Q_1-1,Q_1|Q_2-1,\dots,Q_{k-1}|Q_k-1}} \frac{x}{q_kQ_k}$$
$$\le x\sum_{p>y} R(p,k,x)^2 = O\Big(\frac{x(\log x)^{2k}}{y}\Big)$$

by Lemma 4.2.

Now for case (b)

$$p|q_1 - 1, q_1|q_2 - 1, \dots, q_{j-1}|q_j - 1,$$
$$p|Q_1 - 1, Q_1|Q_2 - 1, \dots, Q_{j-1}|Q_j - 1,$$
$$Q_j = q_j|\phi_{k-j}(n).$$

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

Then following the same logic there exist primes $q_{j+1}, q_{j+2}, \dots, q_k$ such that $q_j | q_{j+1} - 1, \dots, q_{k-1} | q_k - 1, q_k | n$.

We deduce that the total number of possibilities is: s

$$S_3 = \sum_{\substack{y<p<q_1<\cdots<q_j\le x\\ p|q_1-1,q_1|q_2-1,\dots,q_{j-1}|q_j-1}} \Bigg(\sum_{\substack{p<Q_1<\cdots<Q_j=q_j\\ p|Q_1-1,Q_1|Q_2-1,\dots,Q_{j-1}|Q_j-1}} \Bigg(\sum_{\substack{qj<q_{j+1}<\cdots<q_k\le n\le x\\ q_j|q_{j+1}-1,\dots,q_{k-1}|q_k-1,q_k|n}} 1 \Bigg)\Bigg)$$

$$= \sum_{\substack{y<p<q_1<\cdots<q_j\le x\\ p|q_1-1,q_1|q_2-1,\dots,q_{j-1}|q_j-1}} \Bigg(\sum_{\substack{p<Q_1<\cdots<Q_j=q_j\\ p|Q_1-1,Q_1|Q_2-1,\dots,Q_{j-1}|Q_j-1}} S(q_j, k-j, x) \Bigg)$$

$$\le \sum_{\substack{y<p<q_1<\cdots<q_j\le x\\ p|q_1-1,q_1|q_2-1,\dots,q_{j-1}|q_j-1}} \Bigg(\sum_{\substack{p<Q_1<\cdots<Q_j=q_j\\ p|Q_1-1,Q_1|Q_2-1,\dots,Q_{j-1}|Q_j-1}} \frac{x(\log x+1)^{k-j}}{q_j} \Bigg).$$

Now writing $Q_j - 1 = q_j - 1 = mQ_{j-1}q_{j-1}$ we have:

$$\sum_{\substack{q_j\le x\\ q_{j-1},Q_{j-1}|q_j-1}} \frac{1}{q_j} < \sum_{m\le x} \frac{1}{mQ_{j-1}q_{j-1}} \le \frac{\log x+1}{Q_{j-1}q_{j-1}}.$$

Thus by Lemma 4.2

$$S_3 \ll x(\log x)^{k-j+1} \sum_{p>y} R(p, j-1, x)^2 \ll \frac{x(\log x)^{k+j-1}}{y}.$$

We deduce from cases (i), (ii) (a) and (b) that

$$|S_k^*(x,y)| = S_1 + S_2 + S_3 = O\Big(\frac{x(\log x)^{2k}}{y}\Big). \tag{13}$$

Now

$$\begin{aligned}
|S_1(x,y)| &= |S_0(x,y)| + |S_1^*(x,y)| \\
&= \big|\{n \le x : \exists \text{ a prime } p > y, p^2|n\}\big| + O\Big(\frac{x(\log x)^2}{y}\Big) \\
&\le \sum_{\substack{n\le x\\ p>y\\ p^2|n}} 1 + O\Big(\frac{x(\log x)^2}{y}\Big) \le \sum_{p>y} \frac{x}{p^2} + O\Big(\frac{x(\log x)^2}{y}\Big) \\
&= O\Big(\frac{x}{y}\Big) + O\Big(\frac{x(\log x)^2}{y}\Big) = O\Big(\frac{x(\log x)^2}{y}\Big),
\end{aligned}$$

and by simple induction we obtain:

$$|S_k(x,y)| = |S_k^*(x,y)| + \sum_{i=0}^{k-1} |S_i(x,y)| = O\Big(\frac{x(\log x)^{2k}}{y}\Big). \tag{14}$$

Thus by (14) and Lemma 4.3 the result follows. ■

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

5 Proof of Theorem 1.8

Lemma 5.1 *Let χ be a real measurable function for which $\int_1^\infty \chi(t)e^{\xi t}\,dt$ converges for all ξ and such that $C := \int_1^\infty \chi(v)\,dv > 0$. Then for $u \geq C^2$ and for any $\epsilon > 0$, we have*

$$\int_1^\infty \chi(v)e^{(\xi(u)+\epsilon)v}\,dv \geq u^{1+\frac{\epsilon}{2\xi(u)}}.$$

Proof Let $\epsilon' > 0$ and $s > 0$. Using Hölder's inequality we get

$$\Big(\int_1^\infty \chi(v)\,dv\Big)^{\epsilon'}\Big(\int_1^\infty \chi(v)e^{sv}\,dv\Big)^{1-\epsilon'} \geq \int_1^\infty \chi(v)e^{s(1-\epsilon')v}\,dv.$$

Now putting $s = \xi(u)/(1-\epsilon') = \xi(u)(1+\epsilon'')$, from $u \geq C^2$ we deduce that

$$\int_1^\infty \chi(v)e^{\xi(u)(1+\epsilon'')v}\,dv \geq \frac{1}{C^{\epsilon'}}\Big(\int_1^\infty \chi(v)e^{\xi(u)v}\,dv\Big)^{1+\epsilon''} \geq u^{1+\epsilon''/2}.$$

The lemma follows, taking $\epsilon = \xi(u)\epsilon''$. ■

Proof of Theorem 1.8

The Upper Bound: From [8, Lemma 3.4] we note that

$$\sigma(u) = \rho(u) + \sum_{j=1}^\infty \frac{1}{j!}\int_{\substack{t_1,\dots,t_j\geq 1\\ t_1+\cdots+t_j\leq u}} \frac{\chi(t_1)}{t_1}\cdots\frac{\chi(t_j)}{t_j}\rho(u-t_1-\cdots-t_j)\,dt_1\cdots dt_j.$$

Therefore for any $\xi \in \mathbb{R}$

$$\sigma(u)e^{\xi u} = \rho(u)e^{\xi u} + \sum_{j=1}^\infty \frac{1}{j!}$$
$$\int_{\substack{t_1,\dots,t_j\geq 1\\ t_1+\cdots+t_j\leq u}} \frac{\chi(t_1)e^{\xi t_1}}{t_1}\cdots\frac{\chi(t_j)e^{\xi t_j}}{t_j}\rho(u-t_1-\cdots-t_j)e^{\xi(u-t_1-\cdots-t_j)}\,dt_1\ldots dt_j.$$

Setting $F(\xi) = \max_{t\geq 0}\rho(t)e^{\xi t}$ we deduce (by forgetting the condition $t_1+\cdots+t_j \leq u$) that

$$\sigma(u) \leq F(\xi)e^{-\xi u}\sum_{j=0}^\infty \frac{1}{j!}\Big(\int_1^\infty \frac{\chi(t)e^{\xi t}}{t}\,dt\Big)^j = F(\xi)e^{-\xi u}\exp\Big(\int_1^\infty \frac{\chi(t)e^{\xi t}}{t}\,dt\Big).$$

Choose ξ such that $u = \int_1^\infty \chi(t)e^{\xi t}\,dt$, that is $\xi = \xi(u)$.

Now putting $C := \int_1^\infty \chi(v)\,dv$ we have $u = \int_1^\infty \chi(v)e^{\xi(u)v}\,dv \geq Ce^{\xi(u)}$, which implies that

$$F(\xi(u)) \leq \max_{t\geq 0}\left(\frac{(e+o(1))u}{t\log(t)C}\right)^t = e^{O(u/\log(u))},$$

and the upper bound follows. ∎

The Lower Bound: Fix $\epsilon > 0$.

We will show that there exists a constant C_ϵ such that

$$\sigma(u) > C_\epsilon \exp\Big((-\xi(u)-\epsilon)u + \int_1^\infty \frac{\chi(v)e^{\xi(u)v}}{v}\,dv\Big) \quad \text{for all } u \geq 0. \tag{15}$$

Let u_0 be a suitably large number, and define

$$C_\epsilon = C_{\epsilon,u_0} = \inf_{u\leq u_0} \sigma(u)\exp\Big((\xi(u)+\epsilon)u - \int_1^\infty \frac{\chi(v)e^{\xi(u)v}}{v}\,dv\Big).$$

Evidently (15) holds for all $u \leq u_0$.

We use an induction argument. Let $n \in \mathbb{N}$ such that $n > u_0$ and suppose that (15) is verified for all $t \leq n$, then we will show that (15) holds for all $t \in [n, n+1]$.

Define $f(\xi) = \int_1^\infty \frac{\chi(v)e^{\xi v}}{v}\,dv$, and let $u \in [n, n+1]$. Then using our hypothesis we have

$$\begin{aligned}\frac{\sigma(u)e^{((\xi(u)+\epsilon)u)}}{C_\epsilon \exp(f(\xi(u)))} &= \frac{1}{C_\epsilon u}\int_0^u \chi(t)e^{(\xi(u)+\epsilon)t}\sigma(u-t)e^{((\xi(u)+\epsilon)(u-t)-f(\xi(u))\,dt} \\ &\geq \frac{1}{u}\int_1^u \chi(t)\exp\Big((\xi(u)+\epsilon)t + (\xi(u)-\xi(u-t))(u-t) \\ &\qquad + f(\xi(u-t)) - f(\xi(u))\Big)\,dt.\end{aligned} \tag{16}$$

Since $f'(\xi) = \int_1^\infty \chi(v)e^{\xi v}\,dv$, using the mean value theorem we deduce that

$$u - t \leq \frac{f(\xi(u)) - f(\xi(u-t))}{\xi(u)-\xi(u-t)} \leq u. \tag{17}$$

Now differentiating $u = \int_1^\infty \chi(v)e^{\xi(u)v}\,dv$ with respect to u we get that

$$\xi'(u) = \Big(\int_1^\infty v\chi(v)e^{\xi(u)v}\,dv\Big)^{-1} \leq \frac{1}{u}. \tag{18}$$

By (18) and using the mean value theorem again we have

$$\xi(u) - \xi(u-t) \leq \frac{t}{u-t}. \tag{19}$$

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

Therefore by (17), then (19) we deduce that

(20)
$$\begin{aligned}\frac{1}{u}\int_1^u \chi(t)\exp\big((\xi(u)+\epsilon)t+(\xi(u)-\xi(u-t))(u-t)+f(\xi(u-t))-f(\xi(u))\big)\,dt\\ \geq \frac{1}{u}\int_1^u \chi(t)\exp\big((\xi(u)+\epsilon)t-t(\xi(u)-\xi(u-t))\big)\,dt\\ \geq \frac{1}{u}\int_1^u \chi(t)\exp\Big((\xi(u)+\epsilon)t-\frac{t^2}{(u-t)}\Big)\,dt\\ \geq \frac{1}{u}\int_1^{\sqrt{u}} \chi(t)e^{(\xi(u)+\epsilon/2)t}\,dt, \quad \text{for } u\geq u_0.\end{aligned}$$

For case (i), since $\int_T^\infty \chi(t)\,dt = 0$ and $\chi(t)\geq 0$ for all t, then $\text{meas}\{t\geq T : \chi(t)\neq 0\} = 0$ which implies that $\text{meas}\{t\geq T : \chi(t)e^{\xi(u)t}\neq 0\} = 0$, and so $\int_T^\infty \chi(t)e^{\xi(u)t}\,dt = 0$. Then taking $u_0 > T^2$ we have

$$\int_1^{\sqrt{u}} \chi(t)e^{(\xi(u)+\epsilon/2)t}\,dt = \int_1^T \chi(t)e^{(\xi(u)+\epsilon/2)t}\,dt > \int_1^T \chi(t)e^{\xi(u)t}\,dt = u. \tag{21}$$

Now for case (ii), since $\chi(t) = \big(\{1+o(1)\}/h(t)\big)^t$, there exist two constants A_ϵ and B_ϵ for which

$$A_\epsilon\Big(\frac{\exp(-\epsilon/16)}{h(t)}\Big)^t < \chi(t) < B_\epsilon\Big(\frac{\exp(\epsilon/16)}{h(t)}\Big)^t \quad \text{for every } t\geq 0. \tag{22}$$

We consider two cases

Case 1 $\big(\frac{e^{\xi(u)}}{h(\sqrt{u})}\geq \exp(-\frac{\epsilon}{4}).\big)$ Since h is non-decreasing, we have by (22)

(23)
$$\begin{aligned}\int_1^{\sqrt{u}} \chi(t)e^{(\xi(u)+\epsilon/2)t}\,dt &\geq A_\epsilon\int_1^{\sqrt{u}}\Big(\frac{e^{(\xi(u)+7\epsilon/16)}}{h(t)}\Big)^t\,dt\\ &\geq A_\epsilon\int_1^{\sqrt{u}}\Big(\frac{e^{\xi(u)}}{h(\sqrt{u})}\Big)^t e^{(7\epsilon/16)t}\,dt \geq A_\epsilon\int_1^{\sqrt{u}} e^{(3\epsilon/16)t}\,dt\\ &= \frac{16A_\epsilon}{3\epsilon}\big(e^{(3\epsilon/16)\sqrt{u}}-e^{3\epsilon/16}\big) > u,\end{aligned}$$

for $u > u_0$.

Case 2 $\big(\frac{e^{\xi(u)}}{h(\sqrt{u})}\leq \exp(-\frac{\epsilon}{4}).\big)$ Using Lemma 5.1 and (22), then the fact that h is non-

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

decreasing and $u \geq Ce^{\xi(u)}$ we conclude that

$$
\begin{aligned}
(24) \qquad \int_1^{\sqrt{u}} \chi(t)e^{(\xi(u)+\epsilon/2)t}\,dt &\geq \int_1^{\sqrt{u}} \chi(t)e^{(\xi(u)+\epsilon/8)t}\,dt \\
&\geq u^{1+\epsilon/(16\xi(u))} - B_\epsilon \int_{\sqrt{u}}^{\infty} \Big(\frac{e^{(\xi(u)+3\epsilon/16)}}{h(t)}\Big)^t\,dt \\
&\geq u^{1+\epsilon/(16\xi(u))} - B_\epsilon \int_{\sqrt{u}}^{\infty} \Big(\frac{e^{\xi(u)}}{h(\sqrt{u})}\Big)^t e^{(3\epsilon/16)t}\,dt \\
&\geq u^{1+\epsilon/(16\xi(u))} - B_\epsilon \frac{16}{\epsilon}\exp(-\epsilon\sqrt{u}/16) > u,
\end{aligned}
$$

for $u > u_0$. Thus using (16), (20) then (21), (23), and (24) the result follows. ■

6 Getting the Asymptotic Approximation of σ Explicitly

Lemma 6.1 *If $\xi(u) = o(\log(u))$ as $u \to \infty$, then*

$$\int_1^\infty \frac{\chi(v)e^{\xi(u)v}}{v}\,dv = o(u)$$

and so $\sigma(u) = \exp((-\xi(u) + o(1))u)$.

Proof Since $\chi(t) \leq 1$ for every $t \geq 1$ and using our assumption, we have

$$
\begin{aligned}
\int_1^\infty \frac{\chi(v)e^{\xi(u)v}}{v}\,dv &= \int_1^{\frac{\log(u)}{\xi(u)}} \frac{\chi(v)e^{\xi(u)v}}{v}\,dv + \int_{\frac{\log(u)}{\xi(u)}}^\infty \frac{\chi(v)e^{\xi(u)v}}{v}\,dv \\
&\leq \int_1^{\frac{\log(u)}{\xi(u)}} e^{\xi(u)v}\,dv + \frac{\xi(u)}{\log(u)}\int_1^\infty \chi(v)e^{\xi(u)v}\,dv \\
&= \frac{1}{\xi(u)}\left(u - e^{\xi}\right) + \frac{\xi(u)u}{\log(u)} = o(u).
\end{aligned}
$$
■

Proof of Proposition 1.9 Let $\zeta(u)$ be the unique continuous solution to the equation $u = e^{\zeta(u)T}/\zeta(u)$. Since $\chi(t) \leq 1$ for all t, we have

$$\frac{e^{\zeta(u)T}}{\zeta(u)} = \int_1^T \chi(v)e^{\xi(u)v}\,dv \leq \frac{e^{\xi(u)T} - e^{\xi(u)}}{\xi(u)} < \frac{e^{\xi(u)T}}{\xi(u)},$$

and since the function $f(\xi) = e^{\xi T}/\xi$ is non-decreasing for $\xi > 1$ we deduce that $\zeta(u) \leq \xi(u)$. Now fix $\epsilon > 0$ (such that $T(1-\epsilon) > 1$), and suppose that there is

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

arbitrary large u for which $\xi(u) > \zeta(u)(1+\epsilon)$. Define $s_\epsilon = \int_{T(1-\epsilon/3)}^{T} \chi(t)\,dt > 0$ (by the definition of T). We deduce under our assumption that

$$s_\epsilon e^{\zeta(u)(1+\epsilon/3)T} \le s_\epsilon e^{T(1-\epsilon/3)\xi(u)} \le \int_{T(1-\epsilon/3)}^{T} \chi(v) e^{\xi(u)v}\,dv \le \frac{e^{\zeta(u)T}}{\zeta(u)},$$

which is impossible if u is large enough. Thus $\xi(u) = \zeta(u)(1+o(1))$ as $u \to \infty$. Now we trivially have $1 \ll \zeta(u) \ll \log(u)$, then

$$\zeta(u) = \frac{\log(u)}{T} + \frac{\log(\zeta(u))}{T} = \frac{\log(u)}{T}(1+o(1)).$$

We deduce that $\xi(u) = \frac{\log(u)}{T}(1+o(1))$, and the result follows combining Theorem 1.8 with the fact that $\int_1^T \frac{\chi(v)e^{\xi(u)v}}{v}\,dv = O(u)$. ■

Now we prove Proposition 1.10; define $g(u) := h(u)/(uh'(u))$.

Lemma 6.2 *Let $h(u)$ be a real differentiable function with $uh'(u)/h(u) = n + o(1)$, where n is a positive constant. Then for all $k > 0$ we have $h(ku) = h(u)k^{n+o(1)}$.*

Proof We have that

$$\log\Big(\frac{h(ku)}{h(u)}\Big) = \int_u^{ku} \frac{h'(t)}{h(t)}\,dt = \int_u^{ku} \frac{(n+o(1))}{t}\,dt = (n+o(1))\log k. \qquad ■$$

Lemma 6.3 *Assume the hypothesis of Proposition* 1.10(b)*. Then $h(v(u)\log(u)) = (1+o(1))h(\log u)$, where $v(u) := \min(\log(u), \min_{\log(u)\le t\le \log^2(u)} g(t))$, and $v(u) \to \infty$ as $u \to \infty$.*

Proof Since $g(t) \to \infty$ as $t \to \infty$ then $v(u) \to \infty$ as $u \to \infty$, so if u is large, then $v(u)\log(u) > \log u$, so that $h(v(u)\log(u)) \ge h(\log u)$. On the other hand,

$$\begin{aligned}\log\Big(\frac{h(v(u)\log(u))}{h(\log(u))}\Big) &= \int_{\log(u)}^{v(u)\log(u)} \Big(\frac{h'(t)}{h(t)}\Big)\,dt = \int_{\log(u)}^{v(u)\log(u)} \frac{1}{tg(t)}\,dt \\ &\le \frac{1}{\min_{\log(u)\le t\le v(u)\log(u)} g(t)} \int_{\log(u)}^{v(u)\log(u)} \frac{dt}{t} \\ &\le \frac{1}{v(u)}(1+\log(v(u))) = o(1). \qquad ■\end{aligned}$$

Proof of Proposition 1.10 Fix $\epsilon > 0$ and suppose that there is arbitrary large u for which $\xi(u) > \log(h(\zeta\log(u))) + \epsilon$. Then for such u we have in case (a), by (22),

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

Lemma 6.2, and since h is non-decreasing,

$$u = \int_1^\infty \chi(t) e^{\xi(u)t}\,dt > A_\epsilon \int_1^\infty \Big(\frac{e^{\xi(u)-\epsilon/16}}{h(t)}\Big)^t\,dt$$
$$\geq A_\epsilon \int_{\log\log(u)}^{\log(u)/n} e^{(\epsilon/2)t}\Big(\frac{h(e\log(u)/n)}{h(\log(u)/n)}\Big)^t\,dt$$
$$= A_\epsilon \int_{\log\log(u)}^{\log(u)/n} e^{(\epsilon/2+n+o(1))t}\,dt > A_\epsilon \int_{\log\log(u)}^{\log(u)/n} e^{(\epsilon/4+n)t}\,dt > u,$$

for u large enough, which is a contradiction.

Now in case (b), our assumption and Lemma 6.3 imply that

$$\xi(u) > \log\big(h\big(\nu(u)\log(u)\big)\big) + \epsilon/2.$$

Then by (22) and since h is non-decreasing and $\nu(u) \to \infty$ as $u \to \infty$,

$$u = \int_1^\infty \chi(t)e^{\xi(u)t}\,dt > A_\epsilon \int_1^\infty \Big(\frac{e^{\xi(u)-\epsilon/16}}{h(t)}\Big)^t\,dt \geq A_\epsilon \int_1^{\nu(u)\log(u)} e^{(\epsilon/3)t}\,dt$$
$$= A_\epsilon \frac{3}{\epsilon}\big(u^{\nu(u)\epsilon/3} - e^{\epsilon/3}\big) > u,$$

for u large enough, which is a contradiction.

Now we suppose that there is arbitrary large u for which

$$\xi(u) < \log\big(h(\zeta\log(u))\big) - \epsilon.$$

Then for such u let $q(t) := (\xi(u) + \epsilon/16 - \log(h(t)))t$, so that

$$q'(t) = \xi(u) + \frac{\epsilon}{16} - \log(h(t)) - \Big(\frac{th'(t)}{h(t)}\Big).$$

Now in case (a), $q'(t) = \xi(u) + \epsilon/16 - \log(h(t)) - n + o(1)$, therefore the maximum of $q(t)$ holds at some point t_0 for which $q'(t_0) = 0$, so that under our assumption,

$$h(t_0) = e^{\xi(u)+\epsilon/16-n+o(1)} < h(e\log(u)/n)e^{-n-\epsilon/2}. \tag{25}$$

Now we must have

$$t_0 < \log(u)(1 - \epsilon/(4n))/n, \tag{26}$$

otherwise, since h is non-decreasing and by Lemma 6.2,

$$\frac{h(t_0)}{h(e\log(u)/n)} \geq \frac{h\big(\frac{\log(u)}{n}\big(1-\frac{\epsilon}{4n}\big)\big)}{h(e\log(u)/n)} = \Big(\Big(1-\frac{\epsilon}{4n}\Big)e^{-1}\Big)^{n+o(1)} > e^{-n-\epsilon/2},$$

https://doi.org/10.4153/CJM-2007-006-4 Published online by Cambridge University Press

contradicting (25). By (22), (25), and (26) and since h is non-decreasing, we deduce that

$$\begin{aligned} u &= \int_1^\infty \chi(t)e^{\xi(u)t}\,dt < B_\epsilon \int_1^\infty \Big(\frac{e^{\xi(u)+\epsilon/16}}{h(t)}\Big)^t\,dt \\ &= B_\epsilon \int_1^{e\log(u)/n} \Big(\frac{e^{\xi(u)+\epsilon/16}}{h(t)}\Big)^t\,dt + B_\epsilon \int_{e\log(u)/n}^\infty \Big(\frac{e^{\xi(u)+\epsilon/16}}{h(t)}\Big)^t\,dt \\ &\leq B_\epsilon \frac{e\log(u)}{n}\Big(\frac{e^{\xi(u)+\epsilon/16}}{h(t_0)}\Big)^{t_0} + B_\epsilon \int_{e\log(u)/n}^\infty e^{-\epsilon/2t}\,dt \\ &= B_\epsilon \frac{e\log(u)}{n}(e^{n+o(1)})^{t_0} + o(1) < u, \end{aligned}$$

for u large enough, which is a contradiction.

For case (b) $q'(t) = \xi(u)+\epsilon/16-\log(h(t)) - \frac{1}{g(t)}$, and the maximum of $q(t)$ holds at some point t_0 for which $q'(t_0) = 0$ (to avoid redundancy we take $t_0 = \min\{t : q'(t) = 0\}$, which is possible by the continuity of $h(t)$ and $g(t)$). Now $t_0 \to \infty$ as $u \to \infty$, otherwise $q'(t_0) > 0$ for u large enough. Thus,

$$\Big(\frac{e^{\xi(u)+\epsilon/16}}{h(t_0)}\Big)^{t_0} = \exp\Big(\frac{t_0}{g(t_0)}\Big) = e^{o(t_0)}. \tag{27}$$

Now by (22),

$$\begin{aligned} u &= \int_1^\infty \chi(t)e^{\xi(u)t}\,dt \leq B_\epsilon \int_1^\infty \Big(\frac{e^{\xi(u)+\epsilon/16}}{h(t)}\Big)^t\,dt \\ &= B_\epsilon \int_1^{\log(u)} \Big(\frac{e^{\xi(u)+\epsilon/16}}{h(t)}\Big)^t\,dt + B_\epsilon \int_{\log(u)}^\infty \Big(\frac{e^{\xi(u)+\epsilon/16}}{h(t)}\Big)^t\,dt. \end{aligned} \tag{28}$$

Considering the cases $t_0 \leq \log(u)$ and $t_0 > \log(u)$ (in which case $q(t)$ is increasing on $[1, \log(u)]$), and using (27) and our assumption on $\xi(u)$ we get that

$$\int_1^{\log(u)} \Big(\frac{e^{\xi(u)+\epsilon/16}}{h(t)}\Big)^t\,dt \leq \max(\log(u)e^{o(\log(u))}, \log(u)\exp(-\epsilon/2\log(u))) = u^{o(1)},$$

using this, (28) and the assumption on $\xi(u)$ we deduce that

$$u \leq B_\epsilon u^{o(1)} + B_\epsilon \int_{\log(u)}^\infty e^{-\epsilon/2t}\,dt = u^{o(1)} + o(1),$$

which contradicts our hypothesis.

Now in both cases $h'(t)/h(t) \leq c/t$ for some positive constant c and for all t. Then integrating both sides gives $h(t) \ll t^c$, and this with our result implies $\xi(u) \ll \log(\log(u))$. Thus by Lemma 6.1 and Theorem 1.8 the proposition follows. ■

Acknowledgments I sincerely thank my advisor, Professor Andrew Granville, for all his advice and encouragement. I also thank the referee for his rigorous comments and remarks.

References

[1] R. C. Baker and G. Harman, *Shifted primes without large prime factors.* Acta Arith. **83**(1998), no. 4, 331–361.
[2] H. Davenport, *Multiplicative Number Theory.* Second edition. Graduate Texts in Mathematics 74, Springer-Verlag, New York, 1980.
[3] P. Erdős, *Some remarks on the iterates of the φ and σ functions.* Colloq. Math. **17**(1967), 195–202.
[4] ———, *On the normal number of prime factors of $p - 1$ and some other related problems concerning Euler's ϕ-function.* Quart. J. Math. **6**(1935) 205–213.
[5] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions.* In: Analytic Number Theory. Progr. Math. 85, Birkhäuser, Boston, 1990, pp. 165–204.
[6] P. Erdős and C. Pomerance, *On the normal number of prime factors of $\phi(n)$.* Rocky Mountain Math. J. **15**(1985), 343–352.
[7] A. Granville, *Smooth numbers: computational number theory and beyond.* In: Proceedings MSRI Conference on Algorithmic Number Theory, Cambridge University Press, Cambridge, to appear.
[8] A. Granville and K. Soundararajan, *The spectrum of multiplicative functions.* Annals of Math. **153**(2001), 407–470.
[9] H. Halberstam and H.-E. Richert, *Sieve Methods.* London Mathematical Society Monographs 4, Academic Press, London, 1974.
[10] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors.* J. Théor. Nombres Bordeaux **5**(1993), 411–484.
[11] C. Pomerance, *Popular values of Euler's function.* Mathematika **27**(1980), 84–89.
[12] H. Shapiro, *An arithmetic function arising from the ϕ-function.* Amer. Math. Monthly **50**(1943), 18–30.
[13] G. Tenenbaum, *Introduction à la théorie analytique et probabilistique des nombres.* Cours spélialisés 1, Société Mathématique de France, Paris, 1995.

Départment de Mathématiques et Statistique
Université de Montréal
CP 6128 succ Centre-Ville
Montréal, QC
H3C 3J7
e-mail: Lamzouri@dms.umontreal.ca