

Phi, primorials, and Poisson

Paul Pollack and Carl Pomerance

.....

Abstract The primorial $p\#$ of a prime p is the product of all primes $q \leq p$. Let $\text{pr}(n)$ denote the largest prime p with $p\# \mid \phi(n)$, where ϕ is Euler's totient function. We show that the normal order of $\text{pr}(n)$ is $\log \log n / \log \log \log n$; that is, $\text{pr}(n) \sim \log \log n / \log \log \log n$ as $n \rightarrow \infty$ on a set of integers of asymptotic density 1. In fact, we show there is an asymptotic secondary term and, on a tertiary level, there is an asymptotic Poisson distribution. We also show an analogous result for the largest integer k with $k! \mid \phi(n)$.

1. Introduction

Euler's *totient function* $\phi(n)$ may be defined as the number of units in the residue ring $\mathbb{Z}/n\mathbb{Z}$, or equivalently via the formula

$$\phi(n) = n \prod_{\ell \mid n} \left(1 - \frac{1}{\ell}\right),$$

where the product on ℓ is over the distinct primes dividing n . Our starting point in this article is the following remarkable property of ϕ : For every fixed prime number p , almost every value of $\phi(n)$ is divisible by p . Here “almost every” means that, as $x \rightarrow \infty$, all but $o(x)$ values of $n \leq x$ are such that $p \mid \phi(n)$.

How could this possibly be the case? A small piece of probabilistic reasoning dispels the mystery: Observe that $\phi(n)$ is divisible by p whenever n is divisible by a prime $\ell \equiv 1 \pmod{p}$. Those primes ℓ make up a positive proportion of all primes—namely, 1 in $p - 1$, by the prime number theorem for arithmetic progressions. Almost all numbers $n \leq x$ have $\approx \log \log x$ distinct prime factors (a classical result of Hardy and Ramanujan), and it should be unusual for these many prime factors to all avoid the residue class $1 \pmod{p}$. This argument is merely heuristic, but it can be made rigorous by sieve methods or by analytic methods going back to Landau (further developed by Selberg and Delange). An early reference for this fact about ϕ is [1]; that paper treats $\sigma(n)$ (the sum-of-divisors function) rather than $\phi(n)$, but the proof is almost the same.

It follows that there is a function $y = y(x)$, tending monotonically to infinity, with the property that all but $o(x)$ values of $n \leq x$ are divisible by $\prod_{p \leq y} p$, as $x \rightarrow \infty$. It is implicit in the arguments of Erdős in [4] (see also [5]) that $y = (\log \log x)^{1-\epsilon}$ is admissible, for any fixed $\epsilon \in (0, 1)$. Erdős's reasoning is developed in [3] and [12],

where it is shown that we may take $y = c \log \log x / \log \log \log x$ for some positive constant c . Among other things, our main result yields a very precise determination of the allowable choice of y .

We need a bit of set-up to state our main theorem. With \log_k denoting the k -fold iterated logarithm, we set

$$A(x) = \frac{\log_2 x}{\log_3 x} + 3 \frac{\log_2 x \cdot \log_4 x}{(\log_3 x)^2}, \quad B(x) = \frac{\log_2 x}{(\log_3 x)^2}.$$

For $n \leq x$ and Λ real, we set

$$f(n, \Lambda) = \#\{\text{primes } p \leq A(x) + \Lambda \cdot B(x) : p \nmid \phi(n)\}.$$

THEOREM 1

Fix $\lambda > 0$. Then $f(n, \log \lambda)$, as a statistic on integers $n \leq x$, is asymptotically Poisson distributed with parameter λ ; that is, for each fixed non-negative integer k , the proportion of $n \leq x$ with

$$\#\{\text{primes } p \leq A(x) + (\log \lambda)B(x), p \nmid \phi(n)\} = k$$

tends to $e^{-\lambda} \frac{\lambda^k}{k!}$, as $x \rightarrow \infty$.

Taking $k = 0$ in Theorem 1, we deduce

<p>(1) The limiting proportion of $n \leq x$ with $\phi(n)$ divisible by all primes up to $A(x) + (\log \lambda)B(x)$ is $e^{-\lambda}$.</p>
--

This has the following immediate consequence.

COROLLARY 2

Whenever $\Lambda = \Lambda(x) \rightarrow \infty$ as $x \rightarrow \infty$, almost all $n \leq x$ have $\phi(n)$ divisible by all primes up to $A(x) - \Lambda(x)B(x)$, while almost no $n \leq x$ have $\phi(n)$ divisible by all primes up to $A(x) + \Lambda(x)B(x)$.

As the astute reader may have noticed, the argument sketched at the start of the introduction works equally well to show that $\phi(n)$ is almost always divisible by any fixed integer m (not necessarily prime!). This point of view suggests studying the largest factorial dividing $\phi(n)$. In Section 3, we establish the natural factorial analogues of (1) and Corollary 2.

In Section 4, we consider the primorial and factorial problems for Carmichael’s universal exponent function $\lambda(n)$. Finally, in Section 5, we raise the related questions where instead of asking what occurs for almost all n , we ask what occurs for almost all ϕ -values, or λ -values.

Notation

Throughout, we reserve the letters ℓ and p for primes. We use the notation $v_p(n)$ to denote the largest integer v with $p^v \mid n$.

2. Proof of Theorem 1

LEMMA 3

Let \mathcal{P} be a set of primes, let $x \geq 1$, and let $S = \sum_{\ell \in \mathcal{P}, \ell \leq x} \frac{1}{\ell}$. Uniformly for all choices of \mathcal{P} , the proportion of $n \leq x$ free of prime factors from \mathcal{P} is $\ll \exp(-S)$.

Proof

This result follows from Brun’s sieve; see [10, Theorem 2.2]. □

LEMMA 4

Let m be a positive integer, and let $x \geq 3$. Put

$$S(x; m) = \sum_{\substack{\ell \leq x \\ \ell \equiv 1 \pmod{m}}} \frac{1}{\ell}.$$

Then

$$S(x; m) = \frac{\log_2 x}{\phi(m)} + O\left(\frac{\log(2m)}{\phi(m)}\right).$$

Proof

See [14, Remark 1] or the lemma on p. 699 of [13]. □

It will be convenient in proving Theorem 1 to work with a variant of $f(n, \Lambda)$ that seems less natural but is more amenable to analysis. Put

$$\tilde{\phi}(n) = \prod_{\substack{\ell|n \\ \ell \leq x^{1/\log_3 x}}} (\ell - 1),$$

let

$$A_0(x) = \log_2 x / \log_3 x,$$

and define

$$g(n, \Lambda) = \#\{p : A_0(x) < p \leq A(x) + \Lambda \cdot B(x), \text{ and } p \nmid \tilde{\phi}(n)\}.$$

The next lemma assures us that for the density results we aim at, there is no difference dealing with g versus f .

LEMMA 5

Fix a real number Λ . The proportion of $n \leq x$ with $f(n, \Lambda) \neq g(n, \Lambda)$ tends to 0, as $x \rightarrow \infty$.

Proof

Suppose that $f(n, \Lambda) \neq g(n, \Lambda)$. Then either there is a prime p counted by f and not by g , or vice versa.

In the first case, we must have $p \leq A_0(x)$. Since $p \nmid \phi(n)$, there is no prime $\ell \equiv 1 \pmod p$ for which $\ell \mid n$. By Lemmas 3 and 4, the proportion of $n \leq x$ satisfying this latter condition is

$$\ll \exp(-S(x; p)) \leq \exp\left(-\frac{\log_2 x}{p-1} + O(1)\right) \ll \frac{1}{\log_2 x}.$$

Summing on $p \leq A_0(x)$, we find that the proportion of $n \leq x$ occurring in this first case is $O(1/(\log_3 x)^2)$, and so is $o(1)$.

In the second case, $p > A_0(x)$ and $p \mid \phi(n)$, but $p \nmid \tilde{\phi}(n)$. Thus, either

- (i) $p^2 \mid n$, or
- (ii) there is a prime $\ell \mid n$, $\ell \equiv 1 \pmod p$ with $\ell > x^{1/\log_3 x}$.

The proportion of $n \leq x$ for which (i) can occur (for some p) is $\ll \sum_{p > A_0(x)} \frac{1}{p^2}$, and so is $o(1)$. The proportion of $n \leq x$ for which (ii) can occur is

$$\ll \sum_{A_0(x) < p \leq A(x) + \Lambda \cdot B(x)} \sum_{\substack{\ell \equiv 1 \pmod p \\ x^{1/\log_3 x} < \ell \leq x}} \frac{1}{\ell}.$$

By Brun–Titchmarsh and partial summation, the inner sum on ℓ is $O((\log_4 x)/p)$, making the last display (for large x)

$$\begin{aligned} &\ll \log_4 x \sum_{A_0(x) < p \leq A(x) + \Lambda \cdot B(x)} \frac{1}{p} \ll \frac{\log_4 x}{A_0(x)} \cdot \#\{p : A_0(x) < p \leq A(x) + \Lambda \cdot B(x)\} \\ &\leq \frac{\log_4 x}{A_0(x)} \cdot \#\{p : A_0(x) < p \leq 2A_0(x)\} \ll \frac{\log_4 x}{A_0(x)} \cdot \frac{A_0(x)}{\log A_0(x)} \ll \frac{\log_4 x}{\log_3 x}. \end{aligned}$$

Thus, the proportion of $n \leq x$ as in (ii) is also $o(1)$. □

In view of Lemma 5, to prove Theorem 1 it suffices to show that $g(n, \log \lambda)$ is asymptotically Poisson distributed with parameter λ . The Poisson distribution of parameter λ , which we will denote by $\mathcal{P}_O(\lambda)$, is determined by its moments (see, for instance, [2, Theorem 30.1, p. 388; and Example 21.4, p. 279]). It is equivalent, but somewhat simpler here, to work with factorial moments instead of moments. The r th factorial moment of $\mathcal{P}_O(\lambda)$ is λ^r , and so by the Fréchet–Shohat moment theorem (see [8, Theorem 28, p. 81]), it is enough to prove that

$$(2) \quad \lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} g(n, \log \lambda)(g(n, \log \lambda) - 1) \cdots (g(n, \log \lambda) - (r - 1)) = \lambda^r$$

for each fixed $r = 1, 2, 3, \dots$

We recognize the falling factorial in (2) as counting the number of ordered r -tuples of distinct primes $p \in (A_0(x), A(x) + (\log \lambda)B(x)]$ not dividing $\tilde{\phi}(n)$. Thus,

$$(3) \quad \begin{aligned} &\frac{1}{x} \sum_{n \leq x} g(n, \log \lambda)(g(n, \log \lambda) - 1) \cdots (g(n, \log \lambda) - (r - 1)) \\ &= \frac{1}{x} \sum_{\substack{A_0(x) < p_1, \dots, p_r \leq A(x) + (\log \lambda)B(x) \\ p_1, \dots, p_r \text{ distinct}}} \#\{n \leq x : \gcd(\tilde{\phi}(n), p_1 \cdots p_r) = 1\}. \end{aligned}$$

Fix distinct primes p_1, \dots, p_r as in the sum. Putting $\mathcal{L} = \{\ell \leq x^{1/\log_3 x} : \ell \equiv 1 \pmod{p_i} \text{ for some } i\}$, the right-hand summand in (3) counts those $n \leq x$ not divisible by any prime $\ell \in \mathcal{L}$. By the fundamental lemma of the sieve,¹ this count is $\sim x \prod_{\ell \in \mathcal{L}} (1 - \frac{1}{\ell})$ as $x \rightarrow \infty$, where the asymptotic holds uniformly in p_1, \dots, p_r . Since each $\ell > A_0(x)$, this is in turn $\sim x \exp(-T)$, where $T = \sum_{\ell \in \mathcal{L}} \frac{1}{\ell}$. Now

$$T = \sum_{i=1}^r \sum_{\substack{\ell \leq x^{1/\log_3 x} \\ \ell \equiv 1 \pmod{p_i}}} \frac{1}{\ell} + o\left(\max_{i,j} \sum_{\substack{\ell \leq x^{1/\log_3 x} \\ \ell \equiv 1 \pmod{p_i p_j}}} \frac{1}{\ell}\right).$$

(We suppress the dependence of the implied constant on r , which is fixed.) Since each $p_i p_j > A_0(x)^2 > (\log_2 x)^{1.9}$, Lemma 4 implies that the O -term here is $o(1)$, as $x \rightarrow \infty$. Thus, $\exp(-T) \sim \prod_{i=1}^r \exp(-\sum_{\substack{\ell \leq x^{1/\log_3 x} \\ \ell \equiv 1 \pmod{p_i}}} \frac{1}{\ell})$, and

$$(4) \quad \frac{1}{x} \#\{n \leq x : \gcd(\tilde{\phi}(n), p_1 \cdots p_r) = 1\} \sim \prod_{i=1}^r \exp\left(-\sum_{\substack{\ell \leq x^{1/\log_3 x} \\ \ell \equiv 1 \pmod{p_i}}} \frac{1}{\ell}\right).$$

By Lemma 4, the remaining sum on ℓ is $\frac{1}{p_i-1} \log_2(x^{1/\log_3 x}) + o(1) = \frac{1}{p_i} \log_2 x + o(1)$, so that the RHS in (4) is $\sim \prod_{i=1}^r \exp(-\log_2 x / p_i)$. All of our asymptotic results hold uniformly in p_1, \dots, p_r , and so summing on p_1, \dots, p_r yields

$$(5) \quad \frac{1}{x} \sum_{n \leq x} g(n, \log \lambda) (g(n, \log \lambda) - 1) \cdots (g(n, \log \lambda) - (r - 1)) \\ \sim \sum_{\substack{A_0(x) < p_1, \dots, p_r \leq A(x) + (\log \lambda) B(x) \\ p_1, \dots, p_r \text{ distinct}}} \prod_{i=1}^r \exp\left(-\frac{\log_2 x}{p_i}\right).$$

We briefly digress to study the effect of removing the distinctness condition on the p_i from this last expression. The resulting sum is the r th power of

$$(6) \quad \sum_{A_0(x) < p \leq A(x) + (\log \lambda) B(x)} \exp\left(-\frac{\log_2 x}{p}\right) \\ = \int_{A_0(x)}^{A(x) + (\log \lambda) B(x)} \exp\left(-\frac{\log_2 x}{u}\right) d\pi(u).$$

Write $\pi(u) = \int_2^u \frac{du}{\log u} + E(u)$, so that $d\pi(u) = \frac{du}{\log u} + dE(u)$. Using that $E(u) \ll_K u / (\log u)^K$ for every fixed K (a strong form of the prime number theorem), a straightforward computation shows that the integral in (6), with $d\pi(u)$ replaced

1. Specifically, we use the following consequence of [10, Theorem 2.5]: If \mathcal{L} is any set of primes not exceeding $x^{1/\log_3 x}$, then the number of $n \leq x$ not divisible by any member of \mathcal{L} is $\sim x \prod_{\ell \in \mathcal{L}} (1 - 1/\ell)$, as $x \rightarrow \infty$, uniformly in \mathcal{L} .

by $dE(u)$, is $o(1)$. Turning to the remaining piece of integral, we see that

$$\int_{A_0(x)}^{A(x)+(\log \lambda)B(x)} \exp\left(-\frac{\log_2 x}{u}\right) \frac{du}{\log u} \sim \frac{1}{\log_3 x} \int_{A_0(x)}^{A(x)+(\log \lambda)B(x)} \exp\left(-\frac{\log_2 x}{u}\right) du.$$

Make the change of variables $u = A_0(x)(1+z)$. Then

$$\frac{1}{\log_3 x} \int_{A_0(x)}^{A(x)+(\log \lambda)B(x)} \exp\left(-\frac{\log_2 x}{u}\right) du = \frac{A_0(x)}{\log_3 x} \int_0^{\frac{3\log_4 x + \log \lambda}{\log_3 x}} \exp\left(-\frac{\log_3 x}{1+z}\right) dz.$$

Now $\frac{\log_3 x}{1+z} = (\log_3 x)(1-z) + o(1) = \log_3 x - z \log_3 x + o(1)$, uniformly for $0 \leq z \leq \frac{3\log_4 x + \log \lambda}{\log_3 x}$. Therefore,

$$\begin{aligned} \frac{A_0(x)}{\log_3 x} \int_0^{\frac{3\log_4 x + \log \lambda}{\log_3 x}} \exp\left(-\frac{\log_3 x}{1+z}\right) dz &\sim \frac{A_0(x)}{\log_2 x \log_3 x} \int_0^{\frac{3\log_4 x + \log \lambda}{\log_3 x}} \exp(z \log_3 x) dz \\ &\sim \frac{A_0(x)}{\log_2 x (\log_3 x)^2} \exp(3 \log_4 x + \log \lambda) = \lambda. \end{aligned}$$

Collecting all of the estimates of this paragraph, we conclude that as $x \rightarrow \infty$,

$$\sum_{A_0(x) < p \leq A(x) + (\log \lambda)B(x)} \exp\left(-\frac{\log_2 x}{p}\right) \rightarrow \lambda.$$

When $r = 1$, the work of the last paragraph establishes that the left-hand side of (5) converges to λ^r . We also see that the same convergence assertion will follow for $r > 1$ provided that

$$(7) \quad \sum_{\substack{A_0(x) < p_1, \dots, p_r \leq A(x) + (\log \lambda)B(x) \\ \text{some } p_i = p_j \text{ with } i \neq j}} \prod_{i=1}^r \exp\left(-\frac{\log_2 x}{p_i}\right) = o(1).$$

If some $p_i = p_j$, then reordering the p_i , we can force $p_1 = p_2$. Thus, the expression in (7) is

$$\begin{aligned} &\ll \sum_{p, p_3, \dots, p_r} \exp\left(-2\frac{\log_2 x}{p}\right) \prod_{i=3}^r \exp\left(-\frac{\log_2 x}{p_i}\right) \\ &= \left(\sum_p \exp\left(-2\frac{\log_2 x}{p}\right)\right) \prod_{i=3}^r \left(\sum_{p_i} \exp\left(-\frac{\log_2 x}{p_i}\right)\right) \ll \sum_p \exp\left(-2\frac{\log_2 x}{p}\right), \end{aligned}$$

where, as above, p and the p_i range over $(A_0(x), A(x) + (\log \lambda)B(x)]$. The final sum on p is $o(1)$, since each summand is $\ll (\log_2 x)^{-1.9}$ (say), and there are crudely $O(\log_2 x)$ summands. This completes the proof of Theorem 1.

REMARK

One could ask not only for every prime up to a certain height to appear in $\phi(n)$, but for those primes to appear to at least the r th power, for one's favorite fixed positive integer r . The above analysis can be adapted to prove an analogue of Theorem 1 in this

generalized setting. Define

$$A_r(x) = \frac{\log_2 x}{\log_3 x} + (4 - r) \frac{\log_2 x \cdot \log_4 x}{(\log_3 x)^2}.$$

For integers $n \leq x$ and real Λ , set

$$f_r(n, \Lambda) = \#\{p \leq A_r(x) + \Lambda \cdot B(x) : p^r \nmid \phi(n)\}.$$

In analogy with Theorem 1 (the case $r = 1$), we can show that for each fixed $\lambda > 0$, the quantity $f_r(n, \log\{(r - 1)!\lambda\})$, considered on the integers $n \leq x$, is asymptotically Poisson distributed with parameter λ . The broad outline of the proof is the same as before; roughly speaking, the numbers with no small prime factors from the progression $1 \pmod p$ have their role replaced by those with at most $r - 1$ such prime factors. This thought is made more explicit in the next section.

3. From primorials to factorials

In this section we prove the following analogue of (1).

<p>(8) Fix $\lambda > 0$. The limiting proportion of $n \leq x$ with $\phi(n)$ divisible by $[y]!$, where $y = A(x) + (\log \lambda)B(x)$, is $e^{-\lambda}$.</p>
--

Note that the obvious counterpart of Corollary 2 follows as an immediate consequence.

Clearly, if $[y]! \mid \phi(n)$, then n is divisible by the product of all primes up to y . We will show that if $n \leq x$ and $\phi(n)$ is divisible by the product of all primes up to y , then apart from $o(x)$ exceptions, $\phi(n)$ is divisible by $[y]!$. Thus, (8) follows from (1).

For this, we appeal to the following generalization of Lemma 3, due essentially to Halász [9].

PROPOSITION 6

Let \mathcal{P} be a set of primes, let $x \geq 1$, and let $S = \sum_{\ell \in \mathcal{P}, \ell \leq x} \frac{1}{\ell}$. Suppose that $0 < \delta < 2$. Then for each integer m with $0 \leq m \leq (2 - \delta)S$, the proportion of $n \leq x$ with exactly m distinct prime factors from \mathcal{P} is

$$\ll_{\delta} \exp(-S) \frac{S^m}{m!}.$$

Actually, Halász counts prime factors with multiplicity, rather than distinct prime factors. The modifications necessary to establish the proposition as we have stated it are described by Norton [13, p. 688].

We suppose now that $n \leq x$, that $\phi(n)$ is divisible by all primes up to y (with $y = y(x)$ as in (8)), but that $[y]! \nmid \phi(n)$. Then we can find a prime $p \leq y$ with

$$1 \leq v_p(\phi(n)) < v_p([y]!).$$

Since $2 \leq v_p([y]!) = \sum_{r \geq 1} [y/p^r] < \frac{y}{p-1}$, we have $p - 1 < y/2$. Choose the integer $k \geq 2$ with

(9)
$$\frac{y}{k + 1} \leq p - 1 < \frac{y}{k}.$$

Then $v_p(\phi(n)) \leq k$, and so n is divisible by at most k primes from $\mathcal{P} = \{\ell \equiv 1 \pmod p\}$. Put $S = \sum_{\ell \leq x, \ell \equiv 1 \pmod p} \frac{1}{\ell}$, so that

$$S = \frac{1}{p-1} \log_2 x + O(1) \geq k \frac{\log_2 x}{y} + O(1) > \frac{9}{10} k \log_3 x + O(1) > 2k$$

for large x . By Proposition 6, the proportion of n divisible by at most k primes from \mathcal{P} is

$$\ll \exp(-S) \sum_{j=0}^k \frac{S^j}{j!} \ll \exp(-S) \frac{S^k}{k!} \ll \exp(-0.9k \log_3 x) \frac{S^k}{k!}.$$

Using $S \leq \frac{\log_2 x}{p-1} + O(\frac{\log(2p)}{p-1}) \ll \frac{\log_2 x}{p-1} \ll k \log_3 x$ (by Lemma 4) and $k! \geq (k/e)^k$, we find that the last displayed expression is

$$\ll \left(C \frac{\log_3 x}{(\log_2 x)^{0.9}} \right)^k,$$

where C is a certain absolute constant.

It remains to sum on the p 's corresponding to a given k , and then to sum on k . To each $k \geq 2$, there are (very crudely) $\ll y/\log y \ll \log_2 x / (\log_3 x)^2$ primes p in the range determined by (9). Hence, the proportion of n with $\phi(n)$ divisible by all primes up to y , but not by $\lfloor y \rfloor!$, is

$$\ll \sum_{k \geq 2} \frac{\log_2 x}{(\log_3 x)^2} \left(C \frac{\log_3 x}{(\log_2 x)^{0.9}} \right)^k \ll (\log_2 x)^{-0.8},$$

which tends to 0 as desired.

4. Carmichael's function

One might ask about analogues of Theorem 1 and the factorial problem of Section 3 for other number theoretic functions similar to ϕ . As one might expect, we have the same theorems for the sum-of-divisors function σ since the only complications are nontrivial prime powers, and for almost all n , nontrivial prime power divisors are small.

We now ask about Carmichael's function $\lambda(n)$. It is the order of the largest cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$; namely, the exponent of the unit group of $\mathbb{Z}/n\mathbb{Z}$. Carmichael's function is closely related to Euler's function ϕ . In fact, from the theorem on the primitive root and from the Chinese remainder theorem, we have that

$$\begin{aligned} \lambda(p^a) &= \phi(p^a) \quad \text{for } p > 2 \text{ or } p^a < 8, \\ \lambda(2^a) &= \frac{1}{2} \phi(2^a) \quad \text{for } a \geq 3, \\ \lambda(mn) &= \text{lcm}[\lambda(m), \lambda(n)] \quad \text{when } \gcd(m, n) = 1. \end{aligned}$$

(See, for instance, [11, Theorem 3, p. 44].) It is immediate that $p \mid \phi(n)$ if and only if $p \mid \lambda(n)$, so that we have the analogue of Theorem 1 for Carmichael’s function.²

The situation though for factorials is markedly different. Let $k_\lambda(n)$ denote the largest integer k with $k! \mid \lambda(n)$.

LEMMA 7

Let $\xi(n) \rightarrow \infty$ arbitrarily slowly. There is a set of integers S of asymptotic density 1 such that for $n \in S$,

- (i) $\frac{1}{\xi(n)} \log_2 n \leq \max\{2^{v_2(p-1)} : p \mid n\} \leq \xi(n) \log_2 n$,
- (ii) $v_2(\lambda(n)) = \max\{v_2(p-1) : p \mid n\}$,
- (iii) $k_\lambda(n)$ is the largest integer k with $v_2(k!) \leq v_2(\lambda(n))$.

Proof

We may assume that $\xi(x) \leq \log_3 x$. Let 2^m be the least power of 2 exceeding $(\log_2 x)/\xi(x)$ and let 2^M be the largest power of 2 not exceeding $\xi(x) \log_2 x$. It follows from Lemmas 3 and 4 that, but for $o(x)$ choices for integers $n \leq x$, we have a prime $p \mid n$ with $p \equiv 1 \pmod{2^m}$. Further, it follows from Lemma 4 that the proportion of integers $n \leq x$ divisible by a prime $p \equiv 1 \pmod{2^M}$ is $\ll (\log_2 x)/2^M = o(1)$. Thus, we have (i). The only way that (ii) would not hold is if the 2-power in $\lambda(n)$ is $\lambda(2^{v_2(n)})$. If also n satisfies (i), as we may assume, and $n \leq x$, this would imply that $2^{v_2(n)} > 2^m > (\log_2 x)/\xi(x)$. The number of such n is $O(x\xi(x)/\log_2 x) = o(x)$ as $x \rightarrow \infty$. Thus, we have (ii).

Using (i) and (ii), we have but for $o(x)$ choices of $n \leq x$ that

$$(10) \quad v_2(\lambda(n)) = \frac{\log_3 x}{\log 2} + O(\log \xi(x)).$$

It is clear that for any positive integer N , if $k! \mid N$, then $v_2(k!) \leq v_2(N)$. Thus, $k_\lambda(n) \leq k_0 := \max\{k : v_2(k!) \leq v_2(\lambda(n))\}$, so it will suffice to show that $k_0! \mid \lambda(n)$ almost surely.

Note that for any positive integer N we have $v_2(N!) = N + O(\log N)$, and for any prime p , $v_p(N!) \leq N/(p-1)$. Using (10), we may assume for $n \leq x$ that

$$(11) \quad k_0 = \frac{\log_3 x}{\log 2} + O(\log_4 x).$$

For $p \geq 3$, we have

$$p^{v_p(k_0!)} \leq \exp\left(\frac{k_0 \log p}{p-1}\right) \leq \exp\left(\frac{k_0 \log 3}{2}\right) = \exp\left(\frac{\log 3}{2 \log 2} \log_3 x + O(\log_4 x)\right).$$

It follows that we may assume for each prime $p \geq 3$ that $p^{v_p(k_0!)} \leq \exp(0.8 \log_3 x) = (\log_2 x)^{0.8}$.

2. It is unfortunate that mathematics uses the same symbol “ λ ” for a Poisson variable as for Carmichael’s function; we trust there will be no confusion.

For q a prime power at most $(\log_2 x)^{0.8}$, the number of $n \leq x$ not divisible by a prime $r \equiv 1 \pmod q$ is, by Lemmas 3 and 4, at most $x/\exp((\log_2 x)^{0.19})$. Summing this count for prime powers up to $(\log_2 x)^{0.8}$, we obtain an expression that is $o(x)$ as $x \rightarrow \infty$, so it follows that but for $o(x)$ choices of $n \leq x$, we have $p^{v_p(k_0!)} \mid \lambda(n)$ for all primes $3 \leq p \leq k_0$. Since by definition we have $2^{v_2(k_0!)} \mid \lambda(n)$, we have $k_0! \mid \lambda(n)$. This completes the proof of (iii). \square

THEOREM 8

For a set of integers n of asymptotic density 1, we have $k_\lambda(n) = \log_3 n/\log 2 + O(\log_4 n)$.

Proof

This follows immediately from Lemma 7, the definition of k_0 in its proof, and (11). \square

REMARK

Let $s_2(m)$ denote the number of 1's in the binary expansion of m . One can show that on a set of asymptotic density 1, $k_\lambda(n)$ is $m + O(\xi(n))$, where m is the largest integer with $m - s_2(m) \leq v_2(\lambda(n))$. In fact, $m - s_2(m) = v_2(m!)$, so the assertion follows from Lemma 7.

If k is even, then $v_2(k!) = v_2((k + 1)!) < v_2(j!)$ for all $j \geq k + 2$. Thus, Lemma 7 implies that on a set of asymptotic density 1, $k_\lambda(n)$ is an odd integer.

Let $k_\phi(n)$ denote the largest integer k with $k! \mid \phi(n)$; namely, the subject of Section 3. It follows from the arguments there that if p is the largest prime with $p\#$ (the primorial of p) dividing $\phi(n)$, then on a set of n of asymptotic density 1, $p! \mid \phi(n)$. In fact, on a set of asymptotic density 1, $p!M \mid \phi(n)$, where M is the product of all of the composite numbers in $(p, \frac{3}{2}p)$. (To see this, assume n is large and let q run over the primes to p . If $q > \frac{3}{4}p$, then $q \nmid M$. If $\frac{1}{7}p < q < \frac{3}{4}p$, then by the method of Section 3, we may assume that $q^{11} \mid \phi(n)$, so that $v_q(\phi(n)) \geq v_q(p!M)$. In addition, the method of Section 3 can be used to show that, away from a density 0 set, $v_q(\phi(n)) > (\log_2 x)/(2(q - 1)) > v_q(p!M)$ for all $q < p/7$.) Now, by a somewhat stronger version of Bertrand's postulate, we may assume the next prime r after p is $< \frac{3}{2}p$. We conclude that $(r - 1)! \mid \phi(n)$ and $k_\phi(n) = r - 1$. So on a set of asymptotic density 1, $k_\phi(n)$ is even. This is a striking incongruence from the situation with $k_\lambda(n)$.

5. A related problem

Let $\mathbb{V} = \phi(\mathbb{N})$; that is, \mathbb{V} is the set of distinct values of ϕ . Let $V(x)$ denote the number of members of \mathbb{V} in $[1, x]$. After earlier work of Pillai, Erdős, Hall, Maier, and Pomerance, we finally learned the order of magnitude of $V(x)$ in Ford [6]. Ignoring subsets of $\mathbb{V} \cap [1, x]$ of size $o(V(x))$ as $x \rightarrow \infty$, what can be said about the largest primorial (or factorial) which divides most members of $\mathbb{V} \cap [1, x]$? We know that most values of ϕ come from small fibers, and in particular there is a set of integers S of asymptotic density 0 such that $V(x) \sim \#(\phi(S) \cap [1, x])$ as $x \rightarrow \infty$. It seems likely to us that the key function here is exponentially smaller than $\log_2 x/\log_3 x$ and is of the form $(\log_3 x)^{1+o(1)}$. It would be nice to prove this assertion.

The analogous problem for Carmichael's function λ is even murkier. Let $V_\lambda(x)$ denote the number of λ values in $[1, x]$. We do not know the order of magnitude of $V_\lambda(x)$, only recently learning in [7] that $V_\lambda(x) = x/(\log x)^{\eta+o(1)}$ as $x \rightarrow \infty$, where $\eta = 1 - (1 + \log \log 2)/\log 2$.

Acknowledgments. We thank the referee for a careful reading of the manuscript and several helpful suggestions on the presentation. The second author is grateful for the hospitality of Santa Clara University and was funded by their Paul R. and Virginia P. Halmos Endowed Professorship in Mathematics and Computer Science.

References

- [1] L. Alaoglu and P. Erdős, *A conjecture in elementary number theory*, Bull. Amer. Math. Soc. **50** (1944), 881–882. MR 0011086. DOI 10.1090/S0002-9904-1944-08257-8.
- [2] P. Billingsley, *Probability and measure*, 3rd ed., Wiley Ser. Probab. Math. Stat., Wiley, New York, 1995. MR 1324786.
- [3] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, “On the normal behavior of the iterates of some arithmetic functions” in *Analytic Number Theory (Allerton Park, IL, 1989)*, Progr. Math. **85**, Birkhäuser Boston, Boston, 1990, 165–204. MR 1084181. DOI 10.1007/978-1-4612-3464-7_13.
- [4] P. Erdős, *Some asymptotic formulas in number theory*, J. Indian Math. Soc. (N.S.) **12** (1948), 75–78. MR 0029406.
- [5] P. Erdős, *Remarks on number theory, II*, Mat. Lapok **12** (1961), 161–169. MR 0144870.
- [6] K. Ford, *The distribution of totients*, Ramanujan J. **2** (1998), 67–151. MR 1642874. DOI 10.1023/A:1009761909132.
- [7] K. Ford, F. Luca, and C. Pomerance, *The image of Carmichael's λ -function*, Algebra Number Theory **8** (2014), 2009–2025. MR 3285622. DOI 10.2140/ant.2014.8.2009.
- [8] J. Galambos, *Advanced Probability Theory*, 2nd ed., Prob. Pure Appl., Marcel Dekker, New York, 1995. MR 1350792.
- [9] G. Halász, *Remarks to my paper: “On the distribution of additive and the mean values of multiplicative arithmetic functions.”* Acta Math. Acad. Sci. Hungar. **23** (1972), 425–432. MR 0319931. DOI 10.1007/BF01896961.
- [10] H. Halberstam and H.-E. Richert, *Sieve methods*, Lond. Math. Soc. Monogr. No. 4, Academic Press, London, 1974. MR 0424730.
- [11] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts Math. **84**, Springer-Verlag, New York, 1990. MR 1070716. DOI 10.1007/978-1-4757-2103-4.
- [12] F. Luca and C. Pomerance, *On some problems of Makowski–Schinzel and Erdős concerning the arithmetical functions ϕ and σ* , Colloq. Math. **92** (2002), 111–130, acknowledgement of priority in **126** (2012), 139. MR 1899242. DOI 10.4064/cm92-1-10.
- [13] K. K. Norton, *On the number of restricted prime factors of an integer. I*, Illinois J. Math. **20** (1976), no. 4, 681–705. MR 0419382.

- [14] C. Pomerance, *On the distribution of amicable numbers*, J. Reine Angew. Math. **293/294** (1977), 217–222. MR 0447087. DOI 10.1515/crll.1977.293-294.217.

Pollack: Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA;
pollack@uga.edu

Pomerance: Department of Mathematics, Santa Clara University, Santa Clara, California 95053, USA; (current) Department of Mathematics, Dartmouth College, Hanover, New Hampshire 03755, USA; carl.pomerance@dartmouth.edu