TWO REMARKS ON ITERATES OF EULER'S TOTIENT FUNCTION

PAUL POLLACK

Abstract. Let φ_k denote the kth iterate of Euler's φ-function. We study two questions connected with these iterates. First, we determine the average order of φ_k and $1/\varphi_k$; e.g., we show that for each $k \geq 0$,

$$\sum_{n \leq x} \varphi_{k+1}(n) \sim \frac{3}{k! e^{k\gamma} \pi^2} \frac{x^2}{(\log_3 x)^k} \qquad (x \to \infty),$$

where γ is the Euler–Mascheroni constant. Second, for prime values of p, we study the number of distinct primes dividing $\prod_{k=1}^{\infty} \varphi_k(p)$. These prime divisors are precisely the primes appearing in the Pratt tree for p, which has been the subject of recent work by Ford, Konyagin, and Luca. We show that for each $\epsilon > 0$, the number of distinct primes appearing in the Pratt tree for p is $> (\log p)^{1/2-\epsilon}$ for all but $x^{o(1)}$ primes $p \leq x$.

1. Introduction

Let φ be Euler's totient function, so that $\varphi(n) = \#(\mathbf{Z}/n\mathbf{Z})^\times$. For each $k \geq 0$, let φ_k denote the kth iterate of φ, with the understanding that $\varphi_0(n) = n$. The study of the φ_k was initiated by Pillai [12] (cf. Shapiro [14]), who investigated the least $k = k(n)$ for which $\varphi_k(n) = 1$. The study of these iterates was continued by Erdős, Granville, Pomerance, and Spiro [4]. Among other results, these authors showed that the ratio $\varphi(n)/\varphi_{k+1}(n)$ has a smooth, strictly increasing normal order:

Theorem A (see [4, Theorem 4.2])**.** *Fix a natural number k. There is a set $\mathscr{A} = \mathscr{A}(k)$ of asymptotic density 1 with the property that as $n \to \infty$ along $\mathscr{A}$, we have*

$$\varphi(n)/\varphi_{k+1}(n) \sim k! e^{k\gamma} (\log\log\log n)^k.$$

Here $\gamma = 0.57721\ldots$ is the usual Euler–Mascheroni constant.

Our first theorem shows that the average order of φ_k is dictated by the typical integers described in Theorem A (i.e., by the members of $\mathscr{A}$).

Theorem 1.1. *Fix a natural number k. Then as $x \to \infty$, we have*

(i) $$\sum_{n \leq x} \varphi_{k+1}(n) \sim k!^{-1} e^{-k\gamma} (\log_3 x)^{-k} \sum_{n \leq x} \varphi(n),$$

(ii) $$\sum_{n \leq x} \frac{1}{\varphi_{k+1}(n)} \sim k! e^{k\gamma} (\log_3 x)^k \sum_{n \leq x} \frac{1}{\varphi(n)}.$$

2010 *Mathematics Subject Classification.* Primary: 11A25, Secondary: 11N37, 11N56.
Key words and phrases. Euler function, totient, prime chain, Pratt tree, radical expression.
The author is supported by NSF award DMS-0802970.

Remark. It is well-known that as $x \to \infty$,

$$\sum_{n \le x} \varphi(n) \sim \frac{3}{\pi^2} x^2 \quad \text{and} \quad \sum_{n \le x} \frac{1}{\varphi(n)} \sim \frac{\zeta(2)\zeta(3)}{\zeta(6)} \log x. \tag{1}$$

We have chosen to leave these sums unevaluated in the statement of Theorem 1.1 to stress the connection to Theorem A.

Estimates similar to those considered in Theorem 1.1 were established by Warlimont [17] in the case $k = 1$; see the remarks at the end of §2.

We now turn to our second theorem. For each n, let $F(n)$ be the product of the distinct primes dividing $\prod_{k \ge 0} \varphi_k(n)$. The magnitude of F for typical integers n was investigated by Luca and Pomerance [10], who showed that for each fixed K, we have $F(n) > n^K$ for almost all numbers n (i.e., all numbers n outside of a set of density zero).

Luca and Pomerance were motivated by a problem in Galois theory: Let ζ_n denote a primitive nth root of unity. Since $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is a solvable extension, ζ_n can be expressed "by radicals". It requires some care to make this last claim both precise and nontrivial; $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ should be regarded as a satisfactory radical expression, while $\zeta_3 = \sqrt[3]{1}$ should not. We follow van der Waerden [16, §8.6] and impose the strictest possible meaning on the phrase "radical expression"; we require our radical extensions to be built up by irreducible adjunction of pth roots (so called *prime radical extensions*). Thus, our claim about ζ_n becomes the assertion that there is an extension $L/\mathbf{Q}$ containing $\mathbf{Q}(\zeta_n)$ and a tower

$$L_0 = \mathbf{Q} \subset L_1 \subset L_2 \subset \cdots \subset L_r = L \tag{2}$$

where each L_{i+1} has the form $L_i(\sqrt[p_i]{\alpha_i})$, with p_i a prime number, $\alpha_i \in L_i$, and α_i not a p_ith power in L_i. In fact, as shown in [10], there is a minimal such extension L (with respect to inclusion, within a fixed algebraic closure of $\mathbf{Q}$). H. W. Lenstra asked for an estimate of the degree of $L/\mathbf{Q}$. Perhaps surprisingly, L is typically much larger than $\mathbf{Q}(\zeta_n)$; as a consequence of Luca and Pomerance's above estimate, we have [10, Theorem 3] that

$$[L : \mathbf{Q}] > n^K$$

for each fixed K and almost all natural numbers n.

In the case when $n = p$ is prime, the prime divisors of $F(p)$ have a natural tree structure. This tree structure first appears in work of Pratt [13] and was extensively studied in recent work of Ford, Konyagin, and Luca [5]. Our second theorem is a lower bound for the number of distinct primes in the Pratt tree.

Theorem 1.2. *Fix $\epsilon > 0$. As $x \to \infty$, all but $x^{o(1)}$ of the primes $p \le x$ are such that $F(p)$ has at least $(\log p)^{1/2-\epsilon}$ distinct prime divisors.*

Theorem 1.2 should be compared with [4, Theorem 4.5]. That theorem's proof (after easy changes) gives that for some absolute constant $c > 0$ and all but $o(\pi(x))$ primes $p \le x$ (as $x \to \infty$), one of the iterates $\varphi_k(p)$ is divisible by every prime $q \le (\log p)^c$. (Consequently, $F(p)$ is also divisible by all primes $q \le (\log p)^c$.) We prove Theorem 1.2 in §3 below, along with the following corollary of its proof.

Corollary 1.3. *Let $\epsilon > 0$. For all but $x^{o(1)}$ values of $n \le x$, the least $r = r(n)$ for which there is a tower of the form (2) described above satisfies $r(n) > (\log n)^{1/2-\epsilon}$.*

Corollary 1.3 complements the easy upper bound $r(n) \ll \log n$, which can be obtained by a method of Pratt (cf. [13, Theorem 2]). For the convenience of the reader, we include the proof of this upper bound in the remarks concluding §3.

For other results concerning arithmetic properties of φ-iterates, see [1], [2], [6], [8], [9], [3], [7], [11].

Notation and conventions. For the rest of this paper, p_i denotes the ith prime in increasing order, so that $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... We say that the natural number n is *y-smooth* if $p \le y$ for every prime p dividing n, and we write $\Psi(x, y)$ for the number of y-smooth $n \le x$. We use $\omega(n)$ for the number of distinct prime factors of n and $\Omega(n)$ for the total number of prime factors, counted with multiplicity. If p is a prime, we write $p^e \parallel n$ to mean that $p^e \mid n$ but that $p^{e+1} \nmid n$; thus,

$$\omega(n) := \sum_{p \mid n} 1, \quad \text{while} \quad \Omega(n) = \sum_{p^e \parallel n} e.$$

We say a property holds for *almost all numbers* n if it holds away from a set of density zero, and we say a property holds for *almost all primes* p if it holds for all primes not in a set of primes of relative density zero. The Landau–Bachmann Big Oh and little oh notation, as well as the associated symbols "$\ll$" and "$\gg$", appear with their standard meanings. We set $\log_1 x = \max\{1, \log x\}$, and we let $\log_k$ denote the kth iterate of $\log_1$.

2. Proof of Theorem 1.1

We start with the proof of (i), which is shorter and simpler.

Proof of Theorem 1.1(i). Let $\mathscr{A}$ denote the set specified in the statement of Theorem A. By that theorem and the slow growth of $\log_3$, we have

$$\sum_{n \in \mathscr{A} \cap [1,x]} \varphi_{k+1}(n) \sim k!^{-1} \mathrm{e}^{-k\gamma} (\log_3 x)^{-k} \sum_{n \in \mathscr{A} \cap [1,x]} \varphi(n), \tag{3}$$

as $x \to \infty$. Now if $\mathscr{B}$ denotes the complement of $\mathscr{A}$, then

$$\sum_{n \in \mathscr{B} \cap [1,x]} \varphi(n) \le x \cdot \#(\mathscr{B} \cap [1,x]) = o(x^2) = o\left(\sum_{n \le x} \varphi(n) \right). \tag{4}$$

Thus, the final sum in (3) can be extended to all $n \le x$ without affecting the asymptotic behavior. This gives the lower bound of the theorem.

For the upper bound, fix $\epsilon > 0$. For $1 \le j \le k$, let $\mathscr{E}_j$ denote the set of $n \le x$ for which there is a prime $p \le (\log_2 x)^{j-\epsilon}$ not dividing $\varphi_j(n)$. Let us estimate the size of each $\mathscr{E}_j$. If $p \nmid \varphi_j(n)$, then there is no prime q dividing n for which $p \mid \varphi_j(q)$. So by Brun's sieve,

$$\#\{n \le x : p \nmid \varphi_j(n)\} \ll x \prod_{\substack{q \le x \\ p \mid \varphi_j(q)}} \left(1 - \frac{1}{q}\right) \ll x \exp(-S), \quad \text{where} \quad S := \sum_{\substack{q \le x \\ p \mid \varphi_j(q)}} \frac{1}{q}.$$

By [4, Theorem 3.4], we have $S \gg_j (\log_2 x)^{\epsilon}$, uniformly for $p \le (\log_2 x)^{j-\epsilon}$. Summing over all such p, we find that for large x,

$$\#\mathscr{E}_j \le x / \exp((\log_2 x)^{\epsilon/2}).$$

Hence, putting $\mathscr{E} := \cup_{j=1}^{k} \mathscr{E}_j$, we have $\#\mathscr{E} \le x/\exp((\log_2 x)^{\epsilon/4})$. It follows that

$$\sum_{n \in \mathscr{E}} \varphi_{k+1}(n) \le x \cdot \#\mathscr{E} \le x^2/\exp((\log_2 x)^{\epsilon/4}),$$

which is negligible in comparison to the estimate asserted in the theorem. If $n \notin \mathscr{E}$, then

$$\varphi_{k+1}(n) = \varphi(n)\frac{\varphi_2(n)}{\varphi(n)}\frac{\varphi_3(n)}{\varphi_2(n)}\cdots\frac{\varphi_{k+1}(n)}{\varphi_k(n)} \le \varphi(n)\prod_{j=1}^{k}\prod_{p \le (\log_2 x)^{j-\epsilon}}\left(1-\frac{1}{p}\right)$$

$$\le \varphi(n)\left(\mathrm{e}^{-k\gamma}\prod_{1\le j\le k}\frac{1}{j-\epsilon}+o(1)\right)(\log_3 x)^{-k}.$$

Here $o(1)$ indicates the behavior as $x \to \infty$, and is uniform for those $n \le x$ not in $\mathscr{E}$. Now sum over these n and let $\epsilon \downarrow 0$ to obtain the upper bound of the theorem. □

The proof of Theorem 1.1(ii) is more difficult and requires some preparation. The following lemma appears as [4, Theorem 3.5].

Lemma 2.1. *Let $k \ge 0$, and let p be a prime. The number of $n \le x$ for which $p \mid \varphi_k(n)$ is at most $x(C\log_2 x)^k/p$. Here C is an absolute positive constant.*

Lemma 2.2. *Fix an integer $j \ge 0$. As $t \to \infty$, the number of $n \le t$ for which $\varphi_j(n)/\varphi_{j+1}(n) > \exp((\log_3 t)^{2/3})$ is at most $t/Z^{1+o(1)}$, where*

$$Z = Z(t) = \exp(\exp((\log_3 t)^{1/2})).$$

Proof. For those n counted by the lemma,

$$(\log_3 t)^{2/3} \le \log\frac{\varphi_j(n)}{\varphi_{j+1}(n)} = \log\prod_{p\mid\varphi_j(n)}\left(1-\frac{1}{p}\right)^{-1} \ll \sum_{p\mid\varphi_j(n)}\frac{1}{p}.$$

Since $\sum_{p\le Z}\frac{1}{p} \ll (\log_3 t)^{1/2}$, we have $\sum_{\substack{p\mid\varphi_j(n)\\ p>Z}}\frac{1}{p} \gg (\log_3 t)^{2/3}$. So if N denotes the number of n under consideration, then

$$\sum_{n\le t}\sum_{\substack{p\mid\varphi_j(n)\\ p>Z}}\frac{1}{p} \gg N(\log_3 t)^{2/3}. \tag{5}$$

On the other hand,

$$\sum_{n\le t}\sum_{\substack{p\mid\varphi_j(n)\\ p>Z}}\frac{1}{p} \le \sum_{p>Z}\frac{1}{p}\sum_{\substack{n\le t\\ p\mid\varphi_j(n)}}1 \le t(C\log_2 t)^j\sum_{p>Z}\frac{1}{p^2} \ll t(C\log_2 t)^j/Z. \tag{6}$$

Comparing (5) and (6) gives the bound for N asserted by the lemma. (Note that Z grows faster than any fixed power of $\log_2 t$.) □

Lemma 2.3. *Let $\mathscr{B}$ be a set of asymptotic density zero. Then as $x \to \infty$, we have $\sum_{\substack{n\le x\\ n\in\mathscr{B}}}\frac{1}{\varphi(n)} = o(\log x)$.*

Proof. Let u be a large but fixed real parameter. We partition $\mathscr{B}$ into two sets $\mathscr{B}_1$ and $\mathscr{B}_2$, according to whether or not $n/\varphi(n) \le u$. The contribution from $\mathscr{B}_1$ is suitably small, since $\sum_{n\in\mathscr{B}_1} 1/\varphi(n) \le u \sum_{n\le x, n\in\mathscr{B}} 1/n = o(\log x)$, where the last estimate uses that $\mathscr{B}$ has density zero. The contribution from $\mathscr{B}_2$ is bounded by

$$\sum_{k=0}^{\infty} \sum_{\substack{n\le x \\ u\cdot 2^k < n/\varphi(n) \le u\cdot 2^{k+1}}} \frac{1}{\varphi(n)} \le u \sum_{k=1}^{\infty} 2^{k+1} \sum_{\substack{n\le x \\ u\cdot 2^k < n/\varphi(n) \le u\cdot 2^{k+1}}} \frac{1}{n}. \tag{7}$$

To estimate the inner sum in (7), we begin by recalling that for all $t > 0$,

$$\sum_{n\le t} \left(\frac{n}{\varphi(n)}\right)^2 \ll t.$$

(See, e.g., [15, Exercises 8–9, p. 54].) Hence, the number of $n \le t$ with $n/\varphi(n) > u \cdot 2^k$ is $\ll tu^{-2}2^{-2k}$. By partial summation, the final inner sum in (7) is $\ll u^{-2}2^{-2k}\log x$, and so (7) itself is $\ll u^{-1}\log x$. Since we can take u arbitrarily large, the result follows. □

Proof of the lower bound in Theorem 1.1(ii). Using the slow rate of growth of $\log_3$, we quickly deduce from Theorem A that those $n \in \mathscr{A} \cap [1, x]$ make a contribution

$$\sim k!\mathrm{e}^{k\gamma}(\log_3 x)^k \sum_{n\in\mathscr{A}\cap[1,x]} \frac{1}{\varphi(n)}.$$

But the final sum here is asymptotic to the corresponding sum over all $n \le x$, by (1) and Lemma 2.3 (applied with $\mathscr{B}$ taken as the complement of $\mathscr{A}$). □

Proof of the upper bound in Theorem 1.1(ii). Let $\mathscr{E}_0$ be the set of $n \le x$ with the property that

$$\frac{\varphi_j(n)}{\varphi_{j+1}(n)} > \exp((\log_3 x)^{2/3})$$

for some $j = 0, 1, 2, \dots, k$. By Lemma 2.2, the number of $n \in \mathscr{E}_0 \cap [1, t]$ is (crudely) $O_k(t/(\log_2 t)^{k+2})$, for all $1 \le t \le x$. For all $n \le x$, we have $\varphi_{k+1}(n) \gg_k n/(\log_2 x)^{k+1}$ (by the minimal order of the φ-function [15, p. 84]), and so

$$\sum_{n\in\mathscr{E}_0} \frac{1}{\varphi_{k+1}(n)} \ll_k (\log_2 x)^{k+1} \sum_{n\in\mathscr{E}_0} \frac{1}{n} \ll_k (\log_2 x)^{k+1} \int_1^x \frac{dt}{t(\log_2 t)^{k+2}} \ll_k \frac{\log x}{\log_2 x},$$

which is negligible. Next, fix a small $\epsilon > 0$, and let $\mathscr{E}_1$ be the set of $n \le x$ which do not belong to $\mathscr{E}_0$ and which satisfy

$$\sum_{\substack{p\mid\varphi_j(n) \\ p>(\log_2 x)^{j+\epsilon}}} \frac{1}{p} > \frac{1}{\log_3 x}$$

for some $j = 1, 2, \dots, k$. Then letting $\mathscr{E}_1(t) := \mathscr{E}_1 \cap [1, t]$, the averaging argument used in the proof of Lemma 2.2 shows that

$$\#\mathscr{E}_1(t)/\log_3 x \le \sum_{j=1}^{k} \left(\sum_{n\le t} \sum_{\substack{p\mid\varphi_j(n) \\ p>(\log_2 x)^{j+\epsilon}}} \frac{1}{p} \right) \ll_k t(\log_2 x)^{-\epsilon},$$

and so $\#\mathscr{E}_1(t) \le t(\log_2 x)^{-\epsilon/2}$ (for large x, uniformly for $1 \le t \le x$). If $n \in \mathscr{E}_1$ (so that in particular, $n \notin \mathscr{E}_0$), we have

$$\frac{1}{\varphi_{k+1}(n)} = \frac{1}{n}\frac{n}{\varphi(n)}\frac{\varphi(n)}{\varphi_2(n)} \cdots \frac{\varphi_k(n)}{\varphi_{k+1}(n)} \le \frac{1}{n}\exp(k(\log_3 x)^{2/3}) \le \frac{1}{n}(\log_2 x)^{\epsilon/4}.$$

Applying partial summation, we find that

$$\sum_{n \in \mathscr{E}_1} \frac{1}{\varphi_{k+1}(n)} \le (\log_2 x)^{\epsilon/4} \sum_{n \in \mathscr{E}_1} \frac{1}{n} \ll \frac{\log x}{(\log_2 x)^{\epsilon/4}},$$

which is again negligible. Finally, suppose that $n \notin \mathscr{E}_0 \cup \mathscr{E}_1$. For each j with $1 \le j \le k$, we have

$$\frac{\varphi_j(n)}{\varphi_{j+1}(n)} = \prod_{p \mid \varphi_j(n)} \left(1 - \frac{1}{p}\right)^{-1} \le (1 + O(1/\log_3 x)) \prod_{\substack{p \mid \varphi_j(n) \\ p \le (\log_2 x)^{j+\epsilon}}} \left(1 - \frac{1}{p}\right)^{-1},$$

where for the O-term we use that $n \notin \mathscr{E}_1$. By Mertens's theorem, the remaining product does not exceed

$$(1 + o(1))e^{\gamma}(j + \epsilon)\log_3 x,$$

as $x \to \infty$. Hence,

$$\frac{1}{\varphi_k(n)} = \frac{1}{\varphi(n)} \prod_{j=1}^{k} \frac{\varphi_j(n)}{\varphi_{j+1}(n)} \le \frac{1}{\varphi(n)}(\mathrm{e}^{k\gamma} + o(1))(\log_3 x)^k \prod_{j=1}^{k}(j + \epsilon),$$

as $x \to \infty$. The upper bound asserted by the theorem now follows upon summing over n, noting that ϵ may be taken arbitrarily small. □

Remark. Warlimont [17] calculated asymptotic formulas for the partial sums of φ/φ_2, φ_2/φ and $\log \frac{\varphi}{\varphi_2}$. There is no difficulty in calculating corresponding formulas for the partial sums of φ_k/φ_{k+1}, φ_{k+1}/φ_k, or $\log \frac{\varphi_k}{\varphi_{k+1}}$, for any fixed k, by the methods employed in the proof of Theorem 1.1. In each case, one obtains the answer one would expect from the normal order statement of Theorem A.

3. Proof of Theorem 1.2

For each prime p, the *Pratt tree* $\mathscr{T}(p)$ *associated to* p is the tree with root node p and with the property that a node labeled r has child nodes labeled with the distinct primes q dividing $r - 1$ (see Figure 1 for an example). As claimed in the introduction, the primes appearing in $\mathscr{T}(p)$ are exactly the primes dividing $F(p)$. Indeed, induction on k shows that a prime divides $\varphi_k(p)$ precisely when it appears in one of the first k levels of the tree (where the root node corresponds to the level $k = 0$).

We are interested in the distinct primes appearing in $\mathscr{T}(p)$, and so we must prune our tree. With h the number of nodes in $\mathscr{T}(p)$, label the nodes with the ordinal numbers $1, 2, 3, \dots, h$ in such a way that each child node is assigned a larger number than its parent node. (For example, label the nodes with the numbers $h, h-1, h-2, \dots$, starting with the lowest level and working upwards.) Now iterate the following procedure:

(1) Among all remaining nodes, identify that node with the largest ordinal number label.

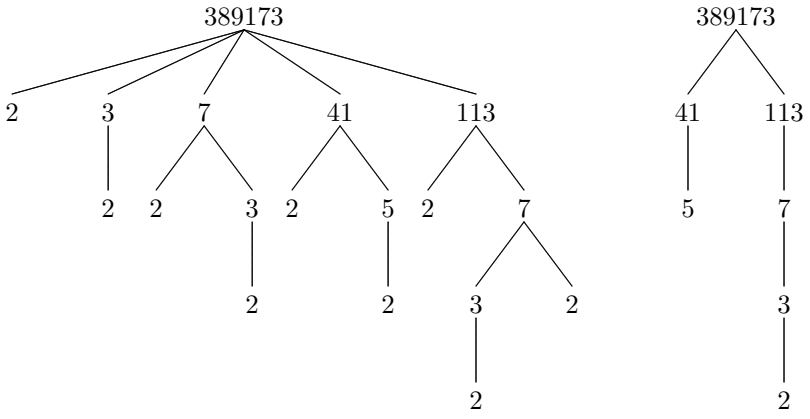

FIGURE 1. *Left*: A picture of $\mathscr{T}(389173)$. *Right*: The same tree, pruned by the procedure described in the proof of Theorem 1.2.

(2) Delete all nodes that have the same prime label but a smaller ordinal number label.

After a finite number of iterations, the remaining nodes have distinct labels corresponding to the distinct primes dividing $F(p)$. (See again Figure 1.) Let h' denote the number of remaining nodes. By removing the ordinal number labels corresponding to deleted nodes and collapsing the numbering, we obtain a labeling of the remaining nodes by $1, 2, \dots, h'$.

We now fix h' and count the number of $p \le x$ for which $\mathscr{T}(p)$ has precisely h' distinct nodes. In the pruned tree, the node labeled with the ordinal number h' is labeled with the prime 2. Moreover, if q is the prime corresponding to the node i, where $i < h'$, then $q-1$ is supported on the primes labeling the nodes $i+1, i+2, \dots, h'$. The total number of integers $q - 1 \le x$ with this property does not exceed the number $\Psi(x, p_{h'-i})$ of integers $n \le x$ supported on the primes $p_1, \dots, p_{h'-i}$. Since p is the prime corresponding to the node labeled with the ordinal number 1, it follows that the number of possible $p \le x$ is bounded above by

$$\prod_{i=1}^{h'-1} \Psi(x, p_{h'-i}).$$

We have the crude upper bound

$$\Psi(x, p_{h'-i}) \le (1 + \log x/\log 2)^{h'-i},$$

obtained by observing that the exponent of any prime appearing in a number $\le x$ is trivially bounded by $\log x/\log 2$. Hence,

$$\prod_{i=1}^{h'-1} \Psi(x, p_{h'-i}) \le (1 + \log x/\log 2)^{h'^2/2} \le \exp(h'^2 \log_2 x)$$

for large x. In particular, if $h' \le (\log x)^{1/2}/\log\log x$ (say), then the number of corresponding $p \le x$ is at most $x^{o(1)}$.

Summing over all $h' \le (\log x)^{1/2}/\log\log x$, it follows that the number of primes $p \le x$ for which $\omega(F(p)) \le (\log x)^{1/2}/\log\log x$ is also $x^{o(1)}$. This proves Theorem 1.2 (in a slightly stronger form).

Proof of Corollary 1.3. In [4], it is shown that the minimal extension containing $\mathbf{Q}(\zeta_n)$ which one can reach by a sequence of prime radical extensions is $L_r := \mathbf{Q}(\zeta_m)$, where

$$m = n \prod_{\substack{p \mid F(n) \\ p \nmid n}} p. \tag{8}$$

Since each extension L_{i+1}/L_i has prime degree, the number r of extensions required is precisely the number of prime factors, counted with multiplicity, of $[L_r : \mathbf{Q}] = \varphi(m)$. From (8), we find that

$$r = \Omega(n) - \omega(n) + \sum_{p \mid F(n)} \Omega(p-1). \tag{9}$$

Since $\Omega(n) \geq \omega(n)$ always and $\Omega(p-1) \geq 1$ for $p > 2$, we have

$$r \geq \omega(F(n)) - 1.$$

To estimate $\omega(F(n))$ from below, we imitate the proof of Theorem 1.2, making use of the observation that a prime divides $F(n)$ precisely when it divides $F(q)$ for some prime q dividing n.

Draw the prime trees $\mathscr{T}(q)$ for all primes q dividing n. If h is the total number of nodes in all these trees, label the nodes with the numbers $1, 2, \dots, h$ in such a way that each parent node has a smaller number than its child nodes. Now carry out the pruning procedure described in the proof of Theorem 1.2. If h' is the number of remaining nodes, then $h' = \omega(F(n))$.

Let us count the number of n for which $r \leq (\log x)^{1/2-\epsilon}$. For any such n, we have $h' \leq r + 1 < \sqrt{\log x}/\log\log x$. Fix h'. The proof of Theorem 1.2 shows that the number of choices for the primes labeling nodes $1, 2, 3, \dots, h'$ is $x^{o(1)}$. Having chosen these primes, we see that the number of possibilities for the set of prime factors of n is bounded by $2^{h'} = x^{o(1)}$, since the prime factors of n form a subset of the primes dividing $F(n)$. Finally, given the set $\mathscr{S}$ of prime factors of n, the number of possibilities for n itself is bounded by $\Psi(x, p_k)$, where k is the size of $\mathscr{S}$. In our case, $k < \sqrt{\log x}$, and so

$$\Psi(x, p_k) < (1 + \log x/\log 2)^{\sqrt{\log x}} = x^{o(1)}.$$

Piecing everything together, the corresponding number of possibilities for n is $x^{o(1)}$. Summing over the $x^{o(1)}$ possibilities for h' completes the proof. □

Remarks.

(i) Perhaps it is true that for each $\epsilon > 0$ and almost all primes p, the number $F(p)$ is divisible by all primes $q < (\log x)^{1-\epsilon}$. (Cf. [4, Conjecture 1].) It is shown in [5, Theorem 2] that almost always the total number of nodes in $\mathscr{T}(p)$ exceeds $0.378 \log p$.

(ii) As remarked in the introduction, it is simple to show that the quantity $r = r(n)$ of Corollary 1.3 satisfies $r \ll \log n$ (cf. [4, Theorem 4.6]): Clearly $2^{\Omega(n)} \leq n$, so that $\Omega(n) \leq \log n/\log 2$. Thus, from (9), it suffices to show that the function $R(n) := \sum_{p \mid F(n)} \Omega(p-1)$ satisfies

$$R(n) \leq 2\frac{\log n}{\log 2} - 2 \tag{10}$$

for all $n > 1$. We first show that (10) holds for prime values of n. By direct calculation, (10) holds for $n = 2$ and $n = 3$. Suppose that $n \geq 5$ is prime and that (10) is known for all primes $< n$. Then by the induction hypothesis,

$$R(n) - \Omega(n-1) \leq \sum_{q|n-1} R(q) \leq \sum_{q^e \| n-1} eR(q) \leq 2\frac{\log(n-1)}{\log 2} - 2\Omega(n-1),$$

so that $R(n) \leq 2\frac{\log n}{\log 2} - \Omega(n-1) \leq 2\frac{\log n}{\log 2} - 2$. This proves (10) for prime n. The general case now follows from the relation $R(n) \leq \sum_{q|n} R(q) \leq \sum_{q^e \| n} eR(q)$.

Acknowledgements

The author thanks Kevin Ford, Carl Pomerance, and Enrique Treviño for useful discussions.

References

[1] N. L. Bassily, I. Kátai, and M. Wijsmuller, *Number of prime divisors of $\varphi_k(n)$, where φ_k is the k-fold iterate of φ*, J. Number Theory **65** (1997), no. 2, 226–239.

[2] ———, *On the prime power divisors of the iterates of the Euler-φ function*, Publ. Math. Debrecen **55** (1999), no. 1-2, 17–32.

[3] J. Bayless, *The Lucas-Pratt primality tree*, Math. Comp. **77** (2008), no. 261, 495–502 (electronic).

[4] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 165–204.

[5] K. Ford, S. V. Konyagin, and F. Luca, *Prime chains and Pratt trees*, Geom. Funct. Anal. **20** (2010), no. 5, 1231–1258.

[6] K.-H. Indlekofer and I. Kátai, *On the normal order of $\varphi_{k+1}(n)/\varphi_k(n)$, where φ_k is the k-fold iterate of Euler's function*, Liet. Mat. Rink. **44** (2004), no. 1, 68–84.

[7] I. Kátai, *On the prime power divisors of the iterates of $\varphi(n)$ and $\sigma(n)$*, Šiauliai Math. Semin. **4(12)** (2009), 125–143.

[8] I. Kátai and M. V. Subbarao, *Some remarks on the φ and on the σ functions*, Ann. Univ. Sci. Budapest. Sect. Comput. **25** (2005), 113–130.

[9] Y. Lamzouri, *Smooth values of the iterates of the Euler phi-function*, Canad. J. Math. **59** (2007), no. 1, 127–147.

[10] F. Luca and C. Pomerance, *Irreducible radical extensions and Euler-function chains*, Combinatorial number theory, de Gruyter, Berlin, 2007, pp. 351–361.

[11] ———, *On the range of the iterated Euler function*, Combinatorial number theory, de Gruyter, Berlin, 2009, pp. 101–116.

[12] S. S. Pillai, *On a function connected with $\varphi(n)$*, Bull. Amer. Math. Soc. **35** (1929), no. 6, 837–841.

[13] V. Pratt, *Every prime has a succinct certificate*, SIAM Journal on Computing **4** (1975), 214–220.

[14] H. N. Shapiro, *An arithmetic function arising from the φ function*, Amer. Math. Monthly **50** (1943), 18–30.

[15] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.

[16] B. L. van der Waerden, *Algebra. Vol. I*, Springer-Verlag, New York, 1991.

[17] R. Warlimont, *On the iterates of Euler's function*, Arch. Math. (Basel) **76** (2001), no. 5, 345–349.

University of Illinois at Urbana-Champaign, Department of Mathematics, Urbana, Illinois 61801

E-mail address: pppollac@illinois.edu