INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 7(2) (2007), #A25

IRREDUCIBLE RADICAL EXTENSIONS AND EULER-FUNCTION CHAINS

Florian Luca
Instituto de Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

Carl Pomerance
Department of Mathematics, Dartmouth College, Hanover, NH 03755–3551, USA
carl.pomerance@dartmouth.edu

Received: 1/21/06, Accepted: 6/12/06

Abstract

We discuss the smallest algebraic number field which contains the nth roots of unity and which may be reached from the rational field $\mathbb{Q}$ by a sequence of irreducible, radical, Galois extensions. The degree $D(n)$ of this field over $\mathbb{Q}$ is $\varphi(m)$, where m is the smallest multiple of n divisible by each prime factor of $\varphi(m)$. The prime factors of m/n are precisely the primes not dividing n but which do divide some number in the "Euler chain" $\varphi(n), \varphi(\varphi(n)), \ldots$. For each fixed k, we show that $D(n) > n^k$ on a set of asymptotic density 1.

–For Ron Graham on his 70th birthday

1. Introduction

Throughout this paper, all fields which appear are of characteristic zero. Let $K \subset L$ be a field extension (which is always assumed to be of finite degree). We say L is *prime radical over* K if $L = K[\alpha]$, where $\alpha^p \in K$ for some prime p, and the polynomial $f(X) = X^p - \alpha^p \in K[X]$ is irreducible. Note that for such an extension to also be Galois it is necessary and sufficient that the pth roots of unity lie in L.

The first author was supported in part by grants PAPIIT IN104505, SEP-CONACyT 46755 and a Guggenheim Fellowship. The second author was supported in part by NSF grant DMS-0401422.

The present paper is motivated by the following situation. Every Galois extension $K \subset L$ with solvable Galois group can be decomposed into a chain of prime cyclic extensions, but these prime cyclic extensions are not necessarily radical. In elementary Galois theory it is shown that if one introduces to K and L the pth roots of unity for p running over the prime factors of $[L : K]$, then one has larger fields $K' \subset L'$, and here we can indeed find a chain of prime radical Galois extensions, but these run from K' to L'. We ask if one can find an extension L'' of L so that there is a chain of prime radical Galois extensions from K to L''. In fact this is always the case, which we record as follows.

Theorem 1. *Let $K \subset L$ be a Galois extension with solvable Galois group of characteristic zero fields lying in an algebraically closed field U. There is a unique minimal extension $L \subset M \subset U$ such that M can be reached from K by a finite sequence of prime radical Galois extensions. The field M is the smallest extension of L in U that contains a primitive pth root of unity for each prime $p \mid [M : K]$.*

For example, say $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{23})$, where in general we let ζ_n denote a primitive nth root of unity. This Galois extension is not only solvable, it is cyclic. The field L has degree 22 over $\mathbb{Q}$, and there is the intermediate field $A = \mathbb{Q}\left(\sum_{i=0}^{10} \zeta_{23}^{3^i}\right)$ of degree 2 over $\mathbb{Q}$. Clearly every field extension of degree 2 is prime radical and Galois, so there is no problem here. But the degree-11 extension from A to L is Galois, so cannot be prime radical, since the eleventh roots of unity are not present. There is no getting around an extension of degree eleven at some point, so we throw in the eleventh roots of 1, giving us a prime radical degree-10 extension B of A. There is the intermediate field $C = A(\zeta_{11} + \zeta_{11}^3 + \zeta_{11}^4 + \zeta_{11}^5 + \zeta_{11}^9)$ of degree 2 over A, which is clearly prime radical and Galois. However the degree 5-extension from C to B is prime radical but not Galois since the fifth roots of unity are not present. So, we throw them in too obtaining a prime radical extension $D = C(\zeta_5)$ which is cyclic of degree 4. Hence, D can be reached from C by a sequence of two prime radical Galois extensions, each of degree two. Further, the extension $E = D(\zeta_{11})$ of D is cyclic of degree five, and with the fifth roots of unity present in D, it follows that it is both prime radical and Galois. Finally, the extension $M = E(\zeta_{23})$ is a cyclic extension of degree eleven of E, and with the 11th roots of unity present in E, it is both prime radical and Galois. So

$$M = \mathbb{Q}(\sum_{i=0}^{10} \zeta_{23}^{3^i})(\sum_{j=0}^{4} \zeta_{11}^{3^j})(\zeta_5)(\zeta_{11})(\zeta_{23}) = \mathbb{Q}(\zeta_{1265}),$$

a field of degree 880 over $\mathbb{Q}$, may be reached from $\mathbb{Q}$ by a sequence of prime radical Galois extensions.

Let us consider more generally the case for $K = \mathbb{Q}(\zeta_n)$. We shall present a formula for $D(n)$, the degree of the field M determined in Theorem 1. Let $\varphi_k(n)$ be the kth iterate of the Euler function φ at n. By convention, we have $\varphi_0(n) = n$ and $\varphi_1(n) = \varphi(n)$.

Theorem 2. *Let $F(n)$ be the product of the primes that divide $\prod_{k \geq 1} \varphi_k(n)$ that do not divide n. Then the field M determined in Theorem 1 with $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_n)$ is $\mathbb{Q}(\zeta_{nF(n)})$, which has degree $D(n) = \varphi(nF(n))$ over $\mathbb{Q}$.*

Some years ago, Hendrik Lenstra communicated these results to one of us (CP) and asked how large $D(n)$ is for most numbers n. We are now in a position to answer this question; the following result shows that $D(n)$, for most positive integers n, grows faster than any fixed power of n.

Theorem 3. *For each $\varepsilon > 0$, the set of natural numbers n for which*

$$D(n) > n^{(1-\varepsilon)\log\log n/\log\log\log n}$$

has asymptotic density 1.

Note that a quantity similar to $F(n)$ appears in the proof of Pratt [8] that every prime has a polynomial-time proof of primality. (This result predates the recent algorithm of Agrawal, Kayal and Saxena that decides in deterministic polynomial time whether a given number is prime or composite. The Pratt theorem shows only that a polynomial-time proof of primality exists; it does not show how to find it quickly.) In particular, if p is prime, then Pratt reduces the primality of p to the primality of the prime factors of $F(p)$. Very recently, Bayless [2] was able to use the methods of this paper and the Brun–Titchmarsh inequality to show that Theorem 3 holds for prime numbers (that is, for all prime numbers except those in a set of relative density 0 within the set of primes). As a consequence he shows that for any number $C > 0$, the number of modular multiplications involved in a Pratt certificate for the prime p exceeds $C \log p$ for all but $o(\pi(x))$ primes $p \le x$.

Throughout this paper, we use $c_0,\ c_1,\ \ldots$ to denote computable positive constants and x to denote a positive real number. We also use the Landau symbols O and o and the Vinogradov symbols $\gg$ and $\ll$ with their usual meanings. We write $\log x$ for the maximum of 1 and the natural logarithm of x. We write p and q for prime numbers.

Acknowledgements. We thank Hendrik Lenstra for asking the question about the normal size of $D(n)$ and for his help with Section 2. We also thank Tom Shemanske for some helpful discussions. This paper started during a very enjoyable visit of the first author to Dartmouth College under a Shapiro Fellowship in May of 2005. He would like to thank this department for its hospitality and support.

2. The Proofs of Theorem 1 and Theorem 2

We prove two lemmas. The first gives a sufficient condition for an extension $K \subset L$ to be decomposable into a tower of prime radical Galois extensions.

Lemma 4. *If $K \subset L$ is Galois with solvable Galois group, and $\zeta_p \in L$ for each prime p dividing $[L : K]$, then L can be reached from K by a sequence of prime radical Galois extensions.*

Proof. The proof relies on the well-known fact from Kummer theory that a cyclic extension of prime degree p of a field K containing a primitive pth root of 1 is prime radical. We now proceed by induction on $[L : K]$. If all $\zeta_p \in K$ for prime $p \mid [L : K]$, we then use the solvability of $\mathrm{Gal}(L/K)$ to break up the extension into a tower of cyclic extensions of prime degrees, and apply the above well-known fact to each of them. Otherwise, let p be minimal with $\zeta_p \notin K$. We now break up the extension $K \subset L$ into $K \subset K(\zeta_p) \subset L$ and deal with each piece inductively. By $[K(\zeta_p) : K] < p$ and the choice of p, the above fact applies to the prime degree pieces into which the abelian extension $K \subset K(\zeta_p)$ can be broken up, while the inductive hypothesis applies to $K(\zeta_p) \subset L$. □

The second lemma shows that the condition on pth roots of 1 is necessary.

Lemma 5. *If $K \subset L$ and L can be reached from K by a finite sequence of prime radical Galois extensions, then $\zeta_p \in L$ for each prime $p \mid [L : K]$.*

Proof. Say the promised sequence of fields is $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$, and let p be a prime factor of $[L : K]$. Then some $[K_{i+1} : K_i] = p$. Since this extension is radical and Galois, we must have $\zeta_p \in K_{i+1}$, so that $\zeta_p \in L$. □

Lenstra points out to us that if one does not assume the radical extensions in Lemma 5 to be Galois, but imposes that L/K is Galois, then the conclusion of Lemma 5 still holds. Indeed, if L/K is Galois, and M is an extension of L such that we can reach M from K by a finite sequence of prime radical extensions (not necessarily Galois), then M contains ζ_p for each prime $p \mid [L : K]$. To see this, let $K = K_0 \subset K_1 \subset \cdots \subset K_t = M$ be a sequence of prime radical extensions, and let p be a prime dividing $[L : K]$. The sequence of fields LK_i runs from $LK_0 = L$ to $LK_t = M$, so the sequence of degrees $[LK_i : K_i]$ runs from $[L : K]$, when $i = 0$, to 1, when $i = t$. Note too that each extension $K_i \subset LK_i$ is Galois. Since

$$[LK_{i+1} : K_{i+1}] = [LK_i : LK_i \cap K_{i+1}], \tag{1}$$

we have each $[LK_{i+1} : K_{i+1}] \mid [LK_i : K_i]$. Thus, there is a largest subscript i such that $p \mid [LK_i : K_i]$. Clearly, $i < t$. We will show that $K_i \subset K_{i+1} \subset LK_i$, and that $[K_{i+1} : K_i] = p$. Since K_{i+1} is prime radical over K_i and LK_i is Galois over K_i, it follows that LK_i contains ζ_p. To see the assertion, note that (1) implies that

$$\begin{aligned} [LK_i : K_i] &= [LK_i : LK_i \cap K_{i+1}][LK_i \cap K_{i+1} : K_i] \\ &= [LK_{i+1} : K_{i+1}][LK_i \cap K_{i+1} : K_i]. \end{aligned}$$

By the choice of i, the left side is divisible by p and the first factor in the last product is not divisible by p. Thus, the last factor in the last product is divisible by p. Since $LK_i \cap K_{i+1} \subset K_{i+1}$ and K_{i+1}/K_i is prime radical, the extension $LK_i \cap K_{i+1}/K_i$ is an extension of degree exactly p and $LK_i \cap K_{i+1} = K_{i+1}$. This proves our assertion, and so the alternate form of Lemma 5.

We are now ready to prove Theorems 1 and 2.

Proof of Theorem 1. This follows immediately from Lemmas 4 and 5. Indeed, to obtain M from L, we first adjoin to $L = L_0$ all ζ_p for $p \mid [L : K]$. The resulting field L_1 is still Galois with a solvable group over K. We now adjoin to L_1 all ζ_p for $p \mid [L_1 : L_0]$ and so reach a solvable extension L_2 of K. We continue to iterate the process, noting that if $[L_i : L_{i-1}] = d_i$, then $[L_{i+1} : L_i]$ is a divisor of $\varphi(d_i)$. Thus, the procedure stabilizes at the smallest field $M = L_n$ which contains all ζ_p for $p \mid [M : K]$.

It follows from Lemma 4 that M may be reached from K by a sequence of prime radical Galois extensions. The minimality, and thus uniqueness of M follows from Lemma 5. □

Proof of Theorem 2. We apply the algorithm described in the proof of Theorem 1 to $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_n)$. We obtain $M = \mathbb{Q}(\zeta_m)$, where m is the least multiple of n that is divisible by all primes dividing $\varphi(m)$. It is easy to see that

$$m = n \prod_{\substack{p \mid \varphi_k(n) \text{ for some } k \geq 1 \\ p \nmid n}} p,$$

and we immediately recognize that $m = nF(n)$. Thus, $D(n) = [\mathbb{Q}[\zeta_m] : \mathbb{Q}] = \varphi(m) = \varphi(nF(n))$. □

Using the alternate form of Lemma 5 described before the proof of Theorem 1 above, we also get the following alternate version of Theorem 1.

Theorem 6. *Let $K \subset L$ be a finite extension of characteristic zero fields lying in an algebraically closed field U. Assume that the Galois group of the normal closure $\overline{L}$ of L over K (in U) is solvable. There is a unique minimal Galois extension $\overline{L} \subset M$ in U such that M can be reached from K by a finite sequence of prime radical extensions. The field M is the smallest extension of $\overline{L}$ in U that contains a primitive pth root of unity for each prime $p \mid [M : K]$.*

3. The Proof of Theorem 3

3.1 Preliminary Results

We recall a result from [4]:

Proposition 7. *There is an absolute constant c_1 such that for each prime p and integer $k \geq 0$, the number of integers $n \leq x$ with $p \mid \varphi_k(n)$ is at most $(x/p)(c_1 \log\log x)^k$.*

Let

$$F_K(n) = \prod_{0 \leq k \leq K} \varphi_j(n).$$

One of our goals will be to establish the following result.

Proposition 8. *There is an absolute constant c_2 such that for all sufficiently large numbers x, all numbers $y \geq 1$ and all integers $K \geq 1$, the number of integers $n \leq x$ with $p^2 \mid F_K(n)$ for some prime $p > y$ is at most $(x/y)K(c_2 \log\log x)^{2K}$.*

Let $\Omega(n)$ denote the number of prime factors of n counted with multiplicity. We will also prove the following result.

Proposition 9. *The number of positive integers $n \leq x$ with the property that $\Omega(F_K(n)) > 2(5\log\log x)^{K+1}$ is $\ll (x/\log x)(c_1 \log\log x)^K$ uniformly in K, where c_1 is the constant from Proposition 7.*

3.2 Proof of Theorem 3

Let x be a large positive real number and let $0 < \varepsilon < 1$ be arbitrarily small and fixed. Put

$$K = \lceil (1-\varepsilon)\log\log x/\log\log\log x \rceil.$$

Assume $n \leq x$, and factor $F_K(n)$ as AB, where each prime in A is at most $(\log x)^3$ and each prime in B exceeds $(\log x)^3$. Since

$$(x/\log x)(c_1 \log\log x)^K = o(x),$$

Proposition 9 implies that but for $o(x)$ choices of the positive integer $n \leq x$, we have

$$A \leq (\log^3 x)^{2(5\log\log x)^{K+1}} \leq \exp(2(5\log\log x)^{K+2}) = x^{o(1)}.$$

By the minimal order of $\varphi(m)/m$ for $m \leq x$, we have that each one of the inequalities $\varphi_{j+1}(n)/\varphi_j(n) > 1/(2\log\log x)$ holds. We also may assume that $n > x/(2\log\log x)$, so that

$$\begin{aligned} F_K(n) &= n^{K+1}\prod_{i=0}^{K}\frac{\varphi_i(n)}{n} = n^{K+1}\prod_{i=0}^{K}\prod_{j=0}^{i-1}\frac{\varphi_{j+1}(n)}{\varphi_j(n)} \\ &> n^{K+1}/(2\log\log x)^{1+2+\cdots+K} > x^{K+1}/(2\log\log x)^{(K+1)(K+2)/2} \\ &> x^{K+1/2} \end{aligned}$$

for x sufficiently large. Thus, but for $o(x)$ choices for $n \leq x$, we have

$$B > x^{K+1/4}.$$

By Proposition 8, the number of $n \leq x$ with $p^2 \mid F_K(n)$ for some prime number $p > \log^3 x$ is $O(x/\log x)$. Thus, for all but $o(x)$ choices of $n \leq x$, the number B is squarefree. It is clear that $B \mid nF(n)$, therefore $\varphi(B) \mid D(n)$. From the minimal order of the Euler function, we have

$$\varphi(B) > \frac{B}{2\log\log B} > \frac{x^{K+1/4}}{2(\log(K+1/4)+\log\log x)} > \frac{x^{K+1/4}}{3\log\log x} > x^K.$$

Thus, $D(n) > x^K$ holds for all $n \leq x$ with at most $o(x)$ exceptions, which completes the proof of the theorem. $\square$

3.3 Proofs of the Preliminary Results

Before we begin the proof of Proposition 8, we establish some helpful notation. For a positive integer m, let

$$\mathcal{P}_m = \{p \text{ prime } : p \equiv 0 \text{ or } 1 \pmod{m}\}.$$

By the Brun–Titchmarsh inequality and partial summation, we have

$$\sum_{\substack{p\in\mathcal{P}_m\\ p\le x}} \frac{1}{p} \le \frac{c_0}{\varphi(m)} \log\log x \tag{2}$$

for some absolute constant c_0 (see Lemma 1 in [3] or formula (3.1) in [4]). Note that from Theorem 3.5 in [4], we may (and do) take the constant c_1 from Proposition 7 equal to $2c_0$. Let

$$\mathcal{S}_k(x,m) = \{n \le x : m \mid \varphi_k(n)\}, \qquad S_k(x,m) = \#\mathcal{S}_k(x,m).$$

Lemma 10. *For all sufficiently large values of x, if $q_1 \le q_2$ are primes and k is any nonnegative integer, then*

$$S_k(x,q_1q_2) \le \frac{x}{q_1q_2}(3c_0\log\log x)^{2k}.$$

Proof. We proceed by induction on k. The result is clearly true for $k=0$. Assume that the result holds at k. If $q_1q_2 \mid \varphi_{k+1}(n)$, then either $p \mid \varphi_k(n)$ for some $p\in\mathcal{P}_{q_1q_2}$, or $p_1p_2 \mid \varphi_k(n)$ for some $p_1\in\mathcal{P}_{q_1}$ and $p_2\in\mathcal{P}_{q_2}$. Thus,

$$S_{k+1}(x,q_1q_2) \le \sum_{p\in\mathcal{P}_{q_1q_2}} S_k(x,p) + \sum_{p_1\in\mathcal{P}_{q_1},\, p_2\in\mathcal{P}_{q_2}} S_k(x,p_1p_2).$$

Thus, by Proposition 7 and the induction hypothesis, we have that

$$S_{k+1}(x,q_1q_2) \le \sum_{\substack{p\in\mathcal{P}_{q_1q_2}\\ p\le x}} \frac{x}{p}(c_1\log\log x)^k + \sum_{\substack{p_1\in\mathcal{P}_{q_1},\, p_2\in\mathcal{P}_{q_2}\\ p_1\le x,\, p_2\le x}} \frac{x}{p_1p_2}(3c_0\log\log x)^{2k}.$$

We now use (2), and so get

$$\begin{aligned} S_{k+1}(x,q_1q_2) &\le \frac{x}{\varphi(q_1q_2)}(c_0\log\log x)(c_1\log\log x)^k \\ &\quad + \frac{x}{\varphi(q_1)\varphi(q_2)}(c_0\log\log x)^2(3c_0\log\log x)^{2k} \\ &\le \frac{x}{q_1q_2}\big(3c_0\log\log x(c_1\log\log x)^k + (2c_0\log\log x)^2(3c_0\log\log x)^{2k}\big). \end{aligned}$$

Thus, using $c_1 = 2c_0$, the inequality at $k+1$ follows for all x beyond some uniform bound. Thus, the lemma has been proved. $\square$

We introduce the following notation. Let

$$\mathcal{S}_K(x,y) = \bigcup_{\substack{0\le k\le K\\ p>y,\, p \text{ prime}}} \mathcal{S}_k(x,p^2), \qquad\qquad S_K(x,y) = \#\mathcal{S}_K(x,y).$$

For nonnegative integers k_1 and k_2 with $k_1 < k_2$, and primes q_1 and q_2, let

$$\mathcal{S}_{k_1,k_2}(x,q_1,q_2) = \{n \le x \,:\, q_1 \mid \varphi_{k_1}(n),\ q_2 \mid \varphi_{k_2}(n)\}.$$

Lemma 11. *Suppose that k_1, k_2 and K are integers with $0 \le k_1 < k_2 \le K$ and q_1 and q_2 are primes with $q_2 > y$ and q_2 not a divisor of $\varphi_{k_2-k_1}(q_1)$. Then*

$$\#\left(\mathcal{S}_{k_1,k_2}(x,q_1,q_2) - \mathcal{S}_K(x,y)\right) \le \frac{x}{q_1q_2}(3c_0\log\log x)^{k_1+k_2}.$$

Proof. We first show that if $\varphi_j(m)$ is not divisible by the square of any prime exceeding y for $0 \le j \le k-1$, then for each prime $q \mid \varphi_k(m)$ with $q > y$, there is a prime $p \mid m$ with $q \mid \varphi_k(p)$. Indeed take $k = 1$. Either there is a prime $p \mid m$ with $q \mid \varphi(p)$ or $p^2 \mid m$. By the hypothesis, the latter case does not occur. Thus, the result is true at $k = 1$. Assume that it is true at k and assume the hypothesis at $k+1$. Then either there is a prime $p' \mid \varphi_k(m)$ with $q \mid \varphi(p')$, or $q^2 \mid \varphi_k(m)$. Again, the latter case does not occur, so we have the former case. By the induction hypothesis, there is a prime $p \mid m$ with $p' \mid \varphi_k(p)$. Then $q \mid \varphi_{k+1}(p)$, and the assertion always holds.

Suppose that $n \in \mathcal{S}_{k_1,k_2}(x,q_1,q_2) - \mathcal{S}_K(x,y)$, where k_1, k_2, K, q_1 and q_2 are as given in the lemma. By the above with $m = \varphi_{k_1}(n)$, there is a prime $p \mid \varphi_{k_1}(n)$ with $q_2 \mid \varphi_{k_2-k_1}(p)$. By the hypothesis of the lemma, we have $p \ne q_1$. Thus, $pq_1 \mid \varphi_{k_1}(n)$. It follows that

$$\begin{aligned}\#\left(\mathcal{S}_{k_1,k_2}(x,q_1,q_2) - \mathcal{S}_K(x,y)\right) &\le \sum_{p:\ q_2\mid\varphi_{k_2-k_1}(p)} S_{k_1}(x,pq_1)\\ &\le \sum_{p:\ q_2\mid\varphi_{k_2-k_1}(p)} \frac{x}{pq_1}(3c_0\log\log x)^{2k_1},\end{aligned}$$

by Lemma 10. But from the remark on p. 190 of [4], we have

$$\sum_{p:\ q_2\mid\varphi_{k_2-k_1}(p)} \frac{1}{p} \le \frac{1}{q_2}(2c_0\log\log x)^{k_2-k_1}.$$

Putting this inequality in the prior one gives the lemma. $\square$

Proof of Proposition 8. The count in Proposition 8 is at most

$$S_K(x,y) + \sum_{p>y}\ \sum_{0\le k_1<k_2\le K} \#\left(\mathcal{S}_{k_1,k_2}(x,p,p) - \mathcal{S}_K(x,y)\right).$$

By Lemma 10 with $q_1 = q_2 = p$, we have

$$S_K(x,y) \le \sum_{p>y} \sum_{0\le k\le K} \frac{x}{p^2}(3c_0 \log\log x)^{2k} \ll \frac{x}{y}(3c_0 \log\log x)^{2K}.$$

We also take $q_1 = q_2 = p$ in Lemma 11. Thus,

$$\begin{aligned}\sum_{p>y} \sum_{0\le k_1<k_2\le K} \#\left(\mathcal{S}_{k_1,k_2}(x,p,p) - \mathcal{S}_K(x,y)\right) &\ll \sum_{p>y} \frac{x}{p^2} K (3c_0 \log\log x)^{2K} \\ &\ll \frac{x}{y} K (3c_0 \log\log x)^{2K}.\end{aligned}$$

Thus, the proposition follows with c_2 any number larger than $3c_0$. $\square$

The next two results will be helpful in establishing Proposition 9. The proofs are suggested in Exercise 05 in [5].

Lemma 12. *Uniformly for* $1 < z < 2$*, we have*

$$\sum_{n\le x} z^{\Omega(n)} \ll \frac{x(\log x)^{z-1}}{2-z}.$$

Proof. Let g be the multiplicative function with $g(p^a) = z^a - z^{a-1}$ for primes p and positive integers a. Then $z^{\Omega(n)} = \sum_{d|n} g(d)$. Thus, the sum in the lemma is equal to

$$\begin{aligned}\sum_{m\le x} g(m) \left\lfloor \frac{x}{m} \right\rfloor &\le x \sum_{m\le x} \frac{g(m)}{m} \le x \prod_{p\le x} \left(1 + \frac{z-1}{p} + \frac{z^2-z}{p^2} + \cdots\right) \\ &= x \prod_{p\le x} \frac{p-1}{p-z} = \frac{x}{2-z} \prod_{3\le p\le x} \frac{p-1}{p-z} \ll \frac{x}{2-z}(\log x)^{z-1}.\end{aligned}$$

This completes the proof of the lemma. $\square$

Lemma 13. *Uniformly for each positive integer* k*,*

$$\sum_{\substack{n\le x \\ \Omega(n)\ge k}} 1 \ll \frac{k}{2^k} x \log x.$$

Proof. This merely involves applying Lemma 12 with $z = 2 - 1/k$. Indeed, if N is the sum in the present lemma, then Lemma 12 implies that

$$N \ll \frac{x(\log x)^{1-1/k}}{(1/k)(2-1/k)^k},$$

and it remains to note that $(2-1/k)^k = 2^k(1-1/(2k))^k \ge 2^{k-1}$. $\square$

A version of Lemma 13 above appears also in [7].

Proof of Proposition 9. By Lemma 13, if $0 < t \leq x$, the number of primes $p \leq t$ with $\Omega(p-1) > 5\log\log x$ is $O(t/\log^2 x)$. This holds since $5\log 2 - 1 > 2$, and indeed the same estimate holds for the number of integers $n \leq t$ with $\Omega(n) > 5\log\log x$. Thus, by partial summation,

$$\sum_{\substack{p \leq x \\ \Omega(p-1) > 5\log\log x}} \frac{1}{p} \ll \frac{1}{\log x}. \tag{3}$$

If $\Omega(n) \leq 5\log\log x$ and if each prime p dividing $F_{K-1}(n)$ has the property that $\Omega(p-1) \leq 5\log\log x$, then for all positive integers $0 \leq k \leq K$ we have $\Omega(\varphi_k(n)) \leq (5\log\log x)^{k+1}$, so that $\Omega(F_K(n)) \leq 2(5\log\log x)^{K+1}$. We conclude that if $\Omega(F_K(n)) > 2(5\log\log x)^{K+1}$, then either $\Omega(n) > 5\log\log x$ or there is some prime $p \mid F_{K-1}(n)$ with $\Omega(p-1) > 5\log\log x$. It follows from Lemma 13, that the number of n in the first category is $O(x/\log^2 x)$, while it follows from (3) and Proposition 7 that the number of n in the second category is $O((x/\log x)(c_1 \log\log x)^{K-1})$. This completes the proof of the proposition. □

4. Thoughts on the Normal Order of $D(n)$

Let $k_\varphi(n)$ be the least integer k with $\varphi_k(n) = 1$. Further, let $\lambda(n)$ denote Carmichael's function, so that $\lambda(n)$ is the order of the largest cyclic subgroup of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. With λ_k as the iterated Carmichael function, let $k_\lambda(n)$ be the least k with $\lambda_k(n) = 1$. It is easy to see that the prime factors of $\prod_{k\geq 1} \varphi_k(n)$ are the same as the prime factors of $\prod_{k\geq 1} \lambda_k(n)$, so that we might have stated Theorem 2 in terms of the iterated λ-function rather than the iterated φ-function. Thus,

$$D(n) = \varphi(nF(n)) \leq nF(n) \leq n^{k_\lambda(n)+1}. \tag{4}$$

It is suggested in [6] that for all n lying outside a set of asymptotic density 0, the inequality $k_\lambda(n) \ll \log\log n$ holds. If so, then apart from a factor of order $\log\log\log n$ in the exponent, Theorem 3 is best possible.

Let $r(n)$ denote the radical of $\varphi(n)$, that is, the largest squarefree divisor of $\varphi(n)$, and let $k_r(n)$ be the number of iterates of r that brings n to 1. We have $k_r(n) \leq k_\lambda(n)$ and $D(n) \leq n^{k_r(n)+1}$, thus strengthening (4). This inequality and Theorem 3 imply that $k_r(n) \geq (1+o(1))\log\log n/\log\log\log n$ for a set of n of asymptotic density 1. It is easy to see that $k_\lambda(n) \gg \log n$ for infinitely many n; just take n of the form 2^m (and with $n = 3^m$, we get a slightly better constant). We do not know how to show that $k_r(n) \gg \log n$ infinitely often, and perhaps we always have $k_r(n) = o(\log n)$. Surely it must be true that $k_r(n) = o(\log n)$ on a set of asymptotic density 1, but we do not know how to prove this assertion. We also do not know how to prove the analogous assertion for $k_R(n)$, where $R(n)$ is defined as the largest prime factor of $\varphi(n)$. We cannot even prove that $k_R(n) = o(\log n)$ for a fixed positive proportion of integers n, nor can we show that $k_R(n) = o(\log n)$ for infinitely many primes n. Here is one more statement showing our state of ignorance. Let $\mathrm{Prime}(n)$ denote the smallest prime that is congruent to 1 modulo n, and let $\mathrm{Prime}_k(n)$ denote the kth iterate. For example, $\mathrm{Prime}_2(3) = \mathrm{Prime}(7) = 29$. Presumably, the sequence $\mathrm{Prime}_{k+1}(n)/\mathrm{Prime}_k(n)$ is unbounded as $k \to \infty$ for each fixed n, but we cannot show this is true for *any* n. Note that if this sequence is bounded for some n, then $k_R(n) \gg \log n$ for infinitely many n. However, we conjecture both of these assertions are false. For some related considerations, see the paper [1].

We close by remarking that we have $k_\lambda(n) \gg \log\log n$ almost always, that is, for all n outside a set of density 0. Indeed, we have from Theorem 4.5 of [4] that there is a positive constant c_3 such that for almost all n, there is some iterate $\varphi_j(n)$ divisible by every prime up to $(\log n)^{c_3}$. Since every prime that divides some iterate of φ at n also divides some iterate of λ at n (as remarked above), we have

$$k_\lambda(n) \geq \max_{p \leq (\log n)^{c_3}} k_\lambda(p).$$

Further, by Linnik's theorem, there exists a positive constant c_4 such that for all sufficiently large values of x, there is a prime $p \leq x$ with $2^u \mid p-1$ for some integer u with $2^u > x^{c_4}$. For this prime p, we have $k_\lambda(p) > u/2 \gg \log x$. Applied with $x = (\log n)^{c_3}$, we have the assertion.

References

[1] W. D. Banks and I. E. Shparlinski, 'On values taken by the largest prime factor of shifted primes', *J. Aust. Math. Soc.*, to appear.

[2] J. Bayless, 'The Lucas–Pratt primality tree', preprint.

[3] N. L. Bassily, I. Kátai and M. Wijsmuller, 'On the prime power divisors of the iterates of the Euler-ϕ function', *Publ. Math. Debrecen* **55** (1999), 17–32.

[4] P. Erdős, A. Granville, C. Pomerance and C. Spiro, 'On the normal behavior of the iterates of some arithmetic functions', in: *Analytic Number Theory, Proc. of a Conference in Honor of P. T. Bateman*, Birkhäuser; Boston, Inc. 1990, 165–204.

[5] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge University Press, Cambridge, 1988.

[6] G. Martin and C. Pomerance, 'The iterated Carmichael λ-function and the number of cycles of the power generator', *Acta Arith.* **118** (2005), 305-335.

[7] J.-L. Nicolas, 'Sur la distribution des nombres entiers ayant une quantité fixée de facteurs premiers', *Acta Arith.* **44** (1984), 191–200.

[8] V. Pratt, 'Every prime has a succinct certificate', *SIAM J. Comput.* **4** (1975), 214–220.