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`

January 9, 2006

for Ron Graham on his 70th birthday

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 $M(n)$ of this field over $\mathbb{Q}$ is $\phi(m)$, where m is the smallest multiple of n divisible by each prime factor of $\phi(m)$. The prime factors of m/n are precisely the primes not dividing n but which do divide some number in the "Euler chain" $\phi(n), \phi(\phi(n)), \dots$. For each fixed k, we show that $M(n) > n^k$ on a set of asymptotic density 1.

Mathematics Subject Classification: 11N37
Key Words: Euler function, solvable Galois extensions.

1 Introduction

Throughout this paper, all fields which appear are of characteristic zero. Let $\mathbb{K} \subset \mathbb{L}$ be a field extension. We say $\mathbb{L}$ is *prime radical* if $\mathbb{L} = \mathbb{K}[\alpha]$, where $\alpha^p \in \mathbb{K}$ for some prime p, and the polynomial $f(X) = X^p - \alpha^p \in \mathbb{K}[X]$ 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 $\mathbb{K}$.

The present paper is motivated by the following situation. Not all solvable extensions $\mathbb{K} \subset \mathbb{L}$ can be decomposed into a chain of prime radical Galois extensions. But perhaps it is possible for such a chain to exist from $\mathbb{K}$ to a field $\mathbb{M}$ containing $\mathbb{L}$. In fact this is always the case, which we record as follows.

Theorem 1. *Let $\mathbb{K} \subset \mathbb{L}$ be a solvable extension of characteristic zero fields lying in an algebraically closed field $\mathbb{U}$. There is a unique minimal extension $\mathbb{L} \subset \mathbb{M} \subset \mathbb{U}$ such that $\mathbb{M}$ can be reached from $\mathbb{K}$ by a sequence of prime radical extensions which are also Galois.*

For example, say $\mathbb{K} = \mathbb{Q}$ and $\mathbb{L} = \mathbb{Q}(\zeta_7)$, where in general we let ζ_n denote a primitive nth root of unity. This extension is not only solvable, it is cyclic. The field $\mathbb{L}$ has degree 6 over $\mathbb{Q}$, and there is the intermediate field $\mathbb{A} = \mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4)$ 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-3 extension from $\mathbb{A}$ to $\mathbb{L}$ is Galois, so cannot be prime radical, since the cube roots of unity are not present. There is no getting around an extension of degree 3 at some point, so we throw in the cube roots of 1, giving us a prime radical degree-2 extension $\mathbb{B}$ of $\mathbb{A}$. It is then possible to show that the degree-3 extension $\mathbb{B}(\zeta_7)$ over $\mathbb{B}$ is in fact prime radical, and of course Galois. So

$$\mathbb{M} = \mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4)(\zeta_3)(\zeta_7) = \mathbb{Q}(\zeta_{21}),$$

a field of degree 12 over $\mathbb{Q}$.

Let us consider more generally the case for $\mathbb{K} = \mathbb{Q}(\zeta_n)$. We write $M(n)$ for the degree of the field $\mathbb{M}$ determined in Theorem 1. Here, we present a formula for $M(n)$. Let $\phi_k(n)$ be the kth iterate of the Euler function ϕ at n. By convention, we have $\phi_0(n) = n$ and $\phi_1(n) = \phi(n)$.

Theorem 2. *Let $F(n)$ be the least common multiple of n and the largest squarefree divisor of $\prod_{k\geq 1} \phi_k(n)$. Then the field $\mathbb{M}$ determined in Theorem 1* *with* $\mathbb{K} = \mathbb{Q}$ *and* $\mathbb{L} = \mathbb{Q}(\zeta_n)$ *is* $\mathbb{Q}(\zeta_{F(n)})$*, which has degree* $M(n) = \phi(F(n))$ *over* $\mathbb{Q}$*.*

These two results were communicated to us by Hendrik Lenstra; we warmly thank him for allowing us to present his argument. Our contribution is in the following result which shows that $M(n)$, 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*

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

has asymptotic density 1.

Note that a quantity similar to $F(n)$ appears in the proof of Pratt [6] 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 n is prime, then Pratt shows that a proof that n is prime follows from the primality of the prime factors of $F(n)/n$. It is probably true 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), but we have not shown this.

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. This paper started during a very enjoyable visit of the first author at Dartmouth College under a Shapiro Fellowship in May of 2005. He would like to thank this department for its hospitality and support. The first author was also 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.

2 The proofs of Theorem 1 and Theorem 2

We prove two lemmas. The first gives a sufficient condition for an extension $\mathbb{K} \subset \mathbb{L}$ to be reached from $\mathbb{K}$ by a sequence of prime radical Galois extensions.

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

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

The second lemma shows that the condition appearing in Lemma 4 is also necessary.

Lemma 5. *If $\mathbb{K} \subset \mathbb{L}$ is Galois and $\mathbb{L}$ can be reached from $\mathbb{K}$ by a finite sequence of prime radical extensions (which are not necessarily Galois), then $\zeta_p \in \mathbb{L}$ for each prime $p \mid [\mathbb{L} : \mathbb{K}]$.*

Proof. Say the promised sequence of fields is $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n = \mathbb{L}$, and let p be a prime factor of $[\mathbb{L} : \mathbb{K}]$. Then some $[K_{i+1} : \mathbb{K}_i] = p$. Since this extension is radical, it must have a polynomial of the form $X^p - a$ where $a \in \mathbb{K}_i$. Thus a has a pth root b in $\mathbb{L}$, and since $\mathbb{L}$ is Galois, all of the conjugates of b are in $\mathbb{L}$. In particular, $b\zeta_p \in \mathbb{L}$, so $\zeta_p \in \mathbb{L}$. $\square$

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 $\mathbb{M}$ from $\mathbb{L}$, we first adjoin to $\mathbb{L} = \mathbb{L}_0$ all ζ_p, for $p \mid [\mathbb{L} : \mathbb{K}]$ for which $\zeta_p \notin \mathbb{L}$. The resulting field $\mathbb{L}_1$ is still Galois with a solvable group over $\mathbb{K}$. We now adjoin to $\mathbb{L}_1$ all ζ_p for $p \mid [\mathbb{L}_1 : \mathbb{K}]$ for which $\zeta_p \notin \mathbb{L}_1$, and so reach a solvable Galois extension $\mathbb{L}_2$ of $\mathbb{K}$. We continue to iterate the process until we reach a field $\mathbb{M} = \mathbb{L}_n$ which contains all ζ_p for $p \mid [\mathbb{M} : \mathbb{K}]$. Note that the iteration does indeed stabilize since the sequence of relative degrees $[\mathbb{L}_{i+1} : \mathbb{L}_i]$ is strictly decreasing. (If $[\mathbb{L}_i : \mathbb{L}_{i-1}] = d_i$, then any ζ_p adjoined to $\mathbb{L}_i$ to form $\mathbb{L}_{i+1}$ must have $p \mid d_i$. Hence this next extension has degree at most $\prod_{p \mid d_i}(p-1) \leq \phi(d_i)$. And if $d_i > 1$, we have $\phi(d_i) < d_i$.)

This construction creates the smallest field extension $\mathbb{M}$ of $\mathbb{L}$ which contains each ζ_p for p prime and $p \mid [\mathbb{M} : \mathbb{K}]$. It follows from Lemma 4 that $\mathbb{M}$ may be reached from $\mathbb{K}$ by a sequence of prime radical Galois extensions. The minimality, and thus uniqueness of $\mathbb{M}$ follows from Lemma 5. $\square$

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

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

and we immediately recognize that $m = F(n)$. Thus, $M(n) = [\mathbb{Q}[\zeta_m] : \mathbb{Q}] = \phi(m) = \phi(F(n))$. $\square$

3 The proof of Theorem 3

3.1 Preliminary results

We recall a result from [3]:

Proposition 6. *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 $p \mid \phi_k(n)$ is at most $(x/p)(c_1 \log\log x)^k$.*

Let

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

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

Proposition 7. *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 8. *The number of positive integers $n \leq x$ with the property that $\Omega(F_K(n)) > 2(5 \log\log x)^K$ is $\ll (x/\log x)(c_1 \log\log x)^K$ uniformly in K, where c_1 is the constant from Proposition 6.*

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 $n \le x$, 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 8 implies that but for $o(x)$ choices of the positive integer $n \le x$, we have

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

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

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

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

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

By Proposition 7, the number of $n \le x$ 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 $n \le x$, the number B is squarefree. It is clear that $B \mid F(n)$, therefore $\phi(B) \mid M(n)$. From the minimal order of the Euler function, we have

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

Thus, $M(n) > x^K$ holds for all $n \le x$ with $o(x)$ exceptions, which completes the proof of the theorem. □

3.3 Proofs of the preliminary results

Before we begin the proof of Proposition 7, 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

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

for some absolute constant c_0 (see Lemma 1 in [2] or formula (3.1) in [3]). Note that from Theorem 3.5 in [3], we may (and do) take the constant c_1 from Proposition 6 equal to $2c_0$. Let

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

Lemma 9. *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 $q_1q_2 \mid \phi_{k+1}(n)$, then either $p \mid \phi_k(n)$ for some $p \in \mathcal{P}_{q_1q_2}$, or $p_1p_2 \mid \phi_k(n)$ 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 6 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 (1), and so get

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

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

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

Lemma 10. *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 $\phi_{k_2-k_1}(q_1)$. 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 $\phi_j(m)$ is not divisible by the square of any prime exceeding y for $0 \le j \le k-1$, then for each prime $q \mid \phi_k(m)$ with $q > y$, there is a prime $p \mid m$ with $q \mid \phi_k(p)$. Indeed take $k = 1$. Either there is a prime $p \mid m$ with $q \mid \phi(p)$ 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 $p' \mid \phi_k(m)$ with $q \mid \phi(p')$, or $q^2 \mid \phi_k(m)$. 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 $p' \mid \phi_k(p)$. Then $q \mid \phi_{k+1}(p)$, 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 $m = \phi_{k_1}(n)$, there is a prime $p \mid \phi_{k_1}(n)$ with $q_2 \mid \phi_{k_2-k_1}(p)$. By the hypothesis of the lemma, we have $p \ne q_1$. Thus, $pq_1 \mid \phi_{k_1}(n)$. It follows that

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

by Lemma 9. But from the remark on p. 190 of [3], we have

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

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

Proof of Proposition 7. The count in Proposition 7 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 9 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 10. 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 $3c_0$. □

The next result will be helpful in establishing Proposition 8.

Lemma 11. *Uniformly for* $1 < z < 2$, *we have*

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

Proof. We follow the suggestion in Exercise 05 in [4]. 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. □

Lemma 12. *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 11 with $z = 2 - 1/k$. Indeed, if N is the sum in the present lemma, then Lemma 11 implies that

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

and it remains to note that $(2-1/k)^k$ and 2^k are uniformly of the same order. ☐

Proof of Proposition 8. By Lemma 12, if $0 < t \le x$, the number of primes $p \le t$ 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 $n \le t$ with $\Omega(n) > 5\log\log x$. Thus, by partial summation,

$$\sum_{\substack{p\le x\\ \Omega(p-1)>5\log\log x}} \frac{1}{p} \ll \frac{1}{\log x}. \tag{2}$$

If $\Omega(n) \le 5\log\log x$ and if each prime p dividing $F_{K-1}(n)$ has the property that $\Omega(p-1) \le 5\log\log x$, then for all positive integers $0 \le k \le K$ we have $\Omega(\phi_k(n)) \le (5\log\log x)^k$, so that $\Omega(F_K(n)) \le 2(5\log\log x)^K$. We conclude that if $\Omega(F_K(n)) > 2(5\log\log x)^K$, 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 12, that the number of n in the first category is $O(x/\log^2 x)$, while it follows from (2) and Proposition 6 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 $M(n)$

Let $k_\phi(n)$ be the least integer k with $\phi_k(n) = 1$. 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 $\prod_{k\ge1}\phi_k(n)$ are the same as the prime factors of $\prod_{k\ge1}\lambda_k(n)$, so that we might have stated Theorem 2 in terms of the iterated λ-function rather than the iterated ϕ-function. Let $G(n)$ be the product of the prime factors of $\prod_{k\ge 1}\lambda_k(n)$ (so that $F(n)$ in Theorem 2 is equal to the least common multiple of n and $G(n)$). Thus,

$$M(n)=\phi(F(n))\le F(n)\le nG(n)\le n^{k_\lambda(n)+1}. \tag{3}$$

It is suggested in [5] 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 $\phi(n)$, that is, the largest squarefree divisor of $\phi(n)$, and let $k_r(n)$ be the number of iterates of r that brings n to 1. We have $k_r(n)\le k_\lambda(n)$ and $M(n)\le n^{k_r(n)+1}$, thus strengthening (3). 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 $\phi(n)$. 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.) From the inequality $M(n)\le n^{k_r(n)+1}$ and Theorem 3, it follows that $k_r(n)\ge(1+o(1))\log\log n/\log\log\log n$ for a set of integers n of asymptotic density 1. 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 [3] that there is a positive constant c_3 such that for almost all n, there is some iterate $\phi_j(n)$ 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

$$k_\lambda(n)\ge\max_{p\le(\log n)^{c_3}}k_\lambda(p).$$

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 $p\le x$ with $2^u\mid p-1$ for some integer u with $2^u>x^{c_4}$. Thus, for this prime p, $k_\lambda(p)>u/2\gg\log x$. 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’, preprint.

[2] 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.

[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, Proc. of a Conference in Honor of P. T. Bateman*, Birkhäuser; Boston, Inc. 1990, 165–204.

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

[5] 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.

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