ACTA ARITHMETICA
122.3 (2006)

Coincidences in the values of the Euler and Carmichael functions

by

William D. Banks (Columbia, MO), John B. Friedlander (Toronto),
Florian Luca (Morelia), Francesco Pappalardi (Roma)
and Igor E. Shparlinski (Sydney)

1. Introduction. Let φ denote the *Euler function*, which, for an integer $n \ge 1$, is defined as usual by

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{p^\nu \| n} p^{\nu-1}(p-1).$$

The *Carmichael function* λ is defined for each integer $n \ge 1$ as the largest order of any element in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. More explicitly, for any prime power p^ν, one has

$$\lambda(p^\nu) = \begin{cases} p^{\nu-1}(p-1) & \text{if } p \ge 3 \text{ or } \nu \le 2, \\ 2^{\nu-2} & \text{if } p = 2 \text{ and } \nu \ge 3, \end{cases}$$

and for an arbitrary integer $n \ge 2$,

$$\lambda(n) = \operatorname{lcm}[\lambda(p_1^{\nu_1}), \ldots, \lambda(p_k^{\nu_k})],$$

where $n = p_1^{\nu_1} \cdots p_k^{\nu_k}$ is the prime factorization of n. Note that $\lambda(1) = 1$.

The Euler function has long been regarded as one of the most basic of the arithmetic functions. More recently, partly driven by the rise in importance of computational number theory, the Carmichael function has drawn an ever-increasing amount of attention. A large number of results have been obtained, both about the growth rate and about various arithmetical properties of the values of these two functions; see for example [2, 3, 5–7, 10–18, 20, 22, 23] and the references therein.

Despite their similarities, the functions φ and λ often exhibit remarkable differences in their arithmetic behavior. In this paper, we focus on their image sets, which we denote by $\mathcal{F}$ and $\mathcal{L}$, respectively. Since $\varphi(p) = \lambda(p) = p - 1$ for every prime p, the sets $\mathcal{F}$ and $\mathcal{L}$ have at least $\pi(x) \sim x/\log x$ common elements in the interval $[1, x]$. Below, we show that $\mathcal{F} \cap \mathcal{L} \cap [1, x]$ is much

2000 *Mathematics Subject Classification*: Primary 11N37; Secondary 11N25, 11N64.

larger than this. To formulate our results in a quantitative form, for a set $\mathcal{A}$ of positive integers and a real number $x \ge 1$, we put $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$.

Theorem 1. *The number of integers $m \le x$ which are values of both λ and φ satisfies the bound*

$$\#(\mathcal{L}(x) \cap \mathcal{F}(x)) \ge \frac{x}{\log x} \exp((C + o(1))(\log\log\log x)^2)$$

for a suitable positive constant C.

The constant C is defined in (5) in Section 3. In fact, apart from the factor $o(1)$, the bound in Theorem 1 cannot be improved since it represents the true state of affairs for the number of distinct values $\#\mathcal{F}(x)$ of φ, as shown by Maier and Pomerance [21]. More recently, the precise order of magnitude of $\#\mathcal{F}(x)$ has been determined by Ford [15].

In the opposite direction, we also obtain lower bounds of the form $x^{1+o(1)}$ for the number of positive integers $m \le x$ in each of the sets $\mathcal{L}_{\mathcal{F}} = \mathcal{L} \setminus \mathcal{F}$ and $\mathcal{F}_{\mathcal{L}} = \mathcal{F} \setminus \mathcal{L}$.

Theorem 2. *The number of integers $m \le x$ which are values of λ but not of φ satisfies the bound*

$$\#\mathcal{L}_{\mathcal{F}}(x) \ge \frac{x}{\log x} \exp((C + o(1))(\log\log\log x)^2)$$

where C is as before.

Theorem 3. *The number of integers $m \le x$ which are values of φ but not of λ satisfies the bound*

$$\#\mathcal{F}_{\mathcal{L}}(x) \gg \frac{x}{(\log x)^{3/2}}.$$

We remark that Theorem 1 implies, in particular, the lower bound

$$\#\mathcal{L}(x) \ge \frac{x}{\log x} \exp((C + o(1))(\log\log\log x)^2),$$

and even this seems to be new. It would be interesting to see whether the techniques of [15] can be adapted to obtain a more precise statement on the growth of $\#\mathcal{L}(x)$ as $x \to \infty$. However, the above theorems suggest that possibly this bound for $\#\mathcal{L}(x)$ is still far from the truth and $\mathcal{L}$ may be a denser set than $\mathcal{F}$.

For both functions φ and λ, we are also interested in the set of values in $\mathcal{F}$ and $\mathcal{L}$, respectively, which occur once but never again. If $A_\varphi(m)$ denotes the number of solutions n to the equation $\varphi(n) = m$, we define

$$\mathcal{B}_\varphi = \{m \ge 1 : A_\varphi(m) = 1\}, \quad \mathcal{C}_\varphi = \{n \ge 1 : A_\varphi(\varphi(n)) = 1\}.$$

Similarly, we define

$$\mathcal{B}_\lambda = \{m \ge 1 : A_\lambda(m) = 1\}, \quad \mathcal{C}_\lambda = \{n \ge 1 : A_\lambda(\lambda(n)) = 1\},$$

where $A_\lambda(m)$ denotes the number of solutions n to the equation $\lambda(n) = m$. The *Carmichael conjecture* is the assertion that $\mathcal{B}_\varphi = \emptyset$; this is clearly equivalent to $\mathcal{C}_\varphi = \emptyset$. There have recently been several very strong results in the direction of this conjecture given by Ford in [15, 16]. In particular, it has been shown in [15] that if $\mathcal{B}_\varphi \neq \emptyset$, then necessarily

$$\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} > 0. \tag{1}$$

Here, we study the natural analogue of the Carmichael conjecture for the Carmichael function, namely the assertion that $\mathcal{B}_\lambda = \mathcal{C}_\lambda = \emptyset$, which we also believe to be true.

The sets $\mathcal{C}_\varphi$ and $\mathcal{C}_\lambda$, if nonempty, provide counterexamples to the above conjectures. Below, we show that $\#\mathcal{C}_\lambda(x) = o(x)$, that is, that the set $\mathcal{C}_\lambda$ has asymptotic density zero. This follows from a lower bound on the number $\ell(n) = A_\lambda(\lambda(n))$ of solutions m to the equation $\lambda(m) = \lambda(n)$, which holds for almost all positive integers n.

THEOREM 4. *For sufficiently large* $x > 0$:

(i) *the bound*

$$\ell(n) \geq \exp((\log\log x)^{10/3})$$

holds for all positive integers $n \leq x$ *except* $O(x/\log\log x)$ *of them*;

(ii) *the following bound holds*:

$$\#\mathcal{C}_\lambda(x) \leq x\exp(-(\log\log x)^{0.77}).$$

We remark that, in view of (1), a similar (but stronger) estimate for $\#\mathcal{C}_\varphi(x)$, namely

$$\#\mathcal{C}_\varphi(x) \leq x\exp(-\log\log x + o((\log\log\log x)^2)), \tag{2}$$

would immediately settle the Carmichael conjecture in the affirmative. At present, we do not have any nontrivial upper bounds on $\#\mathcal{C}_\varphi(x)$, and the bound (2) appears to be far out of reach; nevertheless, we can obtain a rather strong upper bound on the number of *primitive* elements in $\mathcal{C}_\varphi(x)$. We say that $n \in \mathcal{C}_\varphi$ is a *primitive* counterexample to the Carmichael conjecture if $d \notin \mathcal{C}_\varphi$ for every divisor $d \mid n$, $d < n$. We denote by $\mathcal{C}_\varphi^*$ the set of all primitive counterexamples, and we show that this is a very thin set.

THEOREM 5. *The following bound holds*:

$$\#\mathcal{C}_\varphi^*(x) \leq x^{2/3+o(1)}.$$

The same bound holds for the analogously defined quantity $\#\mathcal{B}_\varphi^*(x)$; see the remarks in Section 8.

We can prove a much stronger bound for the quantity $\#\mathcal{C}_\lambda^*(x)$, which counts the number of primitive counterexamples to the analogue of the Carmichael conjecture for λ.

Theorem 6. *A primitive counterexample to the Carmichael conjecture for λ, if it exists, is unique. In other words,*

$$\#\mathcal{C}_\lambda^*(x) \le 1.$$

Thus, all members of $\mathcal{C}_\lambda$ (if any) are multiples of the smallest one. Along the way to the proof we develop some other properties of $\mathcal{C}_\lambda$ and $\mathcal{C}_\lambda^*$. In particular, the smallest element n of $\mathcal{C}_\lambda$ must necessarily be *powerful*, that is, $p^2 \mid n$ for every prime p dividing n.

Throughout the paper, the implied constants in symbols "O" and "$\ll$" are absolute unless specified otherwise (we recall that $U \ll V$ and $U = O(V)$ are both equivalent to the inequality $|U| \le cV$ with some constant $c > 0$).

We use c, with or without a subscript, to denote an absolute constant (and these may change meaning from one section to the next).

The letters p and q, with subscripts or without, always denote prime numbers, as occasionally do l and r, where indicated. We denote by (a, b) and by $[a, b]$, respectively, the greatest common divisor and least common multiple of the integers a and b; we use the same notation for more than two integers.

We use $\ln x$ to denote the natural logarithm of x, however this notation is used only a few times. Typically, it is more convenient for us to work with the function $\log x = \max\{\ln x, 1\}$ since $\log x \ge 1$ for all $x > 0$. For an integer $l > 1$, we denote by $\log_l x$ the lth iterate of $\log x$.

Acknowledgements. We thank the referee for the suggestion of a modification of our original argument in Theorem 3 which led us to sharpen the exponent of $\log x$ from 2 to 3/2. Most of this paper was written during a very enjoyable visit by the first four authors to Macquarie University; these authors wish to express their thanks to that institution for the hospitality and support. Research of W. B. was also supported in part by NSF grant DMS-0070628, that of J. F. by NSERC grant A5123 and a Killam Research Fellowship, that of F. L. by grants SEP-CONACYT 37259-E and 37260-E, that of F. P. by grant COFIN2002, and that of I. S. by ARC grant DP0211459.

2. Some preliminary results. In Section 3 we give the proof of Theorems 1 and 2. Because these are somewhat technical, we provide in this section some weaker bounds which are nevertheless nontrivial and whose proofs, while quite a bit simpler, provide a guide to the argument. Moreover, due to the simplicity of the arguments one can impose various arithmetic conditions on the integers under consideration. For example, although we have not done this here, one can obtain similar results for short intervals or arithmetic progressions (or both).

THEOREM 7. *We have the bounds*

$$\#(\mathcal{L}(x)\cap\mathcal{F}(x)) \gg \frac{x\log_2 x}{\log x}, \qquad \#\mathcal{L}_{\mathcal{F}}(x) \gg \frac{x\log_2 x}{\log x}.$$

Consider the set $\mathcal{P}_2(x)$ of integers $n = q_0q_1 \le x$ such that $q_0 \equiv q_1 \equiv 3 \pmod 4$ and $(q_0-1, q_1-1) = 2$. Then

$$\lambda(n) = \frac{(q_0-1)(q_1-1)}{2} \equiv 2 \pmod 4$$

for every $n \in \mathcal{P}_2(x)$. Let n be one such integer; then obviously

$$\lambda(16n) = [4, \lambda(n)] = 2\lambda(n) = (q_0-1)(q_1-1) = \varphi(n).$$

On the other hand, suppose that we have $\lambda(n) \in \mathcal{F}$ for $n \in \mathcal{P}_2(x)$. If m is any integer for which $\lambda(n) = \varphi(m)$, then m must be a prime power or twice a prime power, and since $\varphi(m) \le x$ it follows that $m \le 3x$. Hence, there are at most $O(x/\log x)$ distinct numbers of the form $\lambda(n)$, with $n \in \mathcal{P}_2(x)$, lying in $\mathcal{F}$.

Hence, to establish Theorem 7 it suffices to show that the value set

$$\mathcal{L}_2(x) = \{\lambda(n) : n \in \mathcal{P}_2(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements, namely that

$$\#\mathcal{L}_2(x) \gg \frac{x}{\log x}\log_2 x. \tag{3}$$

We start by providing a lower bound for $\#\mathcal{P}_2(x)$. In fact, we give such a bound for a slightly more general subset.

LEMMA 8. *Let $Q \le x^{1/4}$ and denote by $N_Q(x)$ the number of integers $n = q_0q_1 \in \mathcal{P}_2(x)$ with $q_1 \le Q$. Then*

$$N_Q(x) \gg \frac{x}{\log x}\log_2 Q.$$

Proof. Let

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t},$$

and let $\pi(z;k,a)$ denote the number of primes $p \le z$ with $p \equiv a \pmod k$. The contribution to $N_Q(x)$ from any given prime $q_1 \le Q$, $q_1 \equiv 3 \pmod 4$ is

$$\sum_{\substack{q_0\le x/q_1\\ q_0\equiv 3 \,(\mathrm{mod}\, 4)}} \sum_{d|((q_0-1)/2,(q_1-1)/2)} \mu(d) = \sum_{d|(q_1-1)/2} \mu(d) \sum_{\substack{q_0\le x/q_1\\ q_0\equiv 3 \,(\mathrm{mod}\, 4)\\ q_0\equiv 1 \,(\mathrm{mod}\, d)}} 1.$$

Therefore

$$N_Q(x) = \sum_{\substack{q\le Q\\ q\equiv 3 \,(\mathrm{mod}\, 4)}} M_q + \sum_{\substack{q\le Q\\ q\equiv 3 \,(\mathrm{mod}\, 4)}} R_q$$

where

$$M_q = \frac{\mathrm{li}(x/q)}{2} \sum_{d\mid(q-1)/2} \frac{\mu(d)}{\varphi(d)}, \qquad R_q = \sum_{d\mid(q-1)/2} \mu(d)\left(\pi(x/q;4d,a_d) - \frac{\mathrm{li}(x/q)}{2\varphi(d)}\right),$$

and a_d is the residue class modulo $4d$ determined by the classes $3 \pmod 4$ and $1 \pmod d$.

For the sum of the remainders R_q over primes $q \le Q$, we apply the Bombieri–Vinogradov theorem (see, for example, Section 28 of [9]), which is valid for our range $Q \le x^{1/4}$. Therefore, for every constant $A > 1$, we obtain

$$\sum_{\substack{q\le Q\\ q\equiv 3 \pmod 4}} R_q \ll \sum_{q\le Q} \sum_{d\mid(q-1)/2} \left|\pi(x/q;4d,a_d) - \frac{1}{2\varphi(d)}\,\mathrm{li}(x/q)\right| \ll \sum_{q\le Q} \frac{x}{q}\,(\log x)^{-A}$$
$$\ll x(\log x)^{1-A},$$

where the implied constants depend on A.

For the sum over q of the main terms M_q, we have

$$\sum_{\substack{q\le Q\\ q\equiv 3 \pmod 4}} M_q \gg \sum_{\substack{q\le Q\\ q\equiv 3 \pmod 4}} \mathrm{li}(x/q) \prod_{p\mid(q-1)/2} \left(1 - \frac{1}{p-1}\right)$$
$$\gg \frac{x}{\log x} \sum_{\substack{q\le Q\\ q\equiv 3 \pmod 4}} \frac{\varphi(q-1)}{q(q-1)}.$$

It is a trivial modification of a formula of Stephens, Lemma 1 of [24], that

$$\sum_{\substack{q\le Q\\ q\equiv 3 \pmod 4}} \frac{\varphi(q-1)}{q-1} = \frac{\alpha}{2}\,\mathrm{li}(Q) + O(Q/(\log Q)^A),$$

where $A > 1$ is again arbitrary, the implied constant depends only on A, and α is the *Artin constant*:

$$\alpha = \sum_{d\ge 1} \frac{\mu(d)}{d\varphi(d)} = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\ldots.$$

Now by partial summation, we immediately derive that

$$\sum_{\substack{q\le Q\\ q\equiv 3 \pmod 4}} M_q \gg \frac{x}{\log x}\log_2 Q,$$

which completes the proof of the lemma. ■

In our next lemma we give an upper bound for the number of coincidences of the Carmichael function in the values taken on by the integers we counted in the previous lemma.

Lemma 9. *Let $Q \le x^{1/4}$ and let $S_Q(x)$ denote the number of quadruples (p_0, p_1, q_0, q_1) of primes satisfying the restrictions*

$$q_1 < p_1 \le Q, \qquad p_0 p_1 \le x, \qquad q_0 q_1 \le x,$$

and the equation

$$(p_0 - 1)(p_1 - 1) = (q_0 - 1)(q_1 - 1).$$

Then

$$S_Q(x) \ll \frac{x}{(\log x)^2} (\log Q)^3.$$

Proof. We first estimate the contribution S_{p_1,q_1} to $S_Q(x)$ arising from a fixed pair p_1, q_1. We see that S_{p_1,q_1} is the number of positive integers

$$m \le x/[p_1 - 1, q_1 - 1]$$

such that the integers

$$\frac{p_1 - 1}{(p_1 - 1, q_1 - 1)} \cdot m + 1 \quad \text{and} \quad \frac{q_1 - 1}{(p_1 - 1, q_1 - 1)} \cdot m + 1$$

are simultaneously prime. Applying the sieve (e.g., [19, Theorem 5.7]), we obtain

$$\begin{aligned} S_{p_1,q_1} &\ll \frac{x}{(\log x)^2} \frac{(p_1 - 1, q_1 - 1)}{(p_1 - 1)(q_1 - 1)} \prod_{p \mid [p_1 - 1, q_1 - 1]} (1 - 1/p)^{-1} \\ &\le \frac{x}{(\log x)^2} \frac{(p_1 - 1, q_1 - 1)}{\varphi(p_1 - 1)\varphi(q_1 - 1)}. \end{aligned}$$

Summing over $q_1 < p_1 \le Q$, and enlarging the sum to include all positive integers up to Q, we obtain

$$\begin{aligned} \sum_{q_1 < p_1 \le Q} \frac{(p_1 - 1, q_1 - 1)}{\varphi(p_1 - 1)\varphi(q_1 - 1)} &\ll \sum_{k,m \le Q} \frac{(k, m)}{\varphi(k)\varphi(m)} \\ &= \sum_{k,m \le Q} \frac{1}{\varphi(k)\varphi(m)} \sum_{\substack{d \mid k \\ d \mid m}} \varphi(d) \\ &\le \sum_{d \le Q} \frac{1}{\varphi(d)} \sum_{k,m \le Q/d} \frac{1}{\varphi(k)\varphi(m)} \ll (\log Q)^3. \end{aligned}$$

This completes the proof of the lemma. ∎

We now see that for any $Q \le x^{1/4}$ we have, for some positive absolute constants c_1, c_2,

$$\#\mathcal{L}_2(x) \ge N_Q(x) - 2S_Q(x) \ge c_1 \frac{x}{\log x} \log_2 Q - c_2 \frac{x}{(\log x)^2} (\log Q)^3$$

by Lemmas 8 and 9. Taking $Q = \exp((\log x)^{1/3})$, we obtain (3), which completes the proof of Theorem 7.

3. Proof of Theorems 1 and 2. We intend to prove these results by extending the arguments of Section 2. By analogy then we consider the set $\mathcal{P}_{L+1}(x)$ of integers $n = p_0 \cdots p_L \le x$ such that $p_j \equiv 3 \pmod 4$ and $(p_i - 1, p_j - 1) = 2$ for each j and for all $i \ne j$. Then

$$\lambda(n) = 2\,\frac{p_0 - 1}{2} \cdots \frac{p_L - 1}{2} \equiv 2 \pmod 4$$

for every $n \in \mathcal{P}_{L+1}(x)$. Let n be one such integer; then obviously

$$\lambda(2^{L+3}n) = [2^{L+1}, \lambda(n)] = 2^{L+1}\lambda(n) = (p_0 - 1)\cdots(p_L - 1) = \varphi(n).$$

Note that 2^L is small compared to $(\log_2 x)^L$.

On the other hand, suppose that $\lambda(n) \in \mathcal{F}$ for $n \in \mathcal{P}_{L+1}(x)$. If m is any integer for which $\lambda(n) = \varphi(m)$, then m must be a prime power or twice a prime power, and since $\varphi(m) \le x$ it follows that $m \le 3x$. Hence, there are at most $O(x/\log x)$ distinct numbers of the form $\lambda(n)$, with $n \in \mathcal{P}_{L+1}(x)$, lying in $\mathcal{F}$.

Hence, to establish Theorems 1 and 2, it suffices to show that the value set

$$\mathcal{L}_{L+1}(x) = \{\lambda(n) : n \in \mathcal{P}_{L+1}(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements, namely that, for suitable L,

$$\#\mathcal{L}_{L+1}(x) \gg \frac{x}{\log x}\,(\log_2 x)^L. \tag{4}$$

This is rather more complicated than before and some new ideas are required. The set $\mathcal{P}_{L+1}(x)$ is quite large and the number of integers giving rise to the same value of λ is difficult to estimate. As a result it turns out to be easier to give the required lower bound for a subset of $\mathcal{L}_{L+1}(x)$ which arises in turn from a subset of $\mathcal{P}_{L+1}(x)$ formed by choosing the $L+1$ prime factors from well spaced intervals. This idea was used to advantage in the paper of Maier and Pomerance [21] and we shall make heavy use of some of their results. We begin by summarizing those parts of their work which are relevant to our argument.

The main result in [21] is the estimate

$$\#\mathcal{F}(x) = \frac{x}{\log x}\exp(C(1 + o(1))(\log_3 x)^2) \tag{5}$$

for $\mathcal{F}(x) = \{\varphi(n) \le x\}$, where the value of the constant C is $0.81781465\ldots$. Such an estimate consists of both an upper and a lower bound and here we shall prove our lower bounds with the same constant C.

The constant C arises as follows. Let $c_0 = 0.54259859\ldots$ be the unique solution to $F(c_0) = 1$, where $F : (0,1) \to \mathbb{R}$ is given by

$$F(x) = \sum_{n\ge 1}^{\infty} a_n x^n, \qquad a_n = (n+1)\ln(n+1) - n\ln n - 1.$$

With these notations we have $C = 1/|2\ln c_0|$.

We also require the notion of (δ, S)-normal primes where $\delta > 0$ and $S > 1$ (see Section 2 in [21]). Namely, writing $\Omega(n, t_1, t_2)$ for the total number of prime factors of n in $[t_1, t_2]$, we say the prime p is (δ, S)-*normal* if $\Omega(p-1, 1, S) < 2\log_2(10S)$ and, for every $t_1 < t_2$ with $S < t_1 < t_2 < p$, we have

$$|\Omega(p-1, t_1, t_2) - (\log_2 t_2 - \log_2 t_1)| < \delta \log_2 t_2. \tag{6}$$

Proposition 2.2 in [21] shows that for any $\delta > 0$ there exists $\varepsilon > 0$ such that the set $\mathcal{Q}(z, \delta, S)$ of primes $p \le z$ which are not (δ, S)-normal satisfies the bound

$$\#\mathcal{Q}(z, \delta, S) \ll \frac{z}{(\log S)^{\varepsilon} \log z}, \tag{7}$$

where the implied constant depends on δ but not on S.

Let $1/2 < \alpha < c_0$ and $0 < \delta < 1$ be arbitrary fixed real numbers. In particular, throughout this section the implied constants may depend on α and δ.

Let x be a large number and put

$$L = \left\lfloor \frac{1-\delta}{|\ln \alpha|} \log_3 x \right\rfloor + 1. \tag{8}$$

For $k = 0, 1, \ldots, L$, put $w_k = \exp((\log x)^{(1-\delta)\alpha^k})$, $z_k = \exp((\log x)^{\alpha^k})$ and $\mathcal{I}_k = [w_k, z_k]$.

Let $\mathcal{Q}_k$ be the set of $(\delta, \log x)$-normal primes in $\mathcal{I}_k$. Thus, we consider only those primes $p < x$ for which

$$\Omega(p-1, 1, \log x) < 2\log_2(10\log x)$$

and (6) holds for all $\log x < t_1 < t_2 < x$.

Consider the set

$$\mathcal{A} = \{n : x/2 \le n \le x,\ n = p_0 p_1 \cdots p_L, \text{ where each } p_i \in \mathcal{Q}_i\}.$$

The following two statements are shown in [21] on pages 265–272:

(i) We have the lower bound
$$\#\mathcal{A} \ge \frac{x}{\log x} \exp\left(\frac{1-\delta^2}{2|\ln \alpha|}(1+o(1))(\log_3 x)^2\right).$$

(ii) Write $\mathcal{B} = \{(n_1, n_2) \in \mathcal{A} \times \mathcal{A} : \varphi(n_1) = \varphi(n_2),\ n_1 \ne n_2\}$. Then $\#\mathcal{B} = o(x/\log x)$.

Maier and Pomerance [21] used these bounds together with the inequality $\#\mathcal{F} \ge \#\mathcal{A} - \#\mathcal{B}$ to obtain the lower bound in (5).

We now construct a set $\widetilde{\mathcal{A}}$, which is a subset both of $\mathcal{A}$ and of $\mathcal{P}_{L+1}(x)$ and is such that the analogue of (i) above still holds, that is,

$$\#\widetilde{\mathcal{A}} \ge \frac{x}{\log x} \exp\left(\frac{1-\delta^2}{2|\ln \alpha|}(1+o(1))(\log_3 x)^2\right). \tag{9}$$

Consider the set

$$\widetilde{\mathcal{B}} = \{(n_1, n_2) \in \widetilde{\mathcal{A}} \times \widetilde{\mathcal{A}} : \lambda(n_1) = \lambda(n_2),\ n_1 \neq n_2\}.$$

Note that if $n \in \widetilde{\mathcal{A}}$, then $\lambda(n) = \varphi(n)/2^L$. Thus, if $n_1 \neq n_2$ are in $\widetilde{\mathcal{A}}$ and have $\lambda(n_1) = \lambda(n_2)$, then $\varphi(n_1) = \varphi(n_2)$, which shows that $\widetilde{\mathcal{B}} \subseteq \mathcal{B}$. In particular,

$$\#\widetilde{\mathcal{B}} \le \#\mathcal{B} = o(x/\log x).$$

Together with (9), this shows that the number of distinct values of $\lambda(n)$ for n in $\widetilde{\mathcal{A}}$, which exceeds $\#\widetilde{\mathcal{A}} - \#\widetilde{\mathcal{B}}$, is at least as large as required by the statements of Theorems 1 and 2.

Finally, since $\widetilde{\mathcal{A}} \subseteq \mathcal{P}_{L+1}(x)$, we see that (4) holds for L given by (8). Thus, to complete the proof of both Theorems 1 and 2 it is enough to construct $\widetilde{\mathcal{A}} \subseteq \mathcal{A} \cap \mathcal{P}_{L+1}(x)$ which satisfies (9).

To construct $\widetilde{\mathcal{A}}$, we take $u = (\log_2 x)^3$, and we replace $\mathcal{Q}_k$ by

$$\widetilde{\mathcal{Q}}_k = \Big\{p \in \mathcal{Q}_k : \Big(p-1, \prod_{2<q<u} q\Big) = 1,\ \mu^2(p-1) = 1\Big\}.$$

In particular, all primes in $\widetilde{\mathcal{Q}}_k$ are $(\delta, \log x)$-normal. Put

$$\bar{\mathcal{A}} = \{n : x/2 \le n \le x,\ n = p_0 p_1 \cdots p_L,\ p_k \in \widetilde{\mathcal{Q}}_k\},$$

and let

$$\widetilde{\mathcal{A}} = \{n \in \bar{\mathcal{A}} : q^2 \nmid \varphi(n) \text{ for all odd primes } q\}.$$

It is easy to see that every integer in $\widetilde{\mathcal{A}}$ is also in $\mathcal{P}_{L+1}(x)$.

It remains to prove (9), which is established with the aid of a sieve method. Since we only remove very small primes the sieve of Eratosthenes–Legendre is sufficient (when combined with the Bombieri–Vinogradov theorem). The following statement is almost identical to one in [4] and is proved in the same way (alternatively, see [19]). As before, we let $\pi(y; k, a)$ denote the number of primes $p \le y$ with $p \equiv a \pmod{k}$.

Lemma 10. *Let $\mathcal{R}(t_1, t_2, y)$ be the set of primes $p \in [t_1, t_2]$ with $p \equiv 3 \pmod 4$ and such that if an odd prime q divides $p-1$, then $q \ge y$ and $q^2 \nmid p-1$. Then, uniformly for $y \le \frac{1}{3}\log t_1$ and $y \to \infty$, we have*

$$\#\mathcal{R}(t_1, t_2, y) = f(y)(\pi(t_2; 4, 3) - \pi(t_1; 4, 3)) + O\bigg(\frac{t_2}{y \log y \log t_2}\bigg),$$

where

$$f(y) = \prod_{2<p<y} \bigg(1 - \frac{1}{p-1}\bigg).$$

Using the above Lemma 10, partial summation, and the fact that the estimate

$$f(y) = 2c_1(1 + o(1))\,\frac{1}{\log y}$$

holds as y tends to infinity, with a positive constant c_1, we get the following:

LEMMA 11. *For every fixed δ with $1 > \delta > 0$, there exists $t_0(\delta)$ such that uniformly for $t_2 > t_1 > t_0(\delta)$, $(1-\delta)\log_2 t_2 \ge \log_2 t_1 \ge (1-\delta)^2 \log_2 t_2$, $y < \frac{1}{3}\log t_1$ and y tending to infinity, we have*

$$\frac{c_1}{2\log y}(\log_2 t_2 - \log_2 t_1) \le \sum_{p \in \mathcal{R}(t_1,t_2,y)} \frac{1}{p} \le \frac{2c_1}{\log y}(\log_2 t_2 - \log_2 t_1).$$

This follows, for example, from arguments almost identical to those on the lower half of page 217 in [4].

We now take $y = u = (\log_2 x)^3$, $t_1 = w_k$ and $t_2 = z_k$ for a given $k \le L$, and we check that the conditions of Lemma 11 are satisfied if x is large enough. Indeed, since $y = u = (\log_2 x)^3$, and since $t_1 \ge \exp(\exp((\log_2 x)^\delta))$ for each $k \le L$, the condition $y < \frac{1}{3}\log t_1$ follows from the inequality

$$3(\log_3 x) < (\log_2 x)^\delta - \log 3,$$

which holds comfortably for sufficiently large x.

Lemma 11 now shows that

$$\frac{c_2(\log_2 z_k - \log_2 w_k)}{2\log_3 x} \le \sum_{p \in \mathcal{R}(w_k,z_k,y)} \frac{1}{p} \le \frac{2c_2(\log_2 z_k - \log_2 w_k)}{\log_3 x} \tag{10}$$

for $k = 0, \ldots, L$, where $c_2 = c_1/3$. Using next the upper bound (7), we see that, if we write $\mathcal{S}_k$ for the set of those primes $p \in \mathcal{I}_k$ which are not $(\delta, \log x)$-normal, then for some $\varepsilon > 0$,

$$\sum_{p \in \mathcal{S}_k} \frac{1}{p} \ll \frac{1}{(\log_2 x)^\varepsilon}(\log_2 z_k - \log_2 w_k) \tag{11}$$

uniformly in $k = 0, 1, \ldots, L$.

Putting (10) and (11) together, we easily find that

$$\frac{c_2(\log_2 z_k - \log_2 w_k)}{3\log_3 x} \le \sum_{p \in \widetilde{\mathcal{Q}}_k} \frac{1}{p} \le \frac{3c_2(\log_2 z_k - \log_2 w_k)}{\log_3 x}$$

for $k = 0, 1, \ldots, L$, and, noting that

$$\log_2 z_k - \log_2 w_k = \delta\alpha^k \log_2 x,$$

we can rewrite this as

$$\frac{c_2(\delta\alpha^k \log_2 x)}{3\log_3 x} \le \sum_{p \in \widetilde{\mathcal{Q}}_k} \frac{1}{p} \le \frac{3c_2(\delta\alpha^k \log_2 x)}{\log_3 x} \tag{12}$$

for $k = 0, 1, \ldots, L$.

We are now ready to compute the cardinality of $\widetilde{\mathcal{A}}$. For this, we first compute the cardinality of $\overline{\mathcal{A}}$, and we then throw away from $\overline{\mathcal{A}}$ those n such that $q^2 \mid \varphi(n)$ for some odd q.

To compute $\bar{\mathcal{A}}$, we use the argument from the proof of Lemma 3.1 on page 266 of [21]. Let $\mathcal{M}$ be the set of all m of the form $m = p_1 \cdots p_L$ with $p_k \in \widetilde{\mathcal{Q}}_k$, $k = 1, \ldots, L$. We have

$$m \le \prod_{k=1}^{L} z_k \le z_1^2$$

for every $m \in \mathcal{M}$.

Now, let $n = p_0 \cdots p_L$ with $p_k \in \widetilde{\mathcal{Q}}_k$, $k = 0, \ldots, L$. Thus, $n = p_0 m$, where $m = p_1 \cdots p_L \in \mathcal{M}$. Because $x/2 \le n \le x$, we have $x/(2m) \le p_0 \le x/m$. Since $p_0 \in \widetilde{\mathcal{Q}}_0$, by Lemma 10 (it is easy to check that the conditions there are met in our situation), we immediately see that for a fixed $m \in \mathcal{M}$, the number $Q_0(m)$ of such p_0 is

$$Q_0(m) \asymp \frac{x}{\log(x/m)\log_3 x} \asymp \frac{x}{\log x \log_3 x}$$

(since for $m < z_1^2$ we have $\log(x/m) \asymp \log x$). Therefore

$$\begin{aligned} \#\bar{\mathcal{A}} &= \sum_{m\in\mathcal{M}} Q_0(m) \\ &\asymp \frac{x}{\log x \log_3 x} \sum_{m\in\mathcal{M}} \frac{1}{m} = \frac{x}{\log x \log_3 x} \prod_{k=1}^{L} \Bigl(\sum_{p \in \widetilde{\mathcal{Q}}_k} \frac{1}{p} \Bigr). \end{aligned} \tag{13}$$

Using (12), we can estimate the product as follows:

$$\begin{aligned} \prod_{k=1}^{L} \Bigl(\sum_{p \in \widetilde{\mathcal{Q}}_k} \frac{1}{p} \Bigr) &\gg \frac{1}{3^L} \Bigl(\frac{c_2}{\log_3 x} \Bigr)^L \prod_{k=1}^{L} (\delta \alpha^k \log_2 x) \\ &\gg \Bigl(\frac{\delta c_2}{3 \log_3 x} \Bigr)^L \alpha^{(L^2+L)/2} (\log_2 x)^L \\ &= \exp\Bigl(\frac{1-\delta^2}{2|\ln \alpha|} (\log_3 x)^2 + O(\log_3 x \log_4 x) \Bigr). \end{aligned}$$

The above is almost what we want, but we now need to eliminate from $\bar{\mathcal{A}}$ those n such that $\varphi(n)$ is divisible by the square of some odd prime. Such a prime is necessarily larger than u. Moreover, if $n = p_0 \cdots p_L$ is such a number, then there exists $q > u$ (because the $p_k - 1$ are free of odd primes less than u for all $k = 0, \ldots, L$), and $i \ne j$ (because the $p_k - 1$ are squarefree for $k = 0, \ldots, L$), such that $q \mid p_i - 1$ and $q \mid p_j - 1$. To estimate the number of such n, we fix i and j.

Assume first that neither i nor j is zero. Then p_i and p_j are chosen in $\mathcal{I}_i$ and $\mathcal{I}_j$, respectively, and these primes are in the arithmetical progression

1 modulo q. The set $\mathcal{N}_{i,j}$ of such numbers satisfies

$$\#\mathcal{N}_{i,j} \ll \frac{x}{\log x \log_3 x}\sum_{m\in\mathcal{M}_{i,j}}\frac{1}{m}, \tag{14}$$

where the sum is over the set $\mathcal{M}_{i,j}$ of all possible m in the representation $n = p_0 m$ with $p_0 \in \widetilde{\mathcal{Q}}_0$ for all $n \in \mathcal{N}_{i,j}$. We bound the sum over m as follows:

$$\begin{aligned}\sum_{m\in\mathcal{M}_{i,j}}\frac{1}{m} &\ll \sum_{q>u}\prod_{\substack{k=1\\ k\neq i,j}}^{L}\Big(\sum_{p\in\widetilde{\mathcal{Q}}_k}\frac{1}{p}\Big)\prod_{k=i,j}\Big(\sum_{\substack{p\in\mathcal{I}_k\\ p\equiv 1\,(\mathrm{mod}\,q)}}\frac{1}{p}\Big)\\ &= \prod_{k=1}^{L}\Big(\sum_{p\in\widetilde{\mathcal{Q}}_k}\frac{1}{p}\Big)\sum_{q>u}\prod_{k=i,j}\Big(\sum_{\substack{p\in\mathcal{I}_k\\ p\equiv 1\,(\mathrm{mod}\,q)}}\frac{1}{p}\Big)\Big(\sum_{p\in\widetilde{\mathcal{Q}}_k}\frac{1}{p}\Big)^{-1}.\end{aligned}$$

Now, by (13) and (14), we conclude that

$$\#\mathcal{N}_{i,j} \ll \#\bar{\mathcal{A}}\Delta_{ij},$$

where

$$\Delta_{ij} = \sum_{q>u}\prod_{k=i,j}\Big(\sum_{\substack{p\in\mathcal{I}_k\\ p\equiv 1\,(\mathrm{mod}\,q)}}\frac{1}{p}\Big)\Big(\sum_{p\in\widetilde{\mathcal{Q}}_k}\frac{1}{p}\Big)^{-1}.$$

Using (12) and the bound (see inequality (3.1) in [12])

$$\sum_{\substack{p\le z\\ p\equiv 1\,(\mathrm{mod}\,q)}}\frac{1}{p} \ll \frac{\log_2 z}{q}$$

we deduce that

$$\begin{aligned}\Delta_{ij} &\ll \prod_{k=i,j}\Big(\frac{c_2\delta\alpha^k\log_2 x}{3\log_3 x}\Big)^{-1}\sum_{q>u}\frac{(\log_2 x)^2}{q^2} = (3\delta)^2 c_2^{-2}\alpha^{-i-j}(\log_3 x)^2\sum_{q>u}\frac{1}{q^2}\\ &\ll \alpha^{-2L}(\log_3 x)^2\,\frac{1}{u\log u}.\end{aligned}$$

Summing up these inequalities over all possible choices of i, j, we get

$$\sum_{1\le i<j\le L} N_{i,j} \ll \#\bar{\mathcal{A}}\sum_{1\le i<j\le L}\Delta_{i,j} \ll \#\bar{\mathcal{A}}\,\frac{L^2\alpha^{-2L}(\log_3 x)^2}{u\log u}.$$

Recalling the definition of L and u, we derive

$$\frac{L^2\alpha^{-2L}(\log_3 x)^2}{u\log u} \ll \frac{(\log_2 x)^{2-2\delta}(\log_3 x)^4}{u\log u} \ll \frac{1}{\log_2 x}.$$

A similar argument applies to the contribution coming from those cases where one of i and j is zero. As a result we only sketch this. In the event that the prime $q > u$ divides both $p_0 - 1$ and $p_j - 1$ for some $j \ge 1$, the latter condition implies the inequality $q < z_1$ and this in turn implies that $y = u < \frac{1}{3}\log(w_0/q)$. This allows one to deduce (by the same proofs) the validity of Lemmas 10 and 11 applied to those primes in the interval $[w_0, z_0]$ which are congruent to 1 mod q in addition to being congruent to 3 mod 4. The results are uniform for q in this range and, in the case of Lemma 11, the upper and lower bounds are to be multiplied by the factor $1/(q-1)$. Proceeding now as before, we obtain in place of (14) the estimate

$$\#\mathcal{N}_{0,j} \ll \frac{x}{q\log x\log_3 x}\sum_{m\in\mathcal{M}_{0,j}}\frac{1}{m},$$

and subsequently we find that

$$\#\mathcal{N}_{0,j} \ll \#\bar{\mathcal{A}}\Delta_{0j}$$

where Δ_{0j} takes the form

$$\Delta_{0j} = \sum_{q>u}\frac{1}{q}\Bigg(\sum_{\substack{p\in\mathcal{I}_j\\ p\equiv 1 \,(\mathrm{mod}\, q)}}\frac{1}{p}\Bigg)\Bigg(\sum_{p\in\widetilde{\mathcal{Q}}_j}\frac{1}{p}\Bigg)^{-1}.$$

The rest of the proof follows as in the other case and, perhaps not surprisingly, the bound is now slightly better.

This shows that $\#\widetilde{\mathcal{A}} = \#\bar{\mathcal{A}} + o(\#\bar{\mathcal{A}})$, which completes the proof that the lower bound (i) also holds for $\#\widetilde{\mathcal{A}}$. Letting δ tend to zero and α tend to c_0, we obtain the specific constant C claimed earlier. This completes the proof of Theorems 1 and 2.

4. Proof of Theorem 3. We begin by fixing a prime $q > 5$ such that $2q + 1$ is a prime but $2q^2 + 1$ and $4q^2 + 1$ are composite. There are many such primes but we require only one. For example, we can choose $q = 11$. Throughout the proof, we allow the implied constants to depend on q.

We say that an integer w is *z-rough* if all prime divisors of w exceed z.

Now let x be sufficiently large and let z be an arbitrary real number with $\log x \le z \le x^{1/5}$. We consider the set $\mathcal{P}$ of primes p in the interval $[x/4q, x/2q]$ of the form

$$p = 2qw + 1,$$

where w is z-rough. Using the lower bound linear sieve and estimating the remainder term by the Bombieri–Vinogradov theorem (e.g., see Theorem 7.4, p. 219, of [19]), we have

$$\#\mathcal{P} \gg \frac{x}{\log x\log z}.$$

We next remove some primes from $\mathcal{P}$, namely the set $\mathcal{Q}$ of primes $p \in \mathcal{P}$ for which $p - 1 = 2qrs$ and either $2q^2r + 1$ or $4q^2r + 1$ is prime. Using the upper bound sieve, say of Brun (e.g., see Theorem 2.2, p. 68, of [19]), we see that for every fixed s the cardinality of the set $\mathcal{Q}_s$ of such primes $p \in \mathcal{P}$ does not exceed

$$\begin{aligned}\#\mathcal{Q}_s &\ll \frac{x}{s} \prod_{\substack{l \le z \\ l \nmid s}} \left(1 - \frac{3}{l}\right) \prod_{\substack{z < l \le x/s \\ l \nmid s}} \left(1 - \frac{2}{l}\right) \prod_{l \mid s} \left(1 - \frac{1}{l}\right) \\ &\ll \frac{x}{s} \cdot \frac{1}{(\log(x/s))^2 \log z} \cdot \frac{s}{\varphi(s)}.\end{aligned}$$

Clearly, any admissible s is either 1 or is z-rough. For $s = 1$, we have

$$\#\mathcal{Q}_1 \ll \frac{x}{(\log x)^2 \log z}.$$

If s is z-rough then, recalling that $z \ge \log x$, we have

$$\sum_{l \mid s} \frac{1}{l} \le \frac{1}{z} \sum_{l \mid s} 1 = o\left(\frac{\log x}{z}\right) = o(1),$$

thus $\varphi(s) = (1 + o(1))s$. We also remark that by the condition on q, we have $r > 1$ and therefore $r > z$ (since $(p-1)/2q$ is z-rough). We thus obtain

$$\begin{aligned}\sum_{\substack{s < x/z \\ s\ z\text{-rough}}} \#\mathcal{Q}_s &\ll \frac{x}{\log z} \sum_{\substack{s < x/z \\ s\ z\text{-rough}}} \frac{1}{s(\log(x/s))^2} \\ &\ll \frac{x}{\log z} \sum_{\log z - 1 \le j \le \log x + 1} \sum_{\substack{x/e^{j-1} \le s < x/e^j \\ s\ z\text{-rough}}} \frac{1}{s(\log(x/s))^2} \\ &\ll \frac{1}{\log z} \sum_{\log z - 1 \le j \le \log x + 1} \frac{e^j}{j^2} \sum_{\substack{x/e^{j-1} \le s < x/e^j \\ s\ z\text{-rough}}} 1.\end{aligned}$$

But, again by the upper bound sieve, for $j \ge \log z - 1$, we have

$$\sum_{\substack{x/e^{j-1} \le s < x/e^j \\ s\ z\text{-rough}}} 1 \le \sum_{\substack{s < x/e^j \\ s\ z\text{-rough}}} 1 \ll \frac{x}{e^j \log z}.$$

Thus,

$$\sum_{\substack{s < x/z \\ s\ z\text{-rough}}} \#\mathcal{Q}_s \ll \frac{x}{(\log z)^2} \sum_{\log z - 1 \le j \le \log x + 1} \frac{1}{j^2} \ll \frac{x}{(\log z)^3}.$$

The above estimate could have been alternatively obtained by partial summation. Hence, from the above bounds, we derive

$$\#\mathcal{Q} \le \#\mathcal{Q}_1 + \sum_{\substack{s < x/z \\ s\ z\text{-rough}}} \#\mathcal{Q}_s \ll \frac{x}{(\log z)^3}.$$

Thus, if we define

$$z = \exp(c\sqrt{\log x}),$$

for some appropriate constant $c > 0$, then the set $\mathcal{R} = \mathcal{P} \setminus \mathcal{Q}$ satisfies

$$\#\mathcal{R} \ge \#\mathcal{P} - \#\mathcal{Q} \gg \frac{x}{\log x \log z} \gg \frac{x}{(\log x)^{3/2}}.$$

For each $p \in \mathcal{R}$, we consider the integer $n = (2q+1)p$. We then have

$$\varphi(n) = 2q(p-1) = 4q^2\,\frac{p-1}{2q},$$

where $(p-1)/2q > q$. The values of $\varphi(n)$ are distinct as p varies, and each of them satisfies $\varphi(n) \le x$. Thus, to complete the proof of Theorem 3, it suffices to show that $\varphi(n) \notin \mathcal{L}$ for each $p \in \mathcal{R}$.

Suppose, on the contrary, that $\varphi(n) \in \mathcal{L}$ for some $p \in \mathcal{R}$; that is,

$$\lambda(m) = 4q^2\,\frac{p-1}{2q} \tag{15}$$

for some m. Since $q^2 \mid \lambda(m)$, we must have $q^2 \mid \lambda(r^e)$ for some prime r with $r^e \parallel m$. This could happen in only two ways, both of which can be ruled out in our situation:

- If $q \mid m$, then $q - 1 \mid \lambda(m)$. But (15) implies that
  $$q - 1 \mid 4\,\frac{p-1}{2q},$$
  which cannot happen for large x since $(p-1)/2q$ is z-rough for $p \in \mathcal{R}$ and $5 < q < z$.
- If $q \nmid m$, then $q^2 \mid \lambda(r^e)$ implies that $q^2 \mid r - 1$ (since $r \mid m$), from which it follows that $2q^2 \mid r - 1$ and
  $$r - 1 \mid 4q^2\,\frac{p-1}{2q}.$$

Thus, r must have one of the following forms:

$$r = 2q^2s + 1 \quad \text{or} \quad r = 4q^2s + 1,$$

for some integer divisor s of $(p-1)/2q$. However, for $s = 1$ this has been already eliminated by the choice of q, and for $s > 1$ this is impossible by our construction of the set $\mathcal{R}$.

This concludes the proof of Theorem 3.

5. Proof of Theorem 4. We begin with a result that is implicit in [12]; see also the variant given explicitly as Lemma 2 of [20].

Lemma 12. *For some absolute constant $c_1 > 0$, $\lambda(n)$ is divisible by all prime powers $l^k \le y$ for a set $\mathcal{N}$ of positive integers $n \le x$ of cardinality*

$$\#\mathcal{N} = x + O(xy\exp(-c_1y^{-1}\log_2 x)).$$

Proof. Following the argument in the proof of Theorem 4.1 of [12] (see also Theorem 3.4 of [12]), we see that if $l^k \le \log_2 x$, then

$$\max_{q|n} \operatorname{ord}_l(q-1) \le k$$

for at most $O(x\exp(-c_1 l^{-k}\log_2 x))$ positive integers $n \le x$, where $c_1 > 0$ is an absolute constant. ∎

We are now ready to prove Theorem 4. We assume that β is a real number in the interval $(0,1)$ such that for some constant $c_2 > 0$ and every sufficiently large $z > 0$, there are at least $z/(\log z)^{c_2}$ primes p in the interval $\mathcal{J} = [z/(\log z)^{c_2}, z]$ such that all prime divisors of $p-1$ are of size at most $w = z^{\beta}$.

For some sufficiently large $y > 0$ we choose $z = (y/(\log y)^{c_2+1})^{1/\beta}$ and let $\mathcal{N}$ be the set of Lemma 12.

For each prime $l \le w$, the number of primes $p \in \mathcal{J}$ for which $l^k \,|\, p-1$ for some power $l^k > y$ is at most $O(z/y)$. Thus the number of primes $p \in \mathcal{J}$ divisible by a power $l^k > y$ of some prime $l \le w$ is at most

$$O(zw/y) = o(z/(\log z)^{c_2})$$

because of the above choice of z. Therefore, there exists a set $\mathcal{P}$ with at least $s = \#\mathcal{P} \ge z/2(\log z)^{c_2}$ primes p in the interval $\mathcal{J}$, such that each prime $p \in \mathcal{P}$ satisfies

$$(p-1) \mid \prod_{l^k \le y} l^k,$$

where the product is taken over all the primes $l \le w$.

It is clear that if $n \in \mathcal{N}$ and m is squarefree, coprime to n, and such that all its prime factors are in $\mathcal{P}$, then $\lambda(n) = \lambda(nm)$; in particular, $n \notin \mathcal{C}_\lambda(x)$.

To prove part (i) of Theorem 4 we begin by applying Lemma 12 with

$$y = c_3 \log_2 x/\log_3 x,$$

where $c_3 = c_1/2$, obtaining the estimate

$$\#\mathcal{N} = x + O(x/\log_2 x).$$

The set $\mathcal{E}$ of $n \in \mathcal{N}$ such that n is divisible by p for at least $r = \lfloor \log z \rfloor$ primes $p \in \mathcal{P}$ has cardinality at most

$$\#\mathcal{E} \le \sum_{\substack{p_1 < \cdots < p_r \\ p_i \in \mathcal{P},\, i=1,\ldots,r}} \frac{x}{p_1 \cdots p_r} \le x\,\frac{1}{r!}\biggl(\sum_{p\in\mathcal{P}} \frac{1}{p}\biggr)^r.$$

Extending the summation in the last sum over all primes in the interval $\mathcal{J}$ and using the Mertens formula, we derive that

$$\sum_{p\in\mathcal{P}} \frac{1}{p} \le \sum_{p\in\mathcal{J}} \frac{1}{p} = \log_2 z - \log_2(z/(\log z)^{c_2}) + O(1/\log z) = o(1).$$

Using the inequality $e^r \ge r^r/r!$ we see that, for sufficiently large x,

$$\#\mathcal{E} \le x\left(\frac{e}{r}\right)^r = xz^{-(1+o(1))\log_2 z} \ll \frac{x}{\log_2 x}.$$

Therefore, for all positive integers $n \in \mathcal{N} \setminus \mathcal{E}$ we have

$$\ell(n) \ge 2^{s-r} = \exp(z^{1+o(1)}) = \exp(y^{1/\beta+o(1)}) = \exp((\log_2 x)^{1/\beta+o(1)}).$$

Clearly $\#(\mathcal{N}\setminus\mathcal{E}) = x + O(x/\log_2 x)$ for the above choice of parameters. By a result of Baker and Harman [1], one can take $\beta = 0.2961$. Since $1/\beta > 10/3$, this finishes the proof of part (i) of Theorem 4.

To prove part (ii) of Theorem 4 we choose

$$y = (\log_2 x)^{\beta/(1+\beta)}$$

so that

$$\#\mathcal{N} = x + O(x\exp(-(\log_2 x)^{1/(1+\beta)+o(1)}))$$

by Lemma 12.

As before, we see that $\ell(n) \ge 2$ for any $n \in \mathcal{N}$ unless

$$\prod_{p\in\mathcal{P}} p \,\Big|\, n,$$

which holds on a set $\widetilde{\mathcal{E}} \subset \mathcal{N}$ of cardinality at most

$$\begin{aligned}\#\widetilde{\mathcal{E}} &\le x\prod_{p\in\mathcal{P}} p^{-1} \le x(z/(\log z)^{c_2})^{-(\#\mathcal{P})} = x\exp(-z^{1+o(1)})\\ &= x\exp(-y^{1/\beta+o(1)}) = x\exp(-(\log_2 x)^{1/(1+\beta)+o(1)}).\end{aligned}$$

Again, using the result of Baker and Harman [1] one can take $\beta = 0.2961$. Since $1/(1+\beta) > 0.77$, this finishes the proof of part (ii) of Theorem 4.

6. Proof of Theorem 5. Let $k(m)$ denote the *squarefree kernel* of an integer $m \in \mathbb{N}$, that is,

$$k(m) = \prod_{p\mid m} p.$$

The following result, which is based on the Rankin method, is contained in Theorem 13 in Section II.1.5 of [25]:

LEMMA 13. *Uniformly for $x \ge y \ge 2$, we have*

$$\#\{m \le x : k(m) \le y\} \ll y(\log y)\exp(\sqrt{8\log(x/y)}).$$

We also need the following result, which is a variant of Lemma 2.9 in [15]:

LEMMA 14. *The number of $n \in \mathcal{C}_\varphi$ with $n \le x$ for which either $d^2 \mid \varphi(n)$ or $d^2 \mid n$ for some $d > y$ is at most $O(x/y)$.*

Proof. For each d there are obviously $O(x/d^2)$ values of n with $d^2 \mid n$, and also $O(x/d^2)$ values of $\varphi(n)$ with $d^2 \mid \varphi(n)$. Because $n \in \mathcal{C}_\varphi$, the total number of possible values of n for each d is $O(x/d^2)$. Summing up over all $d > y$ finishes the proof. ∎

We are now prepared to prove Theorem 5. Let $n \le x$ be a primitive counterexample to the Carmichael conjecture, that is, $n \in \mathcal{C}_\varphi^*(x)$. Let $\varphi(n) = m$. If p is any prime dividing n with $p^\alpha \parallel n$, then

$$m = \varphi(n) = \varphi(p^\alpha)\,\varphi(n/p^\alpha) = p^{\alpha-1}(p-1)\,\varphi(n/p^\alpha).$$

Since n/p^α is a proper divisor of n, and n is primitive, $n/p^\alpha \notin \mathcal{C}_\varphi$; hence, $\varphi(n/p^\alpha) = \varphi(s)$ for some integer $s \ne n/p^\alpha$, and

$$m = p^{\alpha-1}(p-1)\varphi(s). \tag{16}$$

We claim that $p \mid s$. Indeed, if this were not true, then from (16) it would follow that

$$\varphi(n) = m = \varphi(p^\alpha s);$$

however, since $p^\alpha s \ne n$, this contradicts our assumption that $n \in \mathcal{C}_\varphi$. Having shown that $p \mid s$, from (16) we now see that $(p-1)^2 \mid m$, and this holds for *every* prime p dividing n.

Now let q be an arbitrary prime divisor of m. We have

$$q \mid m \quad \text{and} \quad m = \varphi(n) = \prod_{p^\alpha \parallel n} p^{\alpha-1}(p-1).$$

If $q \mid p^{\alpha-1}$ for some p and α, then $p = q$, $\alpha \ge 2$, and therefore $q^2 \mid n$. On the other hand, if $q \nmid p^{\alpha-1}$ whenever $p^\alpha \parallel n$, it follows that $q \mid p-1$ for some $p \mid n$, and by the above analysis we find that $q^2 \mid (p-1)^2 \mid m$. Thus, we have shown that

$$q \mid m \;\Rightarrow\; q^2 \mid m \text{ or } q^2 \mid n. \tag{17}$$

We now write

$$\#\mathcal{C}_\varphi^*(x) = \#\{n \in \mathcal{C}_\varphi^*(x) : k(\varphi(n)) \le z\} + \#\{n \in \mathcal{C}_\varphi^*(x) : k(\varphi(n)) > z\},$$

where z is a real parameter in the interval $[2, x]$, to be specified in a moment. Noting that the map $n \mapsto \varphi(n)$ is injective on $\mathcal{C}_\varphi$, and using Lemma 13, we bound the first contribution by

$$\begin{aligned}\#\{n \in \mathcal{C}_\varphi^*(x) : k(\varphi(n)) \le z\} &\le \#\{m \le x : k(m) \le z\} \\ &\ll z(\log z)\exp(\sqrt{8\log(x/z)}).\end{aligned}$$

For the second contribution, if $n \in \mathcal{C}_\varphi^*(x)$, $m = \varphi(n)$, and $k(m) > z$, we define

$$d_1 = \prod_{q^2 \mid m} q, \qquad d_2 = \prod_{q^2 \mid n} q.$$

Using (17), it follows that

$$d_1 d_2 \geq \prod_{q^2 \mid m \text{ or } q^2 \mid n} q \geq k(m) > z;$$

hence, either $d_1 > \sqrt{z}$ or $d_2 > \sqrt{z}$. Since $d_1^2 \mid m$ and $d_2^2 \mid n$, Lemma 14 implies that

$$\#\{n \in \mathcal{C}_\varphi^*(x) : k(\varphi(n)) > z\} \ll x/\sqrt{z}.$$

Therefore,

$$\#\mathcal{C}_\varphi^*(x) \ll z(\log z)\exp(\sqrt{8\log(x/z)}) + x/\sqrt{z}.$$

Choosing $z = x^{2/3}$ (in order to balance these terms), we complete the proof of Theorem 5.

7. Proof of Theorem 6. We recall that $\mathcal{C}_\lambda$ is the set of counterexamples to the *Carmichael conjecture for* λ, and $\mathcal{C}_\lambda^*$ is the set of *primitive* counterexamples:

$$\mathcal{C}_\lambda = \{n : \lambda(m) \neq \lambda(n) \text{ for all } m \neq n\},$$
$$\mathcal{C}_\lambda^* = \{n \in \mathcal{C}_\lambda : d \notin \mathcal{C}_\lambda \text{ for all } d \mid n,\, d < n\}.$$

For a positive integer n and a prime p, we denote by $\operatorname{ord}_p(n)$ the largest integer $\alpha \geq 0$ such that $p^\alpha \mid n$. We also denote by $\vartheta_p(n)$ the largest integer $\beta \geq 0$ for which $\lambda(p^\beta) \mid \lambda(n)$.

Lemma 15. *If $n \in \mathcal{C}_\lambda$, then $\vartheta_p(n) = \operatorname{ord}_p(n)$ for every prime p.*

Proof. Suppose that $n \in \mathcal{C}_\lambda$, and let p be an arbitrary prime number. Put $\alpha = \operatorname{ord}_p(n)$ and $\beta = \vartheta_p(n)$. Since $p^\alpha \mid n$, it follows that $\lambda(p^\alpha) \mid \lambda(n)$; thus, $\beta \geq \alpha$. On the other hand, since $\lambda(p^\beta) \mid \lambda(n)$, we have

$$\lambda(n) = [\lambda(p^\beta), \lambda(n)] = [\lambda(p^\beta), \lambda(p^\alpha), \lambda(n/p^\alpha)].$$

It cannot be true that $\beta > \alpha$, for otherwise we would have

$$\lambda(n) = [\lambda(p^\beta), \lambda(n/p^\alpha)] = \lambda(np^{\beta-\alpha}),$$

which is impossible since $n \in \mathcal{C}_\lambda$ but $n \neq np^{\beta-\alpha}$. Therefore, $\beta = \alpha$. ■

Corollary 16. *If $n \in \mathcal{C}_\lambda$, then $p \mid n$ if and only if $p - 1 \mid \lambda(n)$.*

Proof. By Lemma 15, for any $n \in \mathcal{C}_\lambda$, we have $\operatorname{ord}_p(n) \geq 1$ if and only if $\vartheta_p(n) \geq 1$, and the result follows. ■

Lemma 17. *If $n \in \mathcal{C}_\lambda$, then $2^4 \mid n$, and for every prime p dividing n, we have*

$$\operatorname{ord}_p(\lambda(n)) = \begin{cases} \operatorname{ord}_2(n) - 2 & \textit{if } p = 2, \\ \operatorname{ord}_p(n) - 1 & \textit{if } p \neq 2. \end{cases}$$

Proof. Let $n \in \mathcal{C}_\lambda$ be fixed. Since $\lambda(1) = \lambda(2)$ and $\lambda(4) = \lambda(8)$, it is easy to see that $2^4 \mid n$. Put $\alpha = \operatorname{ord}_2(\lambda(n)) \geq 2$; since $2^\alpha = \lambda(2^{\alpha+2})$, it follows that $\alpha + 2 = \vartheta_2(n)$. By Lemma 15, $\vartheta_2(n) = \mathrm{ord}_2(n)$; thus, $\mathrm{ord}_2(\lambda(n)) = \mathrm{ord}_2(n) - 2$.

Now let p be an odd prime dividing n. By Corollary 16, $p-1 \mid \lambda(n)$. Put $\beta = \mathrm{ord}_p(\lambda(n)) \geq 0$; since $p^\beta(p-1) = \lambda(p^{\beta+1})$, it follows that $\beta + 1 = \vartheta_p(n)$. By Lemma 15, $\vartheta_p(n) = \mathrm{ord}_p(n)$; therefore, $\mathrm{ord}_p(\lambda(n)) = \mathrm{ord}_p(n) - 1$. ∎

Recall that an integer $n \geq 2$ is said to be *powerful* if $p^2 \mid n$ for every prime p dividing n.

Lemma 18. *If $n \in \mathcal{C}_\lambda^*$, then n is powerful.*

Proof. Let $n \in \mathcal{C}_\lambda^*$ be fixed. Since $2^4 \mid n$ by Lemma 17, it suffices to show that $p^2 \mid n$ for every odd prime p dividing n.

Since n is primitive, $\lambda(n/p) = \lambda(\widetilde{n})$ for some $\widetilde{n} \neq n/p$. Assuming that $\mathrm{ord}_p(n) = 1$, it follows that

$$\lambda(n) = [\lambda(p), \lambda(n/p)] = [p-1, \lambda(\widetilde{n})].$$

If $p \nmid \widetilde{n}$, this implies that $\lambda(n) = \lambda(\widetilde{n}p)$, which is impossible since $n \in \mathcal{C}_\lambda$ but $\widetilde{n}p \neq n$. On the other hand, if $p \mid \widetilde{n}$, then $p - 1 \mid \lambda(\widetilde{n})$, and we deduce that $\lambda(n) = \lambda(\widetilde{n}) = \lambda(n/p)$, which is again impossible. Thus, $\mathrm{ord}_p(n) \geq 2$. ∎

Corollary 19. *If $n \in \mathcal{C}_\lambda^*$, then $p^2 \mid n$ if and only if $p - 1 \mid \lambda(n)$.*

Proof. If $p - 1 \mid \lambda(n)$, then $p \mid n$ by Corollary 16; hence, $p^2 \mid n$ by Lemma 18. The converse is obvious. ∎

For a positive integer n and a prime p, let us denote by $\Theta_p(n)$ the largest integer $\alpha \geq 0$ such that $p^\alpha \mid \lambda(k(n))$; in other words,

$$\Theta_p(n) = \mathrm{ord}_p(\lambda(k(n))) = \max_{q \mid n} \mathrm{ord}_p(q-1),$$

where q varies over the primes dividing n and where, as in Section 6, $k(n)$ is the squarefree kernel of n. Note that, since $\mathrm{ord}_p(p-1) = 0$, $\Theta_p(n) = \Theta_p(n/p^{\mathrm{ord}_p(n)})$.

Lemma 20. *If $n \in \mathcal{C}_\lambda$, then $\Theta_2(n) \geq 1$.*

Proof. If $n \in \mathcal{C}_\lambda$, n must have an odd prime factor p, for otherwise $n = 2^\alpha$ with $\alpha \geq 4$ (Lemma 17), and $\lambda(n) = \lambda(2^\alpha) = \lambda(3 \cdot 2^\alpha) = \lambda(3n)$. Since $2 \mid p-1$, it follows that $\Theta_2(n) \geq 1$. ∎

Lemma 21. *If $n \in \mathcal{C}_\lambda^*$, then for every prime p dividing n, we have*

$$\mathrm{ord}_p(n) = \begin{cases} \Theta_2(n) + 3 & \text{if } p = 2, \\ \Theta_p(n) + 2 & \text{if } p \neq 2. \end{cases}$$

Proof. Let $n \in \mathcal{C}_\lambda^*$ be fixed. If $\alpha = \mathrm{ord}_2(n)$, then $\alpha \geq 4$ and $\mathrm{ord}_2(\lambda(n)) = \alpha - 2$ by Lemma 17. If $\beta = \Theta_2(n)$, we also have $2^\beta \mid \lambda(k(n)) \mid \lambda(n)$; thus, $\alpha \geq \beta + 2$.

Suppose that $\alpha = \beta + 2$. Since $\lambda(n) = [2^{\alpha-2}, \lambda(n/2^\alpha)]$, and

$$\begin{aligned}\mathrm{ord}_2(\lambda(n/2^\alpha)) &= \mathrm{ord}_2([p^{\gamma-1}(p-1) : p^\gamma \parallel n/2^\alpha]) = \mathrm{ord}_2([(p-1) : p \mid n]) \\ &= \mathrm{ord}_2(\lambda(k(n))) = \Theta_2(n) = \beta = \alpha - 2,\end{aligned}$$

it follows that $\lambda(n) = \lambda(n/2^\alpha)$, which is impossible since $n \in \mathcal{C}_\lambda$. Thus, $\alpha \neq \beta + 2$, and it follows that $\alpha \geq \beta + 3$.

To complete the proof in this case, we now show that if $\alpha \geq \beta + 4$, then $n/2 \in \mathcal{C}_\lambda$, contradicting the fact that n is primitive.

Indeed, suppose that $\alpha \geq \beta + 4$ and that $\lambda(n/2) = \lambda(\widetilde{n})$ for some positive integer $\widetilde{n}$. For any prime p dividing $\widetilde{n}$, we have $p - 1 \mid \lambda(\widetilde{n}) = \lambda(n/2) \mid \lambda(n)$; thus, $p^2 \mid n$ by Corollary 19. This shows that the prime factors of $\widetilde{n}$ are among those of n. Put $\gamma = \mathrm{ord}_2(\widetilde{n})$. As before, we have $\mathrm{ord}_2(\lambda(n/2^\alpha)) = \beta$; thus,

$$\lambda(n) = [2^{\alpha-2}, \lambda(n/2^\alpha)] = 2[2^{\alpha-3}, \lambda(n/2^\alpha)] = 2\lambda(n/2) = 2\lambda(\widetilde{n})$$

since $\alpha - 3 > \beta$. As $\mathrm{ord}_2(\lambda(n)) = \alpha - 2$, it follows that

$$2^{\alpha-3} \parallel \lambda(\widetilde{n}) = [\lambda(p^\delta) : p^\delta \parallel \widetilde{n}].$$

It cannot be the case that $2^{\alpha-3} \mid \lambda(p^\delta)$ for an odd prime power $p^\delta > 1$ dividing $\widetilde{n}$, for this would imply that $2^{\alpha-3} \mid p - 1$, and since $p \mid n$, it would then follow that $\beta = \Theta_2(n) \geq \alpha - 3$. Therefore, $2^{\alpha-3} \parallel \lambda(2^\gamma)$, which implies that $\gamma = \alpha - 1$ (note that $\alpha \geq 5$ since $\beta \geq 1$ by Lemma 20). Since the prime factors of $\widetilde{n}$ are among those of n, $\Theta_2(\widetilde{n}) \leq \Theta_2(n)$; therefore,

$$\Theta_2(\widetilde{n}/2^\gamma) = \Theta_2(\widetilde{n}) \leq \Theta_2(n) = \beta < \alpha - 3 = \gamma - 2,$$

which implies that $\mathrm{ord}_2(\lambda(\widetilde{n}/2^\gamma)) < \gamma - 2$. Consequently,

$$\lambda(n) = 2\lambda(\widetilde{n}) = 2[2^{\gamma-2}, \lambda(\widetilde{n}/2^\gamma)] = [2^{\gamma-1}, \lambda(\widetilde{n}/2^\gamma)] = \lambda(2\widetilde{n}).$$

Since $n \in \mathcal{C}_\lambda$, we deduce that $\widetilde{n} = n/2$, and therefore $n/2 \in \mathcal{C}_\lambda$. This completes the proof in this case.

Next, let q be an odd prime dividing n. Put $\alpha = \mathrm{ord}_q(n)$ and $\beta = \Theta_q(n)$. Then $\alpha \geq 2$ by Lemma 18, and $\mathrm{ord}_q(\lambda(n)) = \alpha - 1$ by Lemma 17. We also have $q^\beta \mid \lambda(k(n)) \mid \lambda(n)$; therefore, $\alpha \geq \beta + 1$.

Suppose that $\alpha = \beta + 1$. Since $\lambda(n) = [q^{\alpha-1}(q-1), \lambda(n/q^\alpha)]$, and

$$\begin{aligned}\mathrm{ord}_q(\lambda(n/q^\alpha)) &= \mathrm{ord}_q([\lambda(p^\gamma) : p^\gamma \parallel n/q^\alpha]) = \mathrm{ord}_q([(p-1) : p \mid n]) \\ &= \mathrm{ord}_q(\lambda(k(n))) = \Theta_q(n) = \beta = \alpha - 1,\end{aligned}$$

it follows that $\lambda(n) = \lambda(n/q^{\alpha-1})$, which is impossible since $n \in \mathcal{C}_\lambda$. Thus, $\alpha \neq \beta + 1$, and it follows that $\alpha \geq \beta + 2$.

As before, to complete the proof it suffices to show that $\alpha \geq \beta + 3$ implies $n/q \in \mathcal{C}_\lambda$. Thus, suppose that $\alpha \geq \beta + 3$ and that $\lambda(n/q) = \lambda(\widetilde{n})$ for some positive integer $\widetilde{n}$. Again, it is easy to see that the prime factors of $\widetilde{n}$ are among those of n. Put $\gamma = \mathrm{ord}_q(\widetilde{n})$. Since $\mathrm{ord}_q(\lambda(n/q^\alpha)) = \beta$, we have

$$\lambda(n) = [q^{\alpha-1}(q-1), \lambda(n/q^\alpha)] = q[q^{\alpha-2}(q-1), \lambda(n/q^\alpha)] = q\lambda(n/q) = q\lambda(\widetilde{n})$$

since $\alpha - 2 > \beta$. As $\operatorname{ord}_q(\lambda(n)) = \alpha - 1$, it follows that

$$q^{\alpha-2} \parallel \lambda(\widetilde{n}) = [\lambda(p^\delta) : p^\delta \parallel \widetilde{n}].$$

Arguing as before, it cannot be the case that $q^{\alpha-2} \mid \lambda(p^\delta)$ for a prime power $p^\delta > 1$ dividing $\widetilde{n}$; therefore, $q^{\alpha-2} \parallel \lambda(q^\gamma)$, which implies that $\gamma = \alpha - 1$. Since the prime factors of $\widetilde{n}$ are among those of n, $\Theta_q(\widetilde{n}) \le \Theta_q(n)$; therefore,

$$\Theta_q(\widetilde{n}/q^\gamma) = \Theta_q(\widetilde{n}) \le \Theta_q(n) = \beta < \alpha - 2 = \gamma - 1,$$

which implies that $\operatorname{ord}_q(\lambda(\widetilde{n}/q^\gamma)) < \gamma - 1$. Consequently,

$$\lambda(n) = q\lambda(\widetilde{n}) = q[q^{\gamma-1}(q-1), \lambda(\widetilde{n}/q^\gamma)] = [q^\gamma(q-1), \lambda(\widetilde{n}/q^\gamma)] = \lambda(q\widetilde{n}).$$

Since $n \in \mathcal{C}_\lambda$, we deduce that $\widetilde{n} = n/q$, and therefore $n/q \in \mathcal{C}_\lambda$, which completes the proof. ∎

Corollary 22. *If $n \in \mathcal{C}_\lambda^*$, and $p = P(n)$ is the largest prime factor of n, then $\operatorname{ord}_p(n) = 2$.*

Proof. Indeed, p cannot divide $\lambda(k(n))$. Hence $\Theta_p(n) = 0$, and the result follows from Lemma 21. ∎

Lemma 23. *Let $n \ge 2$ be an integer with the properties:*

- *$\lambda(n/p) = \lambda(n)/p$ for every prime p dividing n;*
- *for any prime power $q^\alpha > 1$, $\lambda(q^\alpha) \mid \lambda(n)$ implies $q^\alpha \mid n$.*

Then $n \in \mathcal{C}_\lambda$.

Proof. Let n be fixed, and suppose that $\lambda(\widetilde{n}) = \lambda(n)$. For any prime power $q^\alpha > 1$ dividing $\widetilde{n}$, we have $\lambda(q^\alpha) \mid \lambda(\widetilde{n}) = \lambda(n)$; therefore, $q^\alpha \mid n$. This shows that $\widetilde{n} \mid n$. If $\widetilde{n} \ne n$, write $n = \widetilde{n}dp$, where p is a prime dividing $n/\widetilde{n}$ and $d = n/(\widetilde{n}p)$. Then

$$\lambda(n) = \lambda(\widetilde{n}) \mid \lambda(\widetilde{n}d) = \lambda(n/p) = \lambda(n)/p,$$

which is impossible. Thus, $\widetilde{n} = n$. ∎

We are now ready to prove Theorem 6. Let n_1 and n_2 be two (not necessarily distinct) elements of $\mathcal{C}_\lambda^*$, and put $n = (n_1, n_2)$. Note that $2^4 \mid n$ by Lemma 17; in particular, $n \ge 16$.

For any prime p dividing n, by Lemma 21 we have

$$\begin{aligned}\operatorname{ord}_p(n) &= \min\{\operatorname{ord}_p(n_1), \operatorname{ord}_p(n_2)\} \\ &= \begin{cases} \min\{\Theta_2(n_1), \Theta_2(n_2)\} + 3 & \text{if } p = 2, \\ \min\{\Theta_p(n_1), \Theta_p(n_2)\} + 2 & \text{if } p \ne 2. \end{cases}\end{aligned}$$

Since n is a divisor of n_1 and n_2, for every prime p dividing n we have

$$\Theta_p(n) \le \min\{\Theta_p(n_1), \Theta_p(n_2)\};$$

therefore,

$$\operatorname{ord}_p(n) \ge \begin{cases} \Theta_2(n)+3 & \text{if } p=2,\\ \Theta_p(n)+2 & \text{if } p\ne 2.\end{cases}$$

Moreover,

$$\Theta_p(n) = \operatorname{ord}_p(\lambda(n/p^{\operatorname{ord}_p(n)}))$$

as in the proof of Lemma 21. Consequently, if $\alpha = \operatorname{ord}_2(n)$, then

$$\lambda(n/2) = [2^{\alpha-3}, \lambda(n/2^\alpha)] = 2^{-1}[2^{\alpha-2}, \lambda(n/2^\alpha)] = \lambda(n)/2,$$

and for any odd prime p dividing n, with $\alpha = \operatorname{ord}_p(n)$, we have

$$\lambda(n/p) = [p^{\alpha-2}(p-1), \lambda(n/p^\alpha)] = p^{-1}[p^{\alpha-1}(p-1), \lambda(n/p^\alpha)] = \lambda(n)/p.$$

This shows that n has the first property stated in Lemma 23.

For any prime power $q^\alpha > 1$ such that $\lambda(q^\alpha) \mid \lambda(n)$, it is clear that $\lambda(q^\alpha) \mid \lambda(n_1)$ and $\lambda(q^\alpha) \mid \lambda(n_2)$. Therefore, using Lemma 15, we have

$$\alpha \le \min\{\vartheta_q(n_1), \vartheta_q(n_2)\} = \min\{\operatorname{ord}_q(n_1), \operatorname{ord}_q(n_2)\} = \operatorname{ord}_q(n).$$

This shows that n has the second property stated in Lemma 23.

By Lemma 23, we conclude that $n \in \mathcal{C}_\lambda$. Since n_1 and n_2 are primitive, this shows that $n_1 = n = n_2$ and completes the proof of the theorem.

8. Numerical results and remarks. Our proofs are constructive and yield specific examples of elements in each of the sets $\mathcal{F}\cap\mathcal{L}$, $\mathcal{F}\setminus\mathcal{L}$ and $\mathcal{L}\setminus\mathcal{F}$. Numerical computations performed with Pari 2.2.7 provide the following data:

x	$\#\mathcal{F}(x)$	$\#\mathcal{L}(x)$	$\#(\mathcal{F}(x)\cap\mathcal{L}(x))$	$\#\mathcal{L}_\mathcal{F}(x)$	$\#\mathcal{F}_\mathcal{L}(x)$
10	6	6	6	0	0
10^2	38	39	38	1	0
10^3	291	328	291	37	0
10^4	2374	2933	2369	564	5
10^5	20254	27155	20220	6935	34
10^6	180184	256158	179871	76287	313
10^7	1634372	2445343	1631666	813677	2706

Here, we apply the elementary criterion that an even integer m lies in $\mathcal{L}$ if and only if $m = \lambda(s)$, where s is the integer defined by

$$s = 2 \prod_{\substack{p\,\text{prime}\\ p-1\mid m}} p^{\operatorname{ord}_p(m)+1}.$$

We also use the fact that if $n \le 10^9$, then $\omega(n) \le 9$, where $\omega(n)$ is the number of distinct prime divisors of n, and

$$\varphi(n) = n \prod_{p \mid n} (1 - p^{-1}) \ge n \prod_{p \le 23} (1 - p^{-1}).$$

Thus, $m \in \mathcal{F}(10^9)$ if and only if $m = \varphi(r)$ for some $r \le 6.113m$. We remark that it has been recently shown in [8] that the problem of deciding whether a given integer m lies in $\mathcal{F}$ is NP-complete.

The thirty smallest integers in $\mathcal{L} \setminus \mathcal{F}$ are the following:

- 90, 174, 230, 234, 246, 290, 308, 318, 364, 390, 410, 414, 450, 510, 516, 530, 534, 572, 594, 638, 644, 666, 678, 680, 702, 714, 728, 740, 770, 804.

For instance, taking $p = 11$ and $q = 19$ in the proof of Theorem 2, we see that $\lambda(11 \cdot 19) = \lambda(209) = 90$ does not lie in the set $\mathcal{F}$. On the other hand, not all elements of $\mathcal{L} \setminus \mathcal{F}$ are captured by the methods of Theorem 2, the smallest example being $\lambda(23 \cdot 29) = \lambda(667) = 308$; this suggests that the lower bound of that theorem is probably not tight.

The twenty smallest integers in $\mathcal{F} \setminus \mathcal{L}$ are the following:

- 1936, 3872, 6348, 7744, 9196, 15004, 15488, 18392, 20812, 21160, 22264, 30008, 35332, 36784, 38416, 41624, 42320, 44528, 51304, 58564.

For example, taking $q = 11$ and $p = 89$ in our proof of Theorem 3, we see that

$$\varphi((2 \cdot 11 + 1) \cdot 89) = \varphi(2047) = 1936$$

cannot lie in the set $\mathcal{L}$.

As mentioned earlier, it can be quite difficult in practice to determine numerically whether a given integer lies in $\mathcal{F} \setminus \mathcal{L}$, in $\mathcal{L} \setminus \mathcal{F}$, or in $\mathcal{F} \cap \mathcal{L}$, since for certain integers $m \in \mathcal{L}$, the preimages $n \in \lambda^{-1}(m)$ are all quite large relative to m. For example, if

$$m = 2^{171} \cdot 1021 \cdot 5419 \cdot 5483,$$

the only odd primes q for which $q - 1 \mid m$ are the Fermat primes $3, 5, 17, 257$, 65537, and the following three primes:

$$2^{112} \cdot 1021 + 1, \qquad 2^{137} \cdot 5483 + 1, \qquad 2^{170} \cdot 5419 + 1.$$

Hence, if $\lambda(n) = m$, it follows that

$$n \ge 2^{173}(2^{112} \cdot 1021 + 1)(2^{137} \cdot 5483 + 1)(2^{170} \cdot 5419 + 1) > m^{3.045}.$$

In light of this example (and many others), one is naturally led to consider the function

$$\pounds(m) = \min\{n : \lambda(n) = m\}, \qquad m \in \mathcal{L},$$

which has not been previously studied in the literature. It would be interesting to know more about the arithmetic properties of $\mathcal{L}(m)$; in particular, the determination of the maximal order of $\mathcal{L}(m)$ seems particularly challenging.

It is certainly expected that one can take any $\beta > 0$ in the proof of Theorem 4, which would imply

$$\ell(n) \geq \exp((\log_2 x)^A)$$

for any $A > 0$ and x sufficiently large relative to A, and

$$\#\mathcal{C}_\lambda(x) \leq x \exp(-(\log_2 x)^{1+o(1)}).$$

We remark that the proof of Theorem 5 can be modified slightly to establish the perhaps more natural bound

$$\#\mathcal{B}_\varphi^*(x) \leq x^{2/3+o(1)},$$

where $\mathcal{B}_\varphi^*$ is the set of integers $m \in \mathcal{B}_\varphi$ such that $d \notin \mathcal{B}_\varphi$ for every proper divisor d of m. In particular, even if $\mathcal{B}_\varphi \neq \emptyset$, it is true that

$$\lim_{x\to\infty} \frac{\#\mathcal{B}_\varphi^*(x)}{\#\mathcal{B}_\varphi(x)} = 0.$$

In particular, almost all counterexamples to the Carmichael conjecture have many proper divisors which are also counterexamples.

Let n_0 be an arbitrary element of $\mathcal{C}_\lambda$, assuming that $\mathcal{C}_\lambda \neq \emptyset$. As $\lambda(1) = \lambda(2)$ and $\lambda(4) = \lambda(8)$, it follows that $2^4 \mid n_0$. Then $3^2 \mid n_0$, since $\lambda(n_0) = \lambda(3n_0)$ if $3 \nmid n_0$, and $\lambda(n_0/3) = \lambda(n_0)$ if $3 \parallel n_0$. By similar arguments, one shows that n_0 is a multiple of $2^4 3^2 5^2 7^2 11^2 13^2$. Putting aside 17 for the moment, we can argue that $19 \mid n_0$ as follows. If $3^2 \parallel n_0$, then

$$\lambda(n_0) = [\lambda(n_0/3^2), \lambda(3^2)] = \lambda(n_0/3^2)$$

since $\lambda(3^2) \mid \lambda(7^2)$; this contradiction shows that $3^3 \mid n_0$ and now it is an easy matter to conclude that $19^2 \mid n_0$, which then further implies that $3^4 \mid n_0$. To show that $17^2 \mid n_0$, we first use the fact that $13^2 \mid n_0$ to conclude that $2^5 \mid n_0$, "bumping up" the power of 2 as we did above for the prime 3. Then $41^2 \mid n_0$ follows, and we can conclude that $2^6 \mid n_0$, and finally $17^2 \mid n_0$. Continuing in this manner, we verified by computer that n_0 is divisible by the square of *every* prime number $p \leq 30000$. It would be interesting to see more extensive numerical results in this direction. Certainly, it should be possible to numerically establish lower bounds of the strength $m_0 \geq 10^{10000000000}$ for the elements m_0 of $\mathcal{B}_\lambda$, as has been done for the set $\mathcal{B}_\varphi$ in the paper [15] of Ford.

References

[1] R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. 83 (1998), 331–361.

[2] W. D. Banks, K. Ford, F. Luca, F. Pappalardi and I. E. Shparlinski, *Values of the Euler function in various sequences*, Monatsh. Math. 146 (2005), 1–19.

[3] W. D. Banks, J. B. Friedlander, C. Pomerance and I. E. Shparlinski, *Multiplicative structure of values of the Euler function*, in: High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Inst. Commun. 41, Amer. Math. Soc., Providence, RI, 2004, 29–47.

[4] W. D. Banks and F. Luca, *Roughly squarefree values of the Euler and Carmichael functions*, Acta Arith. 120 (2005), 211–230.

[5] W. D. Banks, F. Luca, F. Saidak and I. E. Shparlinski, *Values of arithmetical functions equal to a sum of two squares*, Q. J. Math. 56 (2005), 123–139.

[6] W. D. Banks, F. Luca and I. E. Shparlinski, *Arithmetic properties of $\varphi(n)/\lambda(n)$ and the structure of the multiplicative group modulo n*, Comment. Math. Helv. 81 (2006), 1–22.

[7] 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.

[8] S. Contini, E. Croot and I. E. Shparlinski, *Complexity of inverting the Euler function*, Math. Comp. 75 (2006), 983–996.

[9] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, New York, 1980.

[10] J. M. De Koninck, F. Luca and A. Sankaranarayanan, *Positive integers n whose Euler function is a power of the kernel function*, Rocky Mountain J. Math., to appear.

[11] T. Dence and C. Pomerance, *Euler's function in residue classes*, Ramanujan J. 2 (1998), 7–20.

[12] P. Erdős, A. Granville, C. Pomerance and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, in: Analytic Number Theory, Progr. Math. 85, Birkhäuser, Boston, 1990, 165–204.

[13] P. Erdős and C. Pomerance, *On the normal number of prime factors of $\varphi(n)$*, Rocky Mountain J. Math. 15 (1985), 343–352.

[14] P. Erdős, C. Pomerance and E. Schmutz, *Carmichael's lambda function*, Acta Arith. 58 (1991), 363–385.

[15] K. Ford, *The distribution of totients*, Ramanujan J. 2 (1998), 67–151.

[16] —, *The number of solutions of $\varphi(x) = m$*, Ann. of Math. 150 (1999), 283–311.

[17] K. Ford, S. Konyagin and C. Pomerance, *Residue classes free of values of Euler's function*, in: Number Theory in Progress, de Gruyter, Berlin, 1999, 805–812.

[18] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, *Period of the power generator and small values of Carmichael's function*, Math. Comp. 70 (2001), 1591–1605.

[19] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[20] F. Luca and C. Pomerance, *On some problems of Mąkowski–Schinzel and Erdős concerning the arithmetical functions φ and σ*, Colloq. Math. 92 (2002), 111–130.

[21] H. Maier and C. Pomerance, *On the number of distinct values of Euler's ϕ-function*, Acta Arith. 49 (1988), 263–275.

[22] C. Pomerance, *Popular values of Euler's function*, Mathematika 27 (1980), 84–89.

[23] —, *Two methods in elementary analytic number theory*, in: Number Theory and Applications, R. A. Mollin (ed.), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. 265, Kluwer, Dordrecht, 1989, 135–161.

[24] P. J. Stephens, *An average result for Artin's conjecture*, Mathematika 16 (1969), 178–188.

[25] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Univ. Press, Cambridge, 1995.

Department of Mathematics
University of Missouri
Columbia, MO 65211, U.S.A.
E-mail: bbanks@math.missouri.edu

Department of Mathematics
University of Toronto
Toronto, Ontario M5S 3G3, Canada
E-mail: frdlndr@math.toronto.edu

Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
E-mail: fluca@matmor.unam.mx

Dipartimento di Matematica
Università Roma Tre
Largo S. L. Murialdo, 1
Roma, 00146, Italy
E-mail: pappa@mat.uniroma3.it

Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
E-mail: igor@ics.mq.edu.au

Received on 16.9.2004
and in revised form on 14.1.2006 (4851)