On composite integers n for which $\varphi(n) \mid n-1$

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

May 31, 2009

Abstract

Let φ denote Euler's function. Clearly $\varphi(n) \mid n-1$ if $n=1$ or if n is a prime. In 1932, Lehmer asked if any composite numbers n have this property. Improving on some earlier results, we show that the number of composite integers $n \le x$ with $\varphi(n) \mid n-1$ is at most $x^{1/2}/(\log x)^{1/2+o(1)}$ as $x \to \infty$. Key to the proof are some uniform estimates of the distribution of integers n where the largest divisor of $\varphi(n)$ supported on primes from a fixed set is abnormally small. [1]

1 Introduction

Let $\varphi(n)$ be the Euler function of n. Lehmer [6] asked if there exist composite positive integers n such that $\varphi(n) \mid n-1$. In 1977, the second author [8] proved that if one sets

$$\mathcal{L}(x) = \{n \le x : \varphi(n) \mid n-1 \text{ and } n \text{ is composite}\},$$

then

$$\#\mathcal{L}(x) \ll x^{1/2}(\log x)^{3/4}.$$

[1]MSC numbers 11A25, 11N25

This was followed by subsequent improvements in the exponent of the logarithm, by first replacing the above bound by $x^{1/2}(\log x)^{1/2}(\log\log x)^{-1/2}$ in [9], next by $x^{1/2}(\log\log x)^{1/2}$ in [2], and recently by $x^{1/2}(\log x)^{-\Theta+o(1)}$ as $x \to \infty$ in [1], where $\Theta = 0.129398\ldots$ is the least positive solution of the transcendental equation

$$2\Theta(\log\Theta - 1 - \log\log 2) = -\log 2.$$

Here, we continue this trend and present the following result.

Theorem 1. *As $x \to \infty$, we have*

$$\#\mathcal{L}(x) \le \frac{x^{1/2}}{(\log x)^{1/2+o(1)}}. \tag{1}$$

The function $o(1)$ appearing in the above exponent is of order of magnitude $O((\log\log\log\log x)^{1/2}/(\log\log\log x)^{1/3})$. As in the previous works on the subject, the above bound is also an upper bound for the cardinality of the set

$$\mathcal{L}_a(x) = \{n \le x : \varphi(n) \mid n - a \text{ and } n \ne ap \text{ where } p \nmid a \text{ is a prime}\},$$

where $a \ne 0$ is any fixed integer. In that case, the function $o(1)$ in (1) depends on a.

We point out that in spite of all these improvements, there is still no known composite number n with $\varphi(n) \mid n-1$. It is reasonable to conjecture that $\#\mathcal{L}(x) \le x^{o(1)}$ as $x \to \infty$, but we seem to be a long way from improving the exponent $1/2$ on x in the upper bound to anything smaller.

While the proof follows the general approach from [1], we add a detailed study of the distribution of those integers n where the contribution to $\varphi(n)$ from primes in a given set $\mathcal{Q}$ is below normal. Such results (see Proposition 1 in the case when $\mathcal{Q}$ is a small set and Proposition 2 in the case when $\mathcal{Q}$ is large) can be viewed as a generalization of the Hardy–Ramanujan estimates for the distribution of integers with fewer than the normal number of prime factors, which integers usually have the 2-part of $\varphi(n)$ smaller than normal. Hopefully these propositions will have some independent interest.

We use the symbols O, o and $\ll$, $\gg$ with their usual meaning. We also use p and q for prime numbers. For a positive integer n, we use $\omega(n)$ for the number of primes that divide n. For a prime q and a positive integer n we write $v_q(n)$ for the exponent of q in the factorization of n; that is, $q^{v_q(n)} \| n$.

2 Some auxiliary results

It follows from the Hardy–Ramanujan inequality that

$$\begin{aligned}\#\{n \le t : \omega(n) \ge \lambda \log\log t\} &\ll \frac{e^{\lambda} t}{(\log t)^{1+\lambda \log(\lambda/e)}},\\ \#\{n \le t : \omega(n) \le \lambda \log\log t\} &\ll \frac{t}{(\log t)^{1+\lambda \log(\lambda/e)}}\end{aligned} \tag{2}$$

hold uniformly for all $\lambda \ge 1$, and $0 < \lambda \le 1$, respectively. (For λ fixed, a somewhat stronger estimate is known, see Erdős and Nicolas [5, Prop. 3].) These estimates played key roles in the proof in [1].

Since all prime divisors of a positive integer n with at most one possible exception are odd, the bound (2) gives us that the inequality

$$\#\{n \le t : v_2(\varphi(n)) \le \lambda \log\log t\} \ll \frac{t}{(\log t)^{1+\lambda \log(\lambda/e)}} \tag{3}$$

holds for all t uniformly in $\lambda \in (0, 1]$. While the above inequality is correct, it does not capture the full contribution to $v_2(\varphi(n))$ arising from primes p with $p - 1$ a multiple of 4, 8, or a larger power of 2.

In this section, we prove a stronger and more general inequality than (3). Let $\mathcal{Q} \subset [1, M]$ be a set of primes. Put

$$F_{\mathcal{Q}}(n) := \prod_{q \in \mathcal{Q}} q^{v_q(\varphi(n))}$$

for the $\mathcal{Q}$-*part* of $\varphi(n)$. In analogy with (2) and (3), for $\lambda > 0$ put

$$\mathcal{B}_{\mathcal{Q},\lambda}(t) := \{n \le t : F_{\mathcal{Q}}(n) \le (\log t)^{\lambda}\}.$$

Our first result addresses the cardinality of $\mathcal{B}_{\mathcal{Q},\lambda}(t)$. Letting

$$c_{\mathcal{Q}}(s) := \prod_{q \in \mathcal{Q}} \left(\frac{q-2}{q-1} + \frac{1}{q^{s+1}-1}\right),$$

we have the following inequality.

Proposition 1. *For $\mathcal{Q} \subset [1, M]$ a set of primes, the estimate*

$$\#\mathcal{B}_{\mathcal{Q},\lambda}(t) \le \frac{t}{(\log t)^{1-\lambda s - c_{\mathcal{Q}}(s)}} \exp\left(O((\log M)^3)\right) \tag{4}$$

holds uniformly in $\mathcal{Q}$, $M \ge 2$, $\lambda > 0$, $s \ge 0$, and $t \ge 2$.

Note that we are free to choose the number $s \geq 0$ above. Obviously, when $\mathcal{Q}$ and λ are given we would like to choose s in such a way that $\lambda s + c_{\mathcal{Q}}(s)$ is minimal. Before proving Proposition 1, let us give an application.

Take $\mathcal{Q} = \{2\}$. We have $F_{\{2\}}(n) = 2^{v_2(\varphi(n))}$ and $c_{\{2\}}(s) = 1/(2^{s+1} - 1)$. To find the minimum of $\lambda s + c_{\{2\}}(s)$ as a function of s, we take its derivative with respect to s and set it to equal zero getting

$$\lambda = \frac{2^{s+1} \log 2}{(2^{s+1} - 1)^2}.$$

Putting $x = 2^{s+1}$, we get the quadratic equation

$$(x-1)^2 = \frac{\log 2}{\lambda} x,$$

whose solutions are

$$x_\lambda = 1 + \frac{\log 2}{2\lambda} \pm \sqrt{\frac{\log 2}{\lambda} + \frac{(\log 2)^2}{4\lambda^2}}.$$

The one with the negative sign leads to a solution $x_\lambda < 1$, which is impossible because $x = 2^{s+1} \geq 2$. Thus, we must pick the solution x_λ with the positive sign whose corresponding s equals

$$s = \frac{1}{\log 2} \log \left(1 + \frac{\log 2}{2\lambda} + \sqrt{\frac{\log 2}{\lambda} + \frac{(\log 2)^2}{4\lambda^2}} \right) - 1.$$

This number is non-negative only when $\lambda \in (0, 2\log 2]$. The above calculation applied to $\lambda \log 2$ implies the following improvement of (3).

Corollary 1. *Given any $\lambda \in (0, 2]$, we have the estimate*

$$\begin{aligned} \#\{n \leq t : v_2(\varphi(n)) \leq \lambda \log\log t\} &= \#\mathcal{B}_{\{2\},\lambda \log 2}(t) \\ &\ll \frac{t}{(\log t)^{1 + \lambda \log 2 - \lambda \log\left(1 + \frac{1+\sqrt{4\lambda+1}}{2\lambda}\right) - \frac{2\lambda}{1+\sqrt{4\lambda+1}}}}. \end{aligned} \tag{5}$$

When $\mathcal{Q}$ contains more than one element, finding the optimal value of s amounts to solving a polynomial-like equation but with transcendental exponents. In this case one may solve for s via numerical methods.

Taking say $\lambda = 1/2$ in (3), we get the value $0.1534264097\cdots$ for the exponent of the logarithm, while taking $\lambda = 1/2$ in (5), we get the value $0.3220692380\cdots$ for the exponent of the logarithm.

If one goes through the arguments from [1] and replaces inequality (3) by the inequality (5), then one gets that with λ the solution of the equation

$$1+\lambda\log 2-\lambda\log\left(1+\frac{1+\sqrt{4\lambda+1}}{2\lambda}\right)-\frac{2\lambda}{1+\sqrt{4\lambda+1}}=\lambda\log 2,$$

the inequality $\#\mathcal{L}(x)\le x/(\log x)^{\Theta+o(1)}$ holds as $x\to\infty$, where $\Theta=\lambda(\log 2)/2$. Calculation reveals that $\lambda=0.4815450284\cdots$, so that $\Theta=0.1668907893\cdots$, which is already better than the main result from [1]. The improvement to $\Theta=1/2$ in our Theorem 1 arises by allowing more primes into the set $\mathcal{Q}$.

Now that we have hopefully convinced the reader of the usefulness of Proposition 1, let's get to its proof.

Proof. We need the following theorem which appears in [10, III, sec. 3.5].

Lemma 1. *Let f be a multiplicative function such that $f(n)\ge 0$ for all n, and such that there exist numbers A and B such that for all $x>1$ both inequalities*

$$\sum_{p\le x} f(p)\log p\le Ax \tag{6}$$

and

$$\sum_{p}\sum_{\alpha\ge 2}\frac{f(p^\alpha)}{p^\alpha}\log(p^\alpha)\le B \tag{7}$$

hold. Then, for $x>1$, we have

$$\sum_{n\le x} f(n)\le (A+B+1)\frac{x}{\log x}\sum_{n\le x}\frac{f(n)}{n}.$$

We apply Lemma 1 to the multiplicative function $F_{\mathcal{Q}}(n)^{-s}$ whose range is in the set $(0,1]$. Clearly, the estimates (6) and (7) hold with some absolute constants A and B independent of $\mathcal{Q}$ or s. Since $F_{\mathcal{Q}}(n)^{-s}\le 1$,

$$\begin{aligned}\sum_{n\le t}\frac{1}{F_{\mathcal{Q}}(n)^s} &\ll \frac{t}{\log t}\prod_{p\le t}\left(1+\frac{1}{F_{\mathcal{Q}}(p)^s p}+\frac{1}{F_{\mathcal{Q}}(p^2)^s p^2}+\cdots\right)\\ &\le \frac{t}{\log t}\prod_{p\le t}\left(1+\frac{1}{F_{\mathcal{Q}}(p)^s p}+O\left(\frac{1}{p^2}\right)\right)\\ &\ll \frac{t}{\log t}\exp\left(\sum_{p\le t}\frac{1}{F_{\mathcal{Q}}(p)^s p}\right).\end{aligned}$$

We now compute the sum within the above exponential. Let $\mathcal{M}_{\mathcal{Q}}$ be the set of all positive integers m whose prime factors are contained in $\mathcal{Q}$. Then

$$\sum_{p\le t}\frac{1}{F_{\mathcal{Q}}(p)^s p}=\sum_{m\in\mathcal{M}_{\mathcal{Q}}}\frac{1}{m^s}\sum_{\substack{p\le t\\ F_{\mathcal{Q}}(p)=m}}\frac{1}{p}.$$

Given $m\in\mathcal{M}_{\mathcal{Q}}$, then p is a prime such that $F_{\mathcal{Q}}(p)=m$ precisely when $m\mid p-1$ and $(p-1)/m$ is coprime to $Q:=\prod_{q\in\mathcal{Q}}q$. We use the following estimate:

$$\sum_{\substack{p\le t\\ p\equiv 1 \pmod{\ell}}}\frac{1}{p}=\frac{\log\log t}{\varphi(\ell)}+O\left(\frac{\log \ell}{\ell}\right), \tag{8}$$

(see [7] for example). For each $m\in\mathcal{M}_{\mathcal{Q}}$, we have, by the Principle of Inclusion and Exclusion, that

$$\sum_{\substack{p\le t\\ F_{\mathcal{Q}}(p)=m}}\frac{1}{p}=\sum_{d\mid Q}\mu(d)\sum_{\substack{p\le t\\ p\equiv 1 \pmod{md}}}\frac{1}{p}.$$

Using estimate (8) we get that

$$\sum_{\substack{p\le t\\ F_{\mathcal{Q}}(p)=m}}\frac{1}{p}=(\log\log t)\sum_{d\mid Q}\frac{\mu(d)}{\varphi(md)}+O\left(\sum_{d\mid Q}\frac{\log(md)}{md}\right).$$

Certainly,

$$\sum_{d\mid Q}\frac{\log(dm)}{dm}\le\frac{1}{m}\sum_{d\mid Q}\frac{\log d}{d}+\frac{\log m}{m}\sum_{d\mid Q}\frac{1}{d}\ll\frac{(\log M)^2+(\log m)\log M}{m}.$$

We thus get that

$$\begin{aligned}\sum_{p\le t}\frac{1}{F_{\mathcal{Q}}(p)^s p}&=(\log\log t)\sum_{\substack{m\in\mathcal{M}_{\mathcal{Q}}\\ d\mid Q}}\frac{\mu(d)}{m^s\varphi(md)}\\&+\ O\left(\sum_{m\in\mathcal{M}_{\mathcal{Q}}}\frac{(\log M)^2+(\log m)\log M}{m}\right).\end{aligned}$$

Observe that the error term is $O((\log M)^3)$. Thus,

$$\sum_{p\le t}\frac{1}{F_{\mathcal{Q}}(p)^s p}=(\log\log t)\sum_{\substack{m\in\mathcal{M}_{\mathcal{Q}}\\ d\mid Q}}\frac{\mu(d)}{m^s\varphi(md)}+O((\log M)^3). \tag{9}$$

The double sum above is a multiplicative function of the parameter Q (where $\mathcal{Q}$ is the set of Q's prime factors). Its value when $Q = q$ is a prime is

$$1 - \frac{1}{q} + \sum_{\alpha \ge 1} \left(\frac{1}{q^{\alpha s}\varphi(q^\alpha)} - \frac{1}{q^{\alpha s}\varphi(q^{\alpha+1})} \right) = \frac{q-2}{q-1} + \frac{1}{q^{s+1}-1},$$

so that the main term in (9) above is our familiar $c_{\mathcal{Q}}(s)$ multiplied by $\log\log t$. We have shown that

$$\sum_{n \le t} \frac{1}{F_{\mathcal{Q}}(n)^s} \ll \frac{t}{\log t} \exp\left(c_{\mathcal{Q}}(s)\log\log t + O((\log M)^3)\right).$$

Since $s \ge 0$, we deduce immediately that

$$\begin{aligned} \#\mathcal{B}_{\mathcal{Q},\lambda}(t) &\le \frac{t}{\log t} \exp\left((\lambda s + c_{\mathcal{Q}}(s))\log\log t + O((\log M)^3)\right) \\ &= \frac{t}{(\log t)^{1-\lambda s - c_{\mathcal{Q}}(s)}} \exp\left(O((\log M)^3)\right), \end{aligned}$$

which is what we wanted to prove. □

For a specific set $\mathcal{Q}$ of primes that one has in mind, one can use Proposition 1 with a choice of s that minimizes the estimate for $\#\mathcal{B}_{\mathcal{Q},\lambda}(t)$ as we did above in the case $\mathcal{Q} = \{2\}$. It turns out that to prove Theorem 1, we will want to take choices for $\mathcal{Q}$ as large sets of primes and λ far below its "normal" value, in which case we will push up against a best-possible estimate $\#\mathcal{B}_{\mathcal{Q},\lambda}(t) \le t/(\log t)^{1+o(1)}$. In this case it is not necessary to choose the absolute optimal s, merely a "pretty good" value.

For $\mathcal{Q}$ a finite set of primes, let

$$T_{\mathcal{Q}} = \exp\left(\sum_{q \in \mathcal{Q}} \frac{1}{q}\right).$$

We now prove the following consequence of Proposition 1.

Proposition 2. *Suppose that $\mathcal{Q} \subset [1, M]$ is a set of primes with $0 < R \le 1$, where $R := \lambda(\log\log M)/T_{\mathcal{Q}}$. We have, uniformly for $t \ge 2$,*

$$\#\mathcal{B}_{\mathcal{Q},\lambda}(t) \le \frac{t}{(\log t)^{1+O(R^{1/2})}} \exp\left(O((\log M)^3)\right). \tag{10}$$

Proof. We shall apply Proposition 1 with s chosen as the number

$$s = R^{1/2}/\lambda.$$

Thus, the term $-\lambda s$ in the exponent on $\log t$ in (4) is absorbed into the O-estimate in (10). It remains to show that $c_{\mathcal{Q}}(s)$ is likewise majorized.

We have

$$c_{\mathcal{Q}}(s) \le \prod_{\substack{q\in\mathcal{Q}\\ q>2}} \left(\frac{q-2}{q-1}\right) \exp\left(\sum_{\substack{q\in\mathcal{Q}\\ q>2}} \frac{q-1}{(q-2)(q^{1+s}-1)}\right). \tag{11}$$

The product satisfies

$$\prod_{\substack{q\in\mathcal{Q}\\ q>2}} \left(\frac{q-2}{q-1}\right) = \exp\left(-\sum_{\substack{q\in\mathcal{Q}\\ q>2}} \frac{1}{q} + O(1)\right) \ll T_{\mathcal{Q}}^{-1}. \tag{12}$$

We have

$$\begin{aligned}\sum_{\substack{q\in\mathcal{Q}\\ 2<q\le\exp(R^{1/2}T_{\mathcal{Q}})}} \frac{q-1}{(q-2)(q^{1+s}-1)} &\le \sum_{\substack{q\in\mathcal{Q}\\ 2<q\le\exp(R^{1/2}T_{\mathcal{Q}})}} \frac{1}{q-2}\\ &\le \log(R^{1/2}T_{\mathcal{Q}}) + O(1).\end{aligned}$$

Also,

$$\begin{aligned}\sum_{\substack{q\in\mathcal{Q}\\ q>\exp(R^{1/2}T_{\mathcal{Q}})}} \frac{q-1}{(q-2)(q^{1+s}-1)} &\le \exp(-sR^{1/2}T_{\mathcal{Q}}) \sum_{\substack{q\in\mathcal{Q}\\ q>2}} \frac{q-1}{(q-2)(q-q^{-s})}\\ &\ll \exp(-sR^{1/2}T_{\mathcal{Q}}) \log\log M.\end{aligned}$$

Since $sR^{1/2}T_{\mathcal{Q}} = \log\log M$, we have from these calculations that

$$\sum_{\substack{q\in\mathcal{Q}\\ q>2}} \frac{q-1}{(q-2)(q^{1+s}-1)} \le \log(R^{1/2}T_{\mathcal{Q}}) + O(1),$$

so that with (11) and (12), we get

$$c_{\mathcal{Q}}(s) \ll T_{\mathcal{Q}}^{-1} \exp\Big(\log(R^{1/2}T_{\mathcal{Q}})\Big) = R^{1/2}.$$

Thus, we may also absorb $c_{\mathcal{Q}}(s)$ into the O-estimate in the exponent on $\log t$ in (10), completing the proof of the proposition. $\square$

Finally, we shall need an upper bound on the number of $n \le t$ whose Euler function is coprime to the primes $q \in \mathcal{Q}$ for $\mathcal{Q}$ a set of *odd* primes with $\mathcal{Q} \subset [1, M]$. For such a set of primes, put again $Q := \prod_{q\in\mathcal{Q}} q$, let

$$\mathcal{S}_{\mathcal{Q}}(t) = \{n \le t : \gcd(\varphi(n), Q) = 1\},$$

and let

$$g_{\mathcal{Q}} = \prod_{q\in\mathcal{Q}} \frac{q-2}{q-1}.$$

Lemma 2. *Let $t, M \ge 2$ and let $\mathcal{Q} \subset [1, M]$ be a set of odd primes. We have the uniform estimate*

$$\#\mathcal{S}_{\mathcal{Q}}(t) \le \frac{t}{(\log t)^{1-g_{\mathcal{Q}}}} \exp\left(O((\log M)^2)\right).$$

Proof. Writing $f(n)$ for the characteristic function of the numbers n having $\varphi(n)$ coprime to Q, Lemma 1 applied to $f(n)$ shows that

$$\begin{aligned}
\#\mathcal{S}_{\mathcal{Q}}(t) &\ll \frac{t}{\log t} \prod_{\substack{p\le t\\ (p(p-1),Q)=1}} \left(1+\frac{1}{p-1}\right) \prod_{\substack{p\le t\\ (p(p-1),Q)=p}} \left(1+\frac{1}{p}\right)\\
&\ll \frac{t}{\log t} \exp\left(\sum_{\substack{p\le t\\ (p-1,Q)=1}} \frac{1}{p}\right).
\end{aligned}$$

The Principle of Inclusion and Exclusion together with estimate (8) shows that

$$\begin{aligned}
\sum_{\substack{p\le t\\ (p-1,Q)=1}} \frac{1}{p} &= \sum_{d\mid Q} \mu(d) \sum_{\substack{p\le t\\ p\equiv 1 \pmod d}} \frac{1}{p}\\
&= (\log\log t) \sum_{d\mid Q} \frac{\mu(d)}{\varphi(d)} + O\left(\sum_{d\mid Q} \frac{\log d}{d}\right)\\
&= (\log\log t) \prod_{q\in\mathcal{Q}} \left(1-\frac{1}{q-1}\right) + O((\log M)^2)\\
&= g_{\mathcal{Q}} \log\log t + O((\log M)^2).
\end{aligned}$$

The desired conclusion about $\#\mathcal{S}_{\mathcal{Q}}(t)$ now follows. $\square$

3 The Proof of Theorem 1

Let x be large and let $\mathcal{D}(x) = \mathcal{L}(x) \cap (x/2, x]$. It suffices to show that inequality (1) holds with the left hand side replaced by $\#\mathcal{D}(x)$, since afterwards the resulting inequality will follow from the obvious fact that

$$\#\mathcal{L}(x) \le \sum_{0 \le k \le \lfloor (\log x)/(\log 2) \rfloor} \#\mathcal{D}(x/2^k).$$

If $n \in \mathcal{D}(x)$, we have that n is squarefree. Let $K = \omega(n)$ be the number of prime factors of n. In [1], it was shown that the inequality $K < 20 \log\log x$ holds with at most $O(x^{1/2}/\log x)$ exceptional numbers n, which is acceptable for us. So, we shall assume that $K < 20 \log\log x$.

A result of the second author from [8] shows that n has a divisor d such that $d \in [y/(2K), y]$, where we take $y := x^{1/2}/(\log x)^{1/2}$. We let $m = n/d$ be the corresponding cofactor. Clearly,

$$d \in \left[\frac{y}{2K},\, y\right], \quad m \in \left[\frac{y \log x}{2},\, 2Ky \log x\right].$$

In the remainder of the proof we take

$$M = \log\log x$$

and assume that x is large enough that $M \ge 3$. We let D be any odd divisor of $\prod_{q \le M} q$ and study the contribution to $\mathcal{D}(x)$ of those n having

$$D = \gcd(n, \prod_{q \le M} q).$$

Let $\mathcal{Q}_D$ be the set of prime factors of D and let $\bar{\mathcal{Q}}_D$ be the set of primes $q \le M$ not dividing D. Observe that $(n, \varphi(n)) = 1$, so that $(m, \varphi(m)) = 1$. In particular, $(\varphi(m), \prod_{q \in \mathcal{Q}_D} q) = 1$. We distinguish 3 possibly overlapping cases:

1. $\sum_{q \in \mathcal{Q}_D} 1/q \ge (1/3) \log\log M$;
2. $\sum_{q \in \bar{\mathcal{Q}}_D} 1/q \ge (2/3) \log\log M$ and $F_{\bar{\mathcal{Q}}_D}(m) \le (1/2) \log x$;
3. $F_{\bar{\mathcal{Q}}_D}(m) > (1/2) \log x$.

Since $\sum_{q \le M} 1/q > \log\log M$ for all sufficiently large values of x, these 3 cases cover all possibilities.

In case 1, we have $g_{\mathcal{Q}_D} \ll (\log M)^{-1/3}$, so that by Lemma 2 the number of possibilities for $m \le 2Ky\log x$ is

$$\le \frac{Ky(\log x)\exp\left(O((\log M)^2)\right)}{(\log x)^{1+O((\log M)^{-1/3})}} = y\exp\left(O(M/(\log M)^{1/3})\right).$$

Since $dm \equiv 1 \pmod{\varphi(d)\varphi(m)}$, it follows that $d \le x/m$ is uniquely determined modulo $\varphi(m)$, and since $m\varphi(m) > x$ for large values of x, we get that m determines n uniquely.

In case 2, we use Proposition 2 with $t = 2Ky\log x$ and $\lambda = 1$. Note that $T_{\bar{\mathcal{Q}}_D} \ge (\log M)^{2/3}$. We get that the number of possibilities for m, and hence for n, is at most

$$\frac{Ky(\log x)\exp\left(O((\log M)^3)\right)}{(\log x)^{1+O((\log\log M)^{1/2}/(\log M)^{1/3})}} = y\exp\left(O\left(\frac{M(\log\log M)^{1/2}}{(\log M)^{1/3}}\right)\right).$$

Assume next that $F_{\bar{\mathcal{Q}}_D}(m) > (1/2)\log x$. In particular, there exists a divisor ℓ of $\varphi(m)$ in the interval $[(\log x)/(2M), (\log x)/2]$ with each prime factor of ℓ in $[1, M]$. Let us fix this number ℓ. The number of choices for ℓ is at most $\psi(\log x, M)$, where $\psi(X, Y)$ denotes the number of integers in $[1, X]$ composed of primes in $[1, Y]$. Using a result of Erdős [4] (see also [3]) that $\psi(X, \log X) \le 4^{(1+o(1))(\log X)/\log\log X}$ as $X \to \infty$, we have

$$\psi(\log x, M) \le \exp(O(M/\log M)).$$

Let us fix also d. Then the congruence $dm \equiv 1 \pmod{\varphi(d)\varphi(m)}$ puts $m \le x/d$ in a congruence class modulo $\varphi(d)\ell$. Thus, the number of choices for m is at most $1 + x/(d\varphi(d)\ell)$. Summing over $d \in [y/(2K), y]$, we have for this ℓ that the number of possibilities for m, hence for n, is

$$\le \sum_{d\in[y/(2K),y]} \left(1 + \frac{x}{d\varphi(d)\ell}\right) \ll y + \frac{Kx}{y\ell} \le (2KM+1)y \ll M^2 y.$$

Multiplying by the number of choices for ℓ we get a contribution of at most $y\exp(O(M/\log M))$ choices for m, hence for n, in this case.

Thus, we have at most $y\exp\left(O\left(M(\log\log M)^{1/2}/(\log M)^{1/3}\right)\right)$ choices for $n \in \mathcal{D}(x)$ in each case. This bound is to be multiplied by the number of odd D with $D \mid Q$, which is $2^{\pi(M)-1} \ll \exp(M/\log M)$. We therefore have

$$\#\mathcal{D}(x) \le \frac{x^{1/2}}{(\log x)^{1/2+o(1)}},$$

where $o(1)$ here has the order $O((\log\log\log\log x)^{1/2}/(\log\log\log x)^{1/3})$. This concludes our proof.

Acknowledgments. This paper was written while the first author was visiting Dartmouth College; he thanks the Mathematics Department for its hospitality. The work of the first author was supported in part by projects PAPIIT 100508 and SEP-CONACyT 79685, and that of the second author by NSF grant DMS-0703850.

References

[1] W. D. Banks, A. M. Güloglu and C. W. Nevans, 'On the congruence $n \equiv a \pmod{\varphi(n)}$', *INTEGERS* **8** (2008), #A59.

[2] W. D. Banks and F. Luca, 'Composite integers n for which $\varphi(n) \mid n-1$', *Acta Math. Sinica* **23** (2007), 1915–1918.

[3] N. G. de Bruijn, 'On the number of positive integers $\leq x$ and free of prime factors $> y$. II', *Nederl. Akad. Wetensch. Proc. Ser. A* **69** = *Indag. Math.* **28** (1966) 239–247.

[4] P. Erdős, 'Problem and solution No. 1361', *Wisk. Opgaven* **21** (1963), 133–135.

[5] P. Erdős and J.-L. Nicolas, 'Sur la fonction: nombre de facteurs premiers de N', *L'Enseignement Math.* **27** (1981), 3–27.

[6] D. H. Lehmer, 'On Euler's totient function', *Bull. Amer. Math. Soc.* **38** (1932), 745–757.

[7] C. Pomerance, 'On the distribution of amicable numbers', *J. reine angew. Math.* **293/294** (1977), 217–222.

[8] C. Pomerance, 'On composite n for which $\varphi(n) \mid n-1$, II', *Pacific J. Math.* **69** (1977), 177–186.

[9] Z. Shan, 'On composite n for which $\varphi(n) \mid n-1$', *J. China Univ. Sci. Tech.* **15** (1985), 109–112.

[10] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 1995.