Repunit Lehmer numbers

Javier Cilleruelo
Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM)
and Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid
28049, Madrid, España
franciscojavier.cilleruelo@uam.es

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

Abstract

A Lehmer number is a composite positive integer n such that $\phi(n) \mid n-1$. In this paper, we show that given a positive integer $g > 1$ there are at most finitely many Lehmer numbers which are repunits in base g, and they are all effectively computable. Our method is effective and we illustrate it by showing that there is no such Lehmer number when $g \in [2, 1000]$.

2000 Mathematics Subject Classification: Primary 11N25, Secondary 11B39
Keywords: Lehmer numbers, repunits

1 Introduction

Let $\phi(n)$ be the Euler function of the positive integer n. Clearly, $\phi(n) = n-1$ if n is a prime. Lehmer [4] (see also B37 in [3]) conjectured that if $\phi(n) \mid n-1$, then n is prime. To this day, no counterexample to this conjecture has been found. A composite number m such that $\phi(m) \mid m-1$ is called a *Lehmer number*. Thus, Lehmer's conjecture is that Lehmer numbers don't exist but it is not even known that there should be at most finitely many of them.

Given a positive integer $g > 1$ a base g repunit is a number of the form $m = (g^n - 1)/(g - 1)$ for some integer $n \geq 1$. We will refer to such numbers simply as repunits without mentioning the dependence on g. It is not known whether given g there are infinitely many repunit primes. When $g = 2$ such primes are better known as Mersenne primes. In [5], it was shown that there is no Lehmer number in the Fibonacci sequence. Here, we use some ideas from [5] together with finer arguments to prove the following results. In what follows, we write $u_n = (g^n - 1)/(g - 1)$.

Theorem 1. *For each fixed $g > 1$, there are only finitely many positive integers n such that u_n is a Lehmer number, and all are effectively computable.*

Theorem 2. *There is no Lehmer number of the form u_n when $2 \leq g \leq 1000$.*

Acknowledgement. We thank the anonymous referee for numerous comments which improved the quality of this paper. Work on this paper was done during a pleasant visit of F. L. at the Mathematics Department of the Universidad Autónoma de Madrid in Spring of 2008. He thanks the people of that Institution for their hospitality. J. C. was supported in part by Project MTM2005-04730 from MEC (Spain) and the joint Madrid Region-UAM project TENU2 (CCG07-UAM/ESP-1814). F. L. was also supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508.

2 Preliminaries

For a prime q and a nonzero integer m we write $\nu_q(m)$ for the exponent of q in the factorization of m. We start by collecting some elementary and well-known properties of the sequence of general term $u_n = (g^n - 1)/(g - 1)$ for $n \geq 1$.

Lemma 1. *i) $u_n = g^{n-1} + \cdots + g + 1$. In particular, u_n is coprime to g.*

ii) The sequence u_n satisfies the linear recurrence

$$u_1 = 1, \quad u_n = gu_{n-1} + 1, \quad n \geq 2. \tag{1}$$

iii) If $d \mid n$, then $u_d \mid u_n$.

iv) Let q be a prime. If $q \mid n$, then $q \mid \phi(u_n)$.

v) Let q be a prime not dividing g. If $q \mid n$, then $\nu_q(u_{n-1}) \leq \nu_q(u_f) \leq \nu_q(u_{q-1})$, where f is the order of g modulo q.

vi) If u_n is a Lehmer number, then $(u_n, g - 1) = 1$.

Proof. *i)* and *ii)* are obvious. For *iii)*, we observe that

$$u_n = \frac{g^n - 1}{g - 1} = \frac{(g^d)^{n/d} - 1}{g^d - 1} \cdot \frac{g^d - 1}{g - 1} = \left((g^d)^{\frac{n}{d}-1} + \cdots + 1\right) u_d.$$

iv) If $q = 2$, then $u_n \geq u_2 = g + 1 > 2$, therefore $\phi(u_n)$ is even. Assume now that q is odd. Let p be a prime which divides u_q. Then, $g^q \equiv 1 \pmod{p}$, so the order of g modulo p is 1 or q. If it is q, then $q \mid p - 1 \mid \phi(u_q)$. Since by *iii)* we know that $u_q \mid u_n$, we get that $q \mid \phi(u_q) \mid \phi(u_n)$, which is what we wanted. Assume now that the order of g modulo p is 1 for all primes p dividing u_q. Let us show that this cannot happen. If it would, then $p \mid g - 1$ for all such primes p. Since also $p \mid u_q$, we have

$$0 \equiv u_q \equiv \frac{g^q - 1}{g - 1} = g^{q-1} + \cdots + g + 1 \equiv 1 + \cdots + 1 + 1 \equiv q,$$

where all congruences above are modulo p. Thus, $p \mid q$, therefore $p = q$. Hence, $u_q = q^\alpha$ for some positive integer α. However, writing $g - 1 = q\lambda$ with some positive integer λ, we get

$$\begin{aligned} u_q &= (1 + q\lambda)^{q-1} + (1 + q\lambda)^{q-2} + \cdots + (1 + q\lambda) + 1 \\ &\equiv (1 + (q-1)q\lambda) + (1 + (q-2)q\lambda) + \cdots + (1 + q\lambda) + 1 \pmod{q^2} \\ &\equiv q + q\lambda((q-1) + \cdots + 1) \pmod{q^2} \\ &\equiv q + \frac{q^2(q-1)\lambda}{2} \pmod{q^2} \\ &\equiv q \pmod{q^2}. \end{aligned}$$

In the above chain of congruences, we used the fact that q is odd, therefore $(q-1)/2$ is an integer. The above argument shows that $q \| u_q$; hence, $\alpha = 1$. So, $u_q = q$. However, we clearly have $u_q \geq 2^q - 1 > q$, which is a contradiction.

v) We may also assume that $q \mid u_{n-1}$, otherwise $\nu_q(u_{n-1}) = 0$ and the first inequality is clear. Now $g^{n-1} \equiv 1 \pmod{q}$, and so $f \mid n - 1$. We now write

$$u_{n-1} = \left((g^f)^{\frac{n-1}{f}-1} + \cdots + 1\right) u_f.$$

The quantity in brackets above is not divisible by q since it is congruent to $(n-1)/f$ modulo q and $q \mid n$. Thus, $\nu_q(u_{n-1}) \leq \nu_q(u_f) \leq \nu_q(u_{q-1})$, where the last inequality follows because $f \mid q - 1$, so, $u_f \mid u_{q-1}$ by *iii)*.

vi) Suppose that q is a prime dividing both u_n and $g - 1$. We then have that $g \equiv 1 \pmod{q}$ and $u_n = g^{n-1} + \cdots + 1 \equiv n \pmod{q}$. Thus, $q \mid n$. By *iv)*, we know that $q \mid \phi(u_n)$. Since u_n is a Lehmer number, we know that $\phi(u_n) \mid u_n - 1 = gu_{n-1}$. Since q divides $g-1$, it cannot divide g, therefore $q \mid u_{n-1}$. Hence, $q \mid u_n - u_{n-1} = g^{n-1}$, which is not possible. □

In the next lemma, we gather some known facts about Lehmer numbers.

Lemma 2. *i) Any Lehmer number must be odd and square-free.*

ii) If $m = p_1 \cdots p_K$ is a Lehmer number, then $K^{2^K} > m$.

iii) If $m = p_1 \cdots p_K$ is a Lehmer number, then $K \geq 14$.

Proof. i) If $m > 2$ then $\phi(m)$ is even, and since $\phi(m) \mid m-1$, we get that m must be odd. If $p^2 \mid m$, then $p \mid \phi(m)$, and since $\phi(m) \mid m-1$, we have $p \mid m-1$, which is not possible. Part *ii)* was proved by Pomerance in [6], while part *iii)* was proved by Cohen and Hagis in [2]. □

Lemma 3. *Theorems 1 and 2 hold when g is even.*

Proof. Note that

$$2^K \mid (p_1 - 1)\cdots(p_K - 1) = \phi(u_n) \mid u_n - 1 = gu_{n-1}.$$

We observe that if g is even, then u_{n-1} is odd. In that case, we have

$$K \leq \nu_2(\phi(u_n)) \leq \nu_2(gu_{n-1}) = \nu_2(g), \tag{2}$$

implying, by Lemma 2 *ii)*, that

$$g^{n-1} < u_n < K^{2^K} \leq (\nu_2(g))^{2^{\nu_2(g)}} \leq (\nu_2(g))^g.$$

Thus,

$$n \leq 1 + \left\lfloor \frac{g \log(\nu_2(g))}{\log g} \right\rfloor.$$

For Theorem 2, we observe that $\nu_2(g) \leq 9$ for any $g \leq 1000$, and we obtain a contradiction from (2) and Lemma 2 *iii)*. □

From Lemma 1 *i)*, we see that if g is odd and n is even, then u_n is even, so Lemma 2 *i)* shows that u_n cannot be a Lehmer number. From now on, we shall assume that both g and n are odd and larger than 1 and that $u_n = (g^n - 1)/(g-1)$ is a Lehmer number. We also keep the notation:

$$n = q_1^{\alpha_1} \cdots q_s^{\alpha_s}, \qquad \text{where} \quad 2 < q_1 < \cdots < q_s \tag{3}$$

are primes and $\alpha_1, \ldots, \alpha_s$ are positive integers, and

$$u_n = p_1 \cdots p_K, \qquad \text{where} \quad 2 < p_1 < \cdots < p_K \tag{4}$$

are also primes.

3 Proof of Theorem 1

3.1 Primitive divisors

Let $(A_n)_{n\geq 1}$ denote a sequence with integer terms. We say that a prime p is *a primitive divisor* of A_n if $p \mid A_n$ and $\gcd(p, A_m) = 1$ for all non-zero terms A_m with $1 \leq m < n$.

In 1886, Bang [1] showed that if $g > 1$ is any fixed integer, then the sequence $(A_n)_{n\geq 1}$ of nth term $A_n = g^n - 1$ has a primitive divisor for any index $n > 6$.

We will apply this important theorem to our sequence u_n.

Lemma 4. *If $d > 1$ is odd, then u_d has a primitive divisor p_d. Furthermore, $p_d \equiv 1 \pmod{2d}$.*

Proof. We revisit the argument already used at Lemma 1 *iv)*. We write $v_n = g^n - 1$. It is well-known that $\gcd(v_n, v_m) = v_{\gcd(n,m)}$. Observe also that

$$\frac{v_d}{v_1} = u_d = g^{d-1} + \cdots + 1 \equiv d \pmod{g-1},$$

therefore if d is a prime not dividing $g-1$, then v_d has primitive divisors. If $d > 2$ is a prime dividing $g-1$, then the above argument, or the argument from the proof of Lemma 1 *iv*), shows that $\gcd(v_d, v_1)$ is a power of d. Write $g - 1 = d\lambda$ and observe that

$$\begin{aligned}
\frac{v_d}{v_1} &= (1+d\lambda)^{d-1} + (1+d\lambda)^{d-2} + \cdots + 1\\
&\equiv (1+(d-1)d\lambda) + (1+(d-2)d\lambda) + \cdots + 1\\
&= d + d\lambda((d-1)+(d-2)+\cdots+1) \pmod{d^2}\\
&\equiv d + \frac{d^2(d-1)}{2}\lambda \pmod{d^2} \equiv d \pmod{d^2}.
\end{aligned}$$

Thus, $d \,\|\, v_d/v_1$, and therefore

$$\frac{v_d}{dv_1} = \frac{1}{d}(g^{d-1} + \cdots + 1) > 1$$

is an integer coprime to v_1, so v_d again has primitive divisors. Thus, v_3 and v_5 (and, of course, v_1 if $g > 2$) have primitive divisors. The fact that v_d has primitive divisors for all odd $d \geq 7$ follows from Bang's result.

We now note that if p is a primitive prime divisor of v_d for $d > 1$, then $g^d \equiv 1 \pmod{p}$, and d is the order of $g \pmod{p}$. Indeed, for if not, then

$f < d$ and $p \mid v_f$, contradicting the fact that p is primitive for v_d. So, $d \mid p-1$, and since d is odd, we get that $d \mid (p-1)/2$. Thus, $p \equiv 1 \pmod{2d}$.

Since a prime factor of $g-1$ cannot be a primitive divisor for v_d except for $d = 1$, we deduce that if $d > 1$, then the primitive prime divisors for v_d are exactly those of $u_d = v_d/(g-1)$, and we get the first assertion of the lemma. □

In what follows, for a positive integer m we use $\omega(m)$ and $\tau(m)$ for the number of prime divisors and the total number of divisors of m, respectively.

Lemma 5. *If u_n is square-free, n is odd and $(u_n, g-1) = 1$, then*

$$\begin{aligned} \log\left(\frac{u_n}{\phi(u_n)}\right) &< \frac{\omega(n)}{2q}\left(1+\log\left(\frac{q\log g}{\log(2q+1)}\right)\right) \\ &+ \frac{\tau(n)-2}{2q^2}\left(1+\log\left(\frac{q^2\log g}{\log(2q^2+1)}\right)\right), \end{aligned}$$

where q is the smallest prime dividing n.

Proof. We write $\mathcal{P}_d = \{p \text{ is primitive prime divisor for } u_d\}$. We shall first prove that

$$\prod := \prod_{1<d|n} \prod_{p\in P_d} p = u_n.$$

To see the above formula, we observe that if $p \mid u_d$ and $p \nmid g-1$, then $p \in \mathcal{P}_d$ for some $1 < d \mid n$. Since u_n is square-free, we have that $u_n \mid \prod$. On the other hand, the sets $\mathcal{P}_d$ are disjoint, and if $p \in \mathcal{P}_d$, then $p \mid u_d \mid u_n$. Thus, $\prod \mid u_n$.

Now, since u_n is square-free,

$$\phi(u_n) = \prod_{1<d|n} \prod_{p\in\mathcal{P}_d} (p-1),$$

and then

$$\log\left(\frac{u_n}{\phi(u_n)}\right) < \sum_{\substack{d|n \\ d>1}} \sum_{p\in\mathcal{P}_d} \frac{1}{p-1}.$$

Since all the primes $p \in \mathcal{P}_d$ are congruent to $1 \pmod{2d}$, we have

$$S_d := \sum_{p\in\mathcal{P}_d} \frac{1}{p-1} \le \frac{1}{2d}\sum_{j=1}^{\#\mathcal{P}_d} \frac{1}{j} \le \frac{1}{2d}(1+\log\#\mathcal{P}_d).$$

To bound the cardinality of $\mathcal{P}_d$, we observe that $(2d+1)^{\#\mathcal{P}_d} \le u_d < g^d$, so

$$\#\mathcal{P}_d < \frac{d \log g}{\log(2d+1)}.$$

We observe that $d \ge q$ and if d is not a prime, then $d \ge q^2$. Then

$$\sum_{1<d|n} S_d = \sum_{\substack{d|n \\ d \text{ prime}}} S_d + \sum_{\substack{d|n \\ d \text{ composite}}} S_d \le \omega(n) \frac{1}{2q} \left(1 + \log\left(\frac{q \log g}{\log(2q+1)}\right)\right)$$
$$+(\tau(n)-2)\frac{1}{2q^2}\left(1+\log\left(\frac{q^2 \log g}{\log(2q^2+1)}\right)\right).$$

□

3.2 Bounds for q_1 and $\tau(n)$

Recall that we keep the notations from (3) and (4).

Lemma 6. *If u_n is a Lehmer number and n is odd, then*

$$\begin{aligned} \tau(n/q_i) &\le \frac{\alpha_i(\alpha_i+1)}{2}\,\tau(n/q_i^{\alpha_i}) \le \nu_{q_i}(\phi(u_n)) \le \nu_{q_i}(g u_{n-1}) \\ &\le \begin{cases} \nu_{q_i}(g), & \text{if } q_i | g; \\ \nu_{q_i}(u_{q_i-1}), & \text{if } q_i \nmid g \end{cases} \end{aligned} \tag{5}$$

for all $i = 1, \ldots, s$.

Proof. Lemma 4 implies that for each divisor of n of the form $q_i^{\alpha} d$ with $1 \le \alpha \le \alpha_i$ and $d \mid (n/q_i^{\alpha_i})$, the divisor $u_{q_i^{\alpha} d}$ of u_n has a primitive prime factor $p_{q_i^{\alpha} d} \equiv 1 \pmod{d q_i^{\alpha}}$. In particular, $q_i^{\alpha} \mid p_{d q_i^{\alpha}} - 1$, and the primes $p_{d q_i^{\alpha}}$ are distinct as d ranges over the divisors of $n/q_i^{\alpha_i}$. Thus,

$$\begin{aligned} q_i^{(1+\cdots+\alpha_i)\tau(n/q_i^{\alpha_i})} &\mid \prod_{1\le\alpha\le\alpha_i} \prod_{d|n/q_i^{\alpha_i}} (p_{d q_i^{\alpha}} - 1) \mid \prod_{p|u_n} (p-1) \\ &= \phi(u_n) \mid u_n - 1 \mid g u_{n-1}, \end{aligned}$$

which gives the two central inequalities. The first inequality is trivial and the equality holds when $\alpha_i = 1$. When $q_i \mid g$, the last inequality follows from Lemma 1 *i)*, while when $q_i \nmid g$, then $\nu_{q_i}(g u_{n-1}) = \nu_{q_i}(u_{n-1})$, and we apply Lemma 1 *v)* to get the desired conclusion. □

Lemma 7. *Let u_n be a Lehmer number with both n and g odd. If $q_i > \sqrt{g}$, then*

$$\tau(n/q_i) \le q_i - 2.$$

Proof. If $q_i \mid g$ and $q_i > \sqrt{g}$, then $\nu_{q_i}(g) = 1$, and Lemma 6 above gives

$$\tau(n/q_i) \le \nu_{q_i}(g) = 1 \le q_i - 2. \tag{6}$$

If $q_i \nmid g$, then, again by Lemma 6 above, we have

$$\tau(n/q_i) \le \nu_{q_i}(u_{q_i-1}).$$

Observe that

$$u_{q_i-1} \mid g^{q_i-1} - 1 = \left(g^{(q_i-1)/2} - 1\right)\left(g^{(q_i-1)/2} + 1\right).$$

Since q_i cannot divide both factors above, we have that

$$\tau(n/q_i) \le \nu_{q_i}(g^{(q_i-1)/2} + \epsilon) \qquad \text{for some } \epsilon \in \{-1, +1\}.$$

If $\tau(n/q_i) \ge q_i - 1$, then

$$q_i^{q_i-1} \le q_i^{\tau(n/q_i)} \le g^{(q_i-1)/2} + 1 \le (q_i^2 - 1)^{(q_i-1)/2} + 1, \tag{7}$$

and we get a contradiction for $q_i > 3$, because

$$q_i^{q_i-1} = ((q_i^2 - 1) + 1)^{(q_i-1)/2}$$

and the expression on the right is larger that $(q_i^2 - 1)^{(q_i-1)/2} + 1$ except when $q_i = 3$.

Finally, if $q_i = 3$, the only odd $g < q_i^2$ with $q_i \nmid g$ are $g = 5$ and $g = 7$. But in both cases we have $\tau(n/3) \le \nu_3(u_2) \le 1 \le q_i - 2$, which completes the proof of this lemma. □

Lemma 8. *Let u_n be a Lehmer number with both n and g odd. Then*

$$q_1 \le \max\{\sqrt{g}, 19\}. \tag{8}$$

Proof. Assume that the above inequality does not hold. Then $q_1 \ge 23$, $g \le q_1^2 - 1$, and since $q_1 > \sqrt{g}$, we can apply Lemma 7 to deduce that $\tau(n) \le 2\tau(n/q_1) \le 2q_1 - 4$. We also observe that $\tau(n) \ge 2^{\omega(n)}$, so $\omega(n) \le \log(2q_1 - 4)/\log 2$.

Since u_n is a Lehmer number, we have that $2 \leq u_n/\phi(u_n)$. Now Lemma 5 and the bounds above give

$$\begin{aligned}\log 2 &< \frac{\log\left((2q_1-4)/\log 2\right)}{2q_1}\left(1+\log\left(\frac{q_1\log(q_1^2-1)}{\log(2q_1+1)}\right)\right)\\ &+ \frac{2q_1-6}{2q_1^2}\left(1+\log\left(\frac{q_1^2\log(q_1^2-1)}{\log(2q_1^2+1)}\right)\right),\end{aligned}$$

which is false for $q_1 \geq 23$. □

For a given value of g, Lemma 8 gives us our bound for q_1 and then this is used in Lemma 6, since $\tau(n) \leq 2\tau(n/q_1)$, to give a bound for $\tau(n)$. Observe also that $\omega(n) \leq \log\tau(n)/\log 2$.

3.3 The conclusion of the proof of Theorem 1

Since we have already proved that both $s = \omega(n)$ and $\tau(n)$ are bounded by effectively computable constants depending only on g, in order to conclude the proof of Theorem 1 it is enough to prove that all the primes q_i with $i = 1, \ldots, s$ are also bounded by effectively computable constants depending on g. We shall prove this by induction on $i = 1, \ldots, s$ observing that this has already been achieved for $i = 1$. Let $i \leq s-1$ and assume that q_i has been bounded. Put $Q_i = \prod_{j=1}^{j=i} q_j^{\alpha_j}$. There are only finitely many possibilities for this number. We put $g_i = g^{Q_i}$, $n_i = n/Q_i$ and rewrite the condition that u_n is Lehmer as

$$a\phi\left(\frac{g^{Q_i}-1}{g-1}\cdot\frac{g_i^{n_i}-1}{g_i-1}\right) = u_n - 1 = \frac{g^{Q_i}-1}{g-1}\cdot\frac{g_i^{n_i}-1}{g_i-1} - 1$$

with some integer $a \geq 2$. We put $w_m = (g_i^m-1)/(g_i-1)$ for the sequence of repunits in base g_i. Then, since u_n is square-free, we get that

$$a\phi(u_{Q_i})\phi(w_{n_i}) = u_{Q_i}w_{n_i} - 1,$$

therefore

$$a\frac{\phi(u_{Q_i})}{u_{Q_i}} = \frac{w_{n_i}}{\phi(w_{n_i})} - \frac{1}{u_{Q_i}\phi(w_{n_i})}. \tag{9}$$

The left hand side takes only finitely many values, which are all effectively computable. Assume that it takes some value $\delta \leq 1$. Then

$$w_{n_i} - 1 < w_{n_i} - \frac{1}{u_{Q_i}} = \delta\phi(w_{n_i}) \leq \phi(w_{n_i}),$$

a contradiction. Thus, it remains to study the case when the right hand side in (9) is > 1. Let $\delta_i > 1$ be the smallest possible value larger than 1 of the left hand side of (9). Clearly, this is effectively computable. We then get

$$\delta_i < \frac{w_{n_i}}{\phi(w_{n_i})}.$$

We observe that w_{n_i} is a sequence "like" u_n but the new value of g is $g_i = g^{Q_i}$ and the new value of n is $n_i = n/Q_i$. Thus, the smallest prime factor of n_i is q_{i+1}. We also note that $\tau(n_i) = \tau(n/Q_i) < \tau(n)$ which is bounded, and that $\omega(n_i) < \omega(n)$. Finally, we observe that $(w_{n_i}, g^{Q_i}-1) = 1$, otherwise, since $(w_{n_i}, g-1) = 1$, the number $u_n = (g^{Q_i}-1)w_{n_i}/(g-1)$ would not be square-free.

We now apply Lemma 5 to obtain that

$$\begin{aligned} \log \delta_i &< \frac{\omega(n_i)}{2q_{i+1}} \left(1 + \log\left(\frac{Q_i q_{i+1} \log g}{\log(2q_{i+1}+1)}\right)\right) \\ &+ \frac{\tau(n_i)-2}{2q_{i+1}^2} \left(1 + \log\left(\frac{Q_i q_{i+1}^2 \log g}{\log(2q_{i+1}^2+1)}\right)\right). \end{aligned} \tag{10}$$

Hence, $\log \delta_i \ll \frac{\log q_{i+1}}{q_{i+1}}$, where the constant implied by the Vinogradov symbol $\ll$ above depends only on g, implying that q_{i+1} must be bounded by some effectively computable constant depending only on g. This concludes the proof of Theorem 1.

4 Proof of Theorem 2

We assume that g is odd and $3 \le g \le 999$, so that $3 \le q_1 \le 31$ by Lemma 8.

Claim 1: That $\nu_{q_1}(u_{q_1-1}) \le 5$ can be checked with Mathematica. In particular, by Lemma 6, we have that if $q_1 \nmid g$, then $\nu_{q_1}(\phi(u_n)) \le 5$.

Claim 2: $\tau(n/q_1) \le \nu_{q_1}(\phi(u_n)) \le 6$, and $s \le 3$.

Suppose first that $q_1 \mid g$. Then, by Lemma 6,

$$\tau(n/q_1) \le \nu_{q_1}(\phi(u_n)) \le \nu_{q_1}(g u_{n-1}) = \nu_{q_1}(g) \le \left\lfloor \frac{\log g}{\log q_1} \right\rfloor \le \left\lfloor \frac{\log 1000}{\log 3} \right\rfloor = 6.$$

In the above, in fact $\nu_{q_1}(g) < 6$ unless $(q_1, g) = (3, 729)$. Then, for any q_1, by Claim 1, either $q_1 = 3$ and $\tau(n/q_1) \le 6$, or $\tau(n/q_1) \le 5$. In particular, $\tau(n) \le 2\tau(n/q_1) \le 12$, which shows that $s \le 3$.

Claim 3: $s \geq 2$.

Let us see indeed that for our particular case we cannot have $s = 1$. If this were so, then $n = q_1^{\alpha_1}$. Then each prime factor p_j of u_n is primitive for some divisor $d > 1$ of n, which is a power of q_1 (again, this is because $\gcd(u_n, g-1) = 1$). Thus, $p_j \equiv 1 \pmod{q_1}$ for all $j = 1, \ldots, K$, showing that $\nu_{q_1}(\phi(u_n)) \geq K \geq 14$ (see Lemma 2 *iii)*), which contradicts the fact that $\nu_{q_1}(\phi(u_n)) \leq 6$. Hence, $s \geq 2$.

Claim 4: $\alpha_1 = 1$ except when $(\alpha_1, q_1, g) = (2, 3, 729)$.

Put again, as in the proof of Theorem 1, $Q_1 = q_1^{\alpha_1}$. By Lemma 6 and the fact that $s \geq 2$, we have

$$\alpha_1(\alpha_1+1) \leq \frac{\alpha_1(\alpha_1+1)}{2}\tau(n/q_1^{\alpha_1}) \leq \nu_{q_1}(\phi(u_n)).$$

By Claims 1 and 2 above, we know that $\nu_{q_1}(\phi(u_n)) \leq 5$, except when $(\alpha_1, q_1, g) = (2, 3, 729)$. So, $\alpha_1 = 1$ except for this case.

Note that, at any rate, since $s \geq 2$, it follows that $2 \leq \tau(n/q_1) \leq \nu_{q_1}(gu_{q_1-1})$. A computation with Mathematica revealed 431 possibilities for the pairs (q_1, g) in our range satisfying $\nu_{q_1}(gu_{q_1-1}) \geq 2$.

Claim 5: $q_2 \leq 19$.

The smallest left hand side in (9) computed over all the 432 possible pairs (Q_1, g) has $\delta_1 > 1.49$ (it was obtained for $g = 809$, $Q_1 = q_1 = 3$ and $a = 2$, for which the obtained value is > 1.495). Of course, we did not factor all the numbers of the form $(g^{Q_1} - 1)/(g-1)$. If $q_1 = 31$, then the smallest prime $p_1 \equiv 1 \pmod{q_1}$ is 311. The number K of prime factors of u_{31} satisfies therefore

$$K < \frac{\log u_{q_1}}{\log p_1} < \frac{3 \cdot 31 \cdot \log 10}{\log 311} < 38;$$

hence,

$$a\frac{\phi(u_{q_1})}{u_{q_1}} \geq 2\left(1 - \frac{1}{311}\right)^{37} > 1.7.$$

Similarly, using the fact that when $q_1 = 29$ and 23 the first two primes congruent to $1 \pmod{q_1}$ are 59 and 233, and 47 and 139 respectively, and

$$\frac{3 \cdot 29 \cdot \log 10}{\log 233} < 37 \qquad \text{and} \qquad \frac{3 \cdot 23 \cdot \log 10}{\log 139} < 33,$$

we have that

$$
\begin{aligned}
a\frac{\phi(u_{q_1})}{u_{q_1}} & \geq 2\min\left\{\left(1-\frac{1}{59}\right)\left(1-\frac{1}{233}\right)^{36}, \left(1-\frac{1}{47}\right)\left(1-\frac{1}{139}\right)^{32}\right\} \\
& > 1.55,
\end{aligned}
$$

whenever $q_1 \in \{23, 29\}$. Thus, we have factored only the numbers u_{Q_1} with $Q_1 \leq 19$. We now use inequality (10) for $i = 1$ to obtain

$$
\begin{aligned}
\log(1.49) & < \frac{\omega(n_1)}{2q_2}\left(1+\log\left(\frac{Q_1 q_2 \log g}{\log(2q_2+1)}\right)\right) \\
& + \frac{\tau(n_1)-2}{2q_2^2}\left(1+\log\left(\frac{Q_1 q_2^2 \log g}{\log(2q_2^2+1)}\right)\right).
\end{aligned}
$$

If $q_1 > 3$, then $Q_1 = q_1 \leq 31$. If $q_1 = 3$, then $Q_1 = q_1^2 = 9$. Thus, $Q_1 \leq 31$ in both cases. We also saw in Claims 1 and 2 that $\tau(n_1) \leq \tau(n/q_1) \leq 6$, so also $\omega(n_1) \leq 2$. Hence,

$$
\log(1.49) < \frac{1}{q_2}\left(1+\log\left(\frac{31 q_2 \log 999}{\log(2q_2+1)}\right)\right) + \frac{2}{q_2^2}\left(1+\log\left(\frac{31 q_2^2 \log 999}{\log(2q_2^2+1)}\right)\right),
$$

and this inequality does not hold when $q_2 \geq 23$.

4.1 The conclusion of the proof of Theorem 2

Thus, $3 \leq q_1 < q_2 \leq 19$. The argument showing that $\alpha_1 = 2$ except if $(q_1, g) = (3, 729)$ now shows that $\alpha_2 = 1$. We are now able to show that $s = 2$. Indeed, if it were not so, then we would have both $\tau(n/q_1) \geq 4$ and $\tau(n/q_2) \geq 4$. A quick computation with Mathematica shows that while there are pairs (q, g) such that $\nu_q(gu_{q-1}) \geq 4$ in our ranges, there is no odd g in $[3, 999]$ that has the above property with respect to two different primes $3 \leq q_1 < q_2 \leq 19$. Thus, either $n = q_1 q_2$, or $n = 9q_2$ and $g = 729$. To test these last pairs, we proceeded as follows. First we have detected all pairs (n, g) with $n = q_1 q_2$ with $3 \leq q_1 < q_2 \leq 19$ and odd $g \in [3, 999]$ such that $\nu_{q_i}(gu_{n-1}) \geq 2$ holds for both $i = 1, 2$. There are 2043 such pairs. For each one of these we checked that $\nu_2(u_{n-1}) < 14$. Similarly, when $Q_1 = 9$ and $g = 729$, the only possibility for q_2 in our range such that $\nu_{q_2}(u_{q_2-1}) \geq 2$ is $q_2 = 11$, but in this case $n = 99$ and $\nu_2(u_{n-1}) = 1 < 14$. This finishes the proof of Theorem 2.

References

[1] A. S. Bang, "Taltheoretiske Undersølgelser", *Tidskrift f. Math.* **5** (1886), 70–80 and 130–137.

[2] G. L. Cohen and P. Hagis, "On the number of prime factors of n if $\phi(n) \mid n-1$", *Nieuw Arch. Wisk. (3)* **28** (1980), 177–185.

[3] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, 2004.

[4] D. H. Lehmer, "On Euler's totient function", *Bull. Amer. Math. Soc.* **38** (1932), 745–751.

[5] F. Luca, "Fibonacci numbers with the Lehmer property", *Bull. Polish Acad. Sci. Math.* **55** (2007), 7–15.

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