Annales Mathematicae et Informaticae
37 (2010) pp. 107–124
http://ami.ektf.hu

On perfect numbers which are ratios of two Fibonacci numbers*

Florian Luca[a], V. Janitzio Mejía Huguet[b]

[a]Instituto de Matemáticas, Universidad Nacional Autónoma de México

[b] Universidad Autónoma Metropolitana

Submitted 23 August 2010; Accepted 29 October 2010

Abstract

Here, we prove that there is no perfect number of the form F_{mn}/F_m, where F_k is the kth Fibonacci number.

Keywords: Perfect numbers, Fibonacci numbers.

MSC: 11Axx, 11B39, 11Dxx.

1. Introduction

For a positive integer n let $\sigma(n)$ be the sum of its divisors. A number n is called perfect if $\sigma(n) = 2n$ and multiperfect if $n \mid \sigma(n)$. Let $(F_k)_{k\geqslant 0}$ be the Fibonacci sequence given by $F_0 = 0$, $F_1 = 1$ and $F_{k+2} = F_{k+1} + F_k$ for all $k \geqslant 0$.

In [6], it was shown that there is no perfect Fibonacci number. More generally, in [1], it was shown that in fact F_n is not multiperfect for any $n \geqslant 3$.

In [8], it is was shown that the set $\{F_{mn}/F_m \ : \ m,\ n \in \mathbf{N}\}$ contains no perfect number. The proof of this result from [8] uses in a fundamental way the claim that if N is odd and perfect, then

$$N = p^a q_1^{a_1} \cdots q_s^{a_s} \tag{1.1}$$

for some distinct primes p and $q_1, \ldots, q_s$, with $p \equiv a \equiv 1 \pmod 4$, a_i even for $i = 1, \ldots, s$ and $q_i \equiv 3 \pmod 4$ for $i = 1, \ldots, s$. We could not find neither a reference nor a proof for the fact that the primes q_i must necessarily be congruent

*F. L. was supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508, and V. J. M. H. was supported by Grant UAM-A 2232508.

to 3 (mod 4). The remaining assertions about p, a and the exponents a_i for $i = 1, \dots, s$ were proved by Euler.

In this paper, we revisit the question of perfect numbers of the shape F_{mn}/F_m and give a proof of the fact that there are indeed no such perfect numbers. We record our result as follows.

Theorem 1.1. *There are no perfect numbers of the form F_{mn}/F_m for natural numbers m and n.*

Our proof avoids the information about the congruence classes of the primes q_i for $i = 1, \dots, s$ from (1.1). Ingredients of the proof are Ribenboim's description of square-classes for Fibonacci and Lucas numbers [9], as well as an effective version of Runge's theorem from Diophantine equations due to Gary Walsh [11].

In what follows, for a positive integer n we use $\Omega(n)$, $\omega(n)$ and $\tau(n)$ for the number of prime divisors of n (counted with and without multiplicities) and the total numbers of divisors of n, respectively.

From now on, we put $N := F_{mn}/F_m$ for some positive integers m and n, and assume that N is perfect. Clearly, $n > 1$, and by the result from [6] we may assume that $m > 1$ also. A quick computation with Mathematica confirmed that there is no such example with $mn \leqslant 100$. So, from now on, we also suppose that $mn > 100$.

2. The even perfect number case

While there is no problem with the treatment of the even perfect number case from [8], we include it here for the convenience of the reader.

For every positive integer m, let $z(m)$ be the minimal positive integer k such that $m \mid F_k$. This always exists and it is called the *index of appearance* of m in the Fibonacci sequence. Indices of appearance have important properties. For example, m divides F_k if and only if $z(m)$ divides k. Furthermore, if p is prime, then

$$p \equiv \left(\frac{p}{5}\right) \pmod{z(p)}, \tag{2.1}$$

where for an odd prime q and an integer a we write $\left(\dfrac{a}{q}\right)$ for the Legendre symbol of a with respect to q. In particular, from congruence (2.1), we deduce that $p \equiv 1 \pmod{z(p)}$ if $p \equiv \pm 1 \pmod 5$, and $p \equiv -1 \pmod{z(p)}$ provided that $p \equiv \pm 2 \pmod 5$. Clearly, $z(5) = 5$.

So, if p is a prime factor of F_n, then $z(p)$ divides n. If $z(p) = n$, then p is called *primitive* for F_n. Equivalently, p is a primitive prime factor of F_n if p does not divide F_m for any positive integer $m < n$. An important result of Carmichael [2] asserts that F_n has a primitive prime factor for all $n \notin \{1, 2, 6, 12\}$. From congruence (2.1), we have that if p is primitive for F_n, then $p \equiv \pm 1 \pmod n$ unless $p = n = 5$.

So, let us now suppose that $N = F_{mn}/F_m$ is even and perfect. By the structure theorem of even perfect numbers, we have that

$$\frac{F_{mn}}{F_m} = 2^{p-1}(2^p - 1), \tag{2.2}$$

where p and $2^p - 1$ are both primes. If $p \in \{2, 3\}$, then $F_{mn} = 2 \times 3 \times F_m$, or $2^2 \times 7 \times F_m$. However, since $mn > 100$, it follows that F_{mn} has a primitive prime factor q. The prime q does not divide F_m and since $q \equiv \pm 1 \pmod{mn}$, it follows that $q \geqslant mn - 1 > 99$. Thus, q cannot be one of the primes 2, 3, or 7, and we have obtained a contradiction.

Suppose now that $p \geqslant 5$. Then $16 \mid F_{mn}/F_m$. Assume first that $3 \nmid m$. Since $z(2) = 3$ and $3 \nmid m$, it follows that F_m is odd, therefore $16 \mid F_{mn}$. Hence, $12 = z(16) \mid mn$. However, since 9 divides F_{12}, we get that $9 \mid F_{12} \mid F_{mn}$. Relation (2.2) together with the fact that $p \geqslant 5$ implies that N is coprime to 3, therefore $9 \mid F_m$. Hence, $12 = z(9) \mid m$, contradicting our assumption that $3 \nmid m$. Thus, $3 \mid m$. In particular, $2 \mid F_m$, therefore $2^5 \mid F_{mn}$. Write $mn = 2^s \times 3 \times \lambda$ for some odd positive integer λ. Since $2^5 \mid F_{mn}$, we get that $2^3 \times 3 = z(2^5) \mid mn$, therefore $s \geqslant 3$. Next we show that $m \mid 2^{s-3} \times 3 \times \lambda$. Indeed, for is not, since m is a multiple of 3, it would follow that $2^{s-2} \times 3 \mid m$. It is known that if a is positive then the exponent of 2 in the factorization of $F_{2^a \times 3 \times b}$ is exactly $a + 2$ for all odd integers b. Hence, the exponent of 2 in F_{mn} is precisely $s + 2$, while since $2^{s-2} \times 3$ divides m, we get that the exponent of 2 in F_m is at least s. Thus, the exponent of 2 in F_{mn}/F_m cannot exceed $(s + 2) - s = 2$, a contradiction. We conclude that indeed $m \mid 2^{s-3} \times 3 \times \lambda$.

Hence, mn has at least

$$\tau(2^s \times 3 \times \lambda) - \tau(2^{s-3} \times 3 \times \lambda) = (s + 1)\tau(3\lambda) - (s - 2)\tau(3\lambda) = 3\tau(3\lambda) \geqslant 6$$

divisors d which do not divide m. These divisors are of the form $2^\alpha d_1$, where $\alpha \in \{s - 2, s - 1, s\}$, and d_1 is odd. Since these numbers are all even, it follows that for a most three of them (namely, for $d \in \{2, 6, 12\}$), the number F_d might not have a primitive prime factor. Thus, for the remaining even divisors d of mn which do not divide m (at least three of them in number), we have that F_d has a primitive prime factor p_d. The primes p_d for such values of d are distinct and do not divide F_m, therefore they appear in the factorization of $N = F_{mn}/F_m$. Hence, $\omega(N) \geqslant 3$, which contradicts relation (2.2) according to which $\omega(N) = 2$.

Hence, N cannot be even and perfect.

3. The odd perfect number case

Here, we use a result of Ribenboim [9] concerning square-classes of Fibonacci and Lucas numbers. We say that positive integers a and b are in the same *Fibonacci square-class* if $F_a F_b$ is a square. The Fibonacci square-class of a is called trivial if $F_a F_b$ is a square only for $b = a$. Then Ribenboim's result is the following.

Theorem 3.1. *If $a \neq 1, 2, 3, 6, 12$, then the Fibonacci square-class of a is trivial.*

In the same paper [9], Ribenboim also found the square-classes of the Lucas numbers. Recall that the Lucas sequence $(L_k)_{k\geqslant 0}$ is given by $L_0 = 2,\ L_1 = 1$ and $L_{k+2} = L_{k+1} + L_k$ for all $k \geqslant 0$. We say that positive integers a and b are in the same *Lucas square-class* if L_aL_b is a square. As previously, the Lucas square-class of a is called trivial if L_aL_b is a square only for $b = a$. Then Ribenboim's result is the following.

Theorem 3.2. *If $a \neq 0, 1, 3, 6$, then the Lucas square-class of a is trivial.*

We deal with the case of the odd perfect number $N = F_{mn}/F_m$ through a sequence of lemmas. We write N as in (1.1) with odd distinct primes p and $q_1, \ldots, q_s$ and integer exponents a and $a_1, \ldots, a_s$ such that $p \equiv a \equiv 1 \pmod 4$ and a_i are even for $i = 1, \ldots, s$. We use $\square$ to denote a perfect square.

Lemma 3.3. *Both m and n are odd.*

Proof. Assume that n is even. Then $F_{mn} = F_{mn/2}L_{mn/2}$ and $F_m \mid F_{mn/2}$. Thus,

$$N = \frac{F_{mn}}{F_m} = \left(\frac{F_{mn/2}}{F_m}\right) L_{mn/2} = p\square. \tag{3.1}$$

Now it is well-known that $\gcd(F_\ell, L_\ell) \in \{1, 2\}$ and since N is odd, we get that $\gcd(F_{mn/2}, L_{mn/2}) = 1$. Hence, the two factors on the left hand side of equation (3.1) above are coprime, and we conclude that either

$$\begin{cases} \frac{F_{mn/2}}{F_m} = p\square \\ L_{mn/2} = \square \end{cases}, \qquad \text{or} \qquad \begin{cases} \frac{F_{mn/2}}{F_m} = \square \\ L_{mn/2} = p\square \end{cases}.$$

In the first case, since $L_1 = 1$, we get that $mn/2$ is in the same Lucas square-class as 1, which is impossible by Theorem 3.2 because $mn/2 > 50$. In the second case, we get that $mn/2$ and m are in the same Fibonacci square-class, which is impossible by Theorem 3.1 for $mn/2 > 50$ unless $mn/2 = m$, which happens when $n = 2$. But if $n = 2$, we then get that

$$N = \frac{F_{2m}}{F_m} = L_m,$$

and the fact that L_m is not perfect was proved in [6]. The proof of the lemma is complete. $\square$

Lemma 3.4. *We have $a_i \equiv 0 \pmod 4$ for all $i = 1, \ldots, s$.*

Proof. It is well-known that if ℓ is odd then every odd prime factor of F_ℓ is congruent to 1 modulo 4. One of the simplest way of seing this is via the formula $F_{2\ell+1} = F_\ell^2 + F_{\ell+1}^2$ valid for all $\ell \geqslant 0$, together with the fact that F_ℓ and $F_{\ell+1}$ are coprime. Since mn is odd (by Lemma 3.3), it follows that $q_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, s$. Now

$$\sigma(q_i^{a_i}) = 1 + q_i + \cdots + q_i^{a_i} \equiv a_i + 1 \pmod 4.$$

If a_i is a not a multiple of 4 for some $i \in \{1, \ldots, s\}$, then $a_i \equiv 2 \pmod 4$, therefore $\sigma(q_i^{a_i}) \equiv 3 \pmod 4$. Hence, $\sigma(q_i^{a_i})$ has a prime factor $q \equiv 3 \pmod 4$. However, since $q \mid \sigma(q_i^{a_i}) \mid \sigma(N) = 2N$, it follows that q is a divisor of N, which is false because from what we have said above all prime factors of N are congruent to 1 modulo 4. $\square$

Lemma 3.5. *The number n is prime.*

Proof. Say $n = r_1^{b_1} \cdots r_\ell^{b_\ell}$, where $3 \leqslant r_1 < \cdots < r_\ell$ are primes and $b_1, \ldots, b_\ell$ are positive integers. Then

$$\frac{F_{mn}}{F_m} = \left(\frac{F_{mn/r_1}}{F_m}\right)\left(\frac{F_{mn}}{F_{mn/r_1}}\right) = p\square. \tag{3.2}$$

It is well-known that the relation

$$\gcd\left(F_a, \frac{F_{ar}}{F_a}\right) = \begin{cases} r & \text{if } \ r \mid F_a \\ 1 & \text{otherwise} \end{cases} \tag{3.3}$$

holds for all positive integers a and primes r. Furthermore, if the above greatest common divisor is not 1, then $r \| F_{ar}/F_a$. We apply this with $a := mn/r_1$ and $r := r_1$ distinguishing two different cases.

The first case is when F_{mn/r_1} and $F_{mn}/F_{mn/r_1}$ are coprime. In this case, (3.2) implies that

$$\text{either} \qquad \frac{F_{mn/r_1}}{F_m} = \square, \qquad \text{or} \qquad \frac{F_{mn}}{F_{mn/r_1}} = \square.$$

The second instance is impossible by Theorem 3.1 since $mn > 100$. By the same theorem, the first instance is also impossible unless $mn/r_1 = m$, which happens when $n = r_1$, which is what we want to prove.

So, let us analyze the second case. Then $r_1 \mid F_{mn/r_1}$. Since $r_1 \mid F_{z(r_1)}$, we get that $r_1 \mid \gcd(F_{mn/r_1}, F_{z(r_1)}) = F_{\gcd(mn/r_1, z(r_1))}$. We know that $r_1 \geqslant 3$ by Lemma 3.3. If $r_1 = 3$, then $z(r_1) = 4$ and $r_1 \mid F_{\gcd(mn/3,4)} = F_1 = 1$, where the fact that $\gcd(mn/r_1, 4) = 1$ follows from Lemma 3.3 which tells us that the number mn is odd. We have reached a contradiction, so it must be the case that $r_1 \geqslant 5$. Let us observe that if $r_1 \geqslant 7$, then $z(r_1) \mid r_1 \pm 1$. Hence, in this case

$$r_1 \mid F_{\gcd(mn/r_1, r_1 \pm 1)}.$$

Since r_1 is the smallest prime in n, it follows that n/r_1 is coprime to $r_1 \pm 1$, therefore $\gcd(mn/r_1, r_1 \pm 1) = \gcd(m, r_1 \pm 1) \mid m$. Consequently, $r_1 \mid F_m$ if $r_1 \geqslant 7$. We now return to equation (3.2) and use the fact that $r_1 \| F_{mn}/F_{mn/r_1}$ and $r_1 = \gcd(F_{mn/r_1}, F_{mn}/F_{mn/r_1})$.

We distinguish two instances.

The first instance is when $r_1 = p$. We then get that

$$\frac{F_{mn/r_1}}{F_m} = \square, \qquad \text{and} \qquad \frac{F_{mn}}{F_{mn/r_1}} = p\square.$$

By Theorem 3.1, the first equation is not possible unless $n = r_1$, which is what we want.

The second instance is when $r_1 \neq p$. Then, by Lemma 3.4, we have that $r_1^4 \mid N$, and since $r_1 \| F_{mn}/F_{mn/r_1}$, we get that $r_1^3 \mid F_{mn/r_1}/F_m$. If $r_1 = 5$, this implies that $r_1^3 \mid n/r_1$, because it is well-known that the exponent of 5 in the factorization of F_ℓ is the same as the exponent of 5 in the factorization of ℓ. If $r_1 \geqslant 7$, then $r_1 \mid F_m$, so $z(r_1) \mid m$. It is then well-known that if r_1^e denotes the exponent of r_1 in the factorization of $F_{z(r_1)}$, then for every nonzero multiple ℓ of $z(r_1)$, the exponent of r_1 in F_ℓ is f $(\geqslant e)$, where $f - e$ is the precise exponent of r_1 in $\ell/z(r_1)$. It then follows again that the divisibility relation $r_1^3 \mid F_{mn/r_1}/F_m$ together with the fact that $r_1 \mid F_m$ imply that $r_1^3 \mid n/r_1$. Hence, in all cases ($r_1 = 5$, or $r_1 \geqslant 7$), we have that $r_1^4 \mid n$. Now we write

$$N = \frac{F_{mn}}{F_m} = \left(\frac{F_{mn/r_1^2}}{F_m}\right)\left(\frac{F_{mn}}{F_{mn/r_1^2}}\right) = p\square. \tag{3.4}$$

Using (3.3), one proves easily that the greatest common divisor of the two factors on the right above is r_1^2 and that $r_1^2 \| F_{mn}/F_{mn/r_1^2}$. The above equation (3.4) then leads to

$$\text{either} \qquad \frac{F_{mn/r_1^2}}{F_m} = \square, \qquad \text{or} \qquad \frac{F_{mn}}{F_{mn/r_1^2}} = \square.$$

Theorem 3.1 implies that the second instance is impossible and that the first instance is possible only when $n = r_1^2$. However, we have already seen that r_1^4 must divide n. Thus, the first instance cannot appear either. The proof of this lemma is complete. $\square$

From now on, we shall assume that n is prime and we shall denote n by q.

Lemma 3.6. *We have $q \nmid m$.*

Proof. Say $q \mid m$. Then

$$\frac{F_{mq}}{F_m} = \left(\frac{F_m}{F_{m/q}}\right)\left(\frac{F_{mq}/F_m}{F_m/F_{m/q}}\right) = p\square. \tag{3.5}$$

Both factors above are integers.

Suppose first that the two factors above are coprime. Then

$$\text{either} \qquad \frac{F_m}{F_{m/q}} = \square, \qquad \text{or} \qquad \frac{F_{mq}/F_m}{F_m/F_{m/q}} = \square.$$

The first instance is impossible by Theorem 3.1. The second instance leads to $F_{mq}/F_{m/q} = \square$, which is again impossible by the same Theorem 3.1.

Suppose now that the two factors appearing in the right hand side in relation (3.5) are not coprime. But then if r is a prime such that

$$r \mid \gcd\left(\frac{F_m}{F_{m/q}}, \frac{F_{mq}/F_m}{F_m/F_{m/q}}\right), \qquad \text{then} \qquad r \mid \gcd\left(F_m, \frac{F_{mq}}{F_m}\right),$$

therefore $r = q$ by (3.3). Since $q \mid F_m/F_{m/q}$, we get that $q \mid F_{m/q}$ and $q \| F_m/F_{m/q}$, and also $q \| F_{mq}/F_m = N$. Thus, $q = p$, and now equation (3.5) implies

$$\frac{F_m}{F_{m/q}} = p\square, \qquad \text{and} \qquad \frac{F_{mq}/F_m}{F_m/F_{m/q}} = \square.$$

The second relation leads again to $F_{mq}/F_{m/q} = \square$, which is impossible by Theorem 3.1. Hence, indeed $q \nmid m$. $\square$

Lemma 3.7. *We have $q \geqslant 7$.*

Proof. We have $q \geqslant 3$ by Lemma 3.3. If $q = 3$, then since $3 \nmid m$ (by Lemma 3.6), it follows that F_m is odd. But then $N = F_{3m}/F_m$ is even, which is a contradiction. If $q = 5$, then $N = F_{5m}/F_m$ has the property that $5 \| N$. Thus, $p = 5$, and we get the equation

$$\frac{F_{5m}}{F_m} = 5\square,$$

which has no solution (see equation (8) in [1]). The lemma is proved. $\square$

Lemma 3.8. *(i) All primes p and $q_1, \ldots, q_s$ have their orders of appearance divisible by q. In particular, they are all congruent to $\pm 1 \pmod q$;*

(ii) $p \equiv 1 \pmod 5$ and $p \equiv 1 \pmod q$. Furthermore, $N \equiv 1 \pmod 5$ and $N \equiv 1 \pmod q$;

(iii) If $q_i \equiv 1 \pmod q$ for some $i = 1, \ldots, s$, then $a_i \geqslant 2q - 2$;

(iv) We have $q \equiv \pm 1 \pmod{20}$. In particular, $F_q \equiv 1 \pmod 5$;

(v) $F_q \neq p$.

Proof. (i) Observe first that all primes p and $q_1, \ldots, q_s$ are $\geqslant 7$. Indeed, it is clear that they are all odd. If one of them is 3, then $3 \mid F_{mq}$, so that $4 = z(3) \mid mq$, which is impossible by Lemma 3.3, while if one of them is 5, then $5 \mid F_{mq}/F_m$, which implies that $q = 5$, contradicting Lemma 3.7. Thus, p and q_i are congruent to $\pm 1 \pmod{z(p)}$ and $\pm 1 \pmod{z(q_i)}$ for $i = 1, \ldots, s$, respectively. If $q \mid z(p)$ and $q \mid z(q_i)$ for $i = 1, \ldots, s$, we are through. So, assume that for some prime number r in $\{p, q_1, \ldots, q_s\}$ we have that $q \nmid z(r)$. Then $r \mid F_{mq}$ and $r \mid F_{z(r)}$, so that $r \mid \gcd(F_{mq}, F_{z(r)}) = F_{\gcd(mq, z(r))} \mid F_m$. Thus, $r \mid F_m$ and $r \mid N = F_{mq}/F_m$, therefore $r \mid \gcd(F_m, F_{mq}/F_m)$, so $r = q$ by (3.3). In this case, $q \| F_{mq}/F_m$, therefore $q = p$. The above argument shows, up to now, that all prime factors of N are either congruent to $\pm 1 \pmod q$, or the prime q itself, but if this occurs, then $p = q$. But with $p = q$, we have that $(q + 1) = (p + 1) \mid \sigma(N) = 2N$, therefore $(q + 1)/2$ is a divisor of N. Thus, all prime factors of $(q+1)/2$ are either q, which is not possible, or primes which are congruent to $\pm 1 \pmod q$, which is not possible either. This contradiction shows that in fact $q \nmid N$, therefore indeed all prime factors of N have their orders of appearance divisible by q and, in particular, they are all congruent to $\pm 1 \pmod{q}$ by (2.1).

(ii) Clearly, $(p+1) \mid \sigma(N) = 2N$. By (i), $p \equiv \pm 1 \pmod{q}$, and by relation (2.1), we have that $p \equiv \left(\frac{p}{5}\right) \pmod{q}$. If $p \equiv -1 \pmod{q}$, then $q \mid (p+1) \mid 2N$, so that $q \mid N$, which is impossible by (i). So, $p \equiv 1 \pmod{q}$, showing that $\left(\frac{p}{5}\right) \equiv 1 \pmod{5}$, therefore $p \equiv \pm 1 \pmod{5}$. Finally, if $p \equiv -1 \pmod{5}$, then $5 \mid (p+1) \mid \sigma(N) = 2N$, so $5 \mid N$, which is impossible by (i). Thus, indeed $p \equiv 1 \pmod{5}$ and $p \equiv 1 \pmod{q}$. The fact that $N \equiv 1 \pmod{q}$ is now a consequence of the fact that $p \equiv 1 \pmod{5}$, $q_i > 5$ and a_i is a multiple of 4 for all $i = 1, \ldots, s$ (see Lemma 3.4), therefore $q_i^{a_i} \equiv 1 \pmod{5}$ for all $i = 1, \ldots, s$. The fact that $N \equiv 1 \pmod{q}$ follows because by (i) $p \equiv 1 \pmod{q}$, $q_i \equiv \pm 1 \pmod{q}$, and a_i is even for all $i = 1, \ldots, s$.

(iii) Assume that $q_i \equiv 1 \pmod{q}$ for some $i = 1, \ldots, s$. Then

$$\sigma(q_i^{a_i}) = 1 + q_i + \cdots + q_i^{a_i} \equiv a_i + 1 \pmod{q}.$$

Since $\sigma(q_i^{a_i})$ is an odd divisor of $\sigma(N) = 2N$, we get that $\sigma(q_i^{a_i})$ is a divisor of N, so, by (i), all its prime factors are congruent to $\pm 1 \pmod{q}$. Hence, $\sigma(q_i^{a_i}) \equiv \pm 1 \pmod{q}$, showing that $a_i \equiv -2, 0 \pmod{q}$. Since a_i is also even, we get that $a_i \equiv -2, 0 \pmod{2q}$. In particular, $a_i \geqslant 2q - 2$, which is what we wanted.

(iv) We use the formula

$$F_{qm} = \frac{1}{2^{q-1}} \sum_{i=0}^{(q-1)/2} \binom{q}{2i+1} 5^i F_m^{2i+1} L_m^{q-1-2i}. \tag{3.6}$$

Assume that $5^b \| m$ with some integer $b \geqslant 0$. We then see that all the terms in the sum appearing on the right hand side of formula (3.6) above are multiples of 5^{b+1}, whereas the first term (with $i = 0$) is $qF_m L_m^{q-1}$, which is divisible by 5^b, but not by 5^{b+1}. It then follows that

$$\frac{F_{qm}}{F_m} \equiv \frac{q}{2^{q-1}} L_m^{q-1} \pmod{5}. \tag{3.7}$$

Since m is odd, the sequence $(L_k)_{k \geqslant 0}$ is periodic modulo 5 with period 4, and $L_1 = 1$, $L_3 = 4 \equiv -1 \pmod{5}$, it follows that $L_m \equiv \pm 1 \pmod{5}$, so that $L_m^{q-1} \equiv 1 \pmod{5}$. Hence, from congruence (3.7), we get $N \equiv q/2^{q-1} \pmod{5}$. Since also $N \equiv 1 \pmod{5}$ (see (ii)), we get that $q \equiv 2^{q-1} \pmod{5}$. In particular, q is a quadratic residue modulo 5, therefore $q \equiv \pm 1 \pmod{5}$. If $q \equiv 1 \pmod{5}$, we then get that the congruence $2^{q-1} \equiv 1 \pmod{5}$ holds, so that $q \equiv 1 \pmod{4}$ as well. If $q \equiv -1 \pmod{5}$, we then get that the congruence $2^{q-1} \equiv -1 \pmod{5}$ holds, so that $q \equiv -1 \pmod{4}$ as well. Summarizing, we get that $q \equiv \pm 1 \pmod{20}$, and, in particular, $F_q \equiv 1 \pmod{5}$.

(v) Assume that $F_q = p$. Then $F_q + 1 = p + 1$ divides $\sigma(N) = 2N$. Now let us recall that if $a > b$ are odd numbers, then

$$F_a + F_b = F_{(a+\delta b)/2} L_{(a-\delta b)/2},$$

where $\delta \in \{\pm 1\}$ is such that $a \equiv \delta b \pmod 4$. Applying this with $a := q$ and $b := 1$, we get that $5 \mid F_{(q+\delta)/2} L_{(q-\delta)/2}$ divides $2F_{qm}$. Observe that since $q \equiv \delta \pmod 4$, it follows that $(q-\delta)/2$ is even. Now it is well-known and easy to prove that if u is even and v is odd, then $\gcd(L_u, F_v) = 1$, or 2. Thus, $L_{(q-\delta)/2}$ cannot divide $2F_{mq}$, unless $L_{(q-\delta)/2} \leqslant 4$, which is not possible for $q \geqslant 7$. □

From now on, we write r for the minimal prime factor dividing m.

Lemma 3.9. *There exists a divisor $d \in \{r, r^2\}$ of m such that*

$$\frac{F_{mq}/F_{mq/d}}{F_m/F_{m/d}} = \square. \tag{3.8}$$

Furthermore, the case $d = r^2$ can occur only when $r \mid F_q$.

Proof. Write again, as often we did before,

$$N = \frac{F_{mq}}{F_m} = \left(\frac{F_{mq/r}}{F_{m/r}}\right)\left(\frac{F_{mq}/F_{mq/r}}{F_m/F_{m/r}}\right) = p\square. \tag{3.9}$$

Suppose first that the two factors appearing in the left hand side of equation (3.9) above are coprime. Then

$$\text{either} \qquad \frac{F_{mq/r}}{F_{m/r}} = \square, \qquad \text{or} \qquad \frac{F_{mq}/F_{mq/r}}{F_m/F_{m/r}} = \square.$$

The first instance is impossible by Theorem 3.1, while the second instance is the conclusion of our lemma with $d := r$.

So, from now on let's assume that the two factors appearing in the left hand side of equation (3.9) are not coprime. Let λ be any prime dividing both numbers $F_{mq/r}/F_{m/r}$ and $(F_{mq}/F_{mq/r})/(F_m/F_{m/r})$. Then $\lambda \mid \gcd(F_{mq/r}, F_{mq}/F_{mq/r})$. By (3.3), we get that $\lambda = r$. In this last case, $r = \gcd(F_{mq/r}, F_{mq}/F_{mq/r})$, $r \| F_{mq}/F_{mq/r}$, and also $r \mid F_{mq/r}/F_{m/r}$. If $r \mid F_{m/r}$, it then follows that $r \mid \gcd(F_{m/r}, F_{mq/r}/F_{m/r})$, so, by (3.3), we get that $r = q$, which contradicts Lemma 3.6. Hence, $r \nmid F_{m/r}$. Thus, $r \mid F_{mq/r}$ and $r \nmid F_{m/r}$. Now if $r \mid F_m$, then $r \mid \gcd(F_m, F_{mq/r}) = F_{\gcd(m,mq/r)} = F_{m/r}$, which is impossible. Thus, $r \nmid F_m$, so that $r \nmid F_m/F_{m/r}$. Since $r \| F_{mq}/F_{mq/r}$, we get that $r \| (F_{mq}/F_{mq/r})/(F_m/F_{m/r})$.

We now distinguish two instances.

The first instance is when $r = p$, case in which equation (3.9) leads to

$$\frac{F_{mq/r}}{F_{m/r}} = \square, \qquad \text{and} \qquad \frac{F_{mq}/F_{mq/r}}{F_m/F_{m/r}} = p\square. \tag{3.10}$$

The first relation in (3.10) above is impossible by Theorem 3.1.

The second instance is when $r \neq p$.

Let $r = q_i$ for some $i = 1, \ldots, s$, and suppose first that $r \| m$. Then $r^{a_i - 1} \mid F_{mq/r}$. Furthermore, since $r \nmid mq/r$, we also get that $r^{a_i-1} \| F_{z(r)}$. Hence, $r^{a_i-1} \mid$

$\gcd(F_{mq/r}, F_{z(r)}) = F_{\gcd(mq/r, z(r))}$. Since $r \mid N$, we have that $r \geqslant 7$ (by (i) of Lemma 6, for example), therefore $z(r) \mid r \pm 1$. Since r is the smallest prime in m and $r \| m$, we get that $\gcd(mq/r, z(r)) \mid \gcd(mq/r, r \pm 1) \mid q$. Thus, either $\gcd(mq/r, z(r)) = 1$, leading to $r^{a_i - 1} \mid F_1$, which is of course impossible, or $\gcd(mq/r, z(r)) = q$, leading to $r^{a_i-1} \mid F_q$.

Next, we get from equation (3.9) that

$$\text{either} \qquad \frac{F_{mq}/F_{mq/r}}{F_m/F_{m/r}} = r\square, \qquad \text{or} \qquad \frac{F_{mq}/F_{mq/}}{F_m/F_{m/r}} = pr\square. \tag{3.11}$$

By (v) of Lemma 3.8, we have that $q \equiv \pm 1 \pmod{20}$. Hence, $mq \equiv \pm m \pmod{20}$, therefore $F_{mq} \equiv F_{\pm m} \equiv F_m \pmod 5$. The last relation, namely $F_m \equiv F_{-m} \pmod 5$, holds because m is odd. Similarly, $mq/r \equiv \pm m/r \pmod{20}$, so that $F_{mq/r} \equiv F_{m/r} \pmod 5$. Since $F_{m/r}$, $F_{mq/r}$, F_m and F_{mq} are all invertible modulo 5 (because the smallest prime factor of m which is r divides F_q, therefore $r \geqslant 2q - 1 > 5$), it follows that $(F_{mq}/F_{mq/r})/(F_m/F_{m/r}) \equiv 1 \pmod 5$. Relation (3.11) together with the fact that $p \equiv 1 \pmod 5$, which is (ii) of Lemma 3.8, now shows that $1 \equiv r\square \pmod 5$, therefore $\left(\frac{r}{5}\right) = 1$, so, by (2.1), we have $r \equiv 1 \pmod q$. Hence, by (iii) of Lemma 3.8, we have that $a_i \geqslant 2q - 2$, therefore $a_i - 1 \geqslant 2q - 3$. Since $r^{a_i - 1} \mid F_q$ and $r \geqslant 2q - 1$, we get the inequality

$$(2q-1)^{2q-3} \leqslant F_q,$$

which is false for all primes $q \geqslant 7$.

This contradiction shows that in this case it is not possible that $r \| m$. Thus, $r^2 \mid m$, and then we can write

$$N = \frac{F_{mq}}{F_m} = \left(\frac{F_{mq/r^2}}{F_{m/r^2}}\right)\left(\frac{F_{mq}/F_{mq/r^2}}{F_m/F_{m/r^2}}\right) = p\square. \tag{3.12}$$

Furthermore, one shows easily that $r^2 \| (F_{mq}/F_{mq/r^2})/(F_m/F_{m/r^2})$ by applying (3.3) twice. Since $r = q_i$ for some $i \in \{1, \ldots, s\}$ and a_i is even, it follows that the exponent of r in the factorization of $F_{mq/r^2}/F_{m/r^2}$ is also even. We now get from equation (3.12) that

$$\text{either} \qquad \frac{F_{mq/r^2}}{F_{m/r^2}} = \square, \qquad \text{or} \qquad \frac{F_{mq}/F_{mq/r^2}}{F_m/F_{m/r^2}} = \square.$$

The first instance is impossible by Theorem 3.1, while the second instance is the conclusion of our lemma for $d := r^2$. Notice that along the way we also saw that this case is possible only when $r \mid F_q$. The lemma is therefore proved. $\square$

Lemma 3.10. *Let q and $d \in \{r, r^2\}$, where q and r are two distinct odd primes. Then the coefficients of the polynomial*

$$f_{q,d}(X) = \frac{(X^{qd}-1)(X-1)}{(X^q-1)(X^d-1)}$$

are in the set $\{0, \pm 1\}$.

Proof. When $d := r$, the given polynomial is $\Phi_{qr}(X)$, where $\Phi_\ell(X)$ stands for the ℓth cyclotomic polynomial, and the fact that all its coefficients are in $\{0, \pm 1\}$ has appeared in many papers (see, for example, [4] and [5]). When $d := r^2$, we have $f_{q,d}(X) = \Phi_{qr}(X)\Phi_{qr^2}(X)$, and the fact that the coefficients of this polynomial are also in $\{0, \pm 1\}$ was proved in Proposition 4 in [3]. □

Lemma 3.11. *The inequality* $m < 2d^3q^2$ *holds.*

Proof. We start with the Diophantine equation (3.8). Recall that if we put $\alpha := (1+\sqrt{5})/2$ and $\beta := (1-\sqrt{5})/2$ for the two roots of the characteristic polynomial $x^2 - x - 1$ of the Fibonacci and Lucas sequences, then the Binet formulas

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{and} \qquad L_n = \alpha^n + \beta^n \qquad \text{hold for all} \qquad n \geqslant 0.$$

Putting $d \in \{r, r^2\}$, Lemma 3.9 tells us that

$$\frac{(\alpha^{mq} - \beta^{mq})(\alpha^{m/d} - \beta^{m/d})}{(\alpha^m - \beta^m)(\alpha^{mq/d} - \beta^{mq/d})} = \square. \tag{3.13}$$

We recognize the expression on the left of (3.13) above as $f^*_{q,d}(\alpha^{m/d}, \beta^{m/d})$, where for a polynomial $P(X)$ we write $P^*(X,Y)$ for its homogenization, and $f_{q,d}(X)$ is the polynomial appearing in Lemma 3.10. It is clear that $f^*_{q,d}(X,Y)$ is monic and symmetric since it is the homogenization of either the cyclotomic polynomial $\Phi_{qr}(X)$, or of the product $\Phi_{qr^2}(X)\Phi_{qr}(X)$, and both these polynomials have the property that they are monic, their last coefficient is 1, and they are reciprocal, meaning that if ζ is a root of one of these polynomials, so is $1/\zeta$. These conditions lead easily to the conclusion that their homogenizations are symmetric. By the fundamental theorem of symmetric polynomials, we have that $f^*_{q,d}(X,Y) = F_{q,d}(X+Y, XY)$ is a monic polynomial with integer coefficients in the basic symmetric polynomials $X+Y$ and XY. Specializing $X := \alpha^{m/d}$, $Y := \beta^{m/d}$, we have that $X + Y = \alpha^{m/d} + \beta^{m/d} = L_{m/d}$, and $XY = (\alpha\beta)^{m/d} = -1$, where the last equality holds because m is odd. Hence, $f^*_{q,d}(\alpha^{m/d}, \beta^{m/d}) = G_{q,d}(L_{m/d})$ is a monic polynomial in $L_{m/d}$. Its degree is obviously $D := (q-1)(d-1)$, which is even. Hence, equation (3.13) can be written as

$$G_{q,d}(x) = y^2, \tag{3.14}$$

where $x := L_{m/d}$, y is an integer, and $G_{q,d}(X)$ is a monic polynomial of even degree D. The finitely many integer solutions (x,y) of this equation can be easily bounded using Runge's method. This has been done in great generality by Gary Walsh [11]. Here is a particular case of Gary Walsh's theorem.

Lemma 3.12. *Let* $F(X) \in \mathbf{Z}[X]$ *be a monic polynomial of even degree without double roots. Then all integer solutions* (x,y) *of the Diophantine equation*

$$F(x) = y^2$$

satisfy

$$|x| < 2^{2D-2}\left(\frac{D}{2}+2\right)^2 (h(F)+2)^{D+2},$$

where $h(F)$ denotes the maximum absolute value of the coefficients of the polynomial $F(X)$.

From Lemma 3.12, we read that all integer solutions (x, y) of the Diophantine equation (3.14) satisfy

$$|x| \leqslant 2^{2D-2}\left(\frac{D}{2}+2\right)^2 (h(G_{q,d})+2)^{D+2}, \tag{3.15}$$

where $h(G_{q,d})$ is the maximum absolute value of all the coefficients of $G_{q,d}(X)$. Theorem 3.12 requires that the polynomial $G_{q,d}(X)$ has only simple roots. Let's prove that this is indeed the case.

Let us take a closer look at how we got $G_{q,d}(X)$ from $f^*_{q,d}(X, Y)$. Note that the roots of $f_{q,d}(X)$ are the roots of unity ζ of order dq, which are neither of order d, nor of order q. Let ζ and η stand for such roots of unity. Then $G_{q,d}(X)$ is obtained from $f_{q,d}(X)$ first by homogenizing, next by replacing Y by $-X^{-1}$, and finally by rewriting the resulting expression as a polynomial in $X + Y = X - X^{-1}$. Thus, $G_{q,d}(X)$ is a polynomial whose roots are $\zeta - \zeta^{-1}$. To see that they are all distinct, note that if $\zeta - \zeta^{-1} = \eta - \eta^{-1}$, then either $\zeta = \eta$, or $\zeta = -1/\eta$. However, the second option is not possible when both ζ and η are roots of unity of odd orders qd (to see why, raise the equality $\zeta = -1/\eta$ to the odd exponent dq to get the contradiction $1 = -1$). Thus, the numbers $\zeta - \zeta^{-1}$ remain distinct when ζ runs through roots of unity of order dq which are neither of order d nor of order q, showing that $G_{d,q}(X)$ has only simple roots, and therefore inequality (3.15) applies in our instance.

It remains to bound $h(G_{q,d})$. For this, let us start with

$$f^*_{q,d}(X, Y) = \sum_{t=0}^{D} c_t X^t Y^{D-t},$$

where $c_t \in \{0, \pm 1\}$ by Lemma 3.10. Since $f^*_{q,d}(X, Y)$ is symmetric, we have $c_t = c_{D-t}$ for all $t = 0, \ldots, D$, therefore

$$f^*_{q,d}(\alpha^{mt/d}, \beta^{mt/d}) = \sum_{\substack{0 \leqslant t \leqslant D \\ t \equiv 0 \pmod 2}} c_t(\alpha^{mt/d} + \beta^{mt/d})(\alpha\beta)^{(D-t)/2}.$$

Now for even t we have

$$\alpha^{mt/d} + \beta^{mt/d} = L_{mt/d} = \sum_{i=0}^{t/2} \frac{t}{t-i}\binom{t-i}{i}(-1)^i L_{m/d}^{t-2i}. \tag{3.16}$$

The knowledgeable reader would recognize the expression on the right as the Dickson polynomial $D_t(Z, -1)$ specialized in $Z := L_{m/d}$. Thus,

$$G_{q,d}(L_{m/d}) = f^*_{q,d}(\alpha^{mt/d}, \beta^{mt/d})$$

$$= \sum_{\substack{0\leqslant t\leqslant D\\ t\equiv 0 \pmod 2}} c_t(-1)^{(D-t)/2}\sum_{i=0}^{t/2}\frac{t}{t-i}\binom{t-i}{i}(-1)^i L_{m/d}^{t-2i},$$

$$= \sum_{\substack{0\leqslant u\leqslant D\\ u\equiv 0 \pmod 2}} b_u L_{m/r}^{u},$$

where

$$b_u := \sum_{\substack{u\leqslant t\leqslant D\\ t\equiv 0 \pmod 2}} c_t(-1)^{(D-t)/2+(t-u)/2}\frac{2t}{t+u}\binom{\frac{t+u}{2}}{\frac{t-u}{2}}. \tag{3.17}$$

Hence,

$$G_{q,d}(X) = \sum_{\substack{0\leqslant u\leqslant D\\ u\equiv 0 \pmod 2}} b_u X^u,$$

where b_u is given by (3.17). Since $|c_t| \leqslant 1$, $2t/(t+u) \leqslant 2$ and $(t+u)/2 \leqslant D$, we get that

$$|b_u| \leqslant 2\sum_{t=0}^{D}\binom{D}{t} = 2^{D+1} \qquad \text{for all} \qquad u = 0, 1, \ldots, D,$$

therefore $h(G_{q,d}) \leqslant 2^{D+1}$. Inserting this into (3.15) and using the fact that $D > q > 4$, therefore $D > D/2 + 2$, we get

$$L_{m/d} \leqslant 2^{2D-2}\left(\frac{D}{2}+2\right)^2 (2^{D+1}+1)^{D+2} < 2^{2D} D^2 2^{(D+2)^2}. \tag{3.18}$$

Since both sides of the inequality (3.18) are integers, we get that

$$L_{m/d} \leqslant 2^{(D+2)^2} 2^{2D} D^2 - 1,$$

and since $L_{m/d} = \alpha^{m/d} + \beta^{m/d} > \alpha^{m/d} - 1$, we get that

$$\alpha^{m/d} < 2^{(D+2)^2} 2^{2D} D^2,$$

which is equivalent to

$$\frac{m}{d} < \left(\frac{\log 2}{\log\alpha}\right)(D+2)^2\left(1 + \frac{2D}{(D+2)^2} + \frac{2\log D}{(D+2)^2\log 2}\right).$$

Since $q \geqslant 7$ and $r \geqslant 3$, we get that $D \geqslant 12$. The functions $D \mapsto D/(D+2)^2$ and $\log D/(D+2)^2$ are decreasing for $D \geqslant 12$, so the expression in parenthesis is

$$\leqslant 1 + \frac{2\times 12}{(12+2)^2} + \frac{2\log 12}{(12+2)^2\log 2} < 1.2.$$

Since $\log 2/\log\alpha < 1.5$, it follows that

$$\frac{m}{d} < 1.5 \times 1.2(D+2)^2 < 2(D+2)^2.$$

Since $D = (q-1)(d-1)$, it follows that $D+2 = qd - q - d + 3 < qd$, so that

$$m < 2d(qd)^2 = 2d^3q^2,$$

which is what we wanted to prove. □

Lemma 3.13. *The number N has at most three distinct prime factors $< 10^{14}$.*

Proof. Assume that this is not so and that N has at least four distinct primes $< 10^{14}$. One of them might be p, but the other three, let's call them r_i for $i = 1, 2, 3$, have the property that $r_i^4 \mid N$ (see Lemma 3.4). A calculation of McIntosh and Roettger [7] showed that the divisibility relation $r \| F_{z(r)}$ holds for all primes $r < 10^{14}$. In particular, $r_i \| F_{z(r_i)}$ for $i = 1, 2, 3$. Since $r_i^4 \mid N$ for $i = 1, 2, 3$, we get that $r_i^3 \mid m$ for $i = 1, 2, 3$. Hence,

$$r_1^3 r_2^2 r_3^3 \leqslant m \leqslant 2d^3q^2 \leqslant 2r^6q^2.$$

Clearly, $r_1 \geqslant r$ and $r_2 \geqslant r$, since r is the smallest prime factor of m, therefore $r_3^3 \leqslant 2q^2$. Since $r_3 \equiv \pm 1 \pmod q$ (see Lemma 6 (i)), we get that $r_3 \geqslant 2q-1$. Thus, we have arrived at the inequality

$$(2q-1)^3 < 2q^2,$$

which is false for any prime $q \geqslant 7$. Thus, the conclusion of the lemma must hold. □

We are now ready to finally show that there is no such N. By Lemma 3.13, it can have at most three prime factors $< 10^{14}$. Since $q \geqslant 7$ and all prime factors of N are congruent to $\pm 1 \pmod q$, it follows that the smallest three such primes are at least 13, 17, and 19, respectively. Thus,

$$2 = \frac{\sigma(N)}{N} < \frac{N}{\phi(N)} \leqslant \left(1 + \frac{1}{12}\right)\left(1 + \frac{1}{16}\right)\left(1 + \frac{1}{18}\right) \prod_{\substack{p \mid N \\ p > 10^{14}}} \left(1 + \frac{1}{p-1}\right),$$

which, after taking logarithms and using the fact that the inequality $\log(1+x) < x$ holds for all positive real numbers x, leads to

$$0.494 < \log(1.64) < \sum_{\substack{p \mid N \\ p > 10^{14}}} \log\left(1 + \frac{1}{p-1}\right) < \sum_{\substack{p \mid N \\ p > 10^{14}}} \frac{1}{p-1}. \tag{3.19}$$

Let's call a prime *good* if $p < z(p)^3$ and *bad* otherwise. We record the following result.

Lemma 3.14. *We have*

$$\sum_{\substack{p>10^{14}\\ p \text{ bad}}} \frac{1}{p-1} < 0.002. \tag{3.20}$$

Proof. Observe first that since $p > 10^{14}$, it follows that $z(p) \geqslant 69$. For a positive number u let $\mathcal{P}_u := \{p \ : \ z(p) = u\}$. Let $u \geqslant 69$ be any integer and put $\ell_u := \#\mathcal{P}_u$. Then, since $p \equiv \pm 1 \pmod u$ for all $p \in \mathcal{P}_u$, we have that

$$(u-1)^{\ell_u} \leqslant \prod_{p \in \mathcal{P}_u} p \leqslant F_u < \alpha^{u-1},$$

therefore

$$\ell_u < \frac{(u-1)\log\alpha}{\log(u-1)}.$$

Thus, for a fixed u, we have

$$\sum_{\substack{p\in\mathcal{P}_u\\ p \text{ bad}}} \frac{1}{p-1} < \frac{\ell_u}{u^3-1} < \frac{\log\alpha}{(u^2+u+1)\log(u-1)} < \frac{\log\alpha}{u^2\log(u-1)},$$

which leads to

$$\sum_{\substack{p>10^{14}\\ p \text{ bad}}} \frac{1}{p-1} < \sum_{u\geqslant 69} \frac{\log\alpha}{u^2\log(u-1)} < \frac{\log\alpha}{\log 68}\sum_{u\geqslant 69}\frac{1}{u^2} < \frac{\log\alpha}{68\log 68} < 0.002.$$

$\square$

Returning to inequality (3.19), we get

$$0.49 < \sum_{\substack{p>10^{14}\\ p \mid N\\ p \text{ good}}} \frac{1}{p-1}. \tag{3.21}$$

The following result is Lemma 8 in [1].

Lemma 3.15. *The estimate*

$$\sum_{p\in\mathcal{P}_u} \frac{1}{p-1} < \frac{12+2\log\log u}{\phi(u)} \qquad \textit{holds for all} \qquad u \geqslant 3. \tag{3.22}$$

Let $\mathcal{U}$ be the set of divisors u of mq of the form $u := z(p)$ for some good prime factor p of N with $p > 10^{14}$. Observe that all elements of $\mathcal{U}$ exceed $10^{14/3} > 46415$. Inserting the estimate (3.22) of Lemma 3.15 into estimate (3.21), we get

$$0.49 < \sum_{u\in\mathcal{U}} \frac{12+2\log\log u}{\phi(u)}. \tag{3.23}$$

Let u_1 be the smallest element in $\mathcal{U}$. We distinguish two cases.

Case 1. $q < r/\sqrt{2}$.

By Lemma 3.11, we have that $m < 2r^6q^2 < r^8$, therefore $\Omega(m) \leqslant 7$, so $\omega(m) \leqslant 7$, and $\tau(m) \leqslant 2^7$. Observe that $\mathcal{U}$ is contained in the set of divisors of qm which are not divisors of m, and this last set has cardinality $\tau(qm) - \tau(m) = \tau(m) \leqslant 2^7$. Here, we used the fact that $\tau(qm) = 2\tau(m)$, which holds because $q \nmid m$ (see Lemma 3.6). Hence, $\#\mathcal{U} \leqslant 2^7$. Furthermore, since $\omega(m) \leqslant 7$, we get that $\omega(qm) \leqslant 8$ and

$$\frac{qm}{\phi(qm)} \leqslant \prod_{i=1}^{8}\left(1 + \frac{1}{p_i - 1}\right) < 5.9,$$

where we used the notation p_i for the ith prime number. Hence, the inequality

$$\frac{1}{\phi(u)} \leqslant \frac{6}{u}$$

holds for all divisors u of mq. Using also the fact that the functions $u \mapsto 1/u$ and $u \mapsto \log\log u/u$ are decreasing for $u \geqslant q \geqslant 7$, we arrive at the conclusion that inequality (3.23) implies

$$\begin{aligned} 0.49 &< \sum_{u\in\mathcal{U}} \frac{12 + 2\log\log u}{\phi(u)} < 6\sum_{u\in\mathcal{U}} \frac{12 + 2\log\log u}{u} \\ &< 6\#\mathcal{U}\left(\frac{12 + 2\log\log u_1}{u_1}\right) \leqslant 6 \times 2^7\left(\frac{12 + 2\log\log u_1}{u_1}\right). \end{aligned}$$

Since $6 \times 2^7 \times 0.49^{-1} < 1600$, we get that

$$u_1 < 1600(12 + 2\log\log u_1). \tag{3.24}$$

Inequality (3.24) yields $u_1 < 27000 < 46415$, which is a contradiction.

Case 2. $q > r/\sqrt{2}$.

Note that in this case we necessarily have $d = r$, for otherwise we would have $d = r^2$, but by Lemma 3.9 this situation occurs only when r is a prime factor of F_q. If this were so, we would get that $r \geqslant 2q-1$, therefore $q > r/\sqrt{2} > (2q-1)/\sqrt{2}$, but this last inequality is not possible for any $q \geqslant 7$. Hence, $d = r$ and $m < 2r^4q^2 < 8q^6$. Since members u of $\mathcal{U}$ are the product between q and some divisor v of m (see Lemma 3.8 (i)), we deduce from inequality (3.23) that

$$0.49 < \frac{12 + 2\log\log(8q^7)}{q - 1}\sum_{v|m}\frac{1}{\phi(v)}. \tag{3.25}$$

It is easy to prove that the inequality

$$\sum_{v|\ell}\frac{1}{\phi(v)} < \frac{\zeta(2)\zeta(3)}{\zeta(6)}\frac{\ell}{\phi(\ell)} \qquad \text{holds for all positive integers} \quad \ell. \tag{3.26}$$

Inserting inequality (3.26) for $\ell := m$ into inequality (3.25), we get that

$$q - 1 < \left(\frac{\zeta(2)\zeta(3)}{\zeta(6)\cdot 0.49}\right)\left(12 + 2\log\log(8q^7)\right)\frac{m}{\phi(m)}. \tag{3.27}$$

The constant in parenthesis in the right hand side of inequality (3.27) above is < 4. Furthermore, Theorem 15 in [10] says that the inequality

$$\frac{\ell}{\phi(\ell)} < 1.8\log\log\ell + 2.51/\log\log\ell \qquad \text{holds for all} \quad \ell \geqslant 3. \tag{3.28}$$

The function $\ell \mapsto 1.8\log\log\ell + 2.51/\log\log\ell$ is increasing for $\ell \geqslant 26$, and since $m < 8q^6$, we get, by inserting inequality (3.28) with $\ell := m$ into inequality (3.27), that the inequality

$$q - 1 < 4\left(12 + 2\log\log(8q^7)\right)\left(1.8\log\log(8q^6) + 2.51/\log\log(8q^6)\right), \tag{3.29}$$

holds whenever $m \geqslant 26$. Inequality (3.29) yields $q \leqslant 577$. This was if $m \geqslant 26$. On the other hand, if $m < 26$, then $m/\phi(m) \leqslant 15/8 < 2$, so we get

$$q - 1 < 8\left(12 + 2\log\log(8q^7)\right),$$

which yields $q \leqslant 151$. So, we always have $q \leqslant 577$.

Let us now get the final contradiction. The factorizations of all Fibonacci numbers F_ℓ with $\ell \leqslant 1000$ are known. A quick look at this table convinces us that F_q is square-free for all primes $q \leqslant 577$.

If F_q is prime, then $F_q \neq p$ by Lemma 3.8 (v). Furthermore, by Lemma 6 (iv), putting $q_i = F_q$ for some $i = 1, \ldots, s$, we get that $q_i \equiv 1 \pmod q$, therefore $a_i \geqslant 2q - 2$. So q_i^{2q-3} divides m, leading to

$$(2q-1)^{2q-3} \leqslant q_i^{2q-3} \leqslant m \leqslant 8q^6, \tag{3.30}$$

and this last inequality is false for any $q \geqslant 7$.

If F_q is divisible by at least three primes, it follows that at least two of them, let's call them q_i and q_j, are not p. By Lemma 3.4, we get that q_i^3 and q_j^3 divide m. Thus,

$$(2q-1)^6 \leqslant q_i^3 q_j^3 \leqslant m \leqslant 8q^6, \tag{3.31}$$

and again this last inequality is again false for any $q \geqslant 7$.

Finally, if F_q has precisely two prime factors, then either both of them are distinct from p, and then we get a contradiction as in (3.31), or $F_q = pq_i$ for some $i \in \{1, \ldots, s\}$. But in this case, by Lemma 3.8 (ii) and (iv), we get that $q_i \equiv 1 \pmod 5$, therefore $q_i \equiv 1 \pmod q$, so q_i^{2q-3} divides m by Lemma 3.8 (iii), and we get a contradiction as in (3.30).

This completes the proof of our main result.

References

[1] Broughan, K. A., González, M., Lewis, R., Luca, F., Mejía Huguet, V. J., Togbé, A., There are no multiply perfect Fibonacci numbers, *INTEGERS*, to appear.

[2] Carmichael, R. D., On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. Math. (2),* 15 (1913), 3–70.

[3] Kaplan, N., Bounds on the maximal height of divisors of $x^n - 1$, *J. Number Theory,* 129 (2009), 2673–2688.

[4] Lam, T. Y., Leung, K. H., On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly,* 103 (1996) 562–564.

[5] Lenstra, H. W., Vanishing sums of roots of unity, *Proceedings, Bicentennial Congress Wiskundig Genootschap (Vrije Univ., Amsterdam, 1978),* Part II, (1979) 249–268.

[6] Luca, F., Perfect Fibonacci and Lucas numbers, *Rend. Circ. Mat. Palermo (2),* 49 (2000), 313–318.

[7] McIntosh, R., Roettger, E. L., A search for Fibonacci-Wieferich and Wolstenholme primes, *Math. Comp.,* 76 (2007), 2087–2094.

[8] Phong, B. M., Perfect numbers concerning the Fibonacci sequence, *Acta Acad. Paed. Agriensis, Sectio Math.,* 26 (1999), 3–8.

[9] Ribenboim, P., Square-classes of Fibonacci and Lucas numbers, *Portugaliae Math.,* 46 (1989), 159–175.

[10] Rosser, J. B., Schoenfeld, L., Approximate formulas for some functions of prime numbers, *Illinois J. Math.,* 6 (1962), 64–94.

[11] Walsh, P. G., A quantitative version of Runge's theorem on Diophantine equations, *Acta Arith.,* 62 (1992), 157–172; 'Correction to: A quantitative version of Runge's theorem on Diophantine equations', *Acta Arith.,* 73 (1995), 397–398.

Florian Luca
C. P. 58089, Morelia Michoacán, México
e-mail: `fluca@matmor.unam.mx`

V. Janitzio Mejía Huguet
Av. San Pablo # 180
Col. Reynosa Tamaulipas
Azcapozalco, 02200, México DF, México
e-mail: `vjanitzio@gmail.com`