#A8 INTEGERS 12B (2012/13): Integers Conference 2011 Proceedings

ON THE MULTIPLICATIVE ORDER OF F_{N+1}/F_N MODULO F_M

Takao Komatsu[1]
Graduate School of Science and Technology, Hirosaki University, Hirosaki, Japan
komatsu@cc.hirosaki-u.ac.jp

Florian Luca[2]
Fundación Marcos Moshinsky, UNAM, Circuito Exterior, C.U., Apdo. Postal 70-543, México D.F. 04510, México
fluca@matmor.unam.mx

Yohei Tachiya
Graduate School of Science and Technology, Hirosaki University, Hirosaki, Japan
tachiya@cc.hirosaki-u.ac.jp

Received: 3/8/12, Accepted: 2/18/13, Published: 3/1/13

Abstract

Here, we show that if $s \notin \{1, 2, 4\}$ is a fixed positive integer and m and n are coprime positive integers such that the multiplicative order of F_{n+1}/F_n modulo F_m is s, where F_k is the kth Fibonacci number, then $m < 500s^2$.

1. Introduction

Let $\{F_k\}_{k\geq 0}$ be the Fibonacci sequence given by $F_0 = 0,\ F_1 = 1$ and

$$F_{k+2} = F_{k+1} + F_k \quad \text{for all} \quad k \geq 0.$$

Let $m \geq 3$ and n be positive integers such that F_m and F_n are coprime. Since $\gcd(F_m, F_n) = F_{\gcd(m,n)}$, this last property holds when $\gcd(m, n) \in \{1, 2\}$. Then F_n is invertible modulo F_m. Assuming also that F_{n+1} is coprime to F_m, we can think of the rational number F_{n+1}/F_n as an invertible element modulo F_m. Here, we look at its order denoted by s. Formally, s depends on both m and n, but we shall omit this dependence in what follows.

[1]T. K. was supported in part by the Grant-in-Aid for Scientific research (C) (No.22540005), the Japan Society for the Promotion of Science.

[2]F. L. worked on this project during a visit to Hirosaki in January and February of 2012 with a JSPS Fellowship (No.S-11021).

It is quite possible that this order is $s = 1$. Indeed, this happens precisely when $F_{n+1} \equiv F_n \pmod{F_m}$, so $F_m \mid F_{n+1} - F_n = F_{n-1}$, and this holds when $m \mid n-1$. Hence, when $n \equiv 1 \pmod{m}$.

It is also possible that $s = 2$. In this case, $F_{n+1}^2 \equiv F_n^2 \pmod{F_m}$, so

$$F_m \mid F_{n+1}^2 - F_n^2 = (F_{n+1} - F_n)(F_{n+1} + F_n) = F_{n-1}F_{n+2}.$$

Assume that $m > 12$. Then, by Carmichael's Primitive Divisor Theorem (see [1]), F_m has a primitive prime factor p. This primitive prime has the property that $p \mid F_m$ but $p \nmid F_\ell$ for any positive integer $1 \le \ell < m$. Furthermore, $p \mid F_\ell$ if and only if $m \mid \ell$. From the above divisibilities, we see that either $p \mid F_{n-1}$, case in which $m \mid n-1$, or $p \mid F_{n+2}$, case in which $m \mid n+2$. The situation when $m \mid n-1$ leads to $s = 1$ and this is not convenient, so we must have $m \mid n+2$. Thus, $n \equiv -2 \pmod{m}$.

It is also possible that $s = 4$. In this case, $F_{n+1}^4 \equiv F_n^4 \pmod{F_m}$, so

$$F_m \mid F_{n+1}^4 - F_n^4 = (F_{n+1} - F_n)(F_{n+1} + F_n)(F_{n+1}^2 + F_n^2) = F_{n-1}F_{n+2}F_{2n+1}.$$

If $m > 12$, then F_m has a primitive prime factor p. Since p divides the right–hand side of the above divisibility relation, we get that m divides one of $n-1,\ n+2$ or $2n+1$. The first two cases lead to $s \in \{1, 2\}$. The third case is possible only when m is odd and $n \equiv (m-1)/2 \pmod{m}$.

From the above discussion, we see that for each of $s \in \{1, 2, 4\}$, there exist infinitely many positive integers m such that the set of invertible residue classes modulo F_m contains a class representable as F_{n+1}/F_n for some appropriate positive integer n whose multiplicative order is s. We asked ourselves if this property holds for some other positive integers s. Maybe quite surprisingly, the answer is no.

Our main result is the following.

Theorem 1. *If $s \notin \{1, 2, 4\}$ is a positive integer and m is such that there exists an invertible class modulo F_m of the form F_{n+1}/F_n of multiplicative order s, then $m < 500s^2$.*

For an algebraic number field $\mathbb{K}$ we put $\mathcal{O}_{\mathbb{K}}$ for the ring of algebraic integers in $\mathbb{K}$.

2. Preliminary Results

We need the following four lemmas.

Lemma 1. *Let $X \ge 3$ be a real number. Let a and b be positive integers with $\max\{a, b\} \le X$. Then there exist integers u, v not both zero with $\max\{|u|, |v|\} \le \sqrt{X}$ such that $|au + bv| \le 3\sqrt{X}$.*

Proof. Consider the nonnegative numbers $as+bt$ for $s,\ t \in \{0, 1, \ldots, \lfloor \sqrt{X} \rfloor\}$. There are $(\lfloor \sqrt{X} \rfloor + 1)^2 > X$ such numbers all in $[0, 2X\sqrt{X}]$. By the Pigeon Hole Principle, there exist $(s_1, t_1) \neq (s_2, t_2)$ such that

$$|a(s_1 - s_2) + b(t_1 - t_2)| = |(as_1 + bt_1) - (as_2 + bt_2)| \leq \frac{2X\sqrt{X}}{X - 1} \leq 3\sqrt{X}.$$

Putting $u = s_1 - s_2$ and $v = t_1 - t_2$, we get the desired conclusion. □

We put $\alpha = (1 + \sqrt{5})/2$ and $\beta = -\alpha^{-1}$.

Lemma 2. *Let $\zeta = e^{2\pi i u/v}$ with coprime positive integers u and v be a primitive root of unity of order v. If $v \notin \{1, 2, 4\}$, then the two numbers*

$$\alpha \quad \textit{and} \quad \frac{\alpha - \zeta}{\alpha + \overline{\zeta}}$$

are multiplicatively independent.

Proof. Assume on the contrary that there exist integers m and n not both zero such that

$$\left(\frac{\alpha - \zeta}{\alpha + \overline{\zeta}} \right)^m = \alpha^n. \tag{1}$$

If $m = 0$, then $\alpha^n = 1$, therefore $n = 0$, which is impossible. So, we assume that $m \neq 0$. Up to replacing the pair (m, n) by $(-m, -n)$, we may assume that $m > 0$. Assume first that v is coprime to 5. Then $\alpha \in \mathbb{K} = \mathbb{Q}(e^{2\pi i/5})$ and $\zeta \in \mathbb{L} = \mathbb{Q}(e^{2\pi i/v})$ and $\mathbb{K}$ and $\mathbb{L}$ are both Galois extensions of $\mathbb{Q}$ whose intersection is trivial (i.e., equal to $\mathbb{Q}$). Thus, every Galois automorphism σ of $G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ can be extended to a Galois automorphism of the compositum $\mathbb{M} = \mathbb{K}\mathbb{L} = \mathbb{Q}(e^{2\pi i/5v})$ of $\mathbb{K}$ and $\mathbb{L}$ in such a way that $\sigma(\alpha) = \alpha$. Applying an arbitrary such $\sigma \in G$ to (1), we deduce that equation (1) holds when we replace ζ by any conjugate of it. In particular, given $u_1, u_2 \in \{1, \ldots, v\}$ both coprime to v, we have

$$\left(\frac{\alpha - e^{2\pi i u_1/v}}{\alpha + e^{-2\pi i u_1/v}} \right)^m = \alpha^n = \left(\frac{\alpha - 2e^{2\pi i u_2/v}}{\alpha + e^{-2\pi i u_2/v}} \right)^m. \tag{2}$$

Taking absolute values in (2) and then extracting mth roots, we get

$$\begin{aligned}
-1 + \frac{2\alpha^2 + 2}{\alpha^2 + 2\alpha\cos(2\pi u_1/v) + 1} &= \frac{\alpha^2 - 2\alpha\cos(2\pi u_1/v) + 1}{\alpha^2 + 2\alpha\cos(2\pi u_1/v) + 1} \\
&= \left| \frac{\alpha - e^{2\pi i u_1/v}}{\alpha + e^{-2\pi i u_1/v}} \right|^2 = \left| \frac{\alpha - e^{2\pi i u_2/v}}{\alpha + e^{-2\pi i u_2/v}} \right|^2 \\
&= \frac{\alpha^2 - 2\alpha\cos(2\pi u_2/v) + 1}{\alpha^2 + 2\alpha\cos(2\pi u_2/v) + 1} \\
&= -1 + \frac{2\alpha^2 + 2}{\alpha^2 + 2\alpha\cos(2\pi u_2/v) + 1},
\end{aligned}$$

giving

$$\cos(2\pi u_1/v) = \cos(2\pi u_2/v).$$

This gives

$$\begin{aligned}\sin(2\pi u_1/v) &= \pm\sqrt{1-\cos(2\pi u_1/v)^2} = \pm\sqrt{1-\cos(2\pi u_2/v)^2}\\ &= \pm\sin(2\pi u_2/v).\end{aligned}$$

This argument shows that there exist at most 2 primitive roots of unity of order v, therefore $\phi(v) \le 2$, and since $v \notin \{1, 2, 4\}$, we get that $v \in \{3, 6\}$. Let us look at these cases. In this instance, $\mathbb{M} = \mathbb{Q}(\sqrt{5}, i\sqrt{3})$ is of degree 4 over $\mathbb{Q}$. We compute

$$\frac{\alpha-\zeta}{\alpha+\overline{\zeta}} \in \left\{ \left(\frac{2+\sqrt{5}+\varepsilon i\sqrt{3}}{\sqrt{5}+\varepsilon i\sqrt{3}} \right)^{\pm 1} : \varepsilon \in \{\pm 1\} \right\}.$$

Since α is a unit, equation (1) tells us that the principal ideals in $\mathcal{O}_{\mathbb{M}}$ given by $(\sqrt{5}+\varepsilon i\sqrt{3})^m\mathcal{O}_{\mathbb{M}}$ and $(2+\sqrt{5}+\varepsilon i\sqrt{3})^m\mathcal{O}_{\mathbb{M}}$ are equal for some $\varepsilon \in \{\pm 1\}$. By unique factorization of ideals in $\mathcal{O}_{\mathbb{M}}$, we get that

$$(\sqrt{5}+\varepsilon i\sqrt{3})\mathcal{O}_{\mathbb{M}} = (2+\sqrt{5}+\varepsilon i\sqrt{3})\mathcal{O}_{\mathbb{M}}.$$

In particular, we deduce that $\sqrt{5}+\varepsilon i\sqrt{3} \mid 2$. Taking norms in this last divisibility relation, we get that

$$64 = |N_{\mathbb{M}/\mathbb{Q}}(\sqrt{5}+\varepsilon i\sqrt{3})| \mid |N_{\mathbb{M}/\mathbb{Q}}(2)| = 16,$$

which is false.

A similar argument applies when $5 \mid v$. In this case $\mathbb{K} = \mathbb{Q}(e^{2\pi i/5}) \subseteq \mathbb{L}$, so $\mathbb{M} = \mathbb{L}$ and $G = \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ is isomorphic with the group of invertible elements modulo v which has order $\phi(v)$. Further, by Galois theory, there are exactly $\phi(v)/2$ Galois automorphisms σ such that $\sigma(\alpha) = \alpha$. We deduce that there exists a subset $\mathcal{U} \subset \{1, 2, \ldots, v\}$ of positive integers coprime to v having exactly $\phi(v)/2$ elements, such that equation (1) holds for all $\zeta = e^{2\pi i u/v}$ with all $u \in \mathcal{U}$. The preceding argument shows that

$$\cos(2\pi u_1/v) = \cos(2\pi u_2/v) \quad \text{holds for all} \quad u_1, u_2 \in \mathcal{U},$$

therefore

$$\sin(2\pi u_1/v) = \pm\sin(2\pi u_2/v) \quad \text{holds for all} \quad u_1, u_2 \in \mathcal{U}.$$

This shows that the number of elements in $\mathcal{U}$ is at most 2, so $\phi(v) \le 4$. Since we already have that $5 \mid v$, we get that $v \in \{5, 10\}$. We calculated that all numbers of the form

$$\frac{\alpha-\zeta}{\alpha+\overline{\zeta}},$$

when ζ is a primitive root of unity of order $v \in \{5, 10\}$, are algebraic numbers in $\mathbb{M} = \mathbb{Q}(e^{2\pi i/5})$ of norm $11^{\pm 1}$, and therefore equation (1) does not hold in this instance either for any pair of integers m, n with not both zero. $\square$

Lemma 3. *Let $\zeta = e^{2\pi i u/v}$, where $v \neq 4$ is a positive integer and $u \in \{1, 2, \ldots, v\}$ is coprime to v. Then the divisibility relation $1 + \zeta^2 \mid 2v$ holds in $\mathcal{O}_{\mathbb{K}}$, where $\mathbb{K}$ is any number field containing $\mathbb{Q}(\zeta)$.*

Proof. We distinguish four cases. For a positive integer m we put $\Phi_m(X)$ for the mth cyclotomic polynomial.

- If v is odd, then ζ^2 is also a primitive root of order v of unity, so

$$1 + \zeta^2 \mid \Phi_v(-1) \mid X^v - 1\Big|_{X=-1} = -2.$$

- If $2 \mid v$ and $v/2$ is odd, then ζ^2 is a primitive root of unity of order $v/2$ and

$$1 + \zeta^2 \mid \Phi_{v/2}(-1) \mid X^{v/2} - 1\Big|_{X=-1} = -2.$$

- If $4 \mid v$ and $v/4$ is odd, then, since $v/4 > 1$, it follows that $(X^{v/4} - 1)$ and $(X + 1)$ are proper divisors of $X^{v/2} - 1$ and they do not have any common roots. Thus,

$$\begin{aligned} 1 + \zeta^2 \quad &\mid \quad \Phi_{v/2}(-1) \mid \frac{X^{v/2} - 1}{(X^{v/4} - 1)(X + 1)}\Big|_{X=-1} = \frac{X^{v/4} + 1}{X + 1}\Big|_{X=-1} \\ &= \quad X^{v/4-1} - X^{v/4-2} + \cdots + 1\Big|_{X=-1} = v/4. \end{aligned}$$

- If $8 \mid v$, then

$$1 + \zeta^2 \mid \Phi_{v/2}(-1) \mid \frac{X^{v/2} - 1}{X^{v/4} - 1}\Big|_{X=-1} = X^{v/4} + 1\Big|_{X=-1} = 2.$$

$\square$

For a prime number p and a nonzero integer m, we put $\nu_p(m)$ for the exponent of the prime p in the factorization of m. For a finite set of primes $\mathcal{S}$ and a positive integer m, we put

$$m_{\mathcal{S}} = \prod_{p \in \mathcal{S}} p^{\nu_p(m)}$$

for the largest divisor of m whose prime factors are in $\mathcal{S}$.

Lemma 4. *If $\mathcal{S}$ is any finite set of primes and m is a positive integer, then*

$$(F_m)_{\mathcal{S}} \leq 2m \prod_{p \in \mathcal{S}} F_{p+1}.$$

Proof. For a prime p, let f_p be its order of appearance in the Fibonacci sequence, which is the minimal positive integer k such that $p \mid F_k$. It is well-known that

$$\nu_p(F_m) = \begin{cases} 0 & \text{if} \quad m \not\equiv 0 \pmod{f_p}; \\ \nu_p(F_{f_p}) + \nu_p(m/f_p) & \text{if} \quad m \equiv 0 \pmod{f_p}, \quad p \text{ is odd}; \\ 1 & \text{if} \quad m \equiv 3 \pmod{6}, \quad p = 2; \\ 2 + \nu_2(m) & \text{if} \quad m \equiv 0 \pmod{6}, \quad p = 2. \end{cases}$$

In particular, the inequality

$$\nu_p(F_m) \le \nu_p(F_{f_p}) + \nu_p(m) + \delta_{p,2}$$

always holds with $\delta_{p,2}$ being 0 if p is odd and 1 if $p = 2$. Since $f_p \le p + 1$ holds for all primes p, we get that

$$\begin{aligned} (F_m)_{\mathcal{S}} &\le \left(\prod_{p \in \mathcal{S}} p^{\nu_p(F_{f_p})} \right) \left(\prod_{\substack{p \mid m \\ p > 2}} p^{\nu_p(m)} \right) 2^{\nu_2(m)+1} \\ &\le 2m \prod_{p \in \mathcal{S}} F_{f_p} \le 2m \prod_{p \in \mathcal{S}} F_{p+1}, \end{aligned}$$

which is what we wanted to prove. $\square$

3. Proof of Theorem 1

We use the Binet formula

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{valid for all} \quad n \ge 0. \tag{3}$$

We also use the inequalities

$$\alpha^{n-2} \le F_n \le \alpha^{n-1} \quad \text{valid for all} \quad n \ge 1. \tag{4}$$

We also use the fact that if $m \ge 1$, then the sequence $\{F_k\}_{k \ge 0}$ is periodic modulo F_m with period $4m$. Assume now that $s \ne \{1, 2, 4\}$ is a positive integer and that $m > 1000$ is such that there exist n with F_n coprime to F_m and F_{n+1}/F_n is invertible modulo F_m of multiplicative order exactly s. From the periodicity of $\{F_k\}_{k \ge 0}$ modulo F_m, we may assume that $n \le 4m$, and since $F_n F_{n+1}$ and F_m are coprime, we may assume that $n \le 4m - 2$. We shall exploit the relation

$$F_m \mid F_{n+1}^s - F_n^s = \prod_{\zeta : \zeta^s = 1} (F_{n+1} - \zeta F_n). \tag{5}$$

We split F_m into various factors.

Step 1. *We put*

$$\begin{aligned} A &= \gcd(F_m, F_{n+1} - F_n), \\ B &= \gcd(F_m, F_{n+1} + F_n), \\ C &= \gcd(F_m, F_{n+1}^2 + F_n^2), \end{aligned}$$

and we bound ABC.

Then,

$$\begin{array}{rclclcrcl} A &=& \gcd(F_m, F_{n-1}) &=& F_{d_1}, & \text{where} & d_1 &=& \gcd(m, n-1); \\ B &=& \gcd(F_m, F_{n+2}) &=& F_{d_2}, & \text{where} & d_2 &=& \gcd(m, n+2); \\ C &=& \gcd(F_m, F_{2n+1}) &=& F_{d_3}, & \text{where} & d_3 &=& \gcd(m, 2n+1). \end{array}$$

The numbers $d_1,\ d_2,\ d_3$ are divisors of m and they are proper, since if $d_i = m$ for some $i \in \{1, 2, 3\}$, then, from what we have seen in the Introduction, we would get that $s \in \{1, 2, 4\}$, which is not the case. Observe that any two of $d_1,\ d_2,\ d_3$ are coprime, or the greatest common divisors of any two of them is exactly 3. The second condition holds precisely when $m \equiv 0 \pmod 3$ and $n \equiv 1 \pmod 3$. Indeed, this holds because

$$\begin{aligned} \gcd(d_1, d_2) &= \gcd(m, n-1, n+2) = \gcd(m, n-1, 3); \\ \gcd(d_1, d_3) &= \gcd(m, n-1, 2n+1) = \gcd(m, n-1, 3); \\ \gcd(d_2, d_3) &= \gcd(m, n+2, 2n+1) = \gcd(m, n+2, 3) = \gcd(m, n-1, 3). \end{aligned}$$

Let $i \in \{1, 2, 3\}$ be such that $d_i = \max\{d_1, d_2, d_3\}$ and let $j,\ k$ be indices such that $\{i, j, k\} = \{1, 2, 3\}$. Noting that since d_i is a proper divisor of m, we have $d_i \le m/2$. When any two of d_1, d_2, d_3 are coprime, we then have that

$$d_1 d_2 d_3 \le m, \quad \text{therefore} \quad d_j d_k \le m^{2/3}. \tag{6}$$

When the greatest common divisor of any two of the numbers d_1, d_2, d_3 is exactly 3, we get

$$\left(\frac{d_1}{3}\right)\left(\frac{d_2}{3}\right)\left(\frac{d_3}{3}\right) \le \frac{m}{3}, \quad \text{therefore} \quad \left(\frac{d_j}{3}\right)\left(\frac{d_k}{3}\right) \le \left(\frac{m}{3}\right)^{2/3},$$

leading to the slightly worse bound than (6), namely

$$d_j d_k \le 3^{4/3} m^{2/3}. \tag{7}$$

Thus, using (4), we get that

$$ABC = F_{d_1} F_{d_2} F_{d_3} \le \alpha^{d_1+d_2+d_3-3} \le \alpha^{m/2+d_j+d_k-3} \le \alpha^{m/2+3^{4/3}m^{2/3}-2}, \tag{8}$$

where we used also the fact that the inequality $a+b \leq ab+1$ is valid for all positive integers a and b with $a = d_j$ and $b = d_k$.

`Step 2.` *We put* $\mathcal{S} = \{2\} \cup \{p : p \mid s\}$ *and* $D = (F_m)_{\mathcal{S}}$*, and bound* D*.*

By Lemma 4 and inequalities (4), we have that

$$D \leq 2mF_3 \prod_{p \mid s} F_{p+1} < 4m\alpha^{\sum_{p \mid s} p} < \alpha^{s+\log(4m)/\log\alpha}, \tag{9}$$

where we used the fact that $\sum_{p \mid s} p \leq s$, which is easily proved by induction on the number of distinct prime factors of s.

`Step 3.` *We put*

$$E = \frac{F_m}{\gcd(ABCD, F_m)},$$

and bound E*.*

We shall estimate the number E by using the fact that E is coprime to $2s$, as well as divisibility (5), which in particular tell us that

$$F_m \mid ABC \prod_{\substack{\zeta : \zeta^s = 1 \\ \zeta \notin \{\pm 1, \pm i\}}} (F_{n+1} - \zeta F_n),$$

which shows that

$$E \mid \prod_{\substack{\zeta : \zeta^s = 1 \\ \zeta \notin \{\pm 1, \pm i\}}} (F_{n+1} - \zeta F_n). \tag{10}$$

Let $\mathbb{K} = \mathbb{Q}(e^{2\pi i/s}, \sqrt{5})$, which is a number field of degree d equal to $\phi(s)$ or to $2\phi(s)$, according to whether s is a multiple of 5 or not. Assume that there are ℓ roots of unity ζ participating in the product appearing in the right–hand side of (10) and label them $\zeta_1, \ldots, \zeta_\ell$. Clearly, $\ell \in [s-4, s-1]$. Write

$$\mathcal{E}_i = \gcd(E, F_{n+1} - \zeta_i F_n) \quad \text{for all} \quad i = 1, \ldots, \ell, \tag{11}$$

where $\mathcal{E}_i$ are ideals in $\mathcal{O}_{\mathbb{K}}$. Then relations (10) and (11) tell us that

$$E\mathcal{O}_{\mathbb{K}} \mid \prod_{i=1}^{\ell} \mathcal{E}_i. \tag{12}$$

Our next goal is to bound the norm $N_{\mathbb{K}/\mathbb{Q}}(\mathcal{E}_i)$ of $\mathcal{E}_i$ for $i = 1, \ldots, \ell$. First of all, $F_m \in \mathcal{E}_i$. Thus, with formula (3) and the fact that $\beta = -\alpha^{-1}$, we get

$$\alpha^m \equiv (-1)^m \alpha^{-m} \pmod{\mathcal{E}_i}.$$

Multiplying the above congruence by α^m, we get

$$\alpha^{2m} \equiv (-1)^m \pmod{\mathcal{E}_i}. \tag{13}$$

We next use formulae (3) and (11) to deduce that

$$(\alpha^{n+1} - (-1)^{n+1}\alpha^{-n-1}) - \zeta(\alpha^n - (-1)^n\alpha^{-n}) \equiv 0 \pmod{\mathcal{E}_i}, \quad (\zeta = \zeta_i).$$

Multiplying both sides above by α^n, we get

$$\alpha^{2n}(\alpha - \zeta) - (-1)^{n+1}(\alpha^{-1} + \zeta) \equiv 0 \pmod{\mathcal{E}_i}. \tag{14}$$

Let us show that $\alpha - \zeta$ and $\mathcal{E}_i$ are coprime. Assume this is not so and let π be some prime ideal of $\mathcal{O}_{\mathbb{K}}$ dividing both $\alpha - \zeta$ and $\mathcal{E}_i$. Then we get $\alpha \equiv \zeta \pmod{\pi}$ and so $\alpha^{-1} \equiv -\zeta \pmod{\pi}$ by (14). Multiplying these two congruences we get $1 \equiv -\zeta^2 \pmod{\pi}$. Hence, $\pi \mid 1 + \zeta^2$, so by Lemma 3, we get that $\pi \mid 2s$. However, this contradicts the fact that $\pi \mid \mathcal{E}_i \mid E$, with E an integer coprime to $2s$. Thus, indeed $\alpha - \zeta$ and $\mathcal{E}_i$ are coprime, so $\alpha - \zeta$ is invertible modulo $\mathcal{E}_i$. Now congruence (14) shows that

$$\alpha^{2n} \equiv (-1)^{n+1}\frac{\alpha^{-1} + \zeta}{\alpha - \zeta} \pmod{\mathcal{E}_i},$$

therefore

$$\alpha^{2n+1} \equiv (-1)^{n+1}\zeta\left(\frac{\alpha + \overline{\zeta}}{\alpha - \zeta}\right) \pmod{\mathcal{E}_i}. \tag{15}$$

We now apply Lemma 1 to $a = 2m$ and $b = 2n + 1 \le 2(4m - 2) + 1 < 8m$ with the choice $X = 8m$ to deduce that there exist integers u, v not both zero with $\max\{|u|, |v|\} \le \sqrt{X}$ such that $|2mu + (2n+1)v| \le 3\sqrt{X}$. We raise congruence (13) to u and congruence (15) to v and multiply the resulting congruences getting

$$\alpha^{2mu+(2n+1)v} = (-1)^{mu+(n+1)v}\zeta^v\left(\frac{\alpha + \overline{\zeta}}{\alpha - \zeta}\right)^v \pmod{\mathcal{E}_i}.$$

We record this as

$$\alpha^a \equiv \eta\left(\frac{\alpha + \overline{\delta}}{\alpha - \delta}\right)^b \pmod{\mathcal{E}_i} \tag{16}$$

for suitable roots of unity η and δ of order dividing $2s$ with δ not of order $1, 2$ or 4, where $a = 2mu + (2n + 1)v$ and $b = v$. We may assume that $a \ge 0$, for if not, we replace the pair (u, v) by the pair $(-u, -v)$, thus replacing (a, b) by $(-a, -b)$ and η by η^{-1} and leaving δ unaffected. We may additionally assume that $b \ge 0$, for if not, we replace b by $-b$ and $\delta = \zeta$ by $\delta = -\overline{\zeta}$, again a root of unity of order dividing $2s$ but not of order $1, 2$ or 4, and leave a and η unaffected. Thus, $\mathcal{E}_i$ divides the algebraic integer

$$E_i = \alpha^a(\alpha - \delta_i)^b - \eta_i(\alpha + \overline{\delta_i})^b, \tag{17}$$

where $\delta_i \in \{\zeta_i, -\overline{\zeta_i}\}$ and η_i is some suitable root of unity of order dividing $2s$. Let us show that $E_i \neq 0$. If $E_i = 0$, we then get

$$\alpha^a = \eta_i \left(\frac{\alpha + \overline{\delta_i}}{\alpha - \delta_i} \right)^b,$$

and after raising both sides of the above equality to the power $2s$, we get, since $\eta_i^{2s} = 1$, that

$$\alpha^{2sa} = \left(\frac{\alpha + \overline{\delta_i}}{\alpha - \delta_i} \right)^{2bs}.$$

By Lemma 2, we have that $as = bs = 0$, so $a = b = 0$. Since $b = 0$, we get that $v = 0$, and later since $2mu + (2n+1)v = a = 0$ and $v = 0$, we get $mu = 0$, so $u = 0$, therefore $u = v = 0$, but this is not allowed. We now bound the absolute values of the conjugates of E_i. We find it more convenient to work with the associate of E_i given by

$$G_i = \alpha^{-\lfloor a/2 \rfloor} E_i = \alpha^{a - \lfloor a/2 \rfloor} (\alpha - \delta_i)^b - \alpha^{-\lfloor a/2 \rfloor} \eta_i (\alpha + \overline{\delta_i})^b.$$

Note that

$$a \leq |2m + (2n+1)v| \leq 3\sqrt{X} = 6\sqrt{2m}, \quad \text{and} \quad b = |v| \leq \sqrt{X} = 2\sqrt{2m}.$$

Let σ be an arbitrary element of $G = \text{Gal}(\mathbb{K}/\mathbb{Q})$. We then have that $\sigma(\eta_i) = \eta_i'$, $\sigma(\delta_i) = \delta_i'$, where η_i' and δ_i' are roots of unity of order dividing $2s$. Furthermore, $\sigma(\alpha) \in \{\alpha, \beta\}$. If $\sigma(\alpha) = \alpha$, we then get

$$\begin{aligned} |\sigma(G_i)| &= |\alpha^{a-\lfloor a/2 \rfloor} (\alpha - \delta_i')^b - \eta_i' \alpha^{-\lfloor a/2 \rfloor} (\alpha + \overline{\delta_i'})^b| \\ &\leq \alpha^{(a+1)/2} (\alpha + 1)^b + (\alpha + 1)^b \\ &\leq 2\alpha^{(a+1)/2} (\alpha + 1)^b \leq (2\sqrt{\alpha}) \alpha^{3\sqrt{2m}} \times (\alpha^2)^{2\sqrt{2m}} \\ &= (2\sqrt{\alpha}) \alpha^{7\sqrt{2m}}, \end{aligned} \tag{18}$$

while if $\sigma(\alpha) = \beta$, we also get

$$\begin{aligned} |\sigma(G_i)| &= |\beta^{a-\lfloor a/2 \rfloor} (\beta - \delta_i')^b - \beta^{-\lfloor a/2 \rfloor} \eta_i' (\beta + \overline{\delta_i'})^b| \\ &\leq (\alpha^{-1} + 1)^b + \alpha^{a/2} (\alpha^{-1} + 1)^b \\ &= \alpha^b + \alpha^{a/2+b} \leq 2\alpha^{3\sqrt{2m}} \alpha^{2\sqrt{2m}} \\ &= 2\alpha^{5\sqrt{2m}}. \end{aligned}$$

In conclusion, inequality (18) holds for all $\sigma \in G$. Thus, if we write $G_i^{(1)}, \ldots, G_i^{(d)}$ for the d conjugates of G_i in $\mathbb{K}$, we then get that

$$|N_{\mathbb{K}/\mathbb{Q}}(\mathcal{E}_i)| \leq |N_{\mathbb{K}/\mathbb{Q}}(E_i)| = |N_{\mathbb{K}/\mathbb{Q}}(G_i)| \leq (2\sqrt{\alpha})^d \alpha^{7d\sqrt{2m}},$$

where the first inequality above follows because $\mathcal{E}_i$ divides E_i; hence G_i, and $E_i \neq 0$. Multiplying the above inequalities for $i = 1, \ldots, \ell$ we get, using also (12), that

$$\begin{aligned} E^d &= N_{\mathbb{K}/\mathbb{Q}}(E) = N_{\mathbb{K}/\mathbb{Q}}(E\mathcal{O}_{\mathbb{K}}) \leq N\left(\prod_{i=1}^{\ell} \mathcal{E}_i\right) \\ &\leq \prod_{i=1}^{\ell} N_{\mathbb{K}/\mathbb{Q}}(G_i) \leq (2\sqrt{\alpha})^{\ell d} \alpha^{7d\ell\sqrt{2m}}, \end{aligned}$$

and therefore

$$E \leq (2\sqrt{\alpha})^{\ell} \alpha^{7\ell\sqrt{2m}} = \alpha^{7\ell\sqrt{2m}+\ell\log(2\sqrt{\alpha})/\log\alpha}. \tag{19}$$

Thus, we have bounded E.

Step 4. *The final inequality.*

We now use (4) to bound F_m from below as $F_m > \alpha^{m-2}$, and the fact that $F_m \leq ABCDE$ and the estimates (8), (9) and (19), to bound F_m from above as

$$F_m \leq \alpha^{m/2+3^{4/3}m^{2/3}-2+s+\log(4m)/\log\alpha+7\ell\sqrt{2m}+\ell\log(2\sqrt{\alpha})/\log\alpha},$$

to conclude that

$$m - 2 < \frac{m}{2} + 3^{4/3}m^{2/3} - 2 + s + \frac{\log(4m)}{\log\alpha} + 7\ell\sqrt{2m} + \frac{\ell\log(2\sqrt{\alpha})}{\log\alpha}, \tag{20}$$

where $\ell \leq s - 1$. We look at

$$f(m,s) = \frac{m}{2} - 3^{4/3}m^{2/3} - s - \frac{\log(4m)}{\log\alpha} - 7(s-1)\sqrt{2m} - \frac{(s-1)\log(2\sqrt{\alpha})}{\log\alpha}.$$

Computing the partial derivative with respect to m, we get

$$g(m,s) = \frac{\partial f}{\partial m}(m,s) = \frac{1}{2} - \frac{2\times 3^{1/3}}{m^{1/3}} - \frac{1}{m\log\alpha} - \frac{7(s-1)}{\sqrt{2m}}. \tag{21}$$

The function $g(m,s)$ is positive when $m \geq 500s^2$ and $s \geq 3$, because in this range

$$g(m,s) \geq \frac{1}{2} - \frac{2\times 3^{1/3}}{(4500)^{1/3}} - \frac{1}{4500\log\alpha} - \frac{7}{\sqrt{1000}} > 0.103.$$

Thus, in order to prove that $m < 500s^2$, it suffices to prove $f(500s^2, s) > 0$. We checked with Mathematica that this inequality holds for $s \geq 17$. For the remaining values $s \in [3, 16]$, we checked individually by noticing that for each one of these values of s a slightly better inequality than (20) holds. For example, in the case when $s \in \{3, 5, 7, 9, 11, 13, 15\}$, there is no need for d_2 and d_3 because s is odd. Thus, the analogue of inequality (20) for such values of s is simply

$$m - 2 < \frac{m}{2} - 1 + s + \frac{\log(4m)}{\log\alpha} + 7(s-1)\sqrt{2m} + \frac{(s-1)\log(2\sqrt{\alpha})}{\log\alpha}. \tag{22}$$

Plugging in $s = 3, 5, 7, 9, 11, 13$, and 15 into (22), we got m bounded by 2000, 7000, 15000, 26000, 40000, 57000, and 77000, respectively, so definitely the inequality $m < 500s^2$ holds for these values of s as well. When $s = 6, 10, 14$, we keep only two divisors in Case 1, namely d_1 and d_2 since there is no need for d_3. Putting $i \in \{1, 2\}$ such that $d_i = \max\{d_1, d_2\}$ and letting j be such that $\{i, j\} = \{1, 2\}$, the analog of inequality (7) is

$$d_j \le \sqrt{3m}.$$

Since $\ell \le s - 2$, when $s = 6, 10, 14$, the analog of inequality (20) in this case is

$$m - 2 < \frac{m}{2} + \sqrt{3m} - 2 + s + \frac{\log(4m)}{\log \alpha} + 7(s-2)\sqrt{2m} + \frac{(s-2)\log(2\sqrt{\alpha})}{\log \alpha}, \quad (23)$$

giving for $s = 6, 10$, and 14 that m is bounded by $8000, 27000$, and 60000, respectively. Thus, the inequality $m < 500s^2$ holds also for $s = 6, 10, 14$.

Finally, for $s = 8, 12, 16$, we use the analog of inequality (20) with the value $\ell \le s - 4$, yielding

$$m - 2 < \frac{m}{2} + 3^{4/3}m^{2/3} - 2 + s + \frac{\log(4m)}{\log \alpha} + 7(s-4)\sqrt{2m} + \frac{(s-4)\log(2\sqrt{\alpha})}{\log \alpha}, \quad (24)$$

which at $s = 8, 12$, and 16 gives that m is bounded by 16000, 45000, and 88000, respectively, so the inequality $m < 500s^2$ holds in these last three cases as well.

This completes the proof of the theorem.

4. Comments and Numerical Results

Numerical results are few because the bounds of Theorem 1 are very weak. However, from what we have said at Step 4 of the proof of Theorem 1 above, we have that $m < 2000$ when $s = 3$, and $m < 7000$ for $s = 5$. We ran a Mathematica code ran for about a day and searched for all such m and for all $n \in [1, 4m]$ for which F_{n+1}/F_n is indeed an element of order s modulo F_m. No example was found with $s = 3$, and the example F_7/F_6 modulo F_{10} is the only example with $s = 5$.

In [3], it was shown that the Diophantine equation

$$F_n^x + F_{n+1}^x = F_m$$

has no positive integer solutions with $n \ge 2$ and $x \ge 3$. The method there was based on linear forms in logarithms. Since for any potential solution of the above equation it is easy to check that F_{n+1}/F_n is an invertible element modulo F_m which is not of order 1, 2 or 4 but whose order divides $2x$, we get right away from Theorem 1 that $m < 2000x^2$. Next, by (4), we get

$$\alpha^{nx} \le F_{n+1}^x < F_n^x + F_{n+1}^x = F_m < \alpha^{m-1} < \alpha^{2000x^2-1},$$

and we derive that $n < 2000x$. However, we could not find an elementary upper bound on x out of this equation (without appealing to linear forms in logarithms). We conclude by mentioning that all the solutions of the more general Diophantine equation $F_n^x + F_{n+1}^x = F_m^y$ in positive integers (n, m, x, y) were found in [2].

Acknowledgements. We thank the referee for comments which improved the quality of this paper.

References

[1] R. D. Carmichael, "On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$", *Ann. Math. (2)* **15** (1913), 30–70.

[2] N. Hirata-Kohno and F. Luca, "On the Diophantine equation $F_n^x + F_{n+1}^x = F_m^y$", *preprint*, 2012.

[3] F. Luca and R. Oyono, "On the sum of powers of two consecutive Fibonacci numbers", *Proc. Japan Acad. Ser. A.* **87** (2011), 45–50.