*Annales Mathematicae et Informaticae*
***41** (2013) pp. 265–270*

*Proceedings of the*
*15th International Conference on Fibonacci Numbers and Their Applications*
*Institute of Mathematics and Informatics, Eszterházy Károly College*
*Eger, Hungary, June 25–30, 2012*

# When do the Fibonacci invertible classes modulo $M$ form a subgroup?

**Florian Luca[a], Pantelimon Stănică[b], Aynur Yalçiner[c]**

[a]Instituto de Matemáticas, Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México; fluca@matmor.unam.mx

[b]Naval Postgraduate School, Applied Mathematics Department
Monterey, CA 93943; pstanica@nps.edu

[c]Department of Mathematics, Faculty of Science, Selçuk University, Campus
42075 Konya, Turkey; aynuryalciner@gmail.com

**Abstract**

In this paper, we look at the invertible classes modulo $M$ representable as Fibonacci numbers and we ask when these classes, say $\mathcal{F}_M$, form a multiplicative group. We show that if $M$ itself is a Fibonacci number, then $M \leq 8$; if $M$ is a Lucas number, then $M \leq 7$. We also show that if $x \geq 3$, the number of $M \leq x$ such that $\mathcal{F}_M$ is a multiplicative subgroup is $O(x/(\log x)^{1/8})$.

*Keywords:* Fibonacci and Lucas numbers, congruences, multiplicative group

*MSC:* 11B39

## 1. Introduction

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

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

with the corresponding Lucas companion sequence $\{L_k\}_{k\geq 0}$ satisfying the same recurrence with initial conditions $L_0 = 2$, $L_1$=1. The distribution of the Fibonacci numbers modulo some positive integer $M$ has been extensively studied. Here, we put

$$\mathcal{F}_M = \{F_n \pmod M : \gcd(F_n, M) = 1\}$$

and ask when is $\mathcal{F}_M$ a multiplicative group. We present the following conjecture.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **JUN 2012** | | **00-00-2012 to 00-00-2012** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **When do the Fibonacci invertible classes modulo M form a subgroup?** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Department of Applied Mathematics,Monterey,CA,93943** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT
**In this paper, we look at the invertible classes modulo M representable as Fibonacci numbers and we ask when these classes, say FM, form a multiplicative group. We show that if M itself is a Fibonacci number, then M 8 if M is a Lucas number, then M 7. We also show that if x 3, the number of M x such that FM is a multiplicative subgroup is O(x/(log x)1/8).**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **6** | |

**Conjecture 1.1.** *There are only finitely many $M$ such that $\mathcal{F}_M$ is a multiplicative group.*

Shah [5] and Bruckner [1] proved that if $p$ is prime and $\mathcal{F}_p$ is the entire multiplicative group modulo $p$, then $p \in \{2, 3, 5, 7\}$. We do not know of many results in the literature addressing the multiplicative order of a Fibonacci number with respect to another Fibonacci number, although in [3] it was shown that if $F_nF_{n+1}$ is coprime to $F_m$ and $F_{n+1}/F_n$ has order $s \notin \{1, 2, 4\}$ modulo $F_m$, then $m < 500s^2$. Moreover, Burr [2] showed that $F_n \pmod m$ contains a complete set of residues modulo $m$ if and only if $m$ is of the forms: $\{1, 2, 4, 6, 7, 14, 3^j\} \cdot 5^k$, where $k \geq 0, j \geq 1$.

In this paper, we prove that if $M = F_m$ is a Fibonacci number itself, or $M = L_m$, then Conjecture 1.1 holds in the following strong form.

**Theorem 1.2.** *If $M = F_m$ and $\mathcal{F}_M$ is a multiplicative group, then $m \leq 6$. If $M = L_m$ and $\mathcal{F}_M$ is a multiplicative group, then $m \leq 4$.*

We also show that for most positive integers $M$, $\mathcal{F}_M$ is not a multiplicative group.

**Theorem 1.3.** *For $x \geq 3$, the number of $M \leq x$ such that $\mathcal{F}_M$ is a multiplicative subgroup is $O(x/(\log x)^{1/8})$. In particular, the set of $M$ such that $\mathcal{F}_M$ is a multiplicative subgroup is of asymptotic density* 0.

## 2. Proof of Theorem 1.2

We first deal with the case of the Fibonacci numbers. It is well-known that the Fibonacci sequence is purely periodic modulo every positive integer $M$. When $M = F_m$, then the period is at most $4m$. Thus, $\#\mathcal{F}_M \leq 4m$, Let $\omega(m)$ be the number of distinct prime factors of $m$. Assume that $X$ is some positive integer such that

$$\pi(X) \geq \omega(m) + 4. \tag{2.1}$$

Here, $\pi(X)$ is the number of primes $p \leq X$. Then there exist three odd primes $p < q < r \leq X$ none of them dividing $m$. For a triple $(a, b, c) \in \{0, 1, \ldots, \lfloor (4m)^{1/3} \rfloor\}$, we look at the congruence class $F_p^a F_q^b F_r^c \pmod M$. There are $(\lfloor (4m)^{1/3} \rfloor + 1)^3 > 4m \geq \#\mathcal{F}_M$ such elements modulo $M$, so they cannot be all distinct. Thus, there are $(a_1, b_1, c_1) \neq (a_2, b_2, c_2)$ such that

$$F_p^{a_1} F_q^{b_1} F_r^{c_1} \equiv F_p^{a_2} F_q^{b_2} F_r^{c_2} \pmod M.$$

Hence, $F_p^{a_1-a_2} F_q^{b_1-b_2} F_r^{c_1-c_2} \equiv 1 \pmod M$. Observe that the rational number $x = F_p^{a_1-a_2} F_q^{b_1-b_2} F_r^{c_1-c_2} - 1$ cannot be zero because $F_p$, $F_q$, $F_r$ are all larger than 1 and coprime any two. Thus, $M$ divides the numerator of the nonzero rational number $x$, and so we get

$$F_m = M \leq F_p^{|a_1-a_2|} F_q^{|b_1-b_2|} F_r^{|c_1-c_2|}. \tag{2.2}$$

We now use the fact that

$$\alpha^{k-2} \le F_k \le \alpha^{k-1} \quad \text{for all} \quad k = 1, 2 \ldots,$$

where $\alpha = (1+\sqrt{5})/2$, to deduce from (2.2) that

$$\alpha^{m-2} \le F_m \le (F_p F_q F_r)^{(4m)^{1/3}} < (\alpha^{X-1})^{3(4m)^{1/3}},$$

so that

$$m < 3(4m)^{1/3} X + 2 - 3(4m)^{1/3} < 3(4m)^{1/3} X,$$

therefore

$$m < 6\sqrt{3} X^{3/2}. \tag{2.3}$$

Let us now get some bounds on $m$. We take $X = m^{1/2}$. Assuming $X > 17$ (so, $m > 17^2$), we have, by Theorem 2 in [4], that

$$\pi(X) > \frac{X}{\log X} = \frac{2m^{1/2}}{\log m}.$$

Since $2^{\omega(m)} \le m$, we have that

$$\omega(m) \le \frac{\log m}{\log 2}.$$

Thus, inequality (2.1) holds for our instance provided that

$$\frac{2m^{1/2}}{\log m} > \frac{\log m}{\log 2} + 4,$$

which holds for all $m > 5000$. Now inequality (2.3) tells us that

$$m < 6\sqrt{3} m^{3/4}, \quad \text{therefore} \quad m < (6\sqrt{3})^4 < 12000. \tag{2.4}$$

Let us reduce the above bound on $m$. Since

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030 > m,$$

it then follows that $\omega(m) \le 5$, therefore it is enough to choose $X = 23$ to be the 9th prime and then inequality (2.1) holds. Thus, (2.3) tells us that $m \le 6\sqrt{3} \times 23^{3/2} < 1200$. We covered the rest of the range with Mathematica. That is, for each $m \in [10, 1200]$, we took the first two odd primes $p$ and $q$ which do not divide $m$ and checked whether for some positive integer $n \le 4m$ both congruences $F_p^n \equiv 1 \pmod{F_m}$ and $F_q^n \equiv 1 \pmod{F_m}$. The only $m$'s that passed this test were $m = 10, 11$. We covered the rest by hand. The only values $m$ that satisfy the hypothesis of the theorem are $m = 1, 2, 3, 4, 5, 6$.

If $M = L_m$, then, the argument is similar to the one above up and we point out the differences only. The period of the Fibonacci numbers modulo a Lucas number

$L_m$ is at most $8m$, and so $\#\mathcal{F}_M \le 8m$. As before, one takes $X$ as in (2.1), and the triple $(a,b,c) \in \{0,1,\ldots,\lfloor 2m^{1/3}\rfloor\}$, implying an inequality as in (2.2), namely

$$L_m = M \le F_p^{|a_1-a_2|} F_q^{|b_1-b_2|} F_r^{|c_1-c_2|}. \tag{2.5}$$

Since for all $k \ge 1$, $\alpha^{k-1} \le L_k \le \alpha^{k+1}$, then

$$\alpha^{m-1} \le L_m \le (F_p F_q F_r)^{2m^{1/3}} \le \alpha^{6(X+1)m^{1/3}},$$

and so, $m < 6m^{1/3}X + 1 + 6m^{1/3} < 13m^{1/3}X$, which implies

$$m < 13^{3/2} X^{3/2}. \tag{2.6}$$

The argument we used before with $X = m^{1/2}$ works here, as well, rendering the bound $m < 13^6 = 4,826,809$. We can decrease the bound by using the fact that the product of all primes up to 19 is 9,699,690 > 4,826,809, and so, $\omega(m) \le 7$, therefore, it is enough to choose $X = 31$ (the 11th prime) for the inequality (2.1) to hold. We use $X = 31$ in the formula before (2.6) to get $m - 192 \cdot m^{1/3} - 1 < 0$, which implies $m < 14^3 = 2744$ (to see that, label $y := m^{1/3}$ and look at the sign of the polynomial $y^3 - 192y - 1$).

To cover the range from 10 to 2744, we used the same trick as before (which works, since by $F_{2m} = L_m F_m$, then $\gcd(F_p, L_m) = \gcd(F_p, F_{2m}/F_m) | \gcd(F_p, F_{2m}) = F_{\gcd(p,2m)}$). To speed up the computation we used the fact that one can choose one of the primes $p, q$ to be 5, since a Lucas number is never divisible by 5. The only $m$'s that passed the test were $10, 12, 15, 21$, which are easily shown (by displaying the corresponding residues) not to generate a multiplicative group structure. The only values of $m$, for which we do have a multiplicative groups structure for $\mathcal{F}_M$ when $M = L_m$ are $m \in \{1,2,3,4\}$.

# 3. Proof of Theorem 1.3

Consider the following set of primes

$$\mathcal{P} = \left\{ p > 5 : \left(\frac{5}{p}\right) = 1,\ \left(\frac{11}{p}\right) = \left(\frac{46}{p}\right) = -1 \right\}.$$

Here, for an integer $a$ and an odd prime $p$, we use $\left(\frac{a}{p}\right)$ for the Legendre symbol of $a$ with respect to $p$. Let $\mathcal{M}$ be the set of $M$ such that $\mathcal{F}_M$ is a multiplicative subgroup. We show that $M$ is free of primes from $\mathcal{P}$. Since $\mathcal{P}$ is a set of primes of relative density 1/8 (as a subset of all primes), the conclusion will follow from the Brun sieve (see [6, Chapter I.4, Theorem 3]). To see that $M$ is free of primes from $p$, observe that since $F_3 = 2$, $F_4 = 3$, and $\mathcal{F}_M$ is a multiplicative subgroup, it follows that there exists $n$ such that $F_n \equiv 6 \pmod M$. If $p \mid M$ for some $p \in \mathcal{P}$, it follows that

$$F_n - 6 \equiv 0 \pmod p. \tag{3.1}$$

Since $\left(\frac{5}{p}\right) = 1$, it follows that both $\sqrt{5}$ and $\alpha$ are elements of $\mathbb{F}_p$. With the Binet formula, we have

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

Put $t_n = \alpha^n$, $\varepsilon_n = (-1)^n$. Thus, $\beta^n = (-\alpha^{-1})^n = \varepsilon_n t_n^{-1}$, so congruence (3.1) becomes

$$\frac{t_n - \varepsilon_n t_n^{-1}}{\sqrt{5}} - 6 \equiv 0 \pmod{p}$$

giving

$$t_n^2 - 6\sqrt{5}\, t_n - \varepsilon_n \equiv 0 \pmod{p}.$$

Thus, one of the quadratic equations $t^2 - 6\sqrt{5}\, t \pm 1 = 0$ must have a solution $t$ modulo $p$. Since the discriminants of the above quadratic equations are $176 = 16 \times 11$ and $184 = 4 \times 46$, respectively, and since neither 11 nor 46 is a quadratic residue modulo $p$, we get the desired conclusion.

# 4. Comments

The bound $O(x/(\log x)^{1/8})$ of Theorem 1.3 is too weak to allow one to decide via the Abel summation formula whether

$$\sum_{M \in \mathcal{M}} \frac{1}{M}$$

is finite or not. Of course Conjecture 1.1 would imply that the above sum is finite. We leave it as a problem to the reader to improve the bound on the counting function of $\mathcal{M} \cap [1, x]$ from Theorem 1.3 enough to decide that indeed the sum of the above series is convergent.

**Acknowledgment.** F. L. was supported in part by Project PAPIIT IN104512 and a Marcos Moshinsky Fellowship. P. S. acknowledges a research sabbatical leave from his institution.

# References

[1] G. Bruckner, Fibonacci Sequence Modulo a Prime $p \equiv 3 \pmod 4$, *Fibonacci Quart.* **8** (1970), 217–220.

[2] S. A. Burr, On Moduli for Which the Fibonacci Sequence Contains a Complete System of Residues, *Fibonacci Quart.* **9** (1971), 497–504.

[3] T. Komatsu, F. Luca, On the multiplicative order of $F_{n+1}/F_n$ modulo $F_m$, *Preprint*, 2012.

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

[5] A. P. Shah, Fibonacci Sequence Modulo $m$, *Fibonacci Quart.* **6** (1968), 139–141.

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