PAIRWISE MODULAR MULTIPLICATIVE INVERSES AND FIBONACCI NUMBERS

Carlo Sanna[1]
Department of Mathematical Sciences, Politecnico di Torino, Italy
carlo.sanna@polito.it

Received: 6/23/22, Accepted: 12/23/22, Published: 1/13/23

Abstract

Let (p, q) be a pair of relatively prime integers greater than 1. The *pairwise modular multiplicative inverse*, or PMMI for short, of (p, q) is defined as the unique pair (p', q') of positive integers such that $pp' \equiv 1 \pmod{q}$, $p' < q$, $qq' \equiv 1 \pmod{p}$, $q' < p$. In other words, p' is the inverse of p modulo q, and q' is the inverse of q modulo p. Motivated by some results in knot theory, Song (2019) found four families of pairs of Fibonacci numbers such that their PMMIs are pairs of Fibonacci numbers. We determine all pairs of Fibonacci numbers with such property.

1. Introduction

Let (F_n) be the sequence of Fibonacci numbers, which is defined by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for every positive integer n. It is well known that (F_n) is purely periodic modulo every positive integer M. In fact, the length of the period [6, 12, 15, 20], the set of residues [3, 5, 8, 17], and the distribution [4, 7, 13, 18] of (F_n) modulo M have been studied by many authors. However, results regarding modular inverses and Fibonacci numbers are sparse. Komatsu, Luca, and Tachiya [9] studied the multiplicative order of $F_{n+1}F_n^{-1}$ modulo F_m, where m and n are positive integers such that $\gcd(F_m, F_{n+1}F_n) = 1$ (see also [2]). Luca, Stănică, and Yalçiner [11] studied the positive integers M such that the invertible residue classes modulo M represented by Fibonacci numbers form a subgroup. Prempreesuk, Noppakaew, and Pongsriiam [14] determined the Zeckendorf representation of the multiplicative inverse of 2 modulo F_n, for every positive integer n such that F_n is odd. Then Alecci, Murru, and Sanna [1] determined the Zeckendorf representation of the multiplicative inverse of a modulo F_n, for every fixed $a \geq 3$ and for every positive integer n such that $\gcd(a, F_n) = 1$.

DOI: 10.5281/zenodo.7506610

[1] C. Sanna is a member of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of the Politecnico di Torino.

Let (p, q) be a pair of relatively prime integers greater than 1. The *pairwise modular multiplicative inverse*, or PMMI for short, of (p, q) is defined as the unique pair (p', q') of positive integers such that $pp' \equiv 1 \pmod{q}$, $p' < q$, $qq' \equiv 1 \pmod{p}$, $q' < p$. In other words, p' is the inverse of p modulo q, and q' is the inverse of q modulo p. PMMIs make their appearance in the study of binary cyclotomic polynomials. Precisely, if p and q are distinct prime numbers, then the number of nonzero coefficients of the cyclotomic polynomial $\Phi_{pq}(X)$ is equal to $2p'q' - 1$ (see, e.g., [16, Section 2]). Motivated by some results in knot theory [10], Song [19] found four families of pairs of Fibonacci numbers whose PMMIs are pairs of Fibonacci numbers. We prove that these families, together with some isolated pairs, are indeed all the pairs of Fibonacci numbers whose PMMIs are pairs of Fibonacci numbers. Our result is the following.

Theorem 1. *Let a, b, c, d be integers, with $a > b \geq 3$, $c, d \geq 2$, and $\gcd(F_a, F_b) = 1$. Then the PMMI of (F_a, F_b) is equal to (F_c, F_d) if and only if (a, b, c, d) is equal to*

$$\begin{aligned} &(4, 3, 2, 3), \quad (5, 3, 2, 4), \quad (2k+1, 2k, 2k-1, 2k-1), \\ &(2k+2, 2k+1, 2k-1, 2k+1), \quad (2k+2, 2k, 2k-1, 2k), \\ &\text{or} \quad (2k+3, 2k+1, 2k-1, 2k+2), \end{aligned} \tag{1}$$

where k is a positive integer.

Note that, since $F_1 = F_2 = 1$ and by the symmetry of the problem, the conditions $a > b \geq 3$ and $c, d \geq 2$ are not restrictive.

Remark 1. In defining PMMIs, we are using a different convention than [19, Definition 1], so that our (p', q') is their (v, x). Also, we assume $p, q > 1$, which is not a loss of generality.

2. Preliminaries

Let us recall that for every positive integer n we have the *Binet formula*

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \tag{2}$$

where $\alpha := (1 + \sqrt{5})/2$ is the golden ratio and $\beta := (1 - \sqrt{5})/2$ is its algebraic conjugate. In fact, one can use (2) to extend the sequence (F_n) to all integers n.

We shall use the following bounds for the nth Fibonacci number.

Lemma 1. *Let n_0 be an odd positive integer and put*

$$c_1(n_0) := \frac{1 - (\beta/\alpha)^{n_0+1}}{\alpha - \beta} \quad \text{and} \quad c_2(n_0) := \frac{1 - (\beta/\alpha)^{n_0}}{\alpha - \beta}.$$

Then $c_1(n_0)\alpha^n \leq F_n \leq c_2(n_0)\alpha^n$ for all integers $n \geq n_0$.

Proof. Noticing that $\beta/\alpha \in (-1,0)$, the claim follows easily from (2). □

The next lemma determines the solutions of a certain equation involving the Fibonacci numbers.

Lemma 2. *Let m and n be positive integers. Then we have*

$$F_m F_{n-1} - F_{m-1} F_n = 1 \tag{3}$$

if and only if

$$(m,n) \in \big\{(2k+1,2k),(2k+2,2k),(2k-1,2k),(2k-1,2k+1)\big\}$$

for some positive integer k.

Proof. For all integers i and j, let us define the matrix

$$M_{i,j} := \begin{pmatrix} F_i & F_{i-1} \\ F_j & F_{j-1} \end{pmatrix}.$$

We have that

$$M_{i-1,j-1} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_{i-1}+F_{i-2} & F_{i-1} \\ F_{j-1}+F_{j-2} & F_{j-1} \end{pmatrix} = \begin{pmatrix} F_i & F_{i-1} \\ F_j & F_{j-1} \end{pmatrix} = M_{i,j}.$$

Hence, taking the determinant of both sides, we get $\det(M_{i-1,j-1}) = -\det(M_{i,j})$. Iterating this reasoning, it follows that $\det(M_{i-k,j-k}) = (-1)^k \det(M_{i,j})$ for every positive integer k.

Let us prove the "only if" part. Suppose that m and n are positive integers satisfying (3). If $m \le n$ then

$$\begin{aligned} F_{n-m} &= \det(M_{1,n-m+1}) = \det(M_{m-(m-1),n-(m-1)}) \\ &= (-1)^{m-1} \det(M_{m,n}) = (-1)^{m-1}(F_m F_{n-1} - F_{m-1} F_n) = (-1)^{m-1}. \end{aligned}$$

Consequently, we have that m is odd and $n-m \in \{1,2\}$. Hence, we get that

$$(m,n) \in \big\{(2k-1,2k),(2k-1,2k+1)\big\}$$

for some positive integer k. Similarly, if $m > n$ then

$$\begin{aligned} -F_{m-n} &= \det(M_{m-n+1,1}) = \det(M_{m-(n-1),n-(n-1)}) \\ &= (-1)^{n-1} \det(M_{m,n}) = (-1)^{n-1}(F_m F_{n-1} - F_{m-1} F_n) = (-1)^{n-1}. \end{aligned}$$

Consequently, we have that n is even and $m-n \in \{1,2\}$. Hence, we get that

$$(m,n) \in \big\{(2k+1,2k),(2k+2,2k)\big\}$$

for some positive integer k. Thus the "only if" part is proved.

The "if" part can be proved in a similar way using the matrices $M_{i,j}$ or, alternatively, using the Binet formula (2). □

The next lemma belongs to the folklore, especially in the context of binary cyclotomic polynomials. We give the proof for completeness.

Lemma 3. *Let p, q, p', q' be positive integers, with p, q relatively prime and greater than 1. Then (p', q') is the PMMI of (p, q) if and only if $pp' + qq' = pq + 1$.*

Proof. If $pp' + qq' = pq + 1$ then it follows that $pp' \equiv 1 \pmod{q}$ and $qq' \equiv 1 \pmod{p}$. Furthermore, we have that $p' = q + (1 - qq')/p \leq q$ and so $p' < q$, since p' is invertible modulo q. Similarly, one gets that $q' < q$. Hence, (p', q') is the PMMI of (p, q).

Vice versa, if (p', q') is the PMMI of (p, q) then $pp' \equiv 1 \pmod{q}$, $qq' \equiv 1 \pmod{p}$, $p' < q$, and $q' < p$. Consequently, letting $n := pp' + qq'$, we have that $n \equiv pp' \equiv 1 \pmod{q}$ and $n \equiv qq' \equiv 1 \pmod{p}$. Hence, recalling that p and q are relatively prime, we get that $n \equiv 1 \pmod{pq}$. Moreover, it holds that $n < 2pq$. Therefore, we have that $n = pq + 1$, as desired. □

3. Proof of Theorem 1

Let a, b, c, d be integers, with $a > b \geq 3$, $c, d \geq 2$, and $\gcd(F_a, F_b) = 1$. In light of Lemma 3, we have that (F_c, F_d) is the PMMI of (F_a, F_b) if and only if

$$F_a F_c + F_b F_d = F_a F_b + 1. \tag{4}$$

First, using the Binet formula one can readily check that each quadruple (a, b, c, d) given in (1) satisfies (4). (Note also that $\gcd(F_a, F_b) = F_{\gcd(a,b)} = F_{\{1,2\}} = 1$ for such quadruples.) We have to prove that the quadruples in (1) are the only solutions to (4).

Suppose that (a, b, c, d) is a solution to (4). Note that, since (F_c, F_d) is the PMMI of (F_a, F_b), we get that $F_c < F_b$ and $F_d < F_a$, so that $c < b$ and $d < a$. We split the proof into several cases.

`Case I:` Assume that $c = 2$. Then (4) becomes

$$F_a + F_b F_d = F_a F_b + 1.$$

Since $d < a$, we have that $F_d \leq F_{a-1}$. Therefore, we get that

$$3F_{a-2} > F_a - 1 = F_a F_b - F_b F_d = (F_a - F_d)F_b \geq (F_a - F_{a-1})F_b = F_{a-2}F_b,$$

where we used the inequality $3F_{n-2} \geq F_n$, which holds for every integer $n \geq 3$. Consequently, we have that $F_b = 2$ and $b = 3$. In turn, this implies that $2F_d = F_a + 1$, whose only solutions in the desired range are $(a, d) \in \{(4, 3), (5, 4)\}$. Summarizing, we have that

$$(a, b, c, d) \in \{(4, 3, 2, 3), (5, 3, 2, 4)\}.$$

Case II: Assume that $d = 2$. Then (4) becomes

$$F_aF_c + F_b = F_aF_b + 1.$$

Since $c < b$, we have that $F_c \le F_{b-1}$. Therefore, we get that

$$3F_{b-3} > F_b - 1 = F_aF_b - F_aF_c = F_a(F_b - F_c) \ge F_a(F_b - F_{b-1}) = F_aF_{b-2},$$

which implies that $F_a \le 2$. But this is impossible, since $a \ge 4$.

Case III: Assume that $a, b, c, d \ge 3$. With the notation of Lemma 1, let $c_1 := c_1(3)$ and $c_2 := c_2(3)$. Then, from Lemma 1, it follows that

$$c_1^2\alpha^{a+b} \le F_aF_b < F_aF_b + 1 = F_aF_c + F_bF_d \le c_2^2\alpha^{a+c} + c_2^2\alpha^{b+d}.$$

Hence, dividing both sides by $c_2^2\alpha^{a+b}$, we get that

$$(c_1/c_2)^2 < \alpha^{-(b-c)} + \alpha^{-(a-d)}.$$

Recalling that $b > c$ and $a > d$, and since

$$(c_1/c_2)^2 > \max\{\alpha^{-2} + \alpha^{-2}, \alpha^{-1} + \alpha^{-3}\},$$

it follows that $\min\{b - c, a - d\} = 1$ and $\max\{b - c, a - d\} \le 2$, which can happen only in the following three subcases.

Subcase IIIa: Suppose that $b - c = a - d = 1$. Hence, $c = b - 1$ and $d = a - 1$. Therefore, (4) becomes

$$F_aF_{b-1} + F_{a-1}F_b = F_aF_b + 1.$$

Thus, dividing by F_aF_b, we get that

$$1 = \frac{1}{2} + \frac{1}{2} \le \frac{F_{b-1}}{F_b} + \frac{F_{a-1}}{F_a} = \frac{1}{F_aF_b},$$

which is impossible. Here we used the inequality $F_{n-1}/F_n \ge 1/2$, which holds for every integer $n \ge 3$.

Subcase IIIb: Suppose that $b - c = 1$ and $a - d = 2$. Hence, $c = b - 1$ and $d = a - 2$. Thus (4) becomes

$$F_aF_{b-1} + F_bF_{a-2} = F_aF_b + 1.$$

Subtracting F_aF_b from both sides and using the fact that $F_a = F_{a-1} + F_{a-2}$, we get that

$$F_aF_{b-1} - F_{a-1}F_b = 1.$$

Therefore, from Lemma 2 and recalling that $a > b$, we get that

$$(a, b, c, d) \in \big\{(2k+1, 2k, 2k-1, 2k-1), (2k+2, 2k, 2k-1, 2k)\big\}$$

for some positive integer k.

`Subcase IIIc:` Suppose that $b - c = 2$ and $a - d = 1$. Hence, $c = b - 2$ and $d = a - 1$. Thus (4) becomes

$$F_a F_{b-2} + F_b F_{a-1} = F_a F_b + 1.$$

Subtracting $F_a F_b$ from both sides and using the fact that $F_b = F_{b-1} + F_{b-2}$, we get that

$$F_b F_{a-1} - F_{b-1} F_a = 1.$$

Therefore, from Lemma 2 and recalling that $a > b$, we get that

$$(a, b, c, d) \in \big\{(2k+2, 2k+1, 2k-1, 2k+1), (2k+3, 2k+1, 2k-1, 2k+2)\big\}$$

for some positive integer k. (Note that we replaced k with $k+1$ in the statement of Lemma 2 to avoid negative indices.)

The proof is complete.

Acknowledgements. The author thanks the anonymous referee for carefully reading the paper.

References

[1] G. Alecci, N. Murru, and C. Sanna, Zeckendorf representation of multiplicative inverses modulo a Fibonacci number, *Monatsh. Math.* (2022), https://doi.org/10.1007/s00605-022-01724-y.

[2] Y. F. Bilu, T. Komatsu, F. Luca, A. Pizarro-Madariaga, and P. Stănică, On a divisibility relation for Lucas sequences, *J. Number Theory* **163** (2016), 1–18.

[3] G. Bruckner, Fibonacci sequence modulo a prime $p \equiv 3 \pmod 4$, *Fibonacci Quart.* **8** (1970), no. 2, 217–220.

[4] R. Bundschuh and P. Bundschuh, Distribution of Fibonacci and Lucas numbers modulo 3^k, *Fibonacci Quart.* **49** (2011), no. 3, 201–210.

[5] S. A. Burr, On moduli for which the Fibonacci sequence contains a complete system of residues, *Fibonacci Quart.* **9** (1971), no. 5, 497–504, 526.

[6] P. A. Catlin, A lower bound for the period of the Fibonacci series modulo m, *Fibonacci Quart.* **12** (1974), 349–350.

[7] E. T. Jacobson, Distribution of the Fibonacci numbers mod 2^k, *Fibonacci Quart.* **30** (1992), no. 3, 211–215.

[8] M. Javaheri and S. Cambrea, The distribution of Fibonacci numbers modulo primes, *Amer. Math. Monthly* **129** (2022), no. 1, 75–79.

[9] T. Komatsu, F. Luca, and Y. Tachiya, On the multiplicative order of F_{n+1}/F_n modulo F_m, *Integers* **12B** (2012/13), Proceedings of the Integers Conference 2011, #A8, 13pp.

[10] S. Lee, Twisted torus knots that are unknotted, *Int. Math. Res. Not.* (2014), no. 18, 4958–4996.

[11] F. Luca, P. Stănică, and A. Yalçiner, When do the Fibonacci invertible classes modulo M form a subgroup?, *Ann. Math. Inform.* **41** (2013), 265–270.

[12] S. E. Mamangakis, Remarks on the Fibonacci series modulo m, *Amer. Math. Monthly* **68** (1961), 648–649.

[13] H. Niederreiter, Distribution of Fibonacci numbers mod 5^k, *Fibonacci Quart.* **10** (1972), no. 4, 373–374.

[14] B. Prempreesuk, P. Noppakaew, and P. Pongsriiam, Zeckendorf representation and multiplicative inverse of F_m mod F_n, *Int. J. Math. Comput. Sci.* **15** (2020), no. 1, 17–25.

[15] D. W. Robinson, The Fibonacci matrix modulo m, *Fibonacci Quart.* **1** (1963), no. 2, 29–36.

[16] C. Sanna, A survey on coefficients of cyclotomic polynomials, *Expo. Math.* **40** (2022), no. 3, 469–494.

[17] A. P. Shah, Fibonacci sequence modulo m, *Fibonacci Quart.* **6** (1968), no. 2, 139–141.

[18] L. Somer, Distribution of residues of certain second-order linear recurrences modulo p, in *Applications of Fibonacci numbers*, Vol. 3 (Pisa, 1988), Kluwer Acad. Publ., Dordrecht, 1990, pp. 311–324.

[19] H.-J. Song, Modular multiplicative inverses of Fibonacci numbers, *East Asian Math. J.* **35** (2019), no. 3, 285–288.

[20] D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960), 525–532.