Journal of Integer Sequences, Vol. 24 (2021),
Article 21.9.4

The Generalized Bi-Periodic Fibonacci Sequence Modulo m

Hacène Belbachir and Celia Salhi[1]
USTHB
Faculty of Mathematics
RECITS Laboratory
16111 Bab Ezzouar, Algiers
Algeria
hacenebelbachir@gmail.com
salhicelia2@gmail.com
csalhi@usthb.dz

Abstract

For given positive integers a, b, c, and d, we consider the generalized bi-periodic Fibonacci sequence $(F_n)_{n\geq 0}$ defined by the recurrence relation $F_n = aF_{n-1} + cF_{n-2}$ for n even and $F_n = bF_{n-1} + dF_{n-2}$ for n odd, with initial conditions $F_0 = 0$, $F_1 = 1$. In the present paper, we study the periodicity of $(F_n)_{n\geq 0}$ modulo a given integer $m \geq 2$ relatively prime to c and d. We extend some well-known results on the period and the rank of the classical Fibonacci sequence to the bi-periodic case.

1 Introduction

The Fibonacci sequence and its various generalizations have interested mathematicians for many years. Edson and Yayenie [4] introduced the generalized Fibonacci sequence, also known as the bi-periodic Fibonacci sequence, by considering the following piecewise linear recurrence relation with two non-zero real parameters a and b:

$$q_0 = 0, \quad q_1 = 1, \quad q_n = \begin{cases} aq_{n-1} + q_{n-2}, & \text{for } n \text{ even;} \\ bq_{n-1} + q_{n-2}, & \text{for } n \text{ odd,} \end{cases} \quad (n \geq 2). \tag{1}$$

[1] Corresponding author.

Many sequences in the literature are special cases of this sequence. The case $a = b = 1$ corresponds to the classical Fibonacci sequence A000045, and the case $a = b = 2$ gives the Pell sequence A000129, while for $a = b = k$ for some positive integer k, we obtain the k-Fibonacci sequence [5]. A further generalization has been defined in [10, 17] by preserving the initial conditions and modifying the recurrence relation (1) in such a way that the resulting sequence (2) depends on four real parameters a, b, c, and d. Let $(F_n)_{n\geq 0}$ be the generalized bi-periodic Fibonacci sequence defined as follows:

$$F_0 = 0, \quad F_1 = 1, \quad F_n = \begin{cases} aF_{n-1} + cF_{n-2}, & \text{for } n \text{ even;} \\ bF_{n-1} + dF_{n-2}, & \text{for } n \text{ odd,} \end{cases} \quad (n \geq 2). \tag{2}$$

Notice that for $c = d = 1$, $(F_n)_{n\geq 0}$ reduces to the sequence (1). For the case $a = b$ and $c = d$, we have the $(a, c)-$Fibonacci sequence.

The periodicity of linear recurrence sequences reduced modulo an integer m has been studied by several authors. The interest in this topic is the diversity of the fields of application such that cryptography (the generation of pseudo-random numbers), coding theory and electrical engineering. Wall [16] studied the periodicity of the Fibonacci sequence modulo an arbitrary integer m and established many interesting results. Vinson [15] extended the work of Wall and studied the rank of apparition of m in the Fibonacci sequence. Recently, the periodicity of various generalizations of the Fibonacci sequence has been investigated in several papers; see [1, 2, 3, 6, 7, 8, 9, 14].

In the present paper, we investigate the periodicity of the generalized bi-periodic Fibonacci sequence $(F_n)_{n\geq 0}$ modulo $m \geq 2$, where a, b, c, and d are given positive integers. Assuming that m is chosen such that m is relatively prime to c and d, we prove that $(F_n)_{n\geq 0}$ reduced modulo m is periodic, i.e., there exists a positive integer r such that

$$F_{n+r} = F_n, \qquad \text{for all } n \geq 0. \tag{3}$$

We extend some well-known results on the period and the rank of the classical Fibonacci sequences to the bi-periodic case.

Since we are dealing with the generalized bi-periodic Fibonacci sequences, reduced modulo m, the condition $a \not\equiv b \pmod{m}$ or $c \not\equiv d \pmod{m}$ ensures that the considered sequences are actually bi-periodic. For the case where $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ $(F_n \bmod m)$ coincides with the (a, c)-Fibonacci sequence; see [7, 9].

Tascı and Kızılırmak [13] studied the period of the generalized bi-periodic Fibonacci sequences F_n for the case $c = d = 1$. The authors defined the period of F_n modulo m to be the least positive integer r such that $F_r \equiv 0 \pmod{m}$ and $F_{r+1} \equiv 1 \pmod{m}$. However, unlike the case where $a = b$, the integer r does not necessarily satisfy Property (3); see Example 2. Furthermore, we mention that [13, Theorem 4] is true only if we add the condition ab is also a quadratic residue modulo p (see Example 9 for $p = 11$).

2 The periodicity of the generalized bi-periodic Fibonacci sequences modulo m

Let a, b, c, d, and m be positive integers, and assume m is chosen such that $\gcd(c, m) = \gcd(d, m) = 1$. In this section, we investigate the period of $(F_n)_{n\geq 0}$ reduced modulo m. Flacon and Plaza [6] determined the length of the period of the k-Fibonacci sequences reduced modulo an integer m. Notice that for $a = b = k$ and $c = d = 1$, $(F_n)_{n\geq 0}$ corresponds to the k-Fibonacci sequences.

Following the proof of [6, Theorem 2], we show in the next theorem that the sequence $(F_n \bmod m)_n$ is periodic.

Theorem 1. *The sequence $(F_n)_{n\geq 0}$ is periodic modulo m.*

Proof. Since there are only m^2 pairs of integers modulo m, at least one repetition of a pair must occur within the following $m^2 + 1$ pairs of the sequence:

$$(F_0, F_1), (F_2, F_3), \ldots, (F_{2m^2}, F_{2m^2+1}).$$

Let i and j be integers such that $0 \leq i < j \leq m^2$. Let $(F_{2i}, F_{2i+1}) \equiv (F_{2j}, F_{2j+1}) \pmod{m}$, with $r = 2j - 2i$. It follows by induction that

$$F_{n+r} = F_n \qquad \text{for all } n \geq 2i.$$

Now, since c and d are invertible modulo m, by backward induction we see that the sequence F_n is periodic. Indeed, from the recurrence relation (2) we have
$F_{2i-1} \equiv F_{2j-1}, F_{2i-2} \equiv F_{2j-2}, \ldots, F_1 \equiv F_{2j-2i+1} = F_{r+1}$, and $F_0 \equiv F_{2j-2i} = F_r$. □

Let $k(m)$ denote the period of the sequence $(F_n \bmod m)$, i.e., the least positive integer r, for which (3) is satisfied.

Example 2. We consider the generalized bi-periodic Fibonacci sequence generated by $a = 2$ and $b = c = d = 1$ that we find in [11] as A048788. The first few terms of this sequence reduced modulo $p = 3$ are

$$0, 1, 2, 0, 2, 2, 0, 2, 1, 0, 1, 1 \ldots.$$

Then we only have repetitions of these terms, so $k(3) = 12$.

Theorem 3. *Let r be a positive integer. If $a \not\equiv b \pmod{m}$ or $c \not\equiv d \pmod{m}$, the following assertions are equivalent:*

(i) $F_{n+r} \equiv F_n \pmod{m}$ *for all* $n \geq 0$*;*

(ii) $(F_r, F_{r+1}, F_{r+2}, F_{r+3}) \equiv (F_0, F_1, F_2, F_3) \pmod{m}$*;*

(iii) $(F_r, F_{r+1}) \equiv (F_0, F_1) \pmod{m}$*, and the integer r is even.*

In particular, the period $k(m)$ is an even number.

Proof. Let r be a positive integer such that $(F_r, F_{r+1}, F_{r+2}, F_{r+3}) \equiv (F_0, F_1, F_2, F_3) \pmod{m}$. If r is an odd number, we have modulo m

$$a = F_2 \equiv F_{r+2} = bF_{r+1} + dF_r \equiv bF_1 + dF_0 = b,$$

and

$$bF_2 + dF_1 = F_3 \equiv F_{r+3} = aF_{r+2} + cF_{r+1} \equiv aF_2 + cF_1.$$

Contradiction. □

So when $a \not\equiv b \pmod{m}$ or $c \not\equiv d \pmod{m}$, the period $k(m)$ is the smallest integer r satisfying one of the three properties of Theorem 3. Since any positive integer r that satisfies (3) is a multiple of the period $k(m)$ by Theorem 3, we have

$$\begin{cases} F_r \equiv 0 \pmod{m} \\ F_{r+1} \equiv 1 \pmod{m} \end{cases} \iff k(m) \mid r, \tag{4}$$

for any $r \in 2\mathbb{N}$.

The following theorem shows that we can reduce the computation of $k(m)$ to that of $k(p^e)$ for all prime power factor p^e of m.

Theorem 4. *Let $m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be the prime decomposition of m. Then*

$$k(m) = \operatorname{lcm}(k(p_1^{e_1}), k(p_2^{e_2}), \ldots, k(p_s^{e_s})).$$

Proof. The proof is similar to the proof of [16, Theorem 2]. □

Theorem 5. *If $m \mid a$, then we have $k(m) = 2\operatorname{ord}_m(d)$, where $ord_m(d)$ is the multiplicative order of d modulo m.*

Proof. Assume that $a \equiv 0 \pmod{m}$. Using Relation (2), and following a straightforward induction we get

$$F_n \bmod m = \begin{cases} 0, & \text{if } n = 2k; \\ d^k, & \text{if } n = 2k+1. \end{cases}$$

Since $n = 2\operatorname{ord}_m(d)$ is the least integer satisfying the congruences $F_{2n} \equiv 0 \pmod{m}$ and $F_{2n+1} \equiv 1 \pmod{m}$, it follows from (4) that $k(m) = 2\operatorname{ord}_m(d)$. □

2.1 The generalized bi-periodic Fibonacci sequences over a finite field

Sahin [10] provided the Binet formula for even and odd indices as follows:

$$\begin{cases} F_{2n} = a\dfrac{\alpha^n - \beta^n}{\alpha - \beta}; \\ F_{2n+1} = \dfrac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} - c\dfrac{\alpha^n - \beta^n}{\alpha - \beta}, \end{cases} \tag{5}$$

where $\alpha, \beta = \frac{(A \pm \sqrt{\Delta})}{2}$ are the roots of the quadratic equation $f(x) = x^2 - Ax + B = 0$ with $A = ab + c + d$, $B = cd$, and Δ the discriminant of $f(x)$.

Let $\mathbb{F}_q$ denote the finite field of order $q = p^e$ with $e \geq 1$, and let p be an odd prime. In this subsection, we investigate the period of $(F_n)_{n\geq 0}$ over the finite field $\mathbb{F}_q$ using as a main tool the Binet formula (5) and Statement (4).

We assume that $\gcd(c, p) = \gcd(d, p) = 1$ to guarantee that $(F_n)_{n\geq 0}$ is periodic over the field $\mathbb{F}_{p^e}$. We begin by investigating the period modulo a prime p, then we generalize to a power of p. We deal only with the cases where $a \not\equiv b \pmod{p}$ or $c \not\equiv d \pmod{p}$. For analogous results in the case $a \equiv b \pmod{p}$ and $c \equiv d \pmod{p}$; see [7, 8, 9]. We establish a divisibility relation for $k(p)$ according to the nature of the discriminant Δ in $\mathbb{F}_p^*$. When $\Delta \equiv 0 \pmod{p}$, we obtain an equality statement for $k(p)$ in terms of the order of the zero of the polynomial $f(x)$ in $\mathbb{F}_p^*$.

Notice that if $p \mid a$, then we get $k(p) = 2\operatorname{ord}_p(d)$ using Theorem 5, where $ord_p(d)$ is the order of d in $\mathbb{F}_p^*$. So in the sequel, we may assume that $\gcd(a, p) = 1$. We also use the Legendre symbol:

$$\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{for } r \text{ a nonzero quadratic residue modulo } p; \\ -1, & \text{for } r \text{ a quadratic residue modulo } p. \end{cases}$$

Theorem 6. *Let p be an odd prime. If Δ is a nonzero quadratic residue modulo p, then $k(p) \mid 2(p-1)$. Furthermore, if $\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right) = 1$, then $k(p) \mid (p-1)$.*

Proof. Suppose that Δ is a nonzero quadratic residue modulo p. Then we have $\alpha, \beta \in \mathbb{F}_p^*$, and by the Fermat little theorem we get

$$\alpha^{p-1} \equiv 1 \pmod{p} \text{ and } \beta^{p-1} \equiv 1 \pmod{p}.$$

Now, using the Binet formula for even and odd indices (5), we obtain

$$F_{2(p-1)} = a\frac{\alpha^{p-1} - \beta^{p-1}}{\alpha - \beta} \equiv 0 \pmod{p}$$

and

$$F_{2(p-1)+1} = \frac{\alpha^p - \beta^p}{\alpha - \beta} - c\frac{\alpha^{p-1} - \beta^{p-1}}{\alpha - \beta} \equiv 1 \pmod{p}.$$

Thus, by (4), $k(p) \mid 2(p-1)$.

For the second part, suppose that $\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right) = 1$. Then we have

$$\alpha^{\frac{p-1}{2}} = \beta^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Therefore,

$$F_{p-1} = a\frac{\alpha^{\frac{p-1}{2}} - \beta^{\frac{p-1}{2}}}{\alpha - \beta} \equiv 0 \pmod{p}$$

and

$$F_p = \frac{\alpha^{\frac{p+1}{2}} - \beta^{\frac{p+1}{2}}}{\alpha - \beta} - c\frac{\alpha^{\frac{p-1}{2}} - \beta^{\frac{p-1}{2}}}{\alpha - \beta} \equiv 1 \pmod{p}.$$

Thus, by (4), we get $k(p) \mid (p-1)$. □

Remark 7. If $c = d$, then we have $\alpha\beta = c^2$. Using the properties of Legendre symbol, we get

$$\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right)$$

Moreover, since $\alpha \in \mathbb{F}_p^*$, we have $ab = \alpha^{-1}(\alpha - c)^2$, where α^{-1} is the inverse of α modulo p. Thus,

$$\left(\frac{\alpha}{p}\right) = \left(\frac{ab}{p}\right).$$

Now, if Δ is a quadratic nonresidue modulo p, then the polynomial $f(x)$ is irreducible in $\mathbb{F}_p$. Therefore, we work in $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{\Delta}]$, the splitting field of the polynomial $f(x)$ over $\mathbb{F}_p$.

Since the Frobenius automorphism of $\mathbb{F}_{p^2}$ fixes $\mathbb{F}_p$, it must permute the zeros of any irreducible quadratic polynomial of $\mathbb{F}_p[x]$. Therefore, by applying the Frobenius automorphism to α, a root of the equation $f(x) = 0$, we obtain the other root $\beta = \alpha^p$. Hence,

$$\alpha^{p+1} = \beta^{p+1} = \alpha\beta. \tag{6}$$

Theorem 8. *Let p be an odd prime. If Δ is a quadratic nonresidue modulo p, then $k(p) \mid 2\operatorname{ord}_p(cd)(p+1)$.*

Proof. Suppose that Δ is a quadratic nonresidue modulo p. Then we have $\alpha^{p+1} = \beta^{p+1} = cd$. Using the Binet formula (5), we get

$$F_{2\operatorname{ord}_p(cd)(p+1)} = a\frac{(\alpha^{p+1})^{\operatorname{ord}_p(cd)} - (\beta^{p+1})^{\operatorname{ord}_p(cd)}}{\alpha - \beta} \equiv 0 \pmod{p}$$

and

$$\begin{aligned} F_{2\operatorname{ord}_p(cd)(p+1)+1} &= \frac{\alpha(\alpha^{p+1})^{\operatorname{ord}_p(cd)} - \beta(\beta^{p+1})^{\operatorname{ord}_p(cd)}}{\alpha - \beta} \quad -c\frac{(\alpha^{p+1})^{\operatorname{ord}_p(cd)} - (\beta^{p+1})^{\operatorname{ord}_p(cd)}}{\alpha - \beta} \\ &\equiv 1 \pmod{p}. \end{aligned}$$

Therefore, (4) implies that $k(p) \mid 2\operatorname{ord}_p(cd)(p+1)$. □

Example 9. We take $a = c = d = 1$ and $b = 2$. So F_n corresponds to A002530 in [11], and we have $\Delta = 12$.

Let $p = 11$; notice that Δ is a nonzero quadratic residue and ab is a quadratic nonresidue. From Theorem 6, we have $k(p) \mid 2(p-1)$ and $k(p) \nmid (p-1)$. So by giving the first few terms up to $n = 5$ $(0, 1, 1, 3, 4, 0)$ we get $k(11) = 20$.

We take $p = 7$. Since Δ is a quadratic nonresidue modulo p from Theorem 8, we obtain $k(p) \mid 16$. So we only have to calculate 10 terms of this sequence modulo 7

$$0, 1, 1, 3, 4, 4, 1, 6, 0, 6.$$

Thus, we have $k(7) = 16$.

Example 10. Take $a = 3, b = d = 1$, and $c = 4$. For $p = 11$ both Δ and ab are nonzero quadratic residues modulo p, and from Theorem 6 we have $k(p)|(p-1)$. Moreover, $k(p)$ is an even integer and $F_2 \bmod 11 = 3$. So the only possible value is $k(11) = 10$.

In the following, we consider the case where $\Delta \equiv 0 \pmod p$. We begin by giving the Binet formula of F_n for even and odd indices as follows:

$$\begin{cases} F_{2n} = a \displaystyle\sum_{i=1}^{n} \alpha^{n-i}\beta^{i-1}; \\ F_{2n+1} = \alpha^n + \displaystyle\sum_{i=1}^{n} \alpha^{n-(i+1)}\beta^{i}(\alpha - c). \end{cases}$$

Since $\Delta \equiv 0 \pmod p$, the equation $f(x) = 0$ has a repeated root α in $\mathbb{F}_p^*$. So modulo p, we get the following congruences:

$$\begin{cases} F_{2n} \equiv an\alpha^{n-1}; \\ F_{2n+1} \equiv (n+1)\alpha^n - cn\alpha^{n-1}. \end{cases} \tag{7}$$

We give in the next theorem an explicit equality statement for $k(p)$ in terms of the order of α in $\mathbb{F}_p^*$.

Theorem 11. *Let p be an odd prime. If $\Delta \equiv 0 \pmod p$, then we have $k(p) = 2p \cdot \operatorname{ord}_p(\alpha)$.*

Proof. Assume that $\Delta \equiv 0 \pmod p$ and $\gcd(a, p) = 1$. By using (7) we obtain the following:

$$\begin{aligned} F_{2n} \equiv 0 \text{ and } F_{2n+1} \equiv 1 &\Longleftrightarrow n(\alpha)^{n-1} \equiv 0 \text{ and } (\alpha)^n \equiv 1 \\ &\Longleftrightarrow p \mid n \text{ and } \operatorname{ord}_p(\alpha) \mid n \\ &\Longleftrightarrow \operatorname{lcm}(p, \operatorname{ord}_p(\alpha)) \mid n \\ &\Longleftrightarrow p \cdot \operatorname{ord}_p(\alpha) \mid n. \end{aligned}$$

Therefore, $k(p) = 2p \cdot \operatorname{ord}_p(\alpha)$. □

Theorem 4 shows that it is easy to compute $k(m)$ once we know $k(p^e)$ for all prime power factors p^e of m. The corollary of the following theorem is crucial to the investigation of the period modulo p^e.

Theorem 12. *Let p be a prime number and n be a positive integer. If $a \equiv 1 \pmod{p}$, then $a^{p^n} \equiv 1 \pmod{p^{n+1}}$.*

Proof. Let $P(n)$ be the proposition $a^{p^n} \equiv 1 \pmod{p^{n+1}}$. We have

$$a \equiv 1 \pmod{p} \Longrightarrow \exists s \in \mathbb{Z} \text{ such as } a = sp + 1.$$

For $n = 1$, $a^p = (sp+1)^p = \sum_{i=0}^{p} \binom{p}{i} (sp)^i = 1 + sp^2 + \sum_{i=2}^{p} \binom{p}{i} (sp)^i \equiv 1 \pmod{p^2}$.

Thus, $P(1)$ is true. Assume that $P(n)$ is true up to some n and consider $P(n+1)$

$$a^{p^{n+1}} = (a^{p^n})^p = (sp^{n+1}+1)^p = \sum_{i=0}^{p} \binom{p}{i} (sp^{n+1})^i = 1 + sp^{n+2} + \sum_{i=2}^{p} \binom{p}{i} (sp^{n+1})^i.$$

Since $p^{n+2} \mid (sp^{n+1})^i$ for $2 \leq i \leq p$, we obtain $a^{p^{n+1}} \equiv 1 \pmod{p^{n+2}}$.

Thus, $P(n)$ holds by induction. □

Corollary 13. *Let p be an odd prime such that $\gcd(a, p) = 1$, and let e be a positive integer. Then*

$$\alpha^{\frac{k(p)}{2} p^{e-1}} \equiv \beta^{\frac{k(p)}{2} p^{e-1}} \equiv 1 \pmod{p^e}.$$

Proof. If we assume $p \mid \Delta$, then $\alpha \equiv \beta \pmod{p}$. From Theorem 11, we get $k(p) = 2p \cdot \mathrm{ord}_p(\alpha)$. Thus,

$$\alpha^{\frac{k(p)}{2}} \equiv \beta^{\frac{k(p)}{2}} \equiv 1 \pmod{p}.$$

Now, assume that $p \nmid \Delta$. Since $p \nmid a$ by the Binet formula (5), we have

$$F_{k(p)} = a \frac{\alpha^{\frac{k(p)}{2}} - \beta^{\frac{k(p)}{2}}}{\alpha - \beta} \equiv 0 \pmod{p} \iff \alpha^{\frac{k(p)}{2}} \equiv \beta^{\frac{k(p)}{2}} \pmod{p}$$

and

$$\begin{aligned} F_{k(p)+1} &= \frac{\alpha\alpha^{\frac{k(p)}{2}} - \beta\beta^{\frac{k(p)}{2}}}{\alpha - \beta} - c\frac{\alpha^{\frac{k(p)}{2}} - \beta^{\frac{k(p)}{2}}}{\alpha - \beta} \\ &\equiv \alpha^{\frac{k(p)}{2}} \\ &\equiv 1 \pmod{p}. \end{aligned}$$

Hence, by applying Theorem 12 to $\alpha^{\frac{k(p)}{2}}$ and $\beta^{\frac{k(p)}{2}}$ we obtain the desired result. □

Now that we have results helping in the calculation of $k(p)$, we connect $k(p)$ to $k(p^e)$ in Theorem 14.

Theorem 14. *Let p be an odd prime such that $\gcd(a,p)=1$, and let e be a positive integer. Then $k(p^e) \mid p^{e-1}k(p)$.*

Proof. Since $\gcd(a,p)=1$ from Corollary 13, we have

$$\alpha^{\frac{k(p)}{2}p^{e-1}} \equiv \beta^{\frac{k(p)}{2}p^{e-1}} \equiv 1 \pmod{p^e}.$$

- If we assume $p \nmid \Delta$, then we have

$$F_{k(p)p^{e-1}} = a\frac{\alpha^{\frac{k(p)p^{e-1}}{2}} - \beta^{\frac{k(p)p^{e-1}}{2}}}{\alpha-\beta} \equiv 0 \pmod{p^e}$$

  and

$$\begin{aligned} F_{k(p)p^{e-1}+1} &= \frac{\alpha\alpha^{\frac{k(p)p^{e-1}}{2}} - \beta\beta^{\frac{k(p)p^{e-1}}{2}}}{\alpha-\beta} - c\frac{\alpha^{\frac{k(p)p^{e-1}}{2}} - \beta^{\frac{k(p)p^{e-1}}{2}}}{\alpha-\beta} \\ &\equiv 1 \pmod{p^e}. \end{aligned}$$

- If we assume $p \mid \Delta$, then using (7) we obtain

$$F_{k(p)p^{e-1}} = a\frac{k(p)p^{e-1}}{2}\alpha^{\frac{k(p)p^{e-1}}{2}-1}$$

  and

$$\begin{aligned} F_{k(p)p^{e-1}+1} &= (\frac{\beta k(p)p^{e-1}}{2}+1)\alpha^{\frac{k(p)p^{e-1}}{2}} - c\frac{\beta k(p)p^{e-1}}{2}\alpha^{\frac{k(p)p^{e-1}}{2}-1} \\ &\equiv \alpha^{\frac{k(p)}{2}p^{e-1}} \pmod{p^e}. \end{aligned}$$

  Now, since we have $k(p) = 2p \cdot \operatorname{ord}_p(\alpha)$, the following congruences holds

$$\begin{cases} F_{k(p)p^{e-1}} \equiv 0 \pmod{p^e}; \\ F_{k(p)p^{e-1}+1} \equiv 1 \pmod{p^e}. \end{cases}$$

Therefore, by (4), $k(p^e) \mid p^{e-1}k(p)$. □

3 The rank of the generalized bi-periodic Fibonacci sequences modulo m

The rank of $(F_n)_{n\geq 0}$ modulo m is the least positive integer r such that $F_r \equiv 0 \pmod{m}$. Let $d(m)$ denote the rank of $(F_n \bmod m)$. It is obvious that if $m \mid a$, we have $d(m)=2$.

In the rest, we assume that $c=d$ and $\gcd(a,m)=1$.

Lemma 15. *([12]) Let $\zeta(n)$ be the parity function, and assume that $c = d$. The sequences $(F_n)_{n\geq 0}$ satisfies the following identities:*

(i) $(b/a)^{\zeta(ng+n)}F_gF_{n+1} + (b/a)^{\zeta(ng+g)}cF_nF_{g-1} = F_{g+n} \qquad (g \geq 1, n \geq 0).$

(ii) $(b/a)^{\zeta(ng+n)}F_nF_{g+1} + (b/a)^{\zeta(ng+g)}F_{n+1}F_g = (-c)^gF_{n-g} \qquad (g \geq 0, n \geq 0).$

Wall [16, Theorem 3] proved that the indices of the Fibonacci sequence terms that are zero modulo m form an arithmetic progression. In the following theorem we give an analogous result for the bi-periodic case.

Theorem 16. *The terms for which $F_n \equiv 0 \pmod{m}$ have subscripts that form a simple arithmetic progression, i.e., $n = xl$; for $x = 0, 1, 2, \ldots$. Moreover, $l = d(m)$ gives all n with $F_n \equiv 0 \pmod{m}$.*

Proof. Assume that $\gcd(a, m) = 1$, $F_i \equiv 0 \pmod{m}$, and $F_j \equiv 0 \pmod{m}$. By setting $g = i$ and $n = j$ in the identities (i) and (ii) of Lemma 15, we obtain

$$F_{i+j} \equiv 0 \pmod{m}. \tag{8}$$

And with $(i \geq j)$

$$F_{i-j} \equiv 0 \pmod{m}. \tag{9}$$

Let

$$S = \{k \in \mathbb{Z}^* \mid \ F_k \equiv 0 \pmod{m}\}.$$

Since $F_{k(m)} \equiv 0 \pmod{m}$ the set S is not empty. Let d be the smallest integer in S. By using induction and congruence (8), we get $F_{ld} \equiv 0 \pmod{m}$ for $l \in \mathbb{Z}^*$. Now let $\alpha \in S$, and suppose that $d \mid \alpha$. Then there are two nonnegative integers θ and γ such that $\alpha = d\theta + \gamma$ with $0 < \gamma < d$. From (9), we have $F_{\alpha-\theta d} = F_\gamma \equiv 0 \pmod{m}$. This is a contradiction, since d is the smallest integer in S. Thus, α is a multiple of d. □

From Theorem 16, we have

$$F_n \equiv 0 \pmod{m} \Longleftrightarrow d(m) \mid n. \tag{10}$$

In particular, since $F_{k(m)} \equiv F_0 \equiv \pmod{m}$ then $d(m) \mid k(m)$.

Let $c = 1$ and $a, b \in \mathbb{F}_2$. Table 1 gives the rank of $(F_n \bmod 2)$.

a	b	c	$d(p)$
0	1	1	2
1	0	1	4

Table 1: $p = 2$

We are now ready to state our theorem containing some fundamental results about the rank of $(F_n \bmod m)$.

Theorem 17. *Let $m \geq 2$, and p be an odd prime such that $\gcd(a,p) = \gcd(c,p) = 1$. Then*

(a) If Δ is a nonzero quadratic residue modulo p, then $d(p) \mid (p-1)$.

(b) If Δ is a quadratic nonresidue modulo p, then $d(p) \mid 2(p+1)$.

(c) If $\Delta \equiv 0 \pmod{p}$, then if $p \mid b$ we have $d(p) = 2p$ otherwise, $d(p) = p$.

(d) If $n \mid m$, then $d(n) \mid d(m)$.

(e) Let $m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ be the prime decomposition of m. Then

$$d(m) = \operatorname{lcm}(d(p_1^{e_1}), d(p_2^{e_2}), \dots, d(p_n^{e_n})).$$

Proof. Let p be an odd prime, and let $\gcd(a,p) = 1$.

(a) Suppose that Δ is a nonzero quadratic residue modulo p. Then $\alpha, \beta \in \mathbb{F}_p^*$ and $\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right)$. Hence, we have

$$F_{p-1} = a\frac{\alpha^{\frac{p-1}{2}} - \beta^{\frac{p-1}{2}}}{\alpha - \beta} \equiv 0 \pmod{p}.$$

Thus, by (10), $d(p) \mid (p-1)$.

(b) Suppose that Δ is a quadratic nonresidue modulo p. Then by (6), we have

$$F_{2(p+1)} = a\frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} \equiv 0 \pmod{p}.$$

Thus, from (10), we get $d(p) \mid 2\,(p+1)$.

(c) Suppose that $\Delta \equiv 0 \pmod{p}$.

If we assume that $p \mid b$, then we have $\alpha = c$. Using (7), we obtain

$$F_{2n} \equiv an(c)^{n-1} \text{ and } F_{2n+1} \equiv (c)^n.$$

Then we have $F_{2n+1} \not\equiv 0 \pmod{p}$ since $\gcd(c,p) = 1$, and $d(p)$ must be even. Note that we have $F_{2n} \equiv 0 \pmod{p}$ if and only if $p \mid n$. Therefore, we obtain $d(p) = 2p$.

Now, if $p \nmid b$ then $\alpha = -c$, and we have

$$F_{2n} \equiv an(-c)^{n-1} \equiv 0 \pmod{m} \Longleftrightarrow p \mid n$$

and

$$F_{2n+1} \equiv (2n+1)(-c)^n \equiv 0 \pmod{m} \Longleftrightarrow p \mid (2n+1).$$

Since $d(p)$ is the smallest positive integer n for which $F_n \equiv 0 \pmod{p}$, we obtain $d(p) = p$.

(d) Since $F_{d(m)} \equiv 0 \pmod{m}$ and $n \mid m$, then we have $F_{d(m)} \equiv 0 \pmod{n}$. Thus, by (10), $d(n) \mid d(m)$.

For the proof of (e), see [15, Lemma 2].

□

4 Acknowledgments

The authors would like to thank the referee for his/her careful reading and helpful comments which have improved the quality of this paper. We would also like to thank Professor Ait Amrane Yacine for her contribution in the realization of this work. We are grateful for the partial support of DGRSDT under grant number C0656701.

References

[1] L. Ait-Amrane and H. Belbachir, Periods of tribonacci sequences and elliptic curves, *Algebra Discrete Math.* **25** (2018), 1–17.

[2] L. Ait-Amrane, H. Belbachir, and K. Betina, Periods of Morgan-Voyce sequences and elliptic curves *Math. Slovaca* **6** (2016), 1267–1284.

[3] L. Ait-Amrane and H. Belbachir, The three different forms of the periods of the Morgan-Voyce sequence modulo odd primes, *Les annales RECITS* **3** (2016), 27–33.

[4] M. Edson and O. Yayenie, A new generalization of Fibonacci sequences and extended Binet's formula, *Integers* **9** (2009), 639–654.

[5] S. Falcon and Á. Plaza, On the Fibonacci k-numbers, *Chaos Solitons Fractals* **32** (2007), 1615–1624.

[6] S. Falcon and Á. Plaza, k-Fibonacci sequences modulo m, *Chaos Solitons Fractals* **41** (2009), 497–504.

[7] H. C. Li, On second-order linear recurrence sequences, *Fibonacci Quart.* **37** (1999), 342–349.

[8] S. Gupta, P. Rockstroh, and F. E. Su, Splitting fields and periods of Fibonacci sequences modulo primes, *Math. Mag.* **85** (2012), 130–135.

[9] M. Renault, The period, rank and order of the (a, b)-Fibonacci sequence mod m, *Math. Mag.* **86** (2013), 372–380.

[10] M. Sahin, The Gelin-Cesàro identity in some conditional sequences, *Hacet. J. Math. Stat.* **40** (2011), 855–861.

[11] N. J. A. Sloane et al., *The On-Line Encyclopedia of Integer Sequences*, published electronically at https://oeis.org, 2021.

[12] E. Tan and H. Leung, Some basic properties of the generalized bi-periodic Fibonacci and Lucas sequences, *Adv. Difference Equ.* **26** (2020), 1–11.

[13] D. Tascı and G. Ozkan Kızılırmak, On the periods of biperiodic Fibonacci and biperiodic Lucas numbers, *Discrete Dyn. Nat. Soc.* (2016), 1–5.

[14] D. Vella and A. Vella, Cycles in the generalized Fibonacci sequence modulo a prime, *Math. Mag.* **75** (2002), 294–299.

[15] J. Vinson, The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence, *Fibonacci Quart.* **1** (1963), 37–45.

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

[17] O. Yayenie, A note on generalized Fibonacci sequences, *Appl. Math. Comput.* **217** (2011), 5603–5611.

2010 *Mathematics Subject Classification*: Primary 11B39; Secondary 11B50, 11A07.
Keywords: generalized bi-periodic Fibonacci sequence, period, rank, finite field.

(Concerned with sequences A000045, A000129, A002530, and A048788.)

Received July 3 2021; revised versions received July 9 2021; September 20 2021; September 21 2021; September 24 2021. Published in *Journal of Integer Sequences*, October 1 2021.

Return to Journal of Integer Sequences home page.