

GENERALIZED FIBONACCI SEQUENCES MODULO POWERS OF A PRIME

SCOTT SELTZER

1. INTRODUCTION

Let us begin by defining a generalized Fibonacci sequence (g_n) with all g_n in some abelian group as a sequence that satisfies the recurrence $g_n = g_{n-1} + g_{n-2}$ as n ranges over \mathbb{Z} . The Fibonacci sequence (F_n) is the generalized Fibonacci sequence with integer values defined by $F_0 = 0$ and $F_1 = 1$. Recall also the Binet formula: for any integer n , $F_n = (\alpha^n - \beta^n)/\sqrt{5}$, where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$ are the roots of the equation $f(x) = x^2 - x - 1$.

Let us define $(g_n)^{(m)}$ as the generalized Fibonacci sequence (g_n) evaluated modulo m . For example, the sequence $(F_n)^{(3)} = (\dots, 0, 1, 1, 2, 0, 2, 2, 1, 0, \dots)$ is the Fibonacci sequence evaluated modulo 3.

It may be shown that any generalized Fibonacci sequence with all elements in \mathbb{Z} modulo any integer $m > 1$ is a periodic generalized Fibonacci sequence with elements in \mathbb{Z}/m . In this paper we will look at the period of such sequences modulo powers of prime numbers.

2. PROPERTIES OF THE FIBONACCI SEQUENCE MODULO INTEGERS

Define $P(m)$ as the period of the generalized Fibonacci sequence $(F_n)^{(m)}$. Since $F_0 \equiv 0$ and $F_1 \equiv 1 \pmod{m}$, it is clear that if $P(m) = j$, then j is the smallest positive integer k such that $F_k \equiv 0$ and $F_{k+1} \equiv 1 \pmod{m}$.

Note that 5 is a square in \mathbb{Z}/p for $p \neq 2$ or 5 if and only if $p \equiv \pm 1 \pmod{10}$ [1, pp. 185–189]. If 5 is a square in \mathbb{Z}/p , then the equation $x^2 = 5$ has solutions $a, -a$ for some $a \in \mathbb{Z}/p$. Then we may take $\alpha, \beta \in \mathbb{Z}/p$ such that $\alpha = (1 + a)/2$ and $\beta = (1 - a)/2$, where α, β are the roots of the equation $f(x) = x^2 - x - 1$ in \mathbb{Z}/p .

On the other hand, if $p = 2$, then 5 is a square in \mathbb{Z}/p , since $5 \equiv 1 \pmod{2}$. However, $f(x) = x^2 - x - 1$ is irreducible in \mathbb{Z}/p , so $\alpha, \beta \notin \mathbb{Z}/p$.

Throughout this paper, we may consider the field \mathbb{Z}/p if 5 is a square in \mathbb{Z}/p for $p \neq 2$ or 5. On the other hand, if 5 is not a square in \mathbb{Z}/p for $p \neq 5$, or if $p = 2$, then the equation $f(x) = x^2 - x - 1$ has no roots in \mathbb{Z}/p , and we must consider instead the field $(\mathbb{Z}/p)[\alpha]$. In this field, $\beta = -1/\alpha$ and $\sqrt{5} = \alpha - \beta$.

Define $Z(m)$ as the smallest positive integer l such that $F_l \equiv 0 \pmod{m}$.

Theorem 1. *For any prime p , $Z(p)$ divides $P(p)$.*

Proof. First suppose that $p = 5$. Then it may be verified that $Z(p) = 5$ and $P(p) = 20$.

Now suppose that $p \neq 5$. If $\alpha \in \mathbb{Z}/p$, then let A be the field \mathbb{Z}/p . Otherwise, let A be the field $(\mathbb{Z}/p)[\alpha]$. Let $j = Z(p)$ and $k = P(p)$. Then j is the smallest positive

integer n such that $F_n = 0$ in A . I claim that $F_n = 0$ if and only if $\left(\frac{\alpha}{\beta}\right)^n = 1$. By the Binet formula,

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = 0,$$

or

$$\alpha^n - \beta^n = 0.$$

Thus,

$$\alpha^n = \beta^n$$

and

$$\left(\frac{\alpha}{\beta}\right)^n = 1.$$

Since j is the smallest integer n such that $(\alpha/\beta)^n = 1$, it follows that j is the order of α/β in A . If $k = P(p)$, then $F_k \equiv 0 \pmod{p}$, so $(\alpha/\beta)^k = 1$ in A . However, j is the order of α/β in A , so k is a multiple of j . \square

Hereafter, we shall refer to the multiplicative group of a ring A as A^* .

Theorem 2. *If $\alpha \in \mathbb{Z}/p^q$ for some prime $p \neq 5$ and some positive integer q , then let A be the ring \mathbb{Z}/p^q . Otherwise, let A be the ring $(\mathbb{Z}/p^q)[\alpha]$. Suppose that $k = P(p^q)$. Then $k = \text{lcm}(\text{ord}(\alpha), \text{ord}(\beta))$ in the multiplicative group A^* .*

Proof. If $f(x) = x^2 - x - 1$ has a root in \mathbb{Z}/p , then it can be shown that it has a root in \mathbb{Z}/p^q for all $q \in \mathbb{N}$. If $\alpha \in \mathbb{Z}/p^q$, then let A be the ring \mathbb{Z}/p^q , otherwise let A be the ring $(\mathbb{Z}/p^q)[\alpha]$. A is a ring in which $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$. In order to show that the Binet formula may hold in A , we need to show that $\alpha - \beta$ is invertible in A . We may rewrite $\alpha - \beta$:

$$\alpha - \beta = \alpha + \frac{1}{\alpha} = \frac{\alpha^2 + 1}{\alpha} = \frac{\alpha^2 + (\alpha^2 - \alpha)}{\alpha} = 2\alpha - 1.$$

Now evaluate $(2\alpha - 1)^2$:

$$(2\alpha - 1)^2 = 4\alpha^2 - 4\alpha + 1 = (4\alpha + 4) - 4\alpha + 1 = 5.$$

Thus, $1/(\alpha - \beta) = \sqrt{5}/5$. So for $p \neq 5$, $\alpha - \beta$ is invertible in A . Thus, the Binet formula holds in A .

Now suppose that $k = P(p^q)$; in other words, k is the smallest positive integer n such that $F_n = 0$ and $F_{n+1} = 1$ in A . I claim that $F_n = 0$ and $F_{n+1} = 1$ if and only if $\alpha^n = \beta^n = 1$.

Suppose that $F_n = 0$ and $F_{n+1} = 1$ in A . By the Binet formula,

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = 0.$$

Thus,

$$\alpha^n = \beta^n.$$

From the Binet formula for F_{n+1} ,

$$F_{n+1} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} = 1.$$

But $\beta^n = \alpha^n$, so

$$\alpha^n \left(\frac{\alpha - \beta}{\alpha - \beta} \right) = 1,$$

so

$$\alpha^n = 1.$$

Similarly,

$$\beta^n \left(\frac{\alpha - \beta}{\alpha - \beta} \right) = 1,$$

so

$$\beta^n = 1.$$

Conversely, suppose that $\alpha^n = \beta^n = 1$. Then by the Binet formula,

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = 0$$

and

$$F_{n+1} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} = \frac{\alpha - \beta}{\alpha - \beta} = 1.$$

Thus, k is the smallest positive integer n such that $\alpha^n = 1$ and $\beta^n = 1$ in the field A , so k is the least common multiple of the orders of α, β in the multiplicative group A^* , as defined for a particular case of p . \square

Since $\beta = -1/\alpha$, it is clear that either $\text{ord}(\alpha) = \text{ord}(\beta)$, $\text{ord}(\alpha) = 2 \text{ord}(\beta)$, or $\text{ord}(\beta) = 2 \text{ord}(\alpha)$. Thus, as a consequence of Theorem 2, $P(p^q)$ is equal to either $\text{ord}(\alpha)$ or $\text{ord}(\beta)$.

3. THE PERIOD OF THE FIBONACCI SEQUENCE MODULO p

Let us first note that it can be verified that $P(5)=20$. We will now look at $P(p)$ for $p \neq 5$.

Theorem 3. *If $\alpha \in \mathbb{Z}/p$ for a prime $p \neq 5$, then $P(p) \mid (p - 1)$.*

Proof. Let A be the multiplicative group $(\mathbb{Z}/p)^*$. By Theorem 2 and its consequence, either $P(p) = \text{ord}(\alpha)$ or $P(p) = \text{ord}(\beta)$ in A . However, $|A| = p - 1$, and by Lagrange's Theorem, the order of any element of a group must divide the order of the group. Thus, $P(p) \mid p - 1$. \square

This is all that we can say about $P(p)$ for a general value of p , where $\alpha \in \mathbb{Z}/p$, without actually determining $(F_n)^{(p)}$ and calculating $P(p)$.

Before we proceed to determine $P(p)$ for the case where $p \neq 5$ and $\alpha \notin \mathbb{Z}/p$, it will be necessary to prove the following lemma.

Lemma 1. *If $\alpha \notin \mathbb{Z}/p$, then $\alpha^p = \beta$ and $\beta^p = \alpha$ in $(\mathbb{Z}/p) [\alpha]$.*

Proof. Let A be the field $(\mathbb{Z}/p) [\alpha]$, an extension field of \mathbb{Z}/p . Note that α and β are roots of the polynomial $f(x) = x^2 - x - 1$ in the field $((\mathbb{Z}/p) [\alpha]) [x]$. Consider the Frobenius automorphism $\phi : (\mathbb{Z}/p) [\alpha] \rightarrow (\mathbb{Z}/p) [\alpha]$ defined by $\phi(a) = a^p$ [2, pp. 295-296]. Under this automorphism, $\phi(\alpha)$ and $\phi(\beta)$ must be roots of $\phi(f(x))$.

However, ϕ fixes $f(x)$ because the coefficients of $f(x)$ are all in \mathbb{Z}/p , and for any $c \in \mathbb{Z}/p$, $c^p = c$ by Fermat's Little Theorem.

Thus, $\phi(\alpha)$ and $\phi(\beta)$ are roots of $f(x)$. However, $\alpha, \beta \notin \mathbb{Z}/p$, and the equation $x^p = x$ has only the p solutions $\{d \mid d \in \mathbb{Z}/p\}$, so $\phi(\alpha) \neq \alpha$ and $\phi(\beta) \neq \beta$. But since $f(x)$ has only those two roots, $\phi(\alpha) = \beta$ and $\phi(\beta) = \alpha$. Thus, $\alpha^p = \beta$ and $\beta^p = \alpha$. \square

Theorem 4. *If $\alpha \notin \mathbb{Z}/p$ for some prime $p \neq 5$, then $P(p) \mid (2p + 2)$.*

Proof. We need to show that $F_{2p+2} \equiv 0$ and $F_{2p+3} \equiv 1 \pmod{p}$; i.e., $2p+2$ is some multiple of the period $P(p)$. Since $\alpha \notin \mathbb{Z}/p$, let A be the field $(\mathbb{Z}/p)[\alpha]$. We know from Lemma 1 that $\alpha^p = \beta$ and $\beta^p = \alpha$ in A . Thus, we have

$$\begin{aligned} F_{2p+2} &= \frac{\alpha^{2p+2} - \beta^{2p+2}}{\alpha - \beta} \\ &= \frac{\alpha^{2p}\alpha^2 - \beta^{2p}\beta^2}{\alpha - \beta} \\ &= \frac{\beta^2\alpha^2 - \alpha^2\beta^2}{\alpha - \beta} \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} F_{2p+3} &= \frac{\alpha^{2p+3} - \beta^{2p+3}}{\alpha - \beta} \\ &= \frac{\alpha^{2p}\alpha^3 - \beta^{2p}\beta^3}{\alpha - \beta} \\ &= \frac{\beta^2\alpha^3 - \alpha^2\beta^3}{\alpha - \beta} \\ &= (\alpha^2\beta^2) \frac{\alpha - \beta}{\alpha - \beta} \\ &= (-1)^2 \\ &= 1. \end{aligned}$$

Therefore, $F_{2p+2} \equiv 0$ and $F_{2p+3} \equiv 1 \pmod{p}$, so $2p+2$ is a multiple of $P(p)$. \square

Once again, this is all that we can say about $P(p)$ for a general value of p , where $\alpha \notin \mathbb{Z}/p$, without actually determining $(F_n)^{(p)}$ and calculating $P(p)$.

4. THE PERIOD OF THE FIBONACCI SEQUENCE MODULO A POWER OF A PRIME

Theorem 5. *If $P(p^q) = s$ for some prime $p \neq 5$ and some $q \in \mathbb{N}$, then either $P(p^{q+1}) = s$ or $P(p^{q+1}) = ps$.*

Proof. As stated previously, if $f(x) = x^2 - x - 1$ has a root in \mathbb{Z}/p , then it can be shown that it has a root in \mathbb{Z}/p^q for all $q \in \mathbb{N}$. Let us define α and β as the roots of $f(x)$ in either \mathbb{Z}/p^{q+1} or $\mathbb{Z}/p^{q+1}[\alpha]$, depending on whether or not $f(x)$ has a root in \mathbb{Z}/p , with $\beta = -1/\alpha$. It is clear that if α, β satisfy $f(x) = x^2 - x - 1$ modulo p^{q+1} , then they satisfy $f(x)$ modulo p^r for all integers $0 < r < q+1$.

If $\alpha \in \mathbb{Z}/p^{q+1}$, then let A be the ring \mathbb{Z}/p^q and B be the ring \mathbb{Z}/p^{q+1} ; otherwise, let A be the ring $(\mathbb{Z}/p^q)[\alpha]$ and B be the ring $\mathbb{Z}/p^{q+1}[\alpha]$. We know from Theorem

2 that s is the smallest positive integer n such that $\alpha^n = \beta^n = 1$ in A^* . Thus, $\alpha^s = tp^q + 1$ for some $t \in A$, and $\beta^s = up^q + 1$ for some $u \in A$. Thus,

$$\begin{aligned} \alpha^{ps} &= (tp^q + 1)^p \\ &= \binom{p}{p} (tp^q)^p + \binom{p}{p-1} (tp^q)^{p-1} + \dots + \binom{p}{1} tp^q + 1. \end{aligned}$$

However, the second-to-last term is divisible by p^{q+1} , and every preceding term is divisible by p^{2q} , so every term but the last is divisible by p^{q+1} . Thus, $\alpha^{ps} = vp^{q+1} + 1$ for some $v \in B$. Similarly, $\beta^{ps} = wp^{q+1} + 1$ for some $w \in B$. So by Theorem 2, sp is a multiple of $P(p^{q+1})$.

Now suppose that n is a multiple of $P(p^{q+1})$, so that $F_n \equiv 0$ and $F_{n+1} \equiv 1 \pmod{p^{q+1}}$. Then it is clear that $F_n \equiv 0$ and $F_{n+1} \equiv 1 \pmod{p^q}$ as well. Thus, $P(p^{q+1})$ is a multiple of $P(p^q)$.

So sp is a multiple of $P(p^{q+1})$, which in turn is a multiple of $P(p^q) = s$. As a result, either $sp = P(p^{q+1})$, or $sp = pP(p^{q+1})$. □

5. GENERAL FIBONACCI SEQUENCES MODULO A POSITIVE INTEGER

It may be shown that $\{(F_n)^{(a)}, (F_{n+1})^{(a)}\}$ forms a basis for the set of all generalized Fibonacci sequences $(g_n)^{(a)}$, as defined in the introduction.

Theorem 6. *If $(g_n)^{(a)}$ is an arbitrary Fibonacci sequence modulo any integer $a > 1$, then the period of $(g_n)^{(a)}$ divides $P(a)$.*

Proof. We may write $(g_n)^{(a)}$ as a linear combination of the two generalized Fibonacci sequences $(F_n)^{(a)}$ and $(F_{n+1})^{(a)}$: $(g_n)^{(a)} = j(F_n)^{(a)} + k(F_{n+1})^{(a)}$ for some numbers j, k . Looking at g_0 and g_1 , we thus have that

$$\begin{aligned} g_0 &= jF_0 + kF_1 \\ &= j0 + k1 \\ (1) \quad &= k \end{aligned}$$

and

$$\begin{aligned} g_1 &= jF_1 + kF_2 \\ &= j1 + k1 \\ (2) \quad &= j + k. \end{aligned}$$

Thus, if l is the period of $(g_n)^{(a)}$, then $g_l \equiv j$ and $g_{l+1} \equiv j + k \pmod{a}$. All that remains is to show that $P(a)$ is a multiple of l .

If $m = P(a)$, then $F_m \equiv 0$ and $F_{m+1} \equiv 1 \pmod{a}$. Thus, modulo a we see that

$$\begin{aligned} g_m &= jF_m + kF_{m+1} \\ &= j0 + k1 \\ &= k \end{aligned}$$

and

$$\begin{aligned} g_{m+1} &= jF_{m+1} + kF_{m+2} \\ &= j1 + k1 \\ &= j + k. \end{aligned}$$

Thus, m is a multiple of the period of $(g_n)^{(a)}$, so the period of $(g_n)^{(a)}$ divides $P(a)$. \square

A consequence of Theorem 6 is that the period of any generalized Fibonacci sequence modulo a may be at most the period of the Fibonacci sequence modulo a .

Theorem 7. *Given a periodic generalized Fibonacci sequence $(g_n)^{(a)}$ for some integer $a > 0$, if the matrix $\begin{pmatrix} g_0 & g_1 \\ g_1 & g_0 + g_1 \end{pmatrix}$ is invertible in \mathbb{Z}/a , then the period of $(g_n)^{(a)}$ is equal to $P(a)$. If the matrix is not invertible in \mathbb{Z}/a , then the period of $(g_n)^{(a)}$ may be either less than or equal to $P(a)$.*

Proof. If $(F_n)^{(a)}$ can be written as a linear combination of the periodic generalized Fibonacci sequences $(g_n)^{(a)}$, $(g_{n+1})^{(a)}$, then by the same reasoning as for Theorem 6, $P(a)$ divides the period of $(g_n)^{(a)}$. This is possible if, for all $n \in \mathbb{Z}$, $F_n \equiv jg_n + kg_{n+1} \pmod{a}$ for some numbers j, k , which in turn is possible only if the following system of equations has a nonzero solution:

$$\begin{aligned} jg_0 + kg_1 &\equiv F_0 \equiv 0 \pmod{a} \\ jg_1 + kg_2 &= jg_1 + k(g_0 + g_1) \equiv F_1 \equiv 1 \pmod{a} \end{aligned}$$

In other words, the matrix $\begin{pmatrix} g_0 & g_1 \\ g_1 & g_0 + g_1 \end{pmatrix}$ is invertible. If this is so, then $P(a)$ divides the period of $(g_n)^{(a)}$, and by Theorem 6 the period of $(g_n)^{(a)}$ divides $P(a)$, so the periods of $(F_n)^{(a)}$, $(g_n)^{(a)}$ are equal.

On the other hand, if the matrix is not invertible, then the periods of the two sequences are not necessarily equal, so the period of $(g_n)^{(a)}$ may or may not be less than $P(a)$. \square

For example, look at the generalized Fibonacci sequence (h_n) defined by $h_0 = 3$ and $h_1 = 1$. The matrix $\begin{pmatrix} 3 & 1 \\ 1 & 4 \end{pmatrix}$ has determinant 11, so modulo any multiple of 11 it is not invertible, so it need not have its period equal to that of the Fibonacci sequence. For example, modulo 11 its period is 5, which is half of $P(11)$. On the other hand, modulo 4, for example, this sequence has period 6, which is equal to $P(4)$.

Another example is the Lucas sequence (L_n) , defined by $L_0 = 2$ and $L_1 = 1$. The matrix $\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$ has determinant 5, and thus modulo any integer divisible by 5 the period of the Lucas sequence may be less than the period of the Fibonacci sequence.

REFERENCES

- [1] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, 1998.
- [2] S. Lang, *Undergraduate Algebra, Second Edition*, Springer-Verlag, New York, 1990.

BRANDEIS UNIVERSITY, WALTHAM, MA 02454-9110
E-mail address: seltzer@brandeis.edu