CONDITIONS FOR THE EXISTENCE OF GENERALIZED FIBONACCI PRIMITIVE ROOTS

Hua-Chieh Li
Department of Mathematics, National Tsing Hua University
Hsinchu, Taiwan 30043, Republic of China
(Submitted August 1998-Final Revision October 1998)

1. INTRODUCTION

Consider sequences of integers $\{U_n\}_{n=0}^{\infty}$ defined by $U_n = aU_{n-1} + bU_{n-2}$ for all integers $n \geq 2$, where $U_0 = 0$, $U_1 = 1$, a and b are given integers. We call these sequences generalized Fibonacci sequences with parameters a and b. In the case where $a = b = 1$, the sequence $\{U_n\}_{n=0}^{\infty}$ is called the Fibonacci sequence, and we denote its terms by $F_0, F_1, \ldots$.

The polynomial $f(x) = x^2 - ax - b$ with discriminant $D = a^2 + 4b$ is called the characteristic polynomial of the sequence $\{U_n\}_{n=0}^{\infty}$. Suppose that $f(x) = 0$ has two distinct solutions α and β. Then we can express U_n in the *Binet form*,

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

This and its relative $V_n = \alpha^n + \beta^n$ are known as *Lucas functions* as well and have a rich history. Please see the pioneering work of the late D. Lehmer [2] for more detail. Let p be a prime number. If $x = g$ satisfies the congruence $f(x) = x^2 - ax - b \equiv 0 \pmod{p}$, then by setting $W_0 = 1$, $W_1 = g$, and $W_n = aW_{n-1} + bW_{n-2}$, we have that $W_n \equiv g^n \pmod{p}$. We have given particular attention to those cases having the longest possible cycles, i.e., the number g being a primitive root modulo p; these are the most important cases in practical applications of the theory. We call g a generalized Fibonacci primitive root modulo p with parameters a and b if g is a root of $x^2 - ax - b \equiv 0 \pmod{p}$ and g is a primitive root modulo p. In particular, in the case $a = b = 1$, we call g a Fibonacci primitive root.

Fibonacci primitive roots modulo p have an extensive literature (see, e.g., [1], [3], [4], [7], [8], and [9]). For generalized Fibonacci primitive roots modulo p, R. A. Mollin [5] dealt with the case $a = 1$ and B. M. Phong [6] dealt with the case $b = \pm 1$. Mollin's work was the first to introduce the notion of a generalized Fibonacci primitive root based upon the pioneering work of the last D. Shanks [8]. In this paper we consider even more general cases, i.e., with arbitrary a and b. Our main theorem generalizes the results of Mollin and Phong.

2. NOTATIONS AND PRELIMINARY RESULTS

Let $\{U_n\}_{n=0}^{\infty}$ be the generalized Fibonacci sequence with parameters a and b. In this section we always suppose that b is relatively prime to m and suppose that $x^2 - ax - b \equiv 0 \pmod{m}$ has two distinct solutions modulo m.

For convenience, we introduce some notations:

(1) Let α be an integer relatively prime to m. Denote $\mathrm{ord}_m(\alpha)$ the least positive integer x such that $\alpha^x \equiv 1 \pmod{m}$.

(2) $k(m)$ is called the period of the sequence $\{U_n\}_{n=0}^{\infty}$ modulo m if it is the smallest positive integer for which $U_{k(m)} \equiv 0 \pmod{m}$ and $U_{k(m)+1} \equiv 1 \pmod{m}$.

(3) $[x, y]$ is the least common multiple of x and y.

(4) For an odd prime p, (β / p) denotes the Legendre symbol; i.e., $(\beta / p) = 1$ if and only if $y^2 \equiv \beta \pmod{p}$ is solvable.

We now state some elementary results that will be useful later.

Suppose that α and β are distinct solutions to $x^2 - ax - b \equiv 0 \pmod{m}$. Let $l = [\mathrm{ord}_m(\alpha), \mathrm{ord}_m(\beta)]$. Since $\alpha\beta \equiv -b \pmod{m}$, we have that $1 \equiv (\alpha\beta)^l \equiv (-b)^l \pmod{m}$. This implies that

$$\mathrm{ord}_m(-b) \mid [\mathrm{ord}_m(\alpha), \mathrm{ord}_m(\beta)].$$

By a similar argument, we have that

$$\mathrm{ord}_m(\alpha) \mid [\mathrm{ord}_m(-b), \mathrm{ord}_m(\beta)]$$

and

$$\mathrm{ord}_m(\beta) \mid [\mathrm{ord}_m(\alpha), \mathrm{ord}_m(-b)].$$

In particular, if $\mathrm{ord}_m(-b) \mid \mathrm{ord}_m(\alpha)$, then $\mathrm{ord}_m(\beta) \mid \mathrm{ord}_m(\alpha)$ and vice versa. We have the following lemma.

Lemma 2.1: Let α and β be the two distinct solutions to $x^2 - ax - b \equiv 0 \pmod{m}$. Suppose that $\mathrm{ord}_m(-b) \mid \mathrm{ord}_m(\alpha)$. Then we have $\mathrm{ord}_m(\beta) \mid \mathrm{ord}_m(\alpha)$. Furthermore, $\mathrm{ord}_m(\beta) = \mathrm{ord}_m(\alpha)$ if and only if $\mathrm{ord}_m(-b) \mid \mathrm{ord}_m(\beta)$.

Lemma 2.2: Let α and β be the two distinct solutions to $x^2 - ax - b \equiv 0 \pmod{m}$ and let $k(m)$ be the period of the generalized Fibonacci sequence with parameters a and b modulo m. Then

$$k(m) = [\mathrm{ord}_m(\alpha), \mathrm{ord}_m(\beta)].$$

Proof: Since α and β are the two distinct solutions to $x^2 - ax - b \equiv 0 \pmod{m}$,

$$\alpha^n \equiv a\alpha^{n-1} + b\alpha^{n-2} \pmod{m} \quad \text{and} \quad \beta^n \equiv a\beta^{n-1} + b\beta^{n-2} \pmod{m}.$$

Consider the sequence $\{A_n\}_{n=0}^{\infty}$, where $A_n - b\alpha U_{n-2} + \alpha^2 U_{n-1}$. Since $\{A_n\}_{n=0}^{\infty}$ and $\{\alpha^n\}_{n=0}^{\infty}$ both satisfy the same recurrence relation modulo m and $A_2 \equiv \alpha^2$, $A_3 \equiv \alpha^3 \pmod{m}$. Therefore, we have that $A_n \equiv \alpha^n \pmod{m}$ for all $n \geq 2$. Thus, $\alpha^n \equiv b\alpha U_{n-2} + \alpha^2 U_{n-1} \pmod{m}$ and, similarly, we have $\beta^n \equiv b\beta U_{n-2} + \beta^2 U_{n-1} \pmod{m}$. This tells us that if $k(m)$ is the period of the generalized Fibonacci sequence modulo m then

$$\alpha^{k(m)+2} \equiv b\alpha U_{k(m)} + \alpha^2 U_{k(m)+1} \pmod{m}.$$

Hence, $\mathrm{ord}_m(\alpha) \mid k(m)$ and $\mathrm{ord}_m(\beta) \mid k(m)$. On the other hand, consider the Binet form

$$U_n \equiv \frac{\alpha^n - \beta^n}{\alpha - \beta} \pmod{m}.$$

Let $l = [\mathrm{ord}_m(\alpha), \mathrm{ord}_m(\beta)]$. $\alpha^l - \beta^l \equiv 0 \pmod{m}$ and $\alpha^{l+1} - \beta^{l+1} \equiv \alpha - \beta \pmod{m}$. This implies that $U_l \equiv 0 \pmod{m}$ and $U_{l+1} \equiv 1 \pmod{m}$. Thus, $k(m) \mid [\mathrm{ord}_m(\alpha), \mathrm{ord}_m(\beta)]$. □

3. GENERALIZED FIBONACCI PRIMITIVE ROOTS MODULO p

The conditions for the existence of Fibonacci primitive roots modulo p and their properties were studied by several authors. In this section we will generalize their results to generalized Fibonacci primitive roots. Again $\{U_n\}_{n=0}^{\infty}$ is the generalized Fibonacci sequence with parameters a and b. For completeness, we begin with special cases. Since the argument is quite straightforward, we omit the proofs.

Proposition 3.1: Let p be an odd prime and let $\{U_n\}_{n=0}^{\infty}$ be the generalized Fibonacci sequence with parameters a and b.

(1) Suppose that $p \mid b$ but $p \nmid a$. Then there exists a generalized Fibonacci primitive root for $\{U_n\}_{n=0}^{\infty}$ modulo p if and only if $z = p$ is the least integer greater than 1 such that $U_z \equiv 1 \pmod{p}$. Moreover, in this case, a is the unique generalized Fibonacci primitive root for $\{U_n\}_{n=0}^{\infty}$ modulo p.

(2) Suppose that $p \mid a^2+4b$. Then there exists a generalized Fibonacci primitive root for $\{U_n\}_{n=0}^{\infty}$ modulo p if and only if $k(p) = p(p-1)$. Moreover, in this case, $\alpha \equiv a/2 \pmod{p}$ is the unique generalized Fibonacci primitive root for $\{U_n\}_{n=0}^{\infty}$ modulo p.

For the remainder of this section we assume that p is an odd prime with $(D/p)=1$, where $D = a^2+4b$ and $p \nmid b$.

In the Fibonacci case, $\{F_n\}_{n=0}^{\infty}$ possesses a Fibonacci primitive root modulo p if and only if the period of $\{F_n\}_{n=0}^{\infty}$ modulo p equals $p-1$ (for results on Fibonacci primitive roots, we refer to [6]). This is not always true for generalized Fibonacci primitive roots. We have the following example.

Example: Let $a=1, b=2$, and $p=7$. $\{U_n\}_{n=0}^{\infty} \equiv \{0,1,1,3,5,4,0,1,\dots\} \pmod{7}$. The period of $\{U_n\}_{n=0}^{\infty}$ modulo p is $p-1$. $x \equiv 2$ and $6 \pmod{7}$ are distinct roots to $x^2-x-2 \equiv 0 \pmod{7}$ but neither 2 nor 6 is a primitive root modulo 7. Hence, there is no generalized Fibonacci primitive root modulo 7 for $\{U_n\}_{n=0}^{\infty}$ with parameters 1 and 2.

However, by Lemma 2.2, there is no generalized Fibonacci primitive root modulo p if $k(p) \neq p-1$.

Lemma 3.2: Let α and β be two distinct roots of $x^2-ax-b \equiv 0 \pmod{p}$. Then there exists a generalized Fibonacci primitive root modulo p for $\{U_n\}_{n=0}^{\infty}$ with parameters a and b if and only if $k(p)=p-1$ and either $\mathrm{ord}_p(-b) \mid \mathrm{ord}_p(\alpha)$ or $\mathrm{ord}_p(-b) \mid \mathrm{ord}_p(\beta)$.

Proof: Suppose that α is a primitive root modulo p. Then $\mathrm{ord}_p(-b) \mid \mathrm{ord}_p(\alpha)$ by Euler's theorem, and $k(p)=p-1$ by Lemma 2.2. Conversely, suppose that $\mathrm{ord}_p(-b) \mid \mathrm{ord}_p(\alpha)$. Then $\mathrm{ord}_p(\beta) \mid \mathrm{ord}_p(\alpha)$ by Lemma 2.1, and hence $k(p) = \mathrm{ord}_p(\alpha)$ by Lemma 2.2. By the assumption, $k(p)=p-1$, and our proof is complete. □

Theorem 3.3: Suppose that $\mathrm{ord}_p(-b) = q$, where q is a prime power of 1. Then there exists a generalized Fibonacci root modulo p for $\{U_n\}_{n=0}^{\infty}$ with parameters a and b if and only if $k(p)=p-1$.

Proof: Let α and β be two distinct roots of $x^2-ax-b \equiv 0 \pmod{p}$. Since $q = \mathrm{ord}_p(-b) \mid [\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)]$ and q is a prime power, this implies $\mathrm{ord}_p(-b) \mid \mathrm{ord}_p(\alpha)$ or $\mathrm{ord}_p(-b) \mid \mathrm{ord}_p(\beta)$. By Lemma 3.2, our claim follows. □

Example: Consider the Fibonacci sequence. Since $b=1$, $\mathrm{ord}_p(-b)=2$. We have that there exists a Fibonacci primitive root modulo p if and only if the period of the Fibonacci sequence modulo p is $p-1$.

Naturally, we ask if anything more can be said about the existence of generalized Fibonacci primitive roots modulo p with parameters a and b, for $\mathrm{ord}_p(-b)$ not a prime power. The following example shows that nothing more can be said in this case.

Example:

(1) We have that $a=1$, $b=2$, and $p=7$. $\mathrm{ord}_7(-2)=2\cdot 3$, and there is no generalized Fibonacci primitive root modulo 7 with parameters 1 and 2.

(2) Let $a=-1$, $b=2$, and $p=7$.Then $\{U_n\}_{n=0}^{\infty}\equiv\{0,1,6,3,2,4,0,1,\dots\}\pmod 7$. The period of $\{U_n\}_{n=0}^{\infty}$ modulo p is $p-1$, and $x\equiv 5$ and $1 \pmod 7$ are distinct roots of $x^2-x-2\equiv 0 \pmod 7$. 5 is a primitive root modulo 7. Hence, there is a general-ized Fibonacci primitive root modulo 7 for $\{U_n\}_{n=0}^{\infty}$ with parameters -1 and 2.

Suppose that $\mathrm{ord}_p(-b)=q$. Let α and β be two distinct roots of $x^2-ax-b\equiv 0 \pmod p$. Let $\mathrm{ord}_p(\alpha)=n_1$ and let $\mathrm{ord}_p(\beta)=n_2$. Suppose that $q\mid n_1$. Then, by Lemma 2.1, we have that $n_2\mid n_1$. Moreover, since $(\alpha)^{qn_2}\equiv(\alpha\beta)^{qn_2}\equiv(-b)^{qn_2}\equiv 1 \pmod p$, we have that $n_2\mid n_1$ and $n_1\mid qn_2$.

Theorem 3.4: Suppose that $\mathrm{ord}_p(-b)=q$ (hence $q\mid p-1$), where q is a prime power. Suppose also that the period of the generalized Fibonacci sequence with parameters a and b modulo p is $p-1$. Then we have the following:

(1) Suppose that $q^2\mid p-1$. Then there exist two distinct general Fibonacci primitive roots modulo p with parameters a and b.

(2) Suppose that $q\nmid(p-1)/2$. Then there exists exactly one generalized Fibonacci primitive root modulo p with parameters a and b.

Proof:

(1) Let α and β be two distinct roots of $x^2-ax-b\equiv 0 \pmod p$. By Theorem 3.3, the assumption implies that either α or β is a primitive root modulo p; let us say that α is a primitive root. By Lemma 2.1, $q\mid\mathrm{ord}_p(\beta)$ if and only if β is a primitive root modulo p. Suppose that $q\nmid\mathrm{ord}_p(\beta)$. By the assumption $q^2\mid p-1$, it follows that $p-1\nmid q\,\mathrm{ord}_p(\beta)$. This contradicts the argument above which says that $\mathrm{ord}_p(\alpha)=p-1\mid q\,\mathrm{ord}_p(\beta)$. Therefore, β is also a primitive root modulo p.

(2) $\mathrm{ord}_p(-b)\nmid(p-1)/2$ is equivalent to $(-b/p)=-1$. Since $\alpha\beta=-b$, it is impossible that $(\alpha/p)=-1$ and $(\beta/p)=-1$. Our claim follows. □

Remark: Theorems 3.3 and 3.4 generalize Phong ([6], Theorem 1). In his case, $b=1$, and hence $\mathrm{ord}_p(-b)=2$. Therefore, suppose $k(p)=p-1$. $p\equiv 1 \pmod 4$ (i.e., $4\mid p-1$) implies the existence of two distinct generalized Fibonacci primitive roots modulo p, and $p\equiv -1 \pmod 4$ (i.e., $2\nmid(p-1)/2$) implies the existence of exactly one generalized Fibonacci primitive root modulo p.

Suppose that $q^2\nmid p-1$. There may be two or only one generalized Fibonacci primitive root modulo p. Our next example illustrates these cases.

Example:

(1) Consider $a=1, b=2$, and $p=11$. $\text{ord}_p(-b)=5$ and $5^2 \nmid p-1$. $\{U_n\}_{n=0}^{\infty} \equiv \{0, 1, 1, 3, 5, 0, 10, 10, 8, 6, 0, 1, \ldots\}$ (mod 11). The period $\{U_n\}_{n=0}^{\infty}$ modulo p is $p-1$, and $x \equiv 2$ and -1 (mod 11) are distinct roots of $x^2-x-2 \equiv 0$ (mod 11). 2 is a primitive root modulo 11 and -1 is not a primitive root modulo 11. Hence, there is a generalized Fibonacci primitive root modulo 11 for $\{U_n\}_{n=0}^{\infty}$ with parameters 1 and 2.

(2) Consider $a=-1$, $b=6$, and $p=11$. $\text{ord}_p(-b)=5$ and $5^2 \nmid p-1$. $\{U_n\}_{n=0}^{\infty} \equiv \{0, 1, 10, 7, 9, 0, 10, 1, 4, 2, 0, 1, \ldots\}$ (mod 11). The period $\{U_n\}_{n=0}^{\infty}$ modulo p is $p-1$, and $x \equiv 2$ and 8 (mod 7) are distinct roots of $x^2+x-6 \equiv 0$ (mod 11). Both 2 and 8 are primitive roots modulo 11. Hence, there are two generalized Fibonacci primitive roots modulo 11 for $\{U_n\}_{n=0}^{\infty}$ with parameters -1 and 6.

4. SOME INTERESTING EXAMPLES

In [8], D. Shanks asked whether there exist infinitely many primes possessing Fibonacci primitive roots. For generalized Fibonacci primitive roots similar questions can be asked. In [4], Mays proved that if $p=60k-1$ and $q=30k-1$ are both prime, then there exists a Fibonacci primitive root modulo p. Phong (see [6], Corollary 3) generalized Mays' result for a generalized Fibonacci sequence with parameters a and $b=1$, which says that if a is an integer and both q and $p=2q+1$ are primes with $(D/p)=1$, where $D=a^2+4$, then there exists exactly one generalized Fibonacci primitive root modulo p with parameters a and $b=1$. Mollin (see [5], Theorem 1), following Mays' method, proved the following: Suppose that $p>b>2$ and $(D/p)=1$, where $D=4b+1$ and $p=2q+1$ is a prime with q an odd prime. Furthermore, suppose that b has order q modulo p. Then there exists a generalized Fibonacci primitive root modulo p with parameters $a=1$ and b. Our next theorem generalizes Phong and Mollin's results.

Theorem 4.1: Suppose that $p=2q+1$ is a prime with q an odd prime and suppose that $(D/p)=1$, where $D=a^2+4b$. Furthermore, suppose that $1+a-b \not\equiv 0$ (mod p) and $\text{ord}_p(b)=1$ or q. Then there exists exactly one generalized Fibonacci primitive root modulo p with parameters a and b.

Proof: Suppose that $\text{ord}_p(-b)=q$. Then $b^q \equiv -1$ (mod p). This contradicts our assumption that $\text{ord}_p(b)=1$ or q. Our assumption also says that $\text{ord}_p(-b) \neq 1$, because otherwise $\text{ord}_p(b)=2$. Therefore, the possible order for $-b$ modulo p is 2 or $2q$. Let α and β be two distinct roots of $x^2-\alpha x-b \equiv 0$ (mod p). Since $\text{ord}_p(-b) \mid [\text{ord}_p(\alpha), \text{ord}_p(\beta)]$, this implies that either $\text{ord}_p(\alpha)$ is even or $\text{ord}_p(\beta)$ is even; say that $\text{ord}_p(\alpha)$ is even. Now, since -1 is not a root of $x^2-\alpha x-b \equiv 0$ (mod p), by the assumption, it follows that $\text{ord}_p(\alpha)=2q=p-1$, and by the same reasoning as in Theorem 3.4(2), there exists exactly one generalized Fibonacci primitive root modulo p.

Remark: Suppose that $p=2q+1$ is a prime with q an odd prime and suppose that $(D/p)=1$, where $D=a^2+4b$. Furthermore, suppose that $1+a-b \not\equiv 0$ (mod p) and $b \not\equiv -1$ (mod p). Let α and β be two roots of $x^2-\alpha x-b \equiv 0$ (mod p). Then Theorem 4.1 says that among α, β, and $-\alpha\beta$ there exists one primitive root modulo p. Unfortunately, we do not know whether or not there exist infinitely many such p.

In [10], Wall asked whether, for a Fibonacci sequence, $k(p) = k(p^2)$ is always impossible; up to now, this is still an open question. According to Williams [11], $k(p) \neq k(p^2)$ for every odd prime p less than 10^9. Our next proposition states that, for a generalized Fibonacci sequence, it is possible that $k(p) = k(p^2)$.

Proposition 4.2: For any odd prime p, there exists a generalized Fibonacci sequence with parameters a and b such that $k(p) = k(p^2)$.

Proof: For any odd prime p, choose $\alpha \not\equiv 0 \pmod p$ and $\beta \not\equiv 0 \pmod p$ such that $\alpha \not\equiv \beta$ (mod p). By Hensel's lemma, there exist $\alpha' \equiv \alpha \pmod p$ and $\beta' \equiv \beta \pmod p$ such that $\mathrm{ord}_{p^2}(\alpha') = \mathrm{ord}_p(\alpha)$ and $\mathrm{ord}_{p^2}(\beta') = \mathrm{ord}_p(\beta)$. Choose $a = \alpha' + \beta'$ and $b = -\alpha'\beta'$. Consider the generalized Fibonacci sequence $\{U_n\}_{n=0}^{\infty}$ with parameters a and b. Then, by Lemma 2.2,

$$k(p) = [\mathrm{ord}_p(\alpha'), \mathrm{ord}_p(\beta')] = [\mathrm{ord}_{p^2}(\alpha'), \mathrm{ord}_{p^2}(\beta')] = k(p^2). \quad \square$$

Example: For $p = 5$, consider $\alpha = 2$ and $\beta = 1$. We have that $\mathrm{ord}_{25}(7) = \mathrm{ord}_5(2) = 4$ and $\mathrm{ord}_{25}(1) = \mathrm{ord}_5(1) = 1$. Let $a = 7 + 1 = 8$ and $b = -7$. Then $\{U_n\}_{n=0}^{\infty} \equiv \{0, 1, 3, 2, 0, 1, \dots\} \pmod 5$ and $\{U_n\}_{n=0}^{\infty} \equiv \{0, 1, 8, 7, 0, 1, \dots\} \pmod{25}$.

ACKNOWLEDGMENT

The author would like to express his appreciation to the anonymous referee for making valuable suggestions regarding the presentation of this paper.

REFERENCES

1. P. Kiss & B. M. Phong. "On the Connection between the Rank of Apparition of a Prime p in the Fibonacci Sequence and the Fibonacci Primitive Roots." *The Fibonacci Quarterly* **15.4** (1977):347-49.
2. D. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. of Math.* **31** (1930):419-48.
3. M. J. DeLeon. "Fibonacci Primitive Roots and Period of the Fibonacci Numbers Modulo p." *The Fibonacci Quarterly* **15.4** (1977):353-55.
4. M. E. Mays. "A Note on Fibonacci Primitive Roots." *The Fibonacci Quarterly* **20.2** (1982): 111.
5. R. A. Mollin. "Generalized Fibonacci Primitive Roots and Class Numbers of Real Quadratic Fields." *The Fibonacci Quarterly* **24.1** (1986):46-53.
6. B. M. Phong. "Lucas Primitive Roots." *The Fibonacci Quarterly* **29.1** (1991):66-71.
7. D. Shanks. *Solved and Unsolved Problems in Number Theory*. 2nd ed. New York: Chelsea, 1978.
8. D. Shanks. "Fibonacci Primitive Roots." *The Fibonacci Quarterly* **10.2** (1972):162-68.
9. D. Shanks & L. Taylor. "An Observation on Fibonacci Primitive Roots." *The Fibonacci Quarterly* **11.2** (1973):159-60.
10. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* **67** (1960):525-32.
11. H. C. Williams. "A Note on the Fibonacci Quotient $F_{p-\varepsilon}/p$." *Canad. Math. Bull.* **25** (1982): 366-70.

AMS Classification Numbers: 11B39, 11A07, 11B50