FIBONACCI PRIMITIVE ROOTS AND THE PERIOD OF THE FIBONACCI NUMBERS MODULO P

M. J. DE LEON
Florida Atlantic University, Boca Raton, Florida 33432

One says g is a *Fibonacci primitive root* modulo p, where p is a prime, iff g is a primitive root modulo p and $g^2 \equiv g + 1 \pmod p$. In [1], [2], and [3] some interesting properties of Fibonacci primitive roots were developed. In this paper, we shall show that a necessary and sufficient condition for a prime $p \neq 5$ to have a Fibonacci primitive root is $p \equiv 1$ or $9 \pmod{10}$ and $A(p) = p - 1$, where $A(p)$ is the period of the Fibonacci numbers modulo p (Theorem 1); for $p \equiv 11$ or $19 \pmod{20}$, we shall explicitly determine the Fibonacci primitive root if it exists (Proposition 1). In the sequel, F_n will denote the n^{th} Fibonacci number and p will denote a prime greater than five.

Theorem 1. There exists a Fibonacci primitive root modulo p Iff $p \equiv 1$ or $9 \pmod{10}$ and $A(p) = p - 1$.

Before proving six lemmas needed to prove Theorem 1, we shall remark (see [2] for a proof) that the congruence equation $x^2 \equiv x + 1 \pmod p$ has no solutions for $p \equiv 3$ or $7 \pmod{10}$, one solution modulo 5, and two solutions modulo p for $p \equiv 1$ or $9 \pmod{10}$.

Lemma 1. If $g^2 \equiv g + 1 \pmod p$ then $g^n \equiv F_n g + F_{n-1} \pmod p$.

The proof of Lemma 1 follows easily by induction.

Lemma 2. If $g^2 \equiv g + 1 \pmod p$ and if g has order n then $n = A(p)$ or $n = \dfrac{A(p)}{2}$.

Proof. Since

$$g^{A(p)} \equiv F_{A(p)} g + F_{A(p)-1} \equiv 1 \pmod p,$$

$n | A(p)$. Thus $n \leqslant A(p)$.

If $F_n \equiv 0 \pmod p$, then

$$1 \equiv g^n \equiv F_n g + F_{n-1} \equiv F_{n-1} \pmod p .$$

Thus $A(p) \leqslant n$ and hence in this case $n = A(p)$.

If $F_n \not\equiv 0 \pmod p$ then

$$g \equiv \frac{1 - F_{n-1}}{F_n} \pmod p .$$

Thus

$$\begin{aligned} 0 &\equiv 0 \cdot F_n^2 \equiv (g^2 - g - 1)F_n^2 \\ &\equiv -(F_n^2 - F_n F_{n-1} - F_{n-1}^2) - (F_n + F_{n-1}) - F_{n-1} + 1 \\ &\equiv (-1)^n - L_n + 1 \pmod p. \end{aligned}$$

For n even, we have $L_n \equiv 2 \pmod p$ and this implies, since $L_n^2 - 5F_n^2 = 4(-1)^n$, that $F_n \equiv 0 \pmod p$. Thus we must have n odd and hence $L_n \equiv 0 \pmod p$. Since

$$0 \equiv L_n \equiv 3F_{n-1} + F_{n-2} \pmod p,$$

we see that

$$1 = -(F_{n-1}^2 - F_{n-1}F_{n-2} - F_{n-2}^2) \equiv 5F_{n-1}^2 \pmod p.$$

Also we see that

$$-5 = L_n^2 - 5F_n^2 - 1 \equiv -5F_n^2 - 1 \equiv -5(F_n^2 + F_{n-1}^2) = -5F_{2n-1} \pmod p .$$

Thus $F_{2n-1} \equiv 1 \pmod{p}$. Also $F_{2n} = F_nL_n \equiv 0 \pmod{p}$. Hence $A(p) \leqslant 2n$. Thus, since $n \mid A(p)$, $A(p) = n$ or $A(p) = 2n$. In fact, since $F_n \not\equiv 0 \pmod{p}$, $A(p) = 2n$.

Lemma 3. If $g^2 \equiv g + 1 \pmod{p}$, $g^n \equiv 1 \pmod{p}$, and $n < A(p)$, then g is uniquely determined modulo p.

Proof. By Lemma 1,

$$1 \equiv g^n \equiv F_ng + F_{n-1} \pmod{p}.$$

Thus, if $F_n \equiv 0 \pmod{p}$ then $F_{n-1} \equiv 1 \pmod{p}$. Whence $A(p) \leqslant n$. Thus $F_n \not\equiv 0 \pmod{p}$. This implies that

$$g \equiv \frac{1 - F_{n-1}}{F_n} \pmod{p}$$

and therefore g is uniquely determined modulo p.

Lemma 4. Assume $p \equiv 1$ or $9 \pmod{10}$ and assume g_1 and g_2 are two distinct solutions modulo p to the congruence equation $x^2 \equiv x + 1 \pmod{p}$. If $A(p) \equiv 2 \pmod{4}$ then one of g_1, g_2 has order $A(p)$ modulo p and the other has order $A(p)/2$ modulo p. If $A(p) \not\equiv 2 \pmod{4}$ then g_1 and g_2 both have order $A(p)$ modulo p.

Proof. By Lemmas 2 and 3, g_1 and g_2 both have order $A(p)$, or one has order $A(p)$ and the other has order $A(p)/2$. Thus, we may say that at least one of g_1, g_2 has order $A(p)$ and, without loss of generality, let us assume g_1 has order $A(p)$.

If $A(p) \equiv 2 \pmod{4}$ then

$$-1 \equiv (-1)^{A(p)/2} \equiv (g_1g_2)^{A(p)/2} = g_1^{A(p)/2}g_2^{A(p)/2} \equiv -g_2^{A(p)/2} \pmod{p}.$$

Thus the order of g_2 is not $A(p)$ so it must be $A(p)/2$.

If $A(p) \equiv 0 \pmod{4}$ then

$$1 \equiv (-1)^{A(p)/2} \equiv (g_1g_2)^{A(p)/2} = g_1^{A(p)/2}g_2^{A(p)/2} \equiv -g_2^{A(p)/2} \pmod{p}.$$

Thus g_2 does not have order $A(p)/2$ so g_2 has order $A(p)$.

If $A(p)$ is odd then neither g_1 nor g_2 has order $A(p)/2$ so both g_1 and g_2 have order $A(p)$.

Lemma 5. If there exists a Fibonacci primitive root modulo p then $p \equiv 1$ or $9 \pmod{10}$ and $A(p) = p - 1$.

Proof. Assume g is a Fibonacci primitive root modulo p. By the remark after Theorem 1, $p \equiv 1$ or $9 \pmod{10}$. Since g has order $p - 1$, by Lemma 4, $p - 1 = A(p)$, or $p - 1 = A(p)/2$ and $A(p) \equiv 2 \pmod{4}$. This second possibility must be excluded since $p - 1$ is even.

Lemma 6. If $p \equiv 1$ or $9 \pmod{10}$ and $A(p) = p - 1$, then there exists a Fibonacci primitive root modulo p.

Proof. Since $p \equiv 1$ or $9 \pmod{10}$, there exists two solutions to $x^2 \equiv x + 1 \pmod{p}$. By Lemma 4, at least one of these two solutions has order $A(p) = p - 1$.

As a final result we prove

Proposition 1. If $p \equiv 11$ or $19 \pmod{20}$ and if g is a Fibonacci primitive root modulo p then

$$g \equiv -\frac{1 + F_{n-1}}{F_n} \pmod{p},$$

where $n = (p - 1)/2$.

Proof. Let g_2 be the solution other than g to $x^2 \equiv x + 1 \pmod{p}$ and let $n = (p - 1)/2$. By Lemma 5, $A(p) = p - 1 \equiv 2 \pmod{4}$. Thus, by Lemma 4, g_2 has order $A(p)/2 = n$. If $F_n \equiv 0 \pmod{p}$ then

$$-1 \equiv g^n \equiv F_ng + F_{n-1} \equiv F_{n-1} \equiv F_ng_2 + F_{n-1} \equiv g_2^n \equiv 1 \pmod{p}.$$

Hence $F_n \not\equiv 0 \pmod{p}$ and the result follows.

REFERENCES

1. Brother Alfred Brousseau, "Table of Indices with a Fibonacci Relation," *The Fibonacci Quarterly,* Vol. 10, No. 2 (April 1972), pp. 182–184.
2. Daniel Shanks, "Fibonacci Primitive Roots," *The Fibonacci Quarterly,* Vol. 10, No. 2 (April 1972), pp. 163–168, 181.

3. Daniel Shanks and Larry Taylor, "An Observation on Fibonacci Primitive Roots," *The Fibonacci Quarterly,* Vol. 11, No. 2 (April 1973), pp. 159–160.

****