ON THE CONNECTION BETWEEN THE RANK OF APPARITION OF A PRIME p IN FIBONACCI SEQUENCE AND THE FIBONACCI PRIMITIVE ROOTS

PÉTER KISS and BUI MINH PHONG
Teachers Training College, Eger, Hungary

Let the number g be a primitive root (mod p). If $x = g$ satisfies the congruence

$$x^2 \equiv x + 1 \pmod{p}, \tag{1}$$

then the g is called *Fibonacci Primitive Root.* D. Shanks [1] and D. Shanks, L. Taylor [2] dealt with the condition of existence of the Fibonacci Primitive Roots and they proved a few theorems.

In connection with the Fibonacci sequence

$$F_0 = 1,\quad F_1 = 1,\quad F_2 = 1,\quad F_3 = 2, \cdots (F_n = F_{n-1} + F_{n-2}),$$

the natural number $a = a(p)$ is called by D. Jarden [3] the rank of apparition of p if F_a is divisible by p and F_i is not divisible by p in case $i < a$.

In this article, we shall deal with the connections between the rank of apparition of prime p in the Fibonacci sequence and the Fibonacci Primitive Roots. We shall prove the following theorems:

Theorem 1. The congruence $x^2 \equiv x + 1 \pmod{p}$ is solvable if and only if $p - 1$ is divisible by $a(p)$ or $p=5$.

Theorem 2. If $p = 10k \pm 1$ is a prime number and there exist two Fibonacci Primitive Roots (mod p) or no Fibonacci Primitive Root exists, then $a(p) < p - 1$.

Theorem 3. There is exactly one Fibonacci Primitive Root (mod p) if and only if $a(p) = p - 1$ or $p = 5$.

D. Shanks [1] proved that if (1) is solvable then $p = 5$ or $p = 10k \pm 1$. But D. H. Halton [4] proved that $F_{p-(5/p)}$ is divisible by the prime p $(p \neq 5)$, where $(5/p)$ is the Legendre's symbol, and it is well known that if $p = 10k \pm 1$, then $(5/p) = 1$, therefore F_{p-1} is divisible by p. So it is enough to prove the following lemma for the verification of the first part of Theorem 1:

Lemma 1. If F_n is divisible by number p, then n is divisible by the rank $a(p)$ of p and if n is divisible by $a(p)$, then F_n is divisible by p.

Let $a = a(p)$ and $n = a \cdot m + r$, where $0 < r \leqslant a$. N. N. Vorobev proved that $F_{b+c} = F_b \cdot F_{c+1} + F_{b-1} \cdot F_c$ ([5], p. 10) and $F_{b \cdot c}$ is divisible by F_b for every natural numbers b and c ([5], p. 29). For this reason p is a divisor of $F_{a \cdot m}$ and if p is a divisor of F_n, then

$$F_n = F_{am+r} = F_{am} \cdot F_{r+1} + F_{am-1} \cdot F_r \equiv F_{am-1} \cdot F_r \equiv 0 \pmod{p}.$$

But F_{am} and F_{am-1} are neighboring numbers of the Fibonacci sequence, for that very reason F_{am-1} is prime to F_{am} (see [5], p. 30). So p is not a divisor of F_{am-1} because p is a divisor of F_{am} and $F_r \equiv 0 \pmod{p}$. From this follows $a = r$ by reason of definition of $a = a(p)$. Thus n is divisible by $a = a(p)$. Should it happen that n is divisible by $a = a(p)$, then, due to the Vorobev's previous theorem, F_n is divisible by $F_{a(p)}$ and so F_n is divisible by p, too. With this we proved the Lemma 1 and from this follows the proof of the first part of Theorem 1.

If $p - 1$ is divisible by $a(p)$, then by reason of Lemma 1 F_{p-1} is divisible by p. From this follows that $(5/p) = 1$. Namely, if $(5/p) = -1$, then F_{p+1} is divisible by p, too, and so $F_p = F_{p+1} - F_{p-1}$ also is divisible by p. But F_i and F_{i+1} are relatively prime for every natural number i, therefore $(5/p) = 1$. From this follows that $p = 10k \pm 1$ and so the congruence (1) is solvable. It completes the proof of Theorem 1.

Before the proof of Theorem 2 and Theorem 3, we shall prove two Lemmas.

Lemma 2. If the congruence $x^2 \equiv x + 1 \pmod{p}$ is solvable, $p \neq 5$ and the two roots are g_1, g_2, then $g_1 - g_2 \not\equiv 0 \pmod{p}$.

Lemma 3. If x is a solution of the congruence $x^2 \equiv x + 1 \pmod p$, then

$$x^k \equiv F_k \cdot x + F_{k-1} \pmod p$$

for every natural exponent k.

Let us prove the Lemma 2 first. If (1) has solutions g_1 and g_2, then $g_1 + g_2 \equiv 1 \pmod p$ and $g_2 \equiv 1 - g_1 \pmod p$, respectively (see [1]). Let us suppose that $g_1 - g_2 \equiv 0 \pmod p$, that is

$$(2) \qquad 2g_1 \equiv 1 \pmod p.$$

g_1 is a root of (1) and so $g_1^2 \equiv g_1 + 1 \pmod p$. Let us add this congruence to (2). Then we get $g_1^2 + g_1 \equiv 2 \pmod p$ and from this $4g_1^2 + 4g_1 \equiv 8 \pmod p$ and $(2g_1 + 1)^2 \equiv 9 \pmod p$, respectively. From the later congruence we get $2g_1 + 1 \equiv 3$ or $2g_1 + 1 \equiv -3 \pmod p$ and from these subtracting the congruence (2) we get $5 \equiv 0$ or $1 \equiv 0 \pmod p$. But these are true only if $p = 5$ according to $p > 1$, which proves the Lemma 2. In case $p = 5$ really $g_1 - g_2 \equiv 0 \pmod p$ because $g_1 = 3$ and $g_2 \equiv 1 - g_1 = -2 \equiv g_1 \pmod 5$.

We shall carry out the proof of the Lemma 3 by induction over k. In the cases $k = 1$ and $k = 2$ indeed

$$x = x + 0 = F_1 \cdot x + F_0 \quad \text{and} \quad x^2 \equiv x + 1 = F_2 \cdot x + F_1 \pmod p.$$

After this if $k > 2$ and the statement is true for exponents smaller than k, then

$$x^k = x^2 \cdot x^{k-2} \equiv (x+1) \cdot x^{k-2} = x^{k-1} + x^{k-2} \equiv F_{k-1} \cdot x + F_{k-2} + F_{k-2} \cdot x + F_{k-3}$$
$$= F_k \cdot x + F_{k-1} \pmod p$$

which proves Lemma 3.

Now let us suppose that $p = 10k \pm 1$. In this case by reason of [1], (1) is solvable. If both roots g_1 and g_2 are primitive $\pmod p$, then, according to Lemma 3 (using for every primitive root $g^{(p-1)/2} \equiv -1 \pmod p$)

$$g_1^{(p-1)/2} \equiv F_{(p-1)/2} \cdot g_1 + F_{(p-1)/2-1} \equiv -1 \pmod p$$
$$g_2^{(p-1)/2} \equiv F_{(p-1)/2} \cdot g_2 + F_{(p-1)/2-1} \equiv -1 \pmod p.$$

The difference of the congruences gives: $F_{(p-1)/2}(g_1 - g_2) \equiv 0 \pmod p$ and from this follows by reason of Lemma 2 $(p \neq 5)$ that $F_{(p-1)/2} \equiv 0 \pmod p$ which by reason of Lemma 1 proves the first part of Theorem 2.

Let us suppose that neither g_1 nor g_2 is primitive root $\pmod p$ and g_1 belongs to the exponent n_1 and g_2 belongs to the n_2. Then n_1 and n_2 are divisors of $p - 1$ $(n_1, n_2 < p - 1)$ and

$$(3) \qquad g_1^{n_1} \equiv 1, \qquad g_2^{n_2} \equiv 1 \pmod p.$$

If $n_1 = n_2 = n$, then similarly to the previous cases, using the congruences (3) and the Lemma 3, we get $F_n \equiv 0 \pmod p$ and so n is divisible by $a(p)$, that is $a(p) \leqslant n < p - 1$.

If $n_1 \neq n_2$, then we can suppose that $n_1 > n_2$. But $g_1 \cdot g_2 \equiv -1 \pmod p$ (see [1]) for this reason, using the congruences (3),

$$g_1^{n_2} \equiv g_1^{n_2} \cdot g_2^{n_2} = (g_1 \cdot g_2)^{n_2} \equiv (-1)^{n_2} \pmod p.$$

g_1 belongs to the exponent $n_1 \pmod p$ and $n_1 > n_2$, so n_2 must be an odd number and $g_1^{n_2} \equiv -1 \pmod p$. In this case $g_1^{2n_2} \equiv 1 \pmod p$ and from this follows that n_1 is a divisor of $2n_2$. But $2n_2 < 2n_1$, so $n_1 = 2n_2$ and

$$(4) \qquad g_2^{n_1} = g_2^{2n_2} \equiv 1 \pmod p.$$

According to congruences (3) and (4) and Lemma 3:

$$g_1^{n_1} \equiv F_{n_1} \cdot g_1 + F_{n_1 - 1} \equiv 1 \pmod p$$
$$g_2^{n_2} \equiv F_{n_1} \cdot g_2 + F_{n_1 - 1} \equiv 1 \pmod p$$

and from this we get, as above, using Lemma 2: $F_{n_1} = 0 \pmod p$ and so by reason of Lemma 1 n_1 is divisible by $a(p)$. Thus $a(p) \leqslant n_1 < p - 1$ which proves the second part of Theorem 2.

Theorem 3 is true in the case $p = 5$ (see [1]), therefore we can suppose further on that $p \neq 5$. Let it be now $a(p) = p - 1$. In this case, by reason of Theorem 1, the congruence (1) is solvable. There is exactly one primitive root $\pmod p$ between the two roots because otherwise $a(p) < p - 1$ would follow according to Theorem 2.

And conversely, if congruence (1) is solvable, one of the roots is primitive and the other is not (mod p), that is $n_1 = p - 1$, then it follows from the foregoing that $n_2 = (p-1)/2$ and n_2 is an odd number. Let us suppose that $a(p) < p - 1$ as opposed to Theorem 3 and let q denote the least common multiple of n_2 and $a(p)$. q is divisible by n_2 and $a(p)$ therefore

$$1 \equiv g_2^q \equiv F_q \cdot g_2 + F_{q-1} \equiv F_{q-1} \pmod p$$

(because p is a divisor of F_q according to Lemma 1). Using this congruence we get

$$g_1^q \equiv F_q \cdot g_1 + F_{q-1} \equiv F_{q-1} \equiv 1 \pmod p.$$

From this follows $q = p - 1$ because n_2 and $a(p)$ are divisors of $p - 1$ and g_1 is a primitive root (mod p). But $q = p - 1$ is an even number and n_2 is odd, therefore $a(p)$ is an even number.

N. N. Vorobev proved that for every natural number n $F_{n+1}^2 = F_n \cdot F_{n+2} + (-1)^n$ ([5], p. 11). Let us use this equation for the case $n = a(p) - 1$, it derives

$$F_{a(p)-1} \cdot F_{a(p)+1} = F_{a(p)}^2 + (-1)^{a(p)}.$$

But, on the one hand, $a(p)$ is an even number, on the other hand,

$$F_{a(p)+1} = F_{a(p)} + F_{a(p)-1} \equiv F_{a(p)-1} \pmod p,$$

so $F_{a(p)-1}^2 \equiv 1 \pmod p$. From this $F_{a(p)-1} \equiv -1 \pmod p$ follows because in the case $F_{a(p)-1} \equiv 1 \pmod p$ g_1 cannot be a primitive root (mod p) by reason of

$$g_1^{a(p)} \equiv F_{a(p)} \cdot g_1 + F_{a(p)-1} \equiv F_{a(p)-1} \equiv 1 \pmod p \tag{5}$$

and the condition $a(p) < p - 1$. From the latter it follows that, similarly to (5),

$$g_1^{a(p)} \equiv -1 \pmod p.$$

But g_1 is a primitive root (mod p) and $a(p) < p - 1$ therefore $a(p) = (p-1)/2 = n_2$. However, $a(p) = n_2$ is impossible, for $a(p)$ is even and n_2 is an odd number, so the condition $a(p) < p - 1$ is impossible. Then $a(p) = p - 1$, which completes the proof of Theorem 3.

The reverse of Theorem 2 follows from Theorem 3 as well: If the congruence $x^2 \equiv x + 1 \pmod p$ is solvable and $a(p) < p - 1$, then both roots are primitive (mod p) or neither of them is primitive. The point is that in this case, by reason of Theorem 3, there cannot be exactly one primitive root.

REFERENCES

1. D. Shanks, "Fibonacci Primitive Roots," *The Fibonacci Quarterly,* Vol. 10, No. 2 (April 1972), pp. 163–168, 181.
2. D. Shanks and L. Taylor, "An Observation of Fibonacci Primitive Roots," *The Fibonacci Quarterly,* Vol. 11, No. 2 (April 1973), pp. 159–160.
3. D. Jarden, *Recurring Sequences,* Publ. by Riveon Lematematika, Jerusalem, Israel, 1958.
4. J. H. Halton, "On the Divisibility Properties of Fibonacci Numbers," *The Fibonacci Quarterly,* Vol. 4, No. 3 (Oct. 1966), pp.
5. N. N. Vorobev, *Fibonacci Numbers,* Pergamon Press, Oxford, 1961.

****