FIBONACCI PRIMITIVE ROOTS AND WALL'S QUESTION

Hua-Chieh Li
Department of mathematics, National Tsing Hua University, Hsinchu, Taiwan
(Submitted May 1997)

1. INTRODUCTION

Let F_n denote the n^{th} member of the Fibonacci sequence. Fix a positive integer m. We reduce $\{F_n\}_{n=0}^{\infty}$ modulo m, taking least positive residues. If $x = g$ satisfies the congruence

$$f(x) = x^2 - x - 1 \equiv 0 \pmod{m},$$

then, by setting $u_0 = 1$, $u_1 = g$, and $u_n = u_{n-1} + u_{n-2}$, we have that $u_n \equiv g^n \pmod{m}$. We have given particular attention to those cases having the longest possible cycles, i.e., the number g being a primitive root modulo m. We call g a Fibonacci primitive root modulo m if g is a root of $x^2 - x - 1 \equiv 0 \pmod{m}$ and g is a primitive root modulo m. For a fixed prime p, Fibonacci primitive roots modulo p have an extensive literature (see, e.g., [1], [3], [4], [5], [6], and [7]).

Consider the Fibonacci sequence $\{F_n\}_{n=0}^{\infty}$ modulo m. The positive integer $z(m)$ is called the rank of apparition of m in the Fibonacci sequence if it is the smallest positive integer such that $F_{z(m)} \equiv 0 \pmod{m}$; furthermore, $k(m)$ is called the period of the Fibonacci sequence modulo m if it is the smallest positive integer for which $F_{k(m)} \equiv 0 \pmod{m}$ and $F_{k(m)+1} \equiv 1 \pmod{m}$. For a fixed prime p, Wall [10] has proved that, if $k(p) = k(p^e) \neq k(p^{e+1})$, then $k(p^l) = p^{l-e}k(p)$ for $l \geq e$. Wall asked whether $k(p) = k(p^2)$ is always impossible; up to now, this is still an open question. According to Williams [2], $k(p) \neq k(p^2)$ for every odd prime p less than 10^9. Sun and Sun [8] proved that the affirmative answer to Wall's question implies the first case of Fermat's last theorem.

In this paper we reproduce and improve upon some results for the Fibonacci primitive roots mentioned above. Especially, we give connections among the existence of the Fibonacci primitive roots modulo p^n and Wall's question. Our main theorem says that the affirmative answer to Wall's question [i.e., $k(p) \neq k(p^2)$] and the existence of Fibonacci primitive roots modulo p implies the existence of Fibonacci primitive roots modulo p^n for all positive integers n. This theorem overlaps in part with theorems proved by Phong [5], but our point of view and our methods are different from those of Phong, so that we obtain an effective method to decide whether $k(p) = k(p^2)$ or not.

2. PRELIMINARY RESULTS

In this section we briefly review some elementary results concerning primitive roots and some well-known results concerning the rank of apparition and the period of the Fibonacci sequence.

By Euler's theorem, if m is a positive integer and if a is an integer relatively prime to m, then $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m)$ is defined to be the number of positive integers not exceeding m which are relatively prime to m. Denote by $\text{ord}_m(a)$ the least positive integer x such that $a^x \equiv 1 \pmod{m}$. If $\text{ord}_m(a) = \phi(m)$, then a is called a primitive root modulo m.

First, we observe that, if $f(x)$ is a polynomial in x with integer coefficients and x_k is a solution to $f(x) \equiv 0 \pmod{p^k}$, then $x_k + p^k y$ is a solution to $f(x) \equiv 0 \pmod{p^{k+1}}$ exactly when

$$f(x_k)+f'(x_k)p^k y \equiv 0 \pmod{p^{k+1}}.$$

This congruence is equivalent to

$$\frac{f(x_k)}{p^k}+f'(x_k)y \equiv 0 \pmod{p}.$$

In particular, if $p \nmid f'(x_k)$, then $(f'(x_k))^{-1}$ exists modulo p. Therefore,

$$y \equiv \frac{-f(x_k)}{p^k}(f'(x_k))^{-1} \pmod{p}$$

is the unique solution modulo p. On the other hand, if $p \mid f'(x_k)$, then y has p solutions modulo p or no solution depends on $f(x_k) \equiv 0 \pmod{p^{k+1}}$ or not. We now have the following lemma.

Lemma 2.1: Suppose that x_k is a solution to $f(x) \equiv 0 \pmod{p^k}$ and $p \nmid f'(x_k)$. Then there exists a unique x_{k+1} modulo p^{k+1} such that $x_{k+1} \equiv x_k \pmod{p^k}$ and $f(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$. On the other hand, suppose that $p \mid f'(x_k)$ and $f(x_k) \not\equiv 0 \pmod{p^{k+1}}$. Then there exists no solution to $f(x) \equiv 0 \pmod{p^{k+1}}$.

A simple application of Lemma 2.1 is the following: suppose that

$$d \mid p-1 \quad \text{and} \quad a^d \equiv 1 \pmod{p}.$$

Since a is a solution to $f(x) = x^d - 1 \equiv 0 \pmod{p}$ and $f'(a) = da^{d-1} \not\equiv 0 \pmod{p}$ [note that $(d, p) = (a, p) = 1$], we have that there exists exactly one solution b modulo p^2 such that $b \equiv a \pmod{p}$ and $b^d \equiv 1 \pmod{p^2}$.

Lemma 2.2: Suppose that g is a primitive root modulo p. Then there exists a unique g' modulo p^2 such that $g' \equiv g \pmod{p}$ but g' is not a primitive root modulo p^2.

Proof: Suppose that $g' \equiv g \pmod{p}$ and $\operatorname{ord}_{p^2}(g') = m$. We have that

$$p-1 \mid m \quad \text{and} \quad m \mid p(p-1),$$

so $m = p(p-1)$ if and only if $(g')^{p-1} \not\equiv 1 \pmod{p^2}$. By the remark above, our claim follows. □

Let p be an odd prime. Suppose that g is a primitive root modulo p^2. Then we have that $g^{p-1} \not\equiv 1 \pmod{p^2}$. Thus, $g^{p-1} = 1+\lambda p$ for some λ such that $p \nmid \lambda$. Hence,

$$g^{p(p-1)} = (1+\lambda p)^p \equiv 1+\lambda p^2 \pmod{p^3}.$$

By induction, we have that

$$g^{p^k(p-1)} \equiv 1+\lambda p^{k+1} \pmod{p^{k+2}}.$$

Lemma 2.3: Let p be an odd prime and let g be a primitive root modulo p^2. Then g is also a primitive root modulo p^n for all positive integers n.

Proof: Suppose that $\operatorname{ord}_{p^3(g)} = m$. Since g is a primitive root modulo p^2, we have that $p(p-1) \mid m \mid p^2(p-1)$. By the argument above, we have that $g^{p(p-1)} \not\equiv 1 \pmod{p^3}$. This implies that $m = p^2(p-1)$, i.e., g is a primitive root modulo p^3. Again, by the argument above and by induction, our claim follows. □

Let α and β be two distinct solutions to $x^2 - x - 1 \equiv 0 \pmod{m}$. Then we have the Binet form

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

Since $\alpha^n \equiv \alpha^{n-1} + \alpha^{n-2} \pmod{m}$ and $\beta^n \equiv \beta^{n-1} + \beta^{n-2} \pmod{m}$, we also have that

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

This tells us that, if $k(m)$ is the period of the Fibonacci sequence modulo m, then $\text{ord}_m(\alpha) \mid k(m)$ and $\text{ord}_m(\beta) \mid k(m)$.

Lemma 2.4: Let α and β be two distinct solutions to $x^2 - x - 1 \equiv 0 \pmod{m}$ and let $k(m)$ be the period of the Fibonacci sequence modulo m. Then $k(m) = [\text{ord}_m(\alpha), \text{ord}_m(\beta)]$, where $[a, b]$ denotes the least common multiple of a and b.

Proof: Let $l = [\text{ord}_m(\alpha), \text{ord}_m(\beta)]$. By the argument above, we have that $l \mid k(m)$. On the other hand, $\alpha^l - \beta^l \equiv 0 \pmod{m}$ and $\alpha^{l+1} - \beta^{l+1} \equiv \alpha - \beta \pmod{m}$. This implies that $F_l \equiv 0 \pmod{m}$ and $F_{l+1} \equiv 1 \pmod{m}$. Thus, $k(m) \mid l = [\text{ord}_p(\alpha), \text{ord}_p(\beta)]$, and our proof is complete. □

Let $\text{ord}_m(\alpha) = n_1$ and $\text{ord}_m(\beta) = n_2$. Suppose that $n_1 \geq n_2$. Since $\alpha\beta \equiv -1 \pmod{m}$, we have that $(\alpha)^{n_2} \equiv (\alpha\beta)^{n_2} \equiv (-1)^{n_2} \pmod{m}$. If n_2 is even, then $\alpha^{n_2} \equiv 1 \pmod{m}$. Thus, $n_1 \mid n_2$; hence, $n_1 = n_2$ by assumption. If n_2 is odd, then we have that $\alpha^{n_2} \equiv -1 \pmod{m}$ and so $n_1 \mid 2n_2$. This implies that $n_1 = n_2$ if n_1 is also odd and $n_1 = 2n_2$ if n_1 is even. However, it is impossible that $n_1 = n_2 \equiv 1 \pmod{2}$; otherwise, we will have that $1 \equiv (\alpha\beta)^{n_1} \equiv (-1)^{n_1} \equiv -1 \pmod{m}$. Hence, we have that n_1 is always even. Moreover, suppose that n_2 is odd. Then $n_1 = 2n_2$. Therefore, if $n_1 \equiv 0 \pmod{4}$, then $n_1 = n_2$. On the other hand, suppose that m is an odd prime power and suppose that $n_1 = 2r \equiv 2 \pmod{4}$, where r is odd. Then $\alpha^r \equiv -1 \pmod{m}$ and, hence, $-1 \equiv (\alpha\beta)^r \equiv -\beta^r \pmod{m}$. This implies that $\beta^r \equiv 1 \pmod{m}$. Thus, $n_2 = r$, and we have the following lemma.

Lemma 2.5: Let m be an odd prime power and let α and β be distinct roots of $x^2 - x - 1 \equiv 0 \pmod{m}$. Suppose that $\text{ord}_m(\alpha) \geq \text{ord}_m(\beta)$. Then we have either $\text{ord}_m(\alpha) = \text{ord}_m(\beta) \equiv 0 \pmod{4}$ or $\text{ord}_m(\alpha) = 2\text{ord}_m(\beta) \equiv 2 \pmod{4}$.

Let $z(m)$ be the rank of apparition of m and let $k(m)$ be the period modulo m in the Fibonacci sequence. Wall [10] has shown that $z(m) \mid k(m)$. Vinson [9] gave criteria for the evaluation of $k(m) / z(m)$.

Lemma 2.6: Let p be an odd prime and let e be any positive integer. Then:

(1) $k(p^e) = 4z(p^e)$ if $z(p^e) \not\equiv 0 \pmod{2}$;

(2) $k(p^e) = z(p^e)$ if $z(p^e) \equiv 2 \pmod{4}$;

(3) $k(p^e) = 2z(p^e)$ if $z(p^e) \equiv 0 \pmod{4}$.

Proof: Please see Vinson [9, Theorem 2]. □

3. FIBONACCI PRIMITIVE ROOTS MODULO p

We begin with an easy observation that $x^2 - x - 1 \equiv 0 \pmod{p}$ is solvable if and only if $y^2 \equiv 5 \pmod{p}$ has solutions. If $p = 5$, then $x^2 - x - 1 \equiv 0 \pmod{5}$ has a double root $x \equiv 3 \pmod{5}$. Therefore, 3 is the unique Fibonacci primitive root modulo 5. $x^2 - x - 1 \equiv 0 \pmod{p}$ has two distinct solutions modulo p if p is an odd prime with $(5/p) = 1$, where $(5/p)$ is the Legendre symbol.

For the remainder of this section, we assume that p is an odd prime with $(5/p) = 1$.

The relation of the rank of apparition to the period modulo p in the Fibonacci sequence has been studied extensively by Wall [10] and Vinson [9]. We state their results in the next lemma without proof.

Lemma 3.1: Let $z(p)$ and $k(p)$ be the rank of apparition of p and the period modulo p in the Fibonacci sequence, respectively.

(1) Suppose that $p \equiv 11$ and $p \equiv 19 \pmod{20}$ [i.e., $(5/p) = 1$ and $(-1/p) = -1$]. Then we have $z(p) \mid p - 1$, but $z(p) \nmid \frac{p-1}{2}$. Furthermore, $k(p) = z(p)$.

(2) Suppose that $p \equiv 1$ and $p \equiv 9 \pmod{20}$ [i.e., $(5/p) = 1$ and $(-1/p) = 1$]. Then we have $z(p) \mid \frac{p-1}{2}$. Furthermore, $k(p) = z(p)$, $2z(p)$, or $4z(p)$ depending on whether $z(p) \equiv 2$, 0, or $\pm 1 \pmod{4}$, respectively.

The conditions for the existence of Fibonacci primitive roots modulo p and their properties were studied by several authors. Our next theorem overlaps in part with theorems proved by Phong [5].

Theorem 3.2: Let $z(p)$ be the rank of apparition of p in the Fibonacci sequence.

(1) There is exactly one Fibonacci primitive root modulo p if and only if $p \equiv 11$ or $19 \pmod{20}$ and $z(p) = p - 1$.

(2) There are two Fibonacci primitive roots modulo p if and only if $p \equiv 1$ or $9 \pmod{40}$ and $z(p) = \frac{p-1}{2}$ or $p \equiv 21$ or $29 \pmod{40}$ and $z(p) = \frac{p-1}{4}$.

Proof: We know that $(5/p) = 1$ if and only if $p \equiv \pm 1 \pmod{10}$. Let α and β be two distinct roots of $x^2 - x - 1 \equiv 0 \pmod{p}$ with $\operatorname{ord}_p(\alpha) \geq \operatorname{ord}_p(\beta)$.

(1) Suppose that $p \equiv 11$ or $19 \pmod{20}$ and $z(p) = p - 1$. Then, since $p - 1 \equiv 2 \pmod{4}$, by Lemma 2.4, Lemma 2.5, and Lemma 3.1, $z(p) = k(p) = \operatorname{ord}_p(\alpha) = 2\operatorname{ord}_p(\beta) = p - 1$. Conversely, suppose that there exists exactly one Fibonacci primitive root modulo p. Then, by Lemma 2.5, $\operatorname{ord}_p(\alpha) = 2\operatorname{ord}_p(\beta) \equiv 2 \pmod{4}$. Therefore, by Lemma 2.4, $k(p) = \operatorname{ord}_p(\alpha) = p - 1$. Hence, $p \equiv 11$ or $19 \pmod{20}$ and $z(p) = k(p) = p - 1$ by Lemma 3.1.

(2) Suppose that $p \equiv 1$ or $9 \pmod{40}$ and $z(p) = \frac{p-1}{2}$. Then, since $\frac{p-1}{2} \equiv 0 \pmod{4}$, by the lemmas mentioned in (1), $2z(p) = k(p) = \operatorname{ord}_p(\alpha) = \operatorname{ord}_p(\beta) = p - 1$. Suppose that $p \equiv 21$ or $29 \pmod{40}$ and $z(p) = \frac{p-1}{2}$. Then, since $\frac{p-1}{4} \equiv 1 \pmod{2}$, again by the lemmas mentioned in (1), $4z(p) = k(p) = \operatorname{ord}_p(\alpha) = \operatorname{ord}_p(\beta) = p - 1$. Conversely, suppose that there exist two Fibonacci primitive roots modulo p. Then, by Lemma 2.5, $\operatorname{ord}_p(\alpha) = \operatorname{ord}_p(\beta) \equiv 0 \pmod{4}$. Therefore, by Lemma 2.4, $k(p) = p - 1 \equiv 0 \pmod{4}$. Hence, by Lemma 3.1, our claim follows. □

Theorem 3.2 reproduces results for Fibonacci primitive roots modulo p in [1], [3], [4], [6], and [7]. For example, Mays [4] showed that, if both $p = 60k - 1$ and $q = 30k - 1$ are primes, then there is exactly one Fibonacci primitive root modulo p. In fact, since $p \equiv 19 \pmod{20}$ and $2q = p - 1$, by Lemma 3.1, we have either $z(p) = p - 1$ or $z(p) = \frac{p-1}{q} = 2$ (by the assumption that q is a prime). We obtain $z(p) \neq 2$, because $F_2 = 1$. Therefore, $z(p) = p - 1$. By the theorem above, we conclude that there exists exactly one Fibonacci primitive root modulo p. By a similar method, we have the following proposition.

Proposition 3.3: Let p be a prime such that $p \equiv 11$ or $19 \pmod{20}$ and $p - 1 = 2q$, where q is a prime. Then there exists exactly one Fibonacci primitive root modulo p.

Example 1: In the case , $p - 1 = 2 \cdot 5$. There is exactly one Fibonacci primitive root modulo 11, which is 8. When $p = 59$, $p - 1 = 2 \cdot 29$. There is exactly one Fibonacci primitive root modulo 59, which is 34.

When $p \equiv 1$ or $9 \pmod{20}$, the situation is more complicated, because it is possible that $4z(p) \mid p - 1$. There are many articles discussed for which p, $4z(p) \mid p - 1$ (see, e.g., [2], [8], and [11]). Here, we quote the result in [8].

Lemma 3.4: Let p be a prime such that $p \equiv 1$ or $9 \pmod{20}$ and, hence, $p = x^2 + 5y^2$ for some integers x and y. Then $4z(p) \mid p - 1$ if and only if $4 \mid xy$.

Suppose that $p \equiv 1$ or $9 \pmod{40}$ [resp. $p \equiv 21$ or $29 \pmod{40}$]. By Theorem 3.2, there exist Fibonacci primitive roots modulo p only if $4z(p) \nmid p - 1$ [resp. $4z(p) \mid p - 1$].

Proposition 3.5: Let p be a prime such that $p \equiv 1$ or $9 \pmod{20}$ and, hence, $p = x^2 + 5y^2$ for some integers x and y.

(1) Suppose that $p \equiv 1$ or $9 \pmod{40}$. Then there is no Fibonacci primitive root modulo p if $4 \mid xy$. Suppose that $4 \nmid xy$ and $p - 1 = 8q$, where q is a prime. Then there exist two Fibonacci primitive roots modulo p.

(2) Suppose that $p \equiv 21$ or $29 \pmod{40}$. Then there is no Fibonacci primitive root modulo p if $4 \nmid xy$. Suppose that $4 \mid xy$ and $p - 1 = 4q$, where q is a prime. Then there exist two Fibonacci primitive roots modulo p.

Proof:

(1) Suppose that $4 \mid xy$. By Lemma 3.4, $4z(p) \mid p - 1$. We have that $k(p) \leq \frac{p-1}{2}$, by Lemma 2.6. Hence, there is no Fibonacci primitive root modulo p. Suppose that $4 \nmid xy$ and $p - 1 = 8q$, where q is a prime. Then we have either $z(p) = \frac{p-1}{2}$ or $z(p) = \frac{p-1}{2q} = 4$. However, $z(p) \neq 4$, because $F_4 = 3$. By Theorem 3.2, our claim follows.

(2) Suppose that $4 \nmid xy$. By Lemma 3.4, $4z(p) \nmid p - 1$. Since $2z(p) \mid p - 1$, this implies that $k(p) = z(p) \leq \frac{p-1}{2}$, by Lemma 2.6. Hence, there is no Fibonacci primitive root modulo p. Suppose that $4 \mid xy$ and $p - 1 = 4q$, where q is a prime. Then we have either $z(p) = \frac{p-1}{4}$ or $z(p) = \frac{p-1}{4q} = 1$. However, $z(p) \neq 1$, because $F_1 = 1$. By Theorem 3.2, our claim follows.

Example 2: Since $29 = 3^2 + 5(2^2)$ and $4 \nmid 3 \cdot 2$, there is no Fibonacci primitive root modulo 29. Since $41 = 6^2 + 5$, $4 \nmid 6$, and $41 - 1 = 8 \cdot 5$, there are two Fibonacci primitive roots modulo 41

(namely, 35 and 7). There are two Fibonacci primitive roots modulo 149 (namely, 41 and 109), because $149 = 12^2 + 5$, $4 \mid 12$, and $149 - 1 = 4 \cdot 37$.

Remark 1: Since $F_8 = 3 \cdot 7$, $F_{16} = 3 \cdot 7 \cdot 47$, and $F_{32} = 3 \cdot 7 \cdot 47 \cdot 2207$, we have that, for $p \equiv 1$ or 9 (mod 40), $z(p) \neq 8$, 16, or 32. Therefore, part (1) of Proposition 3.5 is also true, if $p - 1 = 16q$, $32q$, or $64q$ for some odd prime q.

4. FIBONACCI PRIMITIVE ROOTS MODULO p^n

It is well known that the positive integer m possesses a primitive root if and only if $m = 2, 4, p^n$, or $2p^n$, where p is an odd prime. Since there is no solution to $x^2 - x - 1 \equiv 0 \pmod 2$, we only have to consider the case $m = p^n$.

First, we consider the case $p = 5$. Let $f(x) = x^2 - x - 1$. We have that $f(3) = 5 \equiv 0 \pmod 5$. However, since $f'(3) = 5 \equiv 0 \pmod 5$, by Lemma 2.1, there is no solution to $f(x) = x^2 - x - 1 \equiv 0 \pmod{5^2}$. Hence, there is no Fibonacci primitive root modulo 5^n for $n \geq 2$. On the other hand, suppose that $p \neq 5$ and $(5/p) = 1$. There exist two distinct roots, α and β such that $f(\alpha) \equiv f(\beta) \equiv 0 \pmod p$. We have that $f'(\alpha) = 2\alpha - 1 \not\equiv 0 \pmod p$; otherwise, $0 \equiv 4\alpha^2 - 4\alpha - 4 \equiv 1 - 2 - 4 \equiv -5 \pmod p$ contradicts our assumption. Using the same reasoning, we have that $f'(\beta) \not\equiv 0 \pmod p$. Therefore, by Lemma 2.1, we conclude that there exist two distinct roots to $x^2 - x - 1 \equiv 0 \pmod{p^2}$. By induction, we have the following lemma.

Lemma 4.1: Let p be an odd prime such that $p \equiv \pm 1 \pmod{20}$. Then there exist two distinct roots to $x^2 - x - 1 \equiv 0 \pmod{p^n}$ for every positive integer n. Furthermore, suppose that α is a root to $x^2 - x - 1 \equiv 0 \pmod p$. Then there exists a unique α_n modulo p^n such that $\alpha_n^2 - \alpha_n - 1 \equiv 0 \pmod{p^n}$ and $\alpha_n \equiv \alpha \pmod p$.

Suppose that α is a Fibonacci primitive root modulo p. By the argument above, there exists exactly one α_2 modulo p^2 such that $\alpha_2^2 - \alpha_2 - 1 \equiv 0 \pmod{p^2}$ and $\alpha_2 \equiv \alpha \pmod p$. Suppose that α_2 is a primitive root modulo p^2. Then α_2 is a Fibonacci primitive root modulo p^2. In this case, by Lemma 2.4, $k(p^2)$, the period of the Fibonacci sequence modulo p^2, is equal to $\mathrm{ord}_{p^2}(\alpha_2) = p(p-1) = pk(p)$, and since p is odd, by Lemma 2.6, this is equivalent to $z(p^2) = pz(p)$, i.e., $p^2 \nmid F_{z(p)}$. On the other hand, suppose that $p^2 \nmid F_{z(p)}$. Then $k(p^2) = pk(p) = p(p-1)$. By Lemma 2.4 and Lemma 2.5, this implies that $\mathrm{ord}_{p^2}(\alpha_2) = \frac{p(p-1)}{2}$ or $\mathrm{ord}_{p^2}(\alpha_2) = p(p-1)$. By assumption, α_2 is a primitive root modulo p and, hence, $\mathrm{ord}_{p^2}(\alpha_2)$ is either $(p-1)$ or $p(p-1)$. This implies that α_2 is a primitive root modulo p^2.

Theorem 4.2: Let p be an odd prime such that $p \equiv \pm 1 \pmod{20}$. Suppose that there is a Fibonacci primitive root modulo p. Then there is a Fibonacci primitive root modulo p^n for every positive integer n if and only if $p^2 \nmid F_{z(p)}$, where $z(p)$ is the least positive integer such that $p \mid F_{z(p)}$.

Proof: We only have to claim that the existence of a Fibonacci primitive root modulo p^2 implies the existence of a Fibonacci primitive root modulo p^n. Suppose that α_2 is a Fibonacci primitive root modulo p^2. By a similar argument as in Lemma 4.1, there exists α_n such that $\alpha_n^2 - \alpha_n - 1 \equiv 0 \pmod{p^n}$ and $\alpha_n \equiv \alpha_2 \pmod{p^2}$. However, Lemma 2.3 says that α_2 is a primitive

root modulo p^n for every positive integer n. $\alpha_n \equiv \alpha_2 \pmod{p^2}$ implies that α_n is also a primitive root modulo p^n. Hence, α_n is a Fibonacci primitive root modulo p^n.

Remark 2: According to Williams [12], $p^2 \nmid F_{p-(5/p)}$ [this is equivalent to $p^2 \nmid F_{z(p)}$] for every odd prime p less than 10^9. Therefore, for $p < 10^9$, suppose that there exists a Fibonacci primitive root modulo p. Then there exists a Fibonacci primitive root modulo p^n. Furthermore, since p is odd, by Lemma 2.5, the number of distinct Fibonacci primitive roots modulo p^n is the same as the number of distinct Fibonacci primitive roots modulo p.

Suppose that α is a root to $x^2 - x - 1 \equiv 0 \pmod{p}$. Then there exists a unique α_2 modulo p^2 such that $\alpha_2 \equiv \alpha \pmod{p}$ and $\alpha_2^2 - \alpha_2 - 1 \equiv 0 \pmod{p^2}$. On the other hand, suppose that α is a primitive root modulo p. By Lemma 2.2, there exists a unique α' modulo p^2 such that $\alpha' \equiv \alpha \pmod{p}$ and α' is not a primitive root modulo p^2. Therefore, $\alpha' \equiv \alpha_2 \pmod{p^2}$ if and only if $p^2 \mid F_{z(p)}$ [or, equivalently, $k(p) = k(p^2)$].

Theorem 4.3: Let p be an odd prime such that $(5/p) = 1$ and let α be a Fibonacci primitive root modulo p. Then there exists a Fibonacci primitive root modulo p^n for every positive integer n if and only if $2\alpha^{p+1} - \alpha^p - \alpha^2 - 1 \not\equiv 0 \pmod{p^2}$.

Proof: By Theorem 4.2, the existence of a Fibonacci primitive root modulo p^2 implies the existence of a Fibonacci primitive root modulo p^n for every positive integer n. By the argument above, there is no Fibonacci primitive root modulo p^2 if and only if there exists λ such that $(\alpha + \lambda p)^2 - (\alpha + \lambda p) - 1 \equiv 0 \pmod{p^2}$ and $(\alpha + \lambda p)^{p-1} - 1 \equiv 0 \pmod{p^2}$. Expand both congruence equations and eliminate λ. This implies that α must satisfy $2\alpha^{p+1} - \alpha^p - \alpha^2 - 1 \equiv 0 \pmod{p^2}$. Conversely, suppose that $\alpha_2 \equiv \alpha + \lambda p \pmod{p^2}$ is a solution to $x^2 - x - 1 \equiv 0 \pmod{p^2}$ and suppose that $2\alpha^{p+1} - \alpha^p - \alpha^2 - 1 \equiv 0 \pmod{p^2}$. We have that

$$\begin{aligned} 2\alpha_2^{p+1} - \alpha_2^p - \alpha_2^2 - 1 &= 2\alpha_2^{p+1} - 2\alpha_2^p - 2\alpha_2^{p-1} + \alpha_2^p + 2\alpha_2^{p-1} - \alpha_2 - 2 \\ &\equiv (\alpha_2 + 2)(\alpha_2^{p-1} - 1) \pmod{p^2}. \end{aligned}$$

Since $2\alpha^{p+1} - \alpha^p - \alpha^2 - 1 \equiv 2\alpha_2^{p+1} - \alpha_2^p - \alpha_2^2 - 1 \pmod{p^2}$, this implies that $(\alpha_2 + 2)(\alpha_2^{p-1} - 1) \equiv 0 \pmod{p^2}$. Suppose that $\alpha_2 + 2 \equiv 0 \pmod{p}$. Then, since $\alpha_2^2 - \alpha_2 - 1 \equiv 0 \pmod{p}$, this implies that $5 \equiv 0 \pmod{p}$, which contradicts our assumption that $p \neq 5$. Hence, $\alpha_2^{p-1} \equiv 1 \pmod{p^2}$. This implies that α_2 is not a primitive root modulo p^2, and our proof is complete. □

Remark 3: From our proof, we have a more general result concerning Wall's question. We have the following result: suppose that α is a solution to $x^2 - x - 1 \equiv 0 \pmod{p}$ (we do not need the assumption that α is a primitive root modulo p). Then $k(p) = k(p^2)$ if and only if

$$2\alpha^{p+1} - \alpha^p - \alpha^2 - 1 \equiv 0 \pmod{p^2}.$$

For the case $(5/p) = -1$, we have a similar result. We should consider everything in the ring $Z\left[\frac{1+\sqrt{5}}{2}\right]$ modulo p. We have the following result: suppose $\alpha \in Z\left[\frac{1+\sqrt{5}}{2}\right]$ is a solution to $x^2 - x - 1 \equiv 0 \pmod{p}$. Then $k(p) = k(p^2)$ if and only if

$$2\alpha^{p^2+1} - \alpha^{p^2} - \alpha^2 - 1 \equiv 0 \pmod{p^2}.$$

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. E. Lehmer. "On the Quadratic Character of the Fibonacci Root." *The Fibonacci Quarterly* **4.2** (1966):135-38.
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. B. M. Phong. "Lucas Primitive Roots." *The Fibonacci Quarterly* **29.1** (1991):66-71.
6. D. Shanks. "Fibonacci Primitive Roots." *The Fibonacci Quarterly* **10.2** (1972):162-68.
7. D. Shanks & L. Taylor. "An Observation on Fibonacci Primitive Roots." *The Fibonacci Quarterly* **11.2** (1973):159-60.
8. Z.-H. Sun & Z.-W. Sun. "Fibonacci Numbers and Fermat's Last Theorem." *Acta Arith.* **60** (1992):371-88.
9. J. Vinson. "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence." *The Fibonacci Quarterly* **1.1** (1963):37-45.
10. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* **67** (1960):525-32.
11. M. Ward. "The Prime Divisors of Fibonacci Numbers." *Pacific J. Math.* **11** (1961):379-86.
12. 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

❖❖❖

NEW PROBLEM WEB SITE

Readers of *The Fibonacci Quarterly* will be pleased to know that many of its problems can now be searched electronically (at no charge) on the World Wide Web at

http://problems.math.umr.edu

Over 23,000 problems from 42 journals and 22 contests are references by the site, which was developed by Stanley Rabinowitz's MathPro Press. Ample hosting space for the site was generously provided by the Department of Mathematics and Statistics at the University of Missouri-Rolla, through Leon M. Hall, Chair.

Problem statements are included in most cases, along with proposers, solvers (whose solutions were published), and other relevant bibliographic information. Difficulty and subject matter vary widely; almost any mathematical topic can be found.

The site is being operated on a volunteer basis. Anyone who can donate journal issues or their time is encouraged to do so. For further information, write to

Mr. Mark Brown
Director of Operations, MathPro Press
1220 East West Highway #1010A
Silver Spring, MD 20910
(301) 587-0618 (Voice mail)
bowron@compuserve.com (e-mail)