LUCAS PRIMITIVE ROOTS

Bui Minh Phong*

Computer Center of E. Lorand University
Budapest H-1117, Bogdanfy u.10/B, Hungary

(Submitted February 1989)

1. Introduction

Let $U = \{U_n\}_{n=0}^{\infty}$ be a Lucas sequence defined by integers $U_0 = 0$, $U_1 = 1$, P, Q, and by the recursion

$$U_{n+1} = PU_n - QU_{n-1}, \text{ for } n \geq 1.$$

The polynomial

$$f(x) = x^2 - Px + Q$$

with discriminant

$$D = P^2 - 4Q$$

is called the characteristic polynomial of the sequence U. In the case where $P = -Q = 1$, the sequence U is the Fibonacci sequence and we denote its terms by $F_0, F_1, F_2, \ldots$.

Let p be an odd prime with $p \nmid Q$ and let $e \geq 1$ be an integer. The positive integer $u = u(p^e)$ is called the rank of apparition of p^e in the sequence U if $p^e | U_u$ and $p^e \nmid U_m$ for $0 < m < u$; furthermore, $\bar{u} = \bar{u}(p^e)$ is called the period of the sequence U modulo p^e if it is the smallest positive integer for which $U_{\bar{u}} \equiv 0$ and $U_{\bar{u}+1} \equiv 1 \pmod{p^e}$. In the Fibonacci sequence, we denote the rank of apparition of p^e and period of F modulo p^e by $f(p^e)$ and $\bar{f}(p^e)$, respectively.

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

$$(1) \qquad f(x) = x^2 - Px + Q \equiv 0 \pmod{p^e},$$

then we say that g is a Lucas primitive root (mod p^e) with parameters P and Q. Throughout this paper, we shall write "Lucas primitive root mod p^e" without including the phrase, "with parameters P and Q," if the sequence U is given. This is the generalization of the definition of Fibonacci primitive roots (FPR) modulo p that was given by D. Shanks [6] for the case $P = -Q = 1$.

The conditions for the existence of FPR (mod p) and their properties were studied by several authors. For example, D. Shanks [6] proved that if there exists a FPR (mod p) then $p = 5$ or $p \equiv \pm 1 \pmod{10}$; furthermore, if $p \neq 5$ and there are FPR's (mod p), then the number of FPR's is two or one, according to whether $p \equiv 1 \pmod 4$ or $p \equiv -1 \pmod 4$. In [7], D. Shanks & L. Taylor have shown that if g is a FPR (mod p) then $g - 1$ is a primitive root (mod p). M. J. DeLeon [4] proved that there is a FPR (mod p) if and only if $\bar{f}(p) = p - 1$. In [2] we studied the connection between the rank of apparition of a prime p and the existence of FPR's (mod p). We proved that there is exactly one FPR (mod p) if and only if $f(p) = p - 1$ or $p = 5$; moreover, if $p \equiv 1 \pmod{10}$ and there exist two FPR's (mod p) or no FPR exists, then $f(p) < p - 1$. M. E. Mays [5] showed that if both $p = 60k - 1$ and $q = 30k - 1$ are primes then there is a FPR (mod p).

*This research was partially supported by Hungarian National Foundation for Scientific Research Grant No. 907.

The purpose of this paper is to give some connections among the rank of apparition of p^e in the Lucas sequence U, the period of U modulo p^e, and the Lucas primitive roots (mod p^e); furthermore, we show necessary and sufficient conditions for the existence of Lucas primitive roots (mod p^e). In the case in which $P = -Q = e = 1$, our results reproduce and improve upon some results for FPR's (mod p) mentioned above.

We shall prove the following two theorems.

Theorem 1: Let U be a Lucas sequence defined by integers $P \neq 0$ and $Q = -1$, let p be an odd prime with $p \nmid D = P^2 + 4$, and let $e \geq 1$ be an integer. Then there is a Lucas primitive root (mod p^e) if and only if

$$\overline{u}(p^e) = \phi(p^e),$$

where ϕ denotes the Euler function. There is exactly one Lucas primitive root (mod p^e) if $\overline{u}(p^e) = \phi(p^e)$ and $p \equiv -1 \pmod 4$, and there are exactly two Lucas primitive roots (mod p^e) if $\overline{u}(p^e) = \phi(p^e)$ and $p \equiv 1 \pmod 4$.

Theorem 2: Let U be a Lucas sequence defined by integers $P \neq 0$ and $Q = -1$, let p be an odd prime with $p \nmid D = P^2 + 4$, and let $e \geq 1$ be an integer. Then there is exactly one Lucas primitive root (mod p^e) if and only if $u(p^e) = \phi(p^e)$ and $p \equiv -1 \pmod 4$, and exactly two Lucas primitive roots (mod p^e) exist if and only if

$$u(p^e) = \phi(p^e)/2 \quad \text{and} \quad p \equiv 1 \pmod 8)$$

or

$$u(p^e) = \phi(p^e)/4 \quad \text{and} \quad p \equiv 5 \pmod 8.$$

From these theorems, some other results follow.

Corollary 1: If U, p, and e satisfy the conditions of Theorem 2 and

$$u(p^e) = \phi(p^e),$$

then g is a Lucas primitive root (mod p^e) if and only if $x = g$ satisfies the congruence

$$(2) \qquad U_n x + U_{n-1} \equiv -1 \pmod{p^e},$$

where $n = \phi(p^e)/2$.

Corollary 2: If U, p, and e satisfy the conditions of Theorem 2 and g is a Lucas primitive root (mod p^e), then $g - P$ is a primitive root (mod p^e).

Corollary 3: If $P \neq 0$ is an integer and both q and $p = 2q + 1$ are primes with conditions $p \nmid P$ and $(D/p) = 1$, where $D = P^2 + 4$ and (D/p) is the Legendre symbol, then there is exactly one Lucas primitive root (mod p) with parameters P and $Q = -1$.

2. Known Results and Lemmas

Let U be a Lucas sequence defined by nonzero integers P and Q, and let $D = P^2 - 4Q$ be the discriminant of the characteristic polynomial of U. If p is an odd prime with $p \nmid Q$ and $e \geq 1$ is an integer, then, as is well known, we have:

(i) $U_n \equiv 0 \pmod{p^e}$ if and only if $u(p^e) \mid n$;

(ii) $U_n \equiv 0$ and $U_{n+1} \equiv 1 \pmod{p^e}$ if and only if $\overline{u}(p^e) \mid n$;

(iii) $u(p) = p$ if $p \mid D$,
$u(p) \mid p - (D/p)$ if $p \nmid D$, where (D/p) is the Legendre symbol;

(iv) $\overline{u}(p^e) = \overline{u}(p) \cdot p^{e-k}$ if $\overline{u}(p) = \cdots = \overline{u}(p^k) \neq \overline{u}(p^{k+1})$ and $e \geq k$;

(v) $u(p) \mid \overline{u}(p)$;

(vi) Let $u(p^e) = 2^a u'$ and $d(p^e) = 2^b d'$, where $d(p^e)$ denotes the least positive integer d for which $Q^d \equiv 1 \pmod{p^e}$ and u', d' are odd integers. We have

$$\overline{u}(p^e) = \begin{cases} [u(p^e),\ d(p^e)] & \text{if } a = b > 0, \\ 2[u(p^e),\ d(p^e)] & \text{if } a \neq b, \end{cases}$$

where [x, y] denotes the least common multiple of integers x and y. (For these properties of Lucas sequences, we refer to [1], [3], [8]).

First, we note that congruence (1) is solvable if and only if the congruence $y^2 \equiv D = P^2 - 4Q \pmod{p^e}$ has solutions. Thus, in case $p \nmid D$, congruence (1) is solvable if and only if $(D/p) = 1$; furthermore, if $(D/p) = 1$, then (1) has two distinct solutions $\pmod{p^e}$.

Let p be an odd prime for which $(D/p) = 1$ and let g_1 and g_2 be the two distinct solutions of (1). Then we have

(3) $$g_1 - g_2 \not\equiv 0 \pmod{p},$$

(4) $$g_1 + g_2 \equiv P,\ g_1 g_2 \equiv Q \pmod{p^e};$$

furthermore, it can easily be seen by induction that

(5) $$g_i^n \equiv U_n g_i - QU_{n-1} \pmod{p^e} \quad (i = 1,\ 2)$$

for every integer $n \geq 1$. Let $n_i = n_i(p^e)$ be the least positive integer for which

$$g_i^{n_i} \equiv 1 \pmod{p^e}.$$

We may assume that $n_1(p^e) \geq n_2(p^e)$.

Lemma 1: If p is an odd prime with conditions $p \nmid Q$, $(D/p) = 1$, and e is a positive integer, then

$$\overline{u}(p^e) = [n_1(p^e),\ n_2(p^e)].$$

Proof: Since $(D/p) = 1$, congruence (1) has two distinct solutions g_1 and g_2 which belong to the exponents $n_1 = n_1(p^e)$ and $n_2 = n_2(p^e)$ $\pmod{p^e}$. Let $\overline{u} = \overline{u}(p^e)$ and $q = [n_1,\ n_2]$. The definition of $\overline{u}$ implies that

$$1 \equiv U_{\overline{u}+1} = PU_{\overline{u}} - QU_{\overline{u}-1} \equiv -QU_{\overline{u}-1} \pmod{p^e};$$

therefore, by (5), for $i = 1$ and $i = 2$, we have

$$g_i^{\overline{u}} \equiv U_{\overline{u}} g_i - QU_{\overline{u}-1} \equiv -QU_{\overline{u}-1} \equiv 1 \pmod{p^e}$$

and so $q \mid \overline{u}$ follows.

On the other hand, by (5) and the definition of q, we have

$$U_q g_1 - U_q g_2 \equiv g_1^q - g_2^q \equiv 0 \pmod{p^e},$$

which with (3) implies $U_q \equiv 0 \pmod{p^e}$. Thus,

$$U_{q+1} = PU_q - QU_{q-1} \equiv -QU_{q-1} \equiv U_q g_1 - QU_{q-1} \equiv g_1^q \equiv 1 \pmod{p^e},$$

and so, by (ii), we have $\overline{u} = q$.

Lemma 2: Let $Q = -1$ and $D = P^2 + 4$. If p is an odd prime with $(D/p) = 1$ and e is a positive integer, then

$$\overline{u}(p^e) = \begin{cases} n_1(p^e) = n_2(p^e) = 4u(p^e) & \text{if } u(p^e) \not\equiv 0 \pmod{2} \\ n_1(p^e) = n_2(p^e) = 2u(p^e) & \text{if } u(p^e) \equiv 0 \pmod{4} \\ n_1(p^e) = 2n_2(p^e) = u(p^e) & \text{if } u(p^e) \equiv 2 \pmod{4}. \end{cases}$$

Proof: Since $Q = -1$ and p is an odd prime, we have $d(p^e) = 2$. Thus, by (vi), we have

$$\text{(6)} \qquad \bar{u} = \bar{u}(p^e) = \begin{cases} 4u & \text{if } u = u(p^e) \not\equiv 0 \pmod 2 \\ 2u & \text{if } u = u(p^e) \equiv 0 \pmod 4 \\ u & \text{if } u = u(p^e) \equiv 2 \pmod 4. \end{cases}$$

Since $(D/p) = 1$, congruence (1) has two distinct solutions, g_1 and g_2, which belong to exponents $n_1 = n_1(p^e)$ and $n_2 = n_2(p^e)$ modulo p^e.

If $n_1 = n_2 = n$, then, by (4), we have

$$1 \equiv (g_1 g_2)^n \equiv Q^n \equiv (-1)^n \pmod{p^e}$$

and so $n = 2m$, where m is a positive integer. Now it can easily be seen that $g_1^m \equiv g_2^m \equiv -1 \pmod{p^e}$; thus, by (5), it follows that

$$U_m g_1 - U_m g_2 \equiv g_1^m - g_2^m \equiv 0 \pmod{p^e}.$$

By (3) and (i), it follows that $u|m$. Hence, $2u|n$. On the other hand, by Lemma 1, $\bar{u} = n$ and so $2u|\bar{u}$; therefore, by (6), we have $\bar{u} = n = 4u$ if $u \not\equiv 0 \pmod 2$ or $\bar{u} = n = 2u$ if $u \equiv 0 \pmod 4$, since in the third case the relation $2u|\bar{u}$ cannot be satisfied.

Now let $n_1 > n_2$. In this case, we have $g_1^{2n_2} \equiv 1 \pmod{p^e}$ and

$$1 \not\equiv g_1^{n_2} \equiv (g_1 g_2)^{n_2} \equiv Q^{n_2} = (-1)^{n_2} \pmod{p^e}.$$

Thus, n_2 is an odd integer; furthermore, $n_1|2n_2$. By our assumption, it follows that $n_1 = 2n_2$. Thus, by Lemma 1, $\bar{u} = n_1 = 2n_2$ follows, and, by (6), we obtain $\bar{u} = n_1 = 2n_2 = u$, because $\bar{u} = 2n_2 \equiv 2 \pmod 4$. This completes the proof.

3. Proofs of Results

Proof of Theorem 1: If there exists a Lucas primitive root (mod p^e), that is, if congruence (1) is solvable and $n_1(p^e) = \phi(p^e)$ or $n_2(p^e) = \phi(p^e)$, then $(D/p) = 1$ and, by Lemma 1, using the relation $n_i|\phi(p^e)$, we get

$$\bar{u}(p^e) = \phi(p^e).$$

Now assume that $\bar{u}(p^e) = \phi(p^e) = p^{e-1}(p-1)$. Using (iv) we get $\bar{u}(p) = p - 1$ and using (iii) and (v) we have

$$u(p) | (p-1,\ p - (D/p)).$$

If $(D/p) = -1$, then $u(p) = 2$ and so $p|P = U_2$. From this

$$(D/p) = ((P^2 + 4)/p) = (4/p) = 1,$$

a contradiction. Thus, $(D/p) = 1$ and (1) is solvable.

If $p \equiv -1 \pmod 4$, then $\bar{u}(p^e) \equiv 2 \pmod 4$. By Lemma 2, we have

$$\bar{u}(p^e) = n_1(p^e) = 2n_2(p^e) = \phi(p^e),$$

which proves that in this case there is exactly one Lucas primitive root (mod p^e).

If $p \equiv 1 \pmod 4$, then $\bar{u}(p^e) \equiv 0 \pmod 4$. In this case, by Lemma 2,

$$\bar{u}(p^e) = n_1(p^e) = n_2(p^e) = \phi(p^e),$$

which proves that there are exactly two Lucas primitive roots (mod p^e). This completes the proof.

Proof of Theorem 2: If there is exactly one Lucas primitive root mod p^e, that is, congruence (1) is solvable and $n_1(p^e) = \phi(p^e)$, $n_2(p^e) < \phi(p^e)$, then $(D/p) = 1$. By Lemma 2, we have

$$\bar{u}(p^e) = n_1(p^e) = 2n_2(p^e) = u(p^e) = \phi(p^e)$$

and $p \equiv -1 \pmod 4$.

If $u(p^e) = \phi(p^e)$ and $p \equiv -1 \pmod 4$, then $u(p^e) \equiv 2 \pmod 4$. Using (6), we have $\overline{u}(p^e) = u(p^e) = \phi(p^e)$; thus, by Theorem 1, it follows that there exists exactly one Lucas primitive root (mod p^e).

Now we assume that there are exactly two Lucas primitive roots (mod p^e). Then $(D/p) = 1$ and, by Lemma 2, we have

$$u(p^e) = \phi(p^e)/2 \quad \text{if } \phi(p^e)/2 \equiv 0 \pmod 4$$

or

$$u(p^e) = \phi(p^e)/4 \quad \text{if } \phi(p^e)/4 \not\equiv 0 \pmod 2.$$

It follows that $u(p^e) = \phi(p^e)/2$ and $p \equiv 1 \pmod 8$ or $u(p^e) = \phi(p^e)/4$ and $p \equiv 5 \pmod 8$.

If $u(p^e) = \phi(p^e)/2$ and $p \equiv 1 \pmod 8$ or $u(p^e) = \phi(p^e)/4$ and $p \equiv 5 \pmod 8$, then $u(p^e) \equiv 0 \pmod 4$ or $u(p^e) \not\equiv 0 \pmod 2$. By (6), we get $\overline{u}(p^e) = \phi(p^e)$. From this, using Theorem 1, it follows that in this case there are exactly two Lucas primitive roots (mod p^e).

Proof of Corollary 1: If g is a Lucas primitive root (mod p^e), then

$$g^{\phi(p^e)/2} \equiv -1 \pmod{p^e};$$

thus, by (5), $x = g$ satisfies congruence (2).

Let $n = \phi(p^e)/2$ and let g be an integer satisfying the congruence

$$U_n g + U_{n-1} \equiv -1 \pmod{p^e}. \tag{7}$$

From this it follows that

$$(U_n g + U_{n-1})^2 = U_n^2(g^2 - Pg - 1) + U_n g(PU_n + 2U_{n-1}) + (U_n^2 + U_{n-1}^2) \equiv 1 \pmod{p^e}. \tag{8}$$

It is well known that

$$U_n(PU_n - 2QU_{n-1}) = U_{2n} \quad \text{and} \quad U_n^2 - QU_{n-1}^2 = U_{2n-1} \tag{9}$$

for any integer $n \geq 1$. In our case, $Q = -1$ and $u(p^e) = \phi(p^e) = 2n$; therefore, by (8) and (9)

$$U_n^2(g^2 - Pg - 1) + U_{2n-1} \equiv 1 \pmod{p^e} \tag{10}$$

follows. But

$$U_{2n-1} = U_{2n+1} - PU_{2n} \equiv U_{2n+1} \equiv 1 \pmod{p^e}, \tag{11}$$

since, by the condition $u(p^e) = \phi(p^e) = 2n$, as we have seen above, we have $u(p^e) = \phi(p^e) = 2n = \overline{u}(p^e)$; furthermore, it can easily be seen that $p \nmid U_n$, so, by (10) and (11), we get

$$g^2 - Pg - 1 \equiv 0 \pmod{p^e}.$$

Thus, by (5) and (7), we have

$$g^n \equiv U_n g + U_{n-1} \equiv -1 \pmod{p^e}. \tag{12}$$

By Lemma 2, using the condition $u(p^e) = \phi(p^e)$ and (12), it follows that g belongs to the exponent $u(p^e) = \phi(p^e)$ modulo p^e, that is, g is a Lucas primitive root (mod p^e).

Proof of Corollary 2: If g is a primitive root (mod p^e) and $g^2 \equiv Pg + 1$ (mod p^e), then $g(g - P) \equiv 1 \pmod{p^e}$. This shows that $g - P$ is a primitive root (mod p^e).

Proof of Corollary 3: Using Lemma 2, by our assumptions we have

$$u(p) = 2q = p - 1.$$

Using Theorem 2, this proves that there exists exactly one Lucas primitive root (mod p).

References

1. P. Bundschuh & J. S. Shiue. "A Generalization of a Paper by D. D. Wall." *Atti Accad. Naz. Lincei, Rend. Cl. Sci. Fis. Mat. Nat.* Ser II *56* (1974): 135-44.
2. 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." *Fibonacci Quarterly* *15* (1977):347-49.
3. D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. of Math.* *31* (1930):419-48.
4. M. J. DeLeon. "Fibonacci Primitive Roots and Period of the Fibonacci Numbers Modulo p." *Fibonacci Quarterly* *15* (1977):353-55.
5. M. E. Mays. "A Note on Fibonacci Primitive Roots." *Fibonacci Quarterly* *20* (1982):111.
6. D. Shanks. "Fibonacci Primitive Roots." *Fibonacci Quarterly* *10* (1972):163-168, 181.
7. D. Shanks & L. Taylor. "An Observation of Fibonacci Primitive Roots." *Fibonacci Quarterly* *11* (1973):159-60.
8. O. Wyler. "On Second Order Recurrences." *Amer. Math. Monthly* *72* (1965):500-506.

*****