PERIODIC LENGTHS OF THE GENERALIZED FIBONACCI SEQUENCE MODULO p

C. C. YALAVIGI AND H. V. KRISHNA
Government College, Mercara India and Manipal Engineering College, Manipal, India

INTRODUCTION

This paper concerns the periodic lengths of the Generalized Fibonacci Sequence modulo p, where p is a prime integer. The GF sequence will be denoted by H_n, $n = 1, 2, \cdots$, for which

(1) $$H_1 = P, \quad H_2 = bP + cQ, \quad H_n = bH_{n-1} + cH_{n-2} \quad (n > 2)$$

and its periodic length reduced modulo p, i.e., the periodic length of the recurring series

(2) $$H_n \pmod{p}, \quad n = 1, 2, \cdots,$$

will be represented by $k(H,p)$. Clearly for $P = 1$, $Q = 0$ the periodic length of the series

(3) $$U_1 = 1, \quad U_2 = b, \quad U_n = bU_{n-1} + cU_{n-2} \quad (n > 2)$$

is given by $k(U,p)$. We prove the following theorems.

2. NATURE OF $k(H,p)$

Theorem a. For primes whose quadratic residue is $b^2 + 4c$, if $(b,c,P,Q) = 1$, then $k(H,p) | (p-1)$.

Proof. In the known formula,

(4) $$H_n = (1r^n - ms^n)/(r-s), \quad (r+s = b, \quad rs = -c, \quad 1 = P - sQ \text{ and } m = P - pQ),$$

let $r,s = (b \pm \sqrt{(b^2+4c)})/2$ so that it may be simplified by the use of binomial theorem to obtain

(5) $$2^nH_n = \left\{ b^n(1-m) + \binom{n}{1} b^{n-1}\sqrt{(b^2+4c)}(1+m) + \binom{n}{2} b^{n-2}(\sqrt{(b^2+4c)})^2(1-m) + \cdots + \binom{n}{n}(\sqrt{(b^2+4c)})^n(1-(-1)^n m)\right\} / (\sqrt{(b^2+4c)}).$$

Then it is easy to show for $n = p$ and $p+1$ that

(6) $$H_p \equiv P \pmod{p}, \quad H_{p+1} \equiv bP + cQ \pmod{p},$$

if $(b^2+4c)^{(p-1)/2} \equiv 1 \pmod{p}$ and $(b,c,P,Q) = 1$. Hence the desired result follows.

Theorem b. For primes whose quadratic nonresidue is $b^2 + 4c$, if $(b,c,P,Q) = 1$, then $k(H,p) | (p^2 - 1)$.

Proof. On using the known formula $H_n = PU_n + cQU_{n-1}$, $(b^2+4c)^{(p-1)/2} \equiv -1 \pmod{p}$ and the following set of congruences, viz.,

(7) $$\begin{gathered} U_p \equiv -1, \quad U_{p+1} \equiv 0, \quad U_{p+2} \equiv -c, \\ U_{2p+1} \equiv 1, \quad U_{2p+2} \equiv 0, \quad U_{2p+2} \equiv (-c)^2 \\ \vdots \\ U_{p(p-1)+p-2} \equiv 1, \quad U_{p(p-1)+p-1} \equiv 0, \quad U_{p(p-1)+p} \equiv (-c)^{p-1}, \end{gathered}$$

it is easy to show that

(8)
$$H_{p+1} \equiv -cQ, \quad H_{p+2} \equiv -cP, \quad H_{p+3} \equiv -c(bP+cQ),$$
$$H_{2p+2} \equiv cQ, \quad H_{2p+3} \equiv (-c)^2P, \quad H_{2p+4} \equiv (-c)^2bP + c(cQ),$$
$$\vdots$$
$$H_{p(p-1)+p-1} \equiv cQ, \quad H_{p(p-1)+p} \equiv (-c)^{p-1}P, \quad H_{p^2+1} \equiv (-c)^{p-1}bP + c(cQ),$$
$$H_{p(p+1)} \equiv -cQ, \quad H_{p(p+1)+1} \equiv (-c)^pP, \quad H_{p(p+1)+2} \equiv (-c)^pbP + c(-cQ).$$

Clearly $(-c)^p \equiv -c \pmod p$ and (8) shows that $k(H,p) | (p^2-1)$.

Theorem c. For primes of the form $2g(2t+1)+1$, where $t \equiv h \pmod{10}$ and $4gh+2g+1 \equiv \pm 1 \pmod{10}$, if
$U_{\{(p-1)/2g\}+1} + cU_{\{(p-1)/2g\}-1} \equiv 0 \pmod p$ and $c^{(p-1)/2g} \equiv 1 \pmod{U_{\{(p-1)/2g\}+1} + cU_{\{(p-1)/2g\}-1}}$,
then $k(H,p) = (p-1)/g$.

Proof. From the well known formulas,

(9) $U_{2n+1} = U_{n+1}(U_{n+1}+cU_{n-1}) + (-1)^{n-1}c^n, \quad U_{2n} = U_n(U_{n+1}+cU_{n-1})$ and $H_n = PU_n + cQU_{n-1}$,

let us set

(10)
$$U_{(p-1)/g} \equiv 0 \pmod{U_{\{(p-1)/2g\}+1} + cU_{\{(p-1)/2g\}-1}},$$
$$U_{(p-1)/g+1} \equiv (-1)^{\{(p-1)/2g\}-1}c^{(p-1)/2g} \pmod{U_{\{(p-1)/2g\}+1} + cU_{\{(p-1)/2g\}-1}},$$

It is then easy to show that

(11)
$$U_{(p-1)/g} \equiv 0 \pmod p, \qquad U_{\{(p-1)/g\}+1} \equiv 1 \pmod p$$

when it follows

(12)
$$H_{(p-1)/g} \equiv Q \pmod p \qquad \text{and} \qquad H_{\{(p-1)/g\}+1} \equiv P \pmod p.$$

Hence, $k(H,p) = (p-1)/g$.

Theorem d. For primes of the form $4gt+1$, where $t \equiv h \pmod{10}$ and $4gh+1 \equiv \pm 1 \pmod{10}$, if
$$U_{(p-1)/2g} \equiv 0 \pmod p \qquad \text{and} \qquad (-c)^{(p-1)/2g} \equiv 1 \pmod p,$$
then $k(H,p) = (p-1)/g$.

Proof. From the known formulas,

(13) $U_{2n} = U_n(U_{n+1}+cU_{n-1}), \quad U_{2n+1} = U_{n+1}(U_{n+1}+cU_{n-1}) + (-1)^{n-1}c^n$ and $U_n^2 - U_{n+1}U_{n-1} = (-c)^{n-1}$,

it is easy to show that

(14)
$$U_{(p-1)/g} \equiv 0 \pmod{U_{(p-1)/2g}}, \quad U_{\{(p-1)/g\}+1} \equiv (-c)^{(p-1)/2g} \pmod{U_{(p-1)/2g}}.$$

when it follows

(15)
$$H_{(p-1)/g} \equiv Q \pmod p, \qquad H_{\{(p-1)/g\}+1} \equiv P \pmod p.$$

Hence $k(H,p) = (p-1)/g$.

Theorem e. For primes of the form $2g(2t+2)+1$, where $t \equiv h \pmod{10}$ and $4g+4gh+1 \equiv \pm 1 \pmod{10}$, if
$$U_{\{(p-1)/2g\}+1} + cU_{(p-1)/2g-1} \equiv 0 \pmod p \quad \text{and} \quad (-c)^{(p-1)/2g} \equiv 1 \pmod p,$$
then $k(H,p) = 2(p-1)/g$.

Proof. We have from (14), $U_{(p-1)/g} \equiv 0 \pmod p$ and $U_{\{(p-1)/g\}+1} \equiv -1 \pmod p$ so that

(16)
$$H_{(p-1)/g} \equiv -Q \pmod p \qquad \text{and} \qquad H_{\{(p-1)/g\}+1} \equiv P \pmod p.$$

Hence the desired result follows.

Theorem f. For primes of the form $2g(2t+1)+1$, where $t \equiv h \pmod{10}$ and $4gh+2g+1 \equiv \pm 1 \pmod{10}$, if

$$U_{(p-1)/2g} \equiv 0 \pmod p \quad \text{and} \quad (-c)^{(p-1)/2g} \equiv 1 \pmod p,$$

then $k(H,p) = 2(p-1)/g$.

Proof. Let us use (13) to obtain

$$U_{(p-1)/g} \equiv 0 \pmod p \quad \text{and} \quad U_{\{(p-1)/g\}+1} \equiv -1 \pmod p.$$

Then it is easy to show that

$$U_{2(p-1)/g} \equiv 0 \pmod p \quad \text{and} \quad U_{\{2(p-1)/g\}+1} \equiv \pmod p \tag{17}$$

when we get

$$H_{2(p-1)/g} \equiv Q \pmod p \quad \text{and} \quad H_{\{2(p-1)/g\}+1} \equiv P \pmod p \tag{18}$$

and the desired result follows.

Analogously, we state the following theorems.

Theorem g. For primes of the form $2g(2t+1)-1$, where $t \equiv h \pmod{10}$ and $4gh+2g-1 \equiv \pm 3 \pmod{10}$, if

$$U_{\{(p+1)/2g\}+1} + cU_{\{(p+1)/2g\}-1} \equiv 0 \pmod p \quad \text{and} \quad c^{(p+1)/2g} \equiv 1 \pmod p,$$

then $k(H,p) = (p+1)/g$.

Theorem h. For primes of the form $4gt-1$, where $t \equiv h \pmod{10}$ and $4gh-1 \equiv \pm 3 \pmod{10}$, if

$$U_{(p+1)/2g} \equiv 0 \pmod p \quad \text{and} \quad (-c)^{(p+1)/2g} \equiv 1 \pmod p,$$

then $k(H,p) = (p+1)/g$.

Theorem i. For primes of the form $2g(2t+2)-1$, where $t \equiv h \pmod{10}$ and $4g+4gh-1 \equiv \pm 3 \pmod p$, if

$$U_{\{(p+1)/2g\}-1} + cU_{\{(p+1)/2g\}-1} \equiv 0 \pmod p \quad \text{and} \quad (-c)^{(p+1)/2g} \equiv 1 \pmod p,$$

then $k(H,p) = 2(p+1)/g$.

Theorem j. For primes of the form $2g(2t+1)-1$, where $t \equiv h \pmod{10}$ and $4gh+2g-1 \equiv \pm 3 \pmod{10}$, if

$$H_{(p+1)/2g} \equiv 0 \pmod p \quad \text{and} \quad (-c)^{(p+1)/2g} \equiv 1 \pmod p,$$

then $k(H,p) = 2(p+1)/g$.

The proofs for Theorems g–j are left to the reader.

REFERENCES

1. C. C. Yalavigi, "On the Periodic Lengths of Fibonacci Sequence Modulo p," *The Fibonacci Quarterly,* to appear.
2. C. C. Yalavigi, "A Further Generalization of Fibonacci Squence," *The Fibonacci Quarterly*, to appear.

****

[Continued from page 112.]

Therefore,

$$F(0,1) = [1,1,1,\cdots] = \frac{1+\sqrt{4+1}}{2} \tag{7}$$

or

$$\lim_{\alpha\to\infty} \frac{I_{\alpha-1}(2a)}{I_\alpha(2a)} = \frac{1+\sqrt{5}}{2} = \phi \text{ (the "golden" ratio)}. \tag{8}$$

Expressing ϕ in this manner as the limit of a ratio of modified Bessel Functions appears to be new [2].

REFERENCES

1. D.H. Lehmer, "Continued Fractions Containing Arithmetic Progressions," *Scripta Mathematica,* Vol. XXIX, No.s 1–2, Spring-Summer 1973, pp. 17–24.
2. D. H. Lehmer, Private Communication.

****