A DIVISIBILITY PROPERTY OF BINARY LINEAR RECURRENCES

Neville Robbins
Mathematics Department, San Francisco State University, San Francisco, CA 94132
E-mail: robbins@math.sfsu.edu
(Submitted April 2000-Final Revision October 2000)

INTRODUCTION

If A is a positive integer, let the polynomial $\lambda^2 - A\lambda - 1$ with discriminant $D = A^2 + 4$ have the roots:

$$\alpha = (A + \sqrt{D})/2, \quad \beta = (A - \sqrt{D})/2. \tag{1}$$

Define a primary binary linear recurrence $\{u_n\}$ and a secondary binary linear recurrence $\{v_n\}$ by

$$u_n = (\alpha^n - \beta^n)/(\alpha - \beta), \quad v_n = \alpha^n + \beta^n, \tag{2}$$

where $n \geq 0$. Equivalently, let

$$u_0 = 0, \; u_1 = 1, \; u_n = Au_{n-1} + u_{n-2} \tag{3}$$

and

$$v_0 = 2, \; v_1 = A, \; v_n = Av_{n-1} + v_{n-2} \tag{4}$$

for $n \geq 2$. Let

$$t = \begin{cases} D & \text{if } A \text{ is odd,} \\ D/4 & \text{if } A \equiv 0 \pmod 4, \\ D/8 & \text{if } A \equiv 2 \pmod 4. \end{cases} \tag{5}$$

Note that, in each case, t is an integer such that $t \equiv 1 \pmod 4$.

Let $\left(\frac{a}{b}\right)$ denote the Jacobi symbol.

In this note, we prove a divisibility property of the $\{u_n\}$ and of the $\{v_n\}$. In so doing, we generalize a recent result by V. Drobot [2] about Fibonacci numbers (the sequence $\{u_n\}$ with $A = 1$). It has been called to our attention that an alternate proof of Drobot's result follows from [1]. Note that, if $A = 2$, then the corresponding u_n sequence is called the *Pell* sequence, and is denoted P_n. Thus, we have $P_1 = 1$, $P_2 = 2$, $P_3 = 5$, $P_4 = 12$, $P_5 = 29$, and so forth.

THE MAIN RESULTS

Theorem 1: Let $\{u_n\}$ and t be defined as above. Let p be an odd integer such that $q = 2p - 1$ is prime, and $q \nmid t$. If $A \not\equiv 2 \pmod 4$, let $\left(\frac{q}{t}\right) = -1$. If $A \equiv 2 \pmod 4$ but $A > 2$, let $q \equiv \pm 1 \pmod 8$ and $\left(\frac{q}{t}\right) = -1$ or $q \equiv \pm 3 \pmod 8$ and $\left(\frac{q}{t}\right) = 1$. If $A = 2$, let $q \equiv \pm 3 \pmod 8$. Then $q \mid u_p$. Furthermore, u_p is composite unless $u_p = q$, which can occur only in the cases $(A, p, q) = (1, 7, 13)$ (Fibonacci) or $(A, p, q) = (2, 3, 5)$ (Pell).

Proof: Equation (1) implies

$$\alpha - \beta = \sqrt{D} \quad \alpha\beta = -1. \tag{6}$$

Applying (2) and (6) with $n = p$, we obtain $\sqrt{D}u_p = \alpha^p - \beta^p$. Squaring and applying (6), we get

$$Du_p^2 = \alpha^{2p} + \beta^{2p} + 2. \tag{7}$$

Multiplying by 2^{2p-1} and applying (1), we have

$$2^{2p-1}Du_p^2 = \frac{1}{2}\{(A+\sqrt{D})^{2p} + (A-\sqrt{D})^{2p}\} + 4^p \tag{8}$$

If we expand the right member of (8) via the binomial theorem and then simplify, we obtain

$$2^{2p-1}Du_p^2 = A^{2p} + \sum_{k=1}^{p-1}\binom{2p}{2k}A^{2p-2k}D^k + D^p + 4^p. \tag{9}$$

Since $q = 2p-1$ is prime by hypothesis, we have

$$q \left| \binom{2p}{2k} \right. \text{ for } 1 \le k \le p-1.$$

Furthermore, by Fermat's Little Theorem, we have $A^{2p} \equiv A^2 \pmod{q}$, $4^p \equiv 4 \pmod{q}$, $2^{2p-1} \equiv 2 \pmod{q}$. Thus, we have

$$2Du_p^2 \equiv A^2 + 4 + D^p \equiv D + D^p \equiv D(1+D^{p-1}) \pmod{q},$$

which yields $2u_p^2 \equiv 1 + D^{p-1} \pmod{q}$.

Since $p-1 = (q-1)/2$, Euler's criterion yields

$$2u_p^2 \equiv 1 + \left(\frac{D}{q}\right) \pmod{q}.$$

Therefore, to prove that $q \mid u_p$, it suffices to show that $\left(\frac{D}{q}\right) = -1$. If $A \not\equiv 2 \pmod 4$, then $\left(\frac{D}{q}\right) = \left(\frac{t}{q}\right)$. Since $t \equiv 1 \pmod 4$ and $t > 1$, we have

$$\left(\frac{t}{q}\right) = \left(\frac{q}{t}\right) = -1$$

by hypothesis, so we are done.

If $A = 2$, so that $D = 8$, then

$$\left(\frac{D}{q}\right) = \left(\frac{8}{q}\right) = \left(\frac{2}{q}\right) = -1$$

since $q \equiv -3 \pmod 8$ by hypothesis. More generally, if $A \equiv 2 \pmod 4$ but $A > 2$, then

$$\left(\frac{D}{q}\right) = \left(\frac{8t}{q}\right) = \left(\frac{2t}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{t}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{q}{t}\right),$$

since $t \equiv \pm 1 \pmod 4$. By hypothesis, we have $\left(\frac{2}{q}\right) = -\left(\frac{q}{t}\right)$ so we are done.

The last sentence of the conclusion of Theorem 1 is now an easy corollary.

Remarks: If $A = 1$, then $u_n = F_n$. (This was the case considered in [2].) If t is composite, then the determination of congruence conditions on q (mod t) such that $\left(\frac{q}{t}\right) = \left(\frac{t}{q}\right) = \pm 1$ may be achieved by factoring t as a product of primes and then applying the Chinese Remainder Theorem.

Corollary 1: If P_n denotes the n^{th} Pell number, the integer $p > 3$, $p \equiv 3 \pmod 4$, and $q = 2p-1$ is prime, then $q \mid u_p$ and $q < u_p$.

Proof: This follows from Theorem 1, with $A = 2$.

We now present an analogous theorem regarding $\{v_n\}$, namely,

Theorem 2: Let $\{v_n\}$ and t be defined as in the Introduction. Let p be an odd integer such that $q = 2p+1$ is prime and $q \nmid t$. If $A \not\equiv 2 \pmod 4$, let $\left(\frac{q}{t}\right) = -1$. If $A \equiv 2 \pmod 4$ but $A > 2$, let $q \equiv \pm 1 \pmod 8$ and $\left(\frac{q}{t}\right) = -1$ or $q \equiv \pm 3 \pmod 8$ and $\left(\frac{q}{t}\right) = 1$. If $A = 2$, let $q \equiv \pm 3 \pmod 8$. Then $q \mid v_{p+1}$.

Proof: The proof is similar to that of Theorem 1 and is therefore omitted here.

REFERENCES

1. D. Bloom. "Problem H-494." *The Fibonacci Quarterly* **33.1** (1995):91.
2. V. Drobot. "Primes in the Fibonacci Sequence." *The Fibonacci Quarterly* **38.1** (2000):71-72.

AMS Classification Number: 11B35