ON THE DIVISORS OF SECOND-ORDER RECURRENCES

PAUL A. CATLIN
Carnegie-Mellon University, Pittsburg, Pennsylvania 15213

1. INTRODUCTION AND NOTATIONS

In this note, we shall give a criterion to determine whether a given prime p divides terms of the second-order recurrence

(1) $$A_{n+2} = PA_{n+1} - QA_n ,$$

with arbitrary initial values A_0 and A_1, and we shall give several applications.

A particular case of (1) is the recurrence

(2) $$U_{n+2} = PU_{n+1} - QU_n, \quad U_0 = 0, \quad U_1 = 1 .$$

We shall denote by Δ the discriminant $P^2 - 4Q$ of the recurrence. The general term U_n of (2) may be denoted by

$$(a^n - b^n)/(a - b) ,$$

where

$$a = \frac{P + \sqrt{\Delta}}{2}$$

and

$$b = \frac{P - \sqrt{\Delta}}{2} .$$

There is an integer $k(m)$ such that m divides U_n if and only if $k(m)|n$. p will denote a prime not dividing Q. In this paper, we shall be working in the field of integers modulo p.

2. THE CRITERION FOR DIVISIBILITY

Let R_n be the quotient $U_{n+1}/U_n \pmod p$: i.e., the solution X of

$$XU_n \equiv U_{n+1} \pmod p .$$

R_n exists, unless p divides U_n, in which case the value of R_n will be denoted by ∞. (All quotients which have a zero divisor will be denoted ∞.) If R_n exists and is nonzero, then

(3) $$R_{n+1} \equiv U_{n+2}/U_{n+1} \equiv P - QR_n^{-1} \pmod p ;$$

if $p | R_n$ then $R_{n+1} \equiv \infty$; if $R_n \equiv \infty$ then $p | U_n$, so $R_{n+1} \equiv P \pmod p$.

Theorem 1. (R_n) is a first-order recurrence mod p and is periodic with primitive period $k(p)$.

Proof. We have already shown that (R_n) is a first-order recurrence (3). That it has primitive period $k(p)$ follows from the definition of k and the fact that $R_n \equiv 0$ if and only if $p | U_{n+1}$.

The following theorem gives a criterion for determining whether p is a divisor of terms of (A_n). It is known that if a number m divides some term A_n of (1), then m divides $A_{n+tk(m)}$ for any integer t for which the subscript is nonnegative, and only those terms.

Theorem 2. (Divisibility criterion). p is a divisor of $A_{tk(p)-n}$ (for any t for which the subscript is nonnegative) if and only if

$$A_1/A_0 \equiv R_n \pmod p .$$

Proof. By Eq. (8) of [6].

$$Q^n A_m = U_{n+1}A_{k(p)} - U_n A_{k(p)+1} ,$$

where $m + n = k(p)$. Thus, $p | A_m$ if and only if

$$A_{k(p)+1}/A_{k(p)} \equiv R_n ,$$

and it is known that

$$A_{k(p)+1}/A_{k(p)} \equiv A_1/A_0 .$$

Furthermore, $p | A_m$ if and only if $p | A_{tk(p)-n}$, and the theorem follows.

3. APPLICATIONS OF THE CRITERION

It is well known that $k(p) | p - (\Delta/p)$. A proof is given in [4] for the Fibonacci series, and it may be easily generalized to the recurrence (2). For most recurrences, there are many primes p such that $k(p) = p - (\Delta/p)$. In the first two theorems in this section, we consider such primes.

The following result was proved in [1] and [2] for the Fibonacci series.

Theorem 3. If

$$k(p) = p + 1$$

then p divides some terms of (A_n) regardless of the initial values A_0 and A_1, and conversely.

Proof. It follows from Theorem 1 that if

$$k(p) = p + 1,$$

then for any residue class c there is an n such that $c \equiv R_n \pmod p$. Therefore, there is an n such that

$$A_1/A_0 \equiv R_n \pmod p,$$

and the first part follows by the criterion of Theorem 2. If $k(p)$ is less than $p + 1$ then not every residue class is included in (R_n), and the converse follows.

Theorem 4. p is a divisor of terms of (A_n) for any initial values A_0 and A_1, excepting when $A_1/A_0 \equiv a$ or b, if and only if $k(p) = p - 1$.

Proof. Since

$$k(p) = p - 1,$$

we have

$$(\Delta/p) = 1,$$

so a and b are in the field of integers modulo p and $p \nmid \Delta$. By definition,

$$R_n \equiv (a^{n+1} - b^{n+1})/(a^n - b^n).$$

If $R_n \equiv a$ (or b) $\pmod p$ then it follows that $a \equiv b$, whence $p | \Delta$, giving a contradiction. Thus, $R_n \not\equiv a$ or b. By Theorem 2 and the fact that $R_n \equiv A_1/A_0$ for some n when

$$k(p) = p - 1$$

and

$$A_1/A_0 \not\equiv a \text{ or } b \pmod p,$$

we see that p divides terms of (A_n). If $k(p)$ is less than $p - 1$, then not every residue class can be included in (R_n), whence the converse follows.

Theorem 5. If

$$A_1/A_0 \equiv a \text{ or } b \pmod p$$

then p divides no term of (A_n).

Proof. If

$$A_1/A_0 \equiv a \text{ or } b$$

then

$$(\Delta/p) = 1$$

and $p \nmid \Delta$. If

$$R_n \equiv a \quad (\text{or } b) \quad (\text{mod } p)$$

then

$$(a^{n+1} - b^{n+1})/(a^n - b^n) \equiv a \quad (\text{or } b)$$

so that $a \equiv b$ and $p|\Delta$, giving a contradiction. Thus, $R_n \not\equiv a$ (or b) $\equiv A_1/A_0$, and so $p \nmid A_n$ for any n, by Theorem 2.

4. CONCLUDING REMARKS

Hall [3] has given a different criterion for whether a prime p divides some terms of (1). Bloom [2] has studied the related question of which composite numbers (as well as which primes) are divisors of recurrences of the form (1) with $P = 1$, $Q = -1$.

Ward [5] has pointed out that the question of whether or not there are infinitely many primes for which $k(p) = p + 1$ or $p - 1$ is a generalization of Artin's conjecture that an integer not -1 or a square is a primitive root of infinitely many primes. For recurrences in which Δ is a square and a or b is 1, the question is equivalent to Artin's conjecture.

REFERENCES

1. Brother U. Alfred, "Primes which are Factors of all Fibonacci Sequences," Fibonacci Quarterly, Vol. 2, No. 1 (February 1964), pp. 33-38.
2. D. M. Bloom, "On Periodicity in Generalized Fibonacci Sequences," Amer. Math. Monthly, 72 (1965), pp. 856-861.
3. Marshall Hall, "Divisors of Second-Order Sequences," Bull. Amer. Math. Soc., 43 (1937), pp. 78-80.
4. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Third Ed., Clarendon Press, Oxford, 1954.
5. Morgan Ward, "Prime Divisors of Second-Order Recurrences," Duke Math. J., 21 (1954) pp. 607-614.
6. Oswald Wyler, "On Second-Order Recurrences," Amer. Math. Monthly, 72 (1965), pp. 500-506.