THE PRIME DIVISORS OF FIBONACCI NUMBERS

MORGAN WARD

1. Introduction. Let

$$(U) : U_0, U_1, U_2, \cdots, U_n, \cdots$$

be a linear integral recurrence of order two; that is,

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

P, Q integers, $Q \neq 0$; U_0, U_1, integers. It is an important arithmetical problem to decide whether or not a given number m is a divisor of (U); that is, to find out whether the diophantine equation

$$U_x = my , \qquad m \geqq 2 \tag{1.1}$$

has a solution in integers x and y. Our information about this problem is scanty except in the cases when it is trivial; that is when the characteristic polynomial of the recursion has repeated roots, or when some term of (U) is known to vanish.

If we exclude these trivial cases, there is no loss in generality in assuming that m in (1.1) is a prime power. It may further be shown by p-adic methods [7] that we may assume that m is a prime. Thus the problem reduces to characterizing the set $\mathfrak{P}$ of all the prime divisors of (U). $\mathfrak{P}$ is known to be infinite [6], and there is also a criterion to decide a priori whether or not a given prime is a member of $\mathfrak{P}$, [2], [6], [7]. But this criterion is local in character and tells little about $\mathfrak{P}$ itself.

I propose in this paper to study in detail a special case of the problem in the hope of throwing light on what happens in general. I shall discuss the prime divisors of the Fibonacci numbers of the second kind:

$$(G) : 2, 1, 3, 4, 7, \cdots, G_n, \cdots$$

These and the Fibonacci numbers of the first kind

$$(F) : 0, 1, 1, 2, 3, 5, \cdots, F_n, \cdots$$

are probably the most familiar of all second order integral recurrences; (F) and (G) have been tabulated out to one hundred and twenty terms by C. A. Laisant [3].

2. Preliminary classification of primes. Let R denote the rational field and $\mathscr{R} = R(\sqrt{5})$ the root field of the characteristic polynomial

Received April 14, 1960.

$$f(x) = x^2 - x - 1 \tag{2.1}$$

of (F) and (G). Then if α and β are the roots of $f(x)$ in $\mathscr{R}$,

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ G_n = \alpha^n + \beta^n\ , \qquad (n = 0, 1, 2, \cdots).$$

If p is any rational prime, by its rank of apparition in (F) or rank, we mean the smallest positive index x such that p divides F_x. We denote the rank of p by ρ_p or ρ. Its most important properties are: $F_n \equiv o \pmod p$ if and only if $n \equiv o \pmod \rho$; $p - (5/p) \equiv o \pmod \rho$. Here $(5/p)$ is the usual Legendre symbol.

The following consequence of (2.1) and the formula $F_{2n} = F_n G_n$ is well known.

LEMMA 2.1. *p is a divisor of (G) if and only if the rank of apparition of p in (F) is even.*

The formula

$$G_n^2 - 5F_n^2 = (-1)^n 4 \tag{2.2}$$

gives more information. For if $p \equiv 1 \pmod 4$, and p divides (G), (2.2) implies that $(5/p) = 1$. On the other hand if $p \equiv 3 \pmod 4$, p must divide (G). For otherwise Lemma 2.1 and formula (2.2) with $n = \rho_p$ imply $(-1/p) = 1$.

On classifying the primes according to the quadratic characters of 5 and -1 modulo p, they are distributed into eight arithmetical progressions $20n + 1$, $20n + 3$, $20n + 7$, $20n + 9$, $20n + 11$, $20n + 13$, $20n + 17$, $20n + 19$. By the remarks above, only primes of the form $20n + 1$ and $20n + 9$ for which both -1 and 5 are quadratic residues need be considered; the following lemma disposes of all others.

LEMMA 2.2. *p is a divisor of (G) if $p \equiv 3 \pmod 4$; that is if $p \equiv 3, 7, 11, 19 \pmod{20}$. p is a non-divisor of (G) if $p = 1 \pmod 4$ and $p \equiv 2$ or $3 \pmod 5$; that is if $p \equiv 13, 17 \pmod{20}$.*

3. Further classification criteria. Let $\mathfrak{Q}$ denote the set of all primes having both 5 and -1 as quadratic residues; that is primes of the $20n+1$ or $20n+9$. For the remainder of the paper all primes considered belong to $\mathfrak{Q}$. Let $\mathfrak{P}$ denote the subset of divisors of (G) and $\mathfrak{P}^* = \mathfrak{Q} - \mathfrak{P}$ the complementary set of non-divisors of (G). We shall derive criteria to decide whether p belongs to $\mathfrak{P}$ or to $\mathfrak{P}^*$.

If p is any element of $\mathfrak{Q}$, we may write

$$p \equiv 2^k + 1 \pmod{2^{k+1}},\ p - 1 = 2^k q,\ q \text{ odd};\ k \geqq 2\ . \tag{3.1}$$

We shall call k the (dyadic) order of p. Thus primes of order two are of the forms $40n + 21$ and $40n + 29$, primes of order three, of the form $80n + 9$ and $80n + 41$ and so on. The difficulty of classifying p as a divisor or non-divisor of (G) increases rapidly with its order.

Let R_p denote the finite field or p elements. For every $p \varepsilon \mathfrak{Q}$, the characteristic polynomial (2.2) splits in R_p:

$$(3.2) \qquad x^2 - x - 1 = (x = a)(x - b), a, b \varepsilon R_p \; .$$

If we represent the elements of R_p by the least positive residues of p, then by a classical theorem of Dedekind's, the factorization of p in the root-field $\mathscr{R}$ of $f(x)$ is given by

$$(3.3) \qquad p = \mathfrak{q}\mathfrak{q}', \; \mathfrak{q} = (p, \alpha - a), \; \mathfrak{q}' = (p, \alpha - b) \; .$$

Here $\mathfrak{q}$ and $\mathfrak{q}'$ are conjugate prime ideals of $\mathscr{R}$ of norm p.

Now assume $p \varepsilon \mathfrak{P}^*$; then rank ρ of p divides q in (3.1). Consequently $F_q \equiv o \pmod p$, so that $\alpha^q \equiv \beta^q (\bmod \mathfrak{q})$ in $\mathscr{R}$. But then $\alpha^{2q} \equiv \alpha^q \beta^q \equiv (-1)^q \equiv -1 \pmod{\mathfrak{q}}$ so that $a^{2q} \equiv -1 \pmod{\mathfrak{q}}$. But then $a^{2q} \equiv -1 \pmod p$ in R. Conversely, assume that $a^{2q} \equiv -1 \pmod p$. Then in $\mathscr{R}$, $\alpha^{2q} \equiv -1 \pmod{\mathfrak{q}}$ or $\alpha^{2q} \equiv (\alpha\beta)^q (\bmod \mathfrak{q})$, $(\alpha - \beta)\alpha^q F_q \equiv O \pmod{\mathfrak{q}}$. But $(\alpha - \beta, \mathfrak{q}) = (\alpha, \mathfrak{q}) = (1)$ in $\mathscr{R}$. Hence $F_q \equiv O \pmod{\mathfrak{q}}$ so that $F_q \equiv O \pmod p$ in R. Thus the rank of p in (F) must divide q and is consequently odd. Hence $p \varepsilon \mathfrak{P}^*$.

It follows that $p \varepsilon \mathfrak{P}^*$ if and only if $a^{2q} = -1$ in R_p. Since $(ab)^{2q} = (-1)^{2q} = +1$ in R_p, it is irrelevant which root of $f(x) = 0$ in R_p we choose for a. An equivalent way of stating this result is that $p \varepsilon \mathfrak{P}^*$ if and only if $a^{4q} \equiv 1 \pmod p$ but $a^{2q} \not\equiv 1 \pmod p$.

For ease of printing, let

$$[u/p]_n = (u/k)_{2^n}$$

denote the $2^n ic$ character of u modulo p. Thus $[u/p]_1$ is an ordinary quadratic character, $[u/p]_2$ or $(u/p)_4$ a biquadratic character and so on. The result we have obtained may be stated as follows:

THEOREM 3.1. *Let p be any prime of order $k \geqq 2$. Then if a is a root of $x^2 - x - 1$ in the finite field R_p, a necessary and sufficient condition that p belong to $\mathfrak{P}^*$ is*

$$(3.3) \qquad [a/p]_{k-1} = -1 \; .$$

There is another useful way of stating this result. Let

$$(3.4) \qquad g(x) = f(x^{2^{k-2}}) = x^{2^{k-1}} - x^{2^{k-2}} - 1 \; .$$

Assume that $p \varepsilon \mathfrak{P}$. Then each of the equations

$$x^{2^{k-2}} = a, \ x^{2^{k-2}} = b$$

where a, b are the roots of $f(x)$ in R_p, has 2^{k-2} roots in R_p. If c is any one of these roots, it follows from (3.4) that c is a root of $g(x)$. Hence the polynomial $g(x)$ splits completely in R_p. On the other hand since neither of the equations

$$x^{2^{k-1}} = a, \ x^{2^{k-1}} = b$$

has a root in R_p, $g(x^2)$ has no roots in R_p. Evidently, by Theorem 3.1, these splitting conditions imply conversely that $p \varepsilon \mathfrak{P}^*$. Hence

THEOREM 3.2. *Necessary and sufficient conditions that p belong to $\mathfrak{P}^*$ are that the polynomial $g(x)$ defined by* (3.4) *splits completely into linear factors modulo p, but the polynomial $g(x^2)$ has no linear factor modulo p.*

For example, assume that $p \equiv 5 \pmod 8$ so that $k = 2$. Then $g(x) = f(x)$ so the first condition of Theorem 3.2 is always satisfied. Since $g(x^2) = x^4 - x^2 - 1$ we may state the following corollary.

COROLLARY 3.1. *If p is of order two, $p \varepsilon \mathfrak{P}$ if and only if the polynomial $x^4 - x^2 - 1$ is completely reducible modulo p.*

In like manner if $p \equiv 1 \pmod 8$ so that $k \geqq 2$, we may state the following corollary

COROLLARY 3.2. *If p is of order three or more, a sufficient condition that $p \varepsilon \mathfrak{P}$ is that the polynomial $x^4 - x^2 - 1$ is not completely reducible modulo p.*

Now let

$$p = u^2 + 4v^2 \tag{3.5}$$

be the representation of p as a sum of two squares. Either u or v is divisible by 5.

LEMMA. *The polynomial $z^4 - z^2 - 1$ splits completely in R_p if and only if in the representation* (3.5) *either* $u \equiv \pm 1 \pmod 5$ *or* $v \equiv \pm 1 \pmod 5$.

Proof. Since $z^4 - z^2 - 1 = ((2z^2 - 1)^2 - 5)/4$, $z^4 - z^2 - 1$ always splits into quadratic factors in R_p. But if i denotes an element of R_p whose square is $p - 1$, then $z^4 - z^2 - 1 = (z^2 + i)^2 - (1 + 2i)z^2$. Hence a necessary and sufficient condition that $z^4 - z^2 - 1$ split completely in R_p is that $1 + 2i = ((-1)(-1 - 2i))$ be a square in R_p.

Now let $\mathfrak{T}$ denote the ring of the Gaussian integers, and let $p = (u + 2iv)(u - 2iv)$ be the decomposition of p into primary factors in $\mathfrak{T}$.

(Bachmann [1]). Then $u - 2iv$ is a prime ideal of norm p so that the residue class ring $\mathfrak{T}/(u - 2iv)$ is isomorphic to R_p. Now $-1 - 2i$ is primary in $\mathfrak{T}$. Also since $p \equiv 1 \pmod 4$, -1 is a quadratic residue of $u - 2iv$. Hence $1 + 2i$ is a square in R_p if and only if $-1 - 2i$ is a quadratic residue of $u - 2iv$ in $\mathfrak{T}$. By the quadratic reciprocity law in $\mathfrak{T}$, (Bachmann [1])

$$\left(\frac{-1-2i}{u-2iv}\right) = \left(\frac{u-2iv}{-2-2i}\right) = \left(\frac{u+v}{-1-2i}\right).$$

Now either u or v must be divisible by $-1 - 2i$. But $(-1 - 2i)$ is a prime ideal in $\mathfrak{T}$ of norm five. Therefore $-1 - 2i$ is a quadratic residue of $u - 2iv$ if and only if $u \equiv 0$, $v \equiv 1, 4 \pmod 5$ or $v \equiv 0$, $u \equiv 1, 4 \pmod 5$. This completes the proof of the lemma.

On combining the results of Corollaries 3.1 and 3.2 into the lemma, we obtain

THEOREM 3.3. *Let p be congruent to* 5 *modulo* 8. *Then a necessary and sufficient condition that $p \varepsilon \mathfrak{P}$ is that in the representation* (3.5) *of p as a sum of two squares, either $u \equiv \pm 1 \pmod 5$ or $v \equiv \pm 1$ mod 5. If p is congruent to* 1 *modulo* 8, *a sufficient condition that $p \varepsilon \mathfrak{P}$ is that $u \equiv \pm 2 \pmod 5$ or $v \equiv \pm 2$ mod 5.*

4. Applications of the criteria. The theorems of § 3 classify unambiguously all primes of $\mathfrak{O}$ either into $\mathfrak{P}$ or into $\mathfrak{P}^*$. But in the absence of workable reciprocity laws beyond the biquadratic case, they tell us little more than Lemma 2.1 for primes of order greater than three; that is, primes of the forms $160n + 9$ or $160n + 81$. However the theorems may be extended so as to give useful information about primes of any order by utilizing the following elementary properties of the character symbol $[u/p]_k$:

$$\begin{aligned} &[uv/p]_k = [u/p]_k[v/p]_k \\ (4.1)\qquad &[u^2/p]_k = [u/p]_k^2 = [u/p]_{k-1} \\ &[u/p]_k = 1 \text{ implies } [u/p]_n = 1 \text{ for } 1 \leqq n \leqq k-1 . \end{aligned}$$

From (4.1) (iii) and Theorem 3.1 we immediately obtain.

THEOREM 4.1. *If p is of order $k \geqq 3$, then a necessary condition that p belong to $\mathfrak{P}^*$ is that*

$$[a/p]_n = 1 \qquad (n = 1, 2, \cdots, k-2) . \tag{4.2}$$

COROLLARY 4.1. *A sufficient condition that p belong to $\mathfrak{P}$ is that* (4.2) *be false for some $n \leqq k - 2$.*

Now suppose that a solution $x = c$ of the congruence $c^2 \equiv a \pmod{p}$ is known, p of order four or more. Then by (4.1) (ii) and the theorem just proved we obtain.

THEOREM 4.2. *If p is of order $k \geqq 4$, then a necessary condition that p belong to $\mathfrak{P}^*$ is that*

$$[c/p]_n = 1\,, \qquad (n - 1, 2, \cdots, k - 3). \tag{4.4}$$

A necessary and sufficient condition that p belong to $\mathfrak{P}^*$ is that

$$[c/p]_{k-2} = -1\,. \tag{4.5}$$

There is a method for obtaining a, the root of (2.1) modulo p, which leads to another useful criterion for primes of low order. For every prime p of $\mathfrak{O}$ there exists a unique representation in the form

$$p = r^2 - 5s^2,\ 0 < r,\ 0 < s < \sqrt{4p/5}\,. \tag{4.6}$$

(Uspensky [5]). If this representation is known, a is easily shown to be the least positive solution of the congruence

$$2sa \equiv (r + s) \quad (\text{mod } p.)\,. \tag{4.7}$$

By using property (4.1) (i) of the character symbol and Theorem 3.1, we see that

$$[2s/p]_{k-1} = -[(r + s)/p]_{k-1}$$

is a necessary and sufficient condition that p belong to $\mathfrak{P}^*$.

If $k = 2$, the criterion becomes $(2s/p) = -((r + s)/p)$. But since $p \equiv 5 \pmod{8}$ and $p = r^2 - 5s^2$, r is odd and $s = 2s'$ where s' is odd. Hence by the reciprocity law for the Jacobi symbol, $(2s/p) = (s'/p) = (p/s') = (r^2/s') = +1$. Hence $p\varepsilon\mathfrak{P}^*$ if and only $((r + s)/p) = -1$. But $((r + s)/p) = ((r^2 - 5s^2)/(r + s)) = (-4s^2/(r + s)) = (-1/(r + s)) = (-1)^{(r+1)/2}$ since $s \equiv 2 \pmod{4}$. We have thus proved

THEOREM 4.3. *If p is of order two, so that p is of the form $40n + 21$ or $40n + 29$, then p belongs to $\mathfrak{P}$ or to $\mathfrak{P}^*$ according as r in the representation* (4.6) *is congruent to three or one modulo* 4.

Now if $k > 2$, $p \equiv 1 \pmod{8}$ so that r in the representation (4.6) is odd. Hence using the corollary to Theorem 4.1 with $n = 1$ and the results established in the proof of Theorem 4.3, we obtain

THEOREM 4.4. *If p is of order greater than two, p belongs to $\mathfrak{P}$ if r in the representation* (4.6) *is congruent to one modulo* 4.

To illustrate, suppose that $p = 101$. Then $p \equiv 5 \pmod{8}$ so that

Theorem 3.3 is applicable. Since $101 = 1^2 + 4\cdot 5^2$, $101 \varepsilon \mathfrak{P}$. Also $101 = 11^2 - 5\cdot 2^2$ and $11 \equiv 3 \pmod 4$. Hence $101 \varepsilon \mathfrak{P}$ by Theorem 4.3. In fact we find from Laisant's table that $G_{50} = 12586269025 = 101 \times 124616525$.

Again, there are seven primes in $\mathfrak{Q}$ less than one thousand of order greater than three; namely 241, 401, 449, 641, 769, 881 and 929. But only two of these need be discussed; Theorem 3.3 assigns 241, 449, 641, 881 and 929 to $\mathfrak{P}$. For $241 = 15^2 + 4.2^2$, $449 = 7^2 + 4.10^2$, $641 = 25^2 + 4.2^2$, $881 = 25^2 + 4.8^2$ and $929 = 23^2 + 4.10^2$. There remain 401 and 729. Now $401 \equiv 17 \pmod{32}$. Hence $k = 4$. Since $112^2 - 112 - 1 = 31 \times 401$, $a = 112$. Hence by Theorem 3.1, $401 \varepsilon \mathfrak{P}^*$ if and only if $[112/401]_3 = -1$. Now using the idea in Theorem 4.2, $112 = 2^4 \times 7$ and $85^2 \equiv 7 \pmod{401}$. Hence $[112/401]_3 = [85/401]_2$. But $(85/401) = -1$. Hence $401 \varepsilon \mathfrak{P}$. This conclusion is easily checked. For $401 - 1 = 25.16$ and by Laisant's table, $F_{25} = 75025 \not\equiv 0 \pmod{401}$. Hence $401 \varepsilon \mathfrak{P}$ by Lemma 2.1.

Finally $769 \equiv 257 \pmod{512}$ so that $k = 8$. Using Jacobi's Canon, $a = 43$, ind $a = 500 \not\equiv 0 \pmod{64}$ so that $769 \varepsilon \mathfrak{P}$. Indeed $769 - 1 = 3\cdot 256$ and $F_3 = 2$. Hence $769 \varepsilon \mathfrak{P}$ by Lemma 2.1.

We have shown incidentally that every prime $p < 1000$ in $\mathfrak{Q}$ of order greater that three is a divisor of (G).

5. Conclusion. The methods of this paper may be easily extended to obtain information about the prime divisors of the Lucas or Lehmer [4] numbers of the second kind $\alpha^n + \beta^n$ where α and β now are the roots of any quadratic polynomial $x^2 - \sqrt{P}x + Q$ with P, Q integers, $Q(P - 4Q) \neq 0$. It is worth noting that just as in the special case $P = 1$ $Q = -1$ investigated here, there will be arithmetical progressions whose primes cannot be characterized as divisors or non-divisors by their quadratic or biquadratic characters alone.

In the absence of any criterion like Lemma 2.1 for a prime divisor of an arbitrarily selected recurrence (U), it seems difficult to characterize the divisor of (U) in any general way. It would be interesting to make a numerical study of several recurrences (U) to endeavor to find out whether the two Lucas sequences $0, 1, P, \cdots$ and $2, P, P^2 - 2Q, \cdots$ and their translates are essentially the only ones for which a global characterization of the divisors is possible.

References

1. Paul Bachmann, *Kreistheilung*, Leipzig (1921), 150-185.

2. Marshall Hall, *Divisors of second order sequences*, Bull. Amer. Math. Soc., **43** (1937), 78-80.

3. C. A. Laisant, *Les deux suites Fibonacciennes fondamentales*, Enseignement Math., **21** (1920), 52-56.

4. D. H. Lehmer, *An extended theory of Lucas functions*, Annals of Math., **31** (1930), 419-448.

5. J. V. Uspensky and M. A. Heaslet, *Elementary number theory,* New York (1939), 358–359.
6. Morgan Ward, *Prime divisiors of second order recurrences,* Duke Math. Journal **21** (1954), 607–614.
7. ———, *The linear p-adic recurrence of order two,* Unpublished.

CALIFORNIA INSTITUTE, PASADENA.