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.