THE LINEAR p-ADIC RECURRENCE OF ORDER TWO

Dedicated to Hans Rademacher on the occasion of his seventieth birthday

BY

MORGAN WARD

I. Introduction and summary of results

1. Let P and $Q \neq 0$ be fixed elements of R_p, the p-adic completion of the rational field R, and consider a second order linear recurrence

$$(W): \quad W_0, \quad W_1, \quad \cdots, \quad W_n, \quad \cdots$$

defined by

$$W_{n+2} = PW_{n+1} - QW_n \qquad (n = 0, 1, 2, \cdots) \tag{1.1}$$

whose initial values W_0, W_1 are elements of R_p. If P, Q, W_0, W_1 are p-adic integers, all the W_n are p-adic integers, and we say that (W) is integral.

Any element $X \neq 0$ of the field R_p may be written as $X = p^x U$, where U is a unit of R_p. We call x the (p-adic) value of X, writing $x = \phi(X)$, with the usual convention that if $X = 0$, $x = +\infty$. In particular, we write

$$w_n = \phi(W_n) \qquad (n = 0, 1, 2, \cdots). \tag{1.2}$$

The sequence (w) is called the value function of the recurrence (W).

We solve completely here the problem of determining the value function of any such recurrence (W); indeed we shall give specific formulas for (w). Since R_p contains the rational field R, our results give a far-reaching generalization of Lucas's "Laws of apparition and repetition" for the appearance of multiples of p in the special recurrences (Lucas [4]):

$$(L): \quad L_0 = 0, \quad L_1 = 1, \quad \cdots, \quad L_n, \quad \cdots,$$

$$(S): \quad S_0 = 2, \quad S_1 = P, \quad \cdots, \quad S_n, \quad \cdots.$$

It should be possible to carry out a similar generalization for the functions (L) and (S) discussed by Lehmer in his thesis (Lehmer [3]), where P is replaced by the square root of an integer of R, but this will not be done here.

2. Let

$$f(z) = z^2 - Pz + Q \tag{2.1}$$

be the polynomial associated with the recurrence (1.1), and let D denote its discriminant. If p divides D, we call p a discriminantal divisor of $f(z)$ or of (W).

It turns out that the only case presenting any difficulty occurs when P

Received August 31, 1960.