PRIME DIVISORS OF SECOND ORDER RECURRING SEQUENCES

By Morgan Ward

1. **Statement of result.** In some unpublished investigations of linear divisibility sequences [6] I have had occasion to use an arithmetical property of recurring sequences which appears interesting on its own account.

Let

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

be a linear integral recurring sequence of order two; that is

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

where W_0, W_1, P and $Q \neq 0$ are given integers. Let

(1.2) $$f(z) = z^2 - Pz + Q$$

be the polynomial associated with the recurrence. The sequence, the recurrence, and the polynomial are all said to be "degenerate" if the ratio of the roots of $f(z)$ is a root of unity.

A positive integer is called a "divisor" of the sequence (W) if it divides some term of (W). We shall prove here:

THEOREM 1. *A linear integral recurring sequence of order two which is not degenerate always has an infinite number of distinct prime divisors.*

(W) is trivially degenerate if $f(z)$ has repeated roots. The theorem is still true in this case, for if a is the root of $f(z)$, then $W_n = (A + Bn)a^n$ where A and B are rational and $B \neq 0$ since (W) is of order two. For all other degenerate sequences, the theorem is false save in the trivial case when some term of (W) is zero.

It appears likely that a similar result holds for recurring sequences of any order greater than one, but the proof given here rests heavily on the fact that (W) is of order two.

The plan of the paper is sufficiently indicated by the section headings.

2. **Notations used in paper.** We shall refer whenever convenient to the subscript n of the term W_n as an index. We shall denote the root field of $f(z)$ by $\mathfrak{R}$, using Greek letters $\alpha, \beta, \cdots$ for integers of $\mathfrak{R}$ and German letters $\mathfrak{m}, \cdots, \mathfrak{p}, \cdots$ for ideals of $\mathfrak{R}$ regardless of whether $\mathfrak{R}$ is the rational field or a quadratic extension of it. Italic letters $a, b, \cdots$ stand for rational integers, non-negative if used as exponents or suffices.

We shall use the standard notations $\mathfrak{m} \mid \mathfrak{k}$, $\mathfrak{m} \nmid \mathfrak{k}$, $m \mid k$, $m \nmid k$, $(\mathfrak{m}, \mathfrak{n})$, (m, n), of Landau's *Vorlesungen* for division and greatest common divisor. If $\mathfrak{m}$ has

Received September 16, 1953.