EQUIDISTRIBUTION OF RESIDUES IN SEQUENCES

By Marshall Hall

1. **Introduction.** A sequence of rational integers $v_0, v_1, \cdots$ satisfying a rational integral linear recurrence

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n \tag{1.1}$$

is periodic[1] modulo an arbitrary prime p, that is,

$$u_{n+\tau} \equiv u_n \pmod{p} \tag{1.2}$$

for a fixed τ and all $n \geqq n_0(p)$. The polynomial $f(x) = x^k - a_1 x^{k-1} - \cdots - a_k$ is called the characteristic of (1.1). This paper is concerned with the distribution of the residues $0, 1, \cdots, p - 1 \pmod{p}$ in sequences satisfying (1.1). This distribution has been investigated in two papers, one by Ward[2] supposing $f(x)$ to be a cubic irreducible modulo p, and another by the author[3] supposing $f(x)$ to be any polynomial irreducible modulo p.

Here it is shown that if $f(x)$ is the product of a linear factor and an irreducible factor modulo p, the number of zeros in the different blocks will satisfy equations similar to those found in H. (Compare equations (2.3) in this paper with equations (13.8) in H.)

By a simple device these results may be used to show that when $f(x)$ is irreducible modulo p and the period of (v_n) is τ, an arbitrary residue $a \pmod{p}$ will occur $\tau p^{-1} + c_a$ times in any τ consecutive terms of (v_n), where $| c_a | < p^{\frac{1}{2}(k-1)}$.

The notation and terminology throughout are those of H.

2. **Distribution of zeros.** Suppose

$$f(x) \equiv (x - d)h(x) \pmod{p}, \tag{2.1}$$

where $h(x)$ is irreducible modulo p and at least of second degree.[4] A sequence

$$(v_n) \rightleftarrows g(x) \tag{2.2}$$

Received April 28, 1938.

[1] R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quarterly Journal of Mathematics, vol. 48(1920), pp. 343–372.

[2] Morgan Ward, *The distribution of residues in a sequence satisfying a linear recursion relation*, Transactions of the American Mathematical Society, vol. 33(1931), pp. 166–190.

[3] Marshall Hall, *An isomorphism between linear recurring sequences and algebraic rings*, Transactions of the American Mathematical Society, vol. 44 (1938), pp. 196–218. This paper will be referred to as H.

[4] For second order sequences see Marshall Hall, *Divisors of second order sequences*, Bulletin of the American Mathematical Society, vol. 43(1937), pp. 78–80, and the note to Theorem 13.5 of H.