AN ARITHMETICAL PROPERTY OF RECURRING SERIES OF THE SECOND ORDER*

BY MORGAN WARD

1. *Statement of Property.* Let us denote by

$$(W_n): \quad W_0, W_1, W_2, \cdots, W_n, \cdots,$$

a sequence of rational integers satisfying the difference equation

$$\Omega_{n+2} = P\Omega_{n+1} - Q\Omega_n, \qquad (P, Q \text{ rational integers}), \tag{1}$$

and let p be an odd prime dividing neither Q nor $P^2-4Q = (\alpha-\beta)^2$, the discriminant of the polynomial

$$x^2 - Px + Q = (x - \alpha)(x - \beta) \tag{2}$$

associated with (1).†

We write as usual $U_n=(\alpha^n-\beta^n)/(\alpha-\beta)$, $V_n=\alpha^n+\beta^n$ for the two Lucas functions built upon the roots α and β of (2).

The distribution of the multiples of p in the corresponding sequences $(U)_n$ and $(V)_n$ is well known: namely, *multiples of p always occur in $(U)_n$*; more specifically, $U_n\equiv 0 \pmod{p}$ *when and only when* $n\equiv 0 \pmod{\tau}$, where τ is the restricted period‡ of $(U)_n$ modulo p. In the sequence $(V)_n$, *multiples of p occur when and only when τ is even.* In this case, $V_n\equiv 0 \pmod{p}$ *when and only when* $n\equiv 0 \pmod{\tau/2}$, $n\not\equiv 0 \pmod{\tau}$.

For the sequences $(U)_n$ and $(V)_n$ then, we know not only when multiples of p will occur, but where multiples of p will occur. Under the assumption that τ is odd, I propose to obtain a criterion which reduces the problem of determining *when* multiples of p will appear in *any* sequence $(W)_n$ (specified only by its two initial values W_0 and W_1) to the more fundamental (unsolved) problem of determining the characteristic number‡ and restricted period‡ of the Lucas functions associated with any given quadratic polynomial of the form (2).

---

* Presented to the Society, June 20, 1934.

† The excluded values of p are evidently trivial for the theorem that follows.

‡ For definitions of these terms, see my *Note on the period of a mark in a finite field*, this Bulletin, vol. 40 (1934), pp. 279–281.