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.

In fact, let P' and Q' be rational integers satisfying the congruences

$$(3)\qquad \begin{aligned} P' &\equiv W_0 \pmod{p}, \\ (4Q - P^2)Q' &\equiv W_1^2 - W_0W_1P + W_0^2Q \pmod{p}, \end{aligned}$$

and let $U_n' = (\alpha'^n - \beta'^n)/(\alpha' - \beta')$ be the Lucas function associated with the polynomial $x^2 - P'x + Q' = (x - \alpha')(x - \beta')$. Then *a necessary and sufficient condition that the sequence* $(W)_n$ *should contain multiples of* p *is that the restricted period of* U_n' *modulo* p *should be an even divisor of* 2τ.

2. *Illustration.* As a numerical illustration, take $P = 1$, $Q = -1$, $p = 89$, $W_0 = 1$, $W_1 = 4$. The sequence $(U)_n$ is then the familiar Fibonacci series

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \cdots$$

so that $\tau = 11$. The congruences (3) become $P' \equiv 1 \pmod{89}$, $-5Q' \equiv 11 \pmod{89}$, so that we may take $P' = 1$, $Q' = -20$. The Lucas sequence $(U')_n$ for $\Omega_{n+2} = \Omega_{n+1} + 20\Omega_n$ runs $0, 1, 1, 21, 41, 461, 1281, 10501, \cdots$ and by actual computation we find that $U_{22}' \equiv 69 \pmod{89}$. Hence the restricted period of $(U')_n$ modulo 89 is not an even divisor of $2\tau = 22$, and we conclude that all elements of the sequence $1, 4, 5, 9, 14, 23, 37, \cdots$ are prime to 89, as may be easily verified.

3. *A Preliminary Identity.* My proof of this result is based upon a well known identity in the theory of partitions discovered by Euler,* which we formulate as follows.

Let q be any complex number,

$$[n] \begin{cases} = (q^n - 1)/(q - 1), & q \neq 1, \\ = \lim\limits_{q \to 1} (q^n - 1)/(q - 1) = n, & q = 1. \end{cases}$$

Writing $[n]!$ for $[1][2] \cdots [n]$, $[0]! = 1$, we see that the basic bi-

* *Introductio in Analysin Infinitorum*, 1748, Chapter VII; Netto, *Combinatorik*, 2d ed., 1927, p. 143.

nomial coefficient* $(n;r)$ is defined by $(n;r) = [n]!/\{[n-r]![r]!\}$. This expression, as Gauss showed,† is a polynomial in q which reduces to the ordinary binomial coefficient when $q=1$. The identity in question may now be written as follows:

$$(4) \qquad \sum_{r=0}^{\tau} (\tau; r)q^{r(r+1)/2}z^r = (1 + qz)(1 + q^2z) \cdots (1 + q^\tau z).$$

4. *Proof.* The general term of the sequence $(W)_n$ may be expressed in the form

$$W_n = W_0U_{n+1} + (W_1 - PW_0)U_n.$$

Thus the restricted period of $(W)_n$ modulo p is a divisor of the restricted period τ modulo p of the Lucas function U_n. Therefore the sequence $(W)_n$ will contain terms divisible by p when and only when the rational integer

$$(5) \qquad \mathfrak{W} = \prod_{n=1}^{\tau} W_n$$

is divisible by p.

Now W_n can also be expressed in the form $W_n = A\alpha^n + B\beta^n$, where the constants A and B are determined by

$$(6) \qquad W_0 = A + B, \qquad W_1 = A\alpha + B\beta.$$

If we let‡ $\beta/\alpha = q$, $B/A = z$, we may write $W_n = A\alpha^n(1+q^nz)$. Therefore by (5) and (4),

$$(7) \qquad \begin{aligned} \mathfrak{W} &= \prod_{n=1}^{\tau} A\alpha^n(1 + q^nz) = A^\tau\alpha^{\tau(\tau+1)/2} \prod_{n=1}^{\tau} (1 + q^nz) \\ &= A^\tau\alpha^{\tau(\tau+1)/2} \sum_{r=0}^{\tau} (\tau; r)q^{r(r+1)/2}z^r. \end{aligned}$$

---

* This terminology is due to F. H. Jackson who in recent years has made an extensive study of the basic numbers $[n]$. (See, for example, Proceedings of the London Mathematical Society, (2), vol. 1 (1903–04), pp. 63–68; Proceedings of the Royal Society, (A), vol. 76 (1905), pp. 127–144.)

† *Summatio quarundam Serierum Singularium*, 1808; Works, vol. 2, p. 16.

‡ If A and B are rational integers modulo p, they cannot both be congruent to zero, and we take for A that one which is incongruent to zero modulo p. We have $\alpha \not\equiv 0 \bmod p$, since p was assumed prime to Q.

Now $[n]=(q^n-1)/(q-1)=(\alpha^n-\beta^n)/[(\alpha-\beta)\alpha^{n-1}]=\alpha^{-n+1}U_n$. Hence

$$(n;r) = U_nU_{n-1}\cdots U_{n-r+1}/(U_1U_2\cdots U_r\alpha^{-(n-r)r}).$$

But the first $\tau-1$ of the numbers $U_1, U_2, \cdots, U_\tau$ are prime to p, while U_τ is divisible by p. Hence $(\tau;r)\equiv 0 \pmod p$ unless $r=0$ or $r=\tau$, when it equals one. We therefore obtain from (7) the congruence

$$\mathfrak{W} \equiv A^\tau\alpha^{\tau(\tau+1)/2}(1+q^{\tau(\tau+1)/2}z^\tau) \equiv A^\tau\alpha^{\tau(\tau+1)/2} + B^\tau\beta^{\tau(\tau+1)/2} \pmod p.$$

Now $\alpha^n = U_n\alpha - QU_{n-1}$, $\beta^n = U_n\beta - QU_{n-1}$. Therefore since τ is odd,*

$$\alpha^{\tau(\tau+1)/2} \equiv (U_\tau\alpha - QU_{\tau-1})^{(\tau+1)/2} \equiv (-QU_{\tau-1})^{(\tau+1)/2} \pmod p,$$
$$\beta^{\tau(\tau+1)/2} \equiv (-QU_{\tau-1})^{(\tau+1)/2} \pmod p,$$

and

$$\mathfrak{W} \equiv (-QU_{\tau-1})^{(\tau+1)/2}(A^\tau + B^\tau) \pmod p. \tag{8}$$

Hence $\mathfrak{W}\equiv 0 \pmod p$ *when and only when* $A^\tau+B^\tau\equiv 0 \pmod p$.

Finally, write α', β' for A, B. Then $A^n+B^n = V_n'$, the Lucas function associated with the quadratic polynomial $x^2-P'x+Q' = (x-\alpha')(x-\beta')$.

On referring back to (6) and recalling that p is prime to P^2-4Q, we find that we may assign to P' and Q' the rational integral values specified by the congruences (3). Our theorem now follows immediately from the laws of apparition for multiples of p in the Lucas functions stated in section 1 as applied to the sequence $(V')_n$.

CALIFORNIA INSTITUTE OF TECHNOLOGY

* It is at precisely this point that the assumption that τ is odd becomes vital. For if we assume that τ is even, we obtain in place of (8) the barren result $\mathfrak{W} = (U_{\tau+1})^{\tau/2}(A^\tau\alpha^{\tau/2}+B^\tau\beta^{\tau/2}) \pmod p$.