SOME ARITHMETICAL PROPERTIES OF SEQUENCES SATISFYING A LINEAR RECURSION RELATION.[1]

BY MORGAN WARD.

1. Let

$$(U)_n: \quad U_0,\, U_1,\, U_2,\, \cdots$$

denote a sequence of integers satisfying the recursion relation

$$\Omega_{N+1+n} = P_1\,\Omega_{N+n} + P_2\,\Omega_{N+n-1} + \cdots + P_{N+1}\,\Omega_n \tag{1.1}$$

where $P_1, \cdots, P_{N+1}$ and the $N+1$ initial values $U_0, \cdots, U_N$ of $(U)_n$ are all fixed integers.

Let p denote a fixed prime, and assume furthermore that the characteristic function of (1.1)

$$F(x) = x^{N+1} - P_1 x^N - \cdots - P_{N+1}$$

is irreducible modulo p.

Denote the $N+1$ roots of the equation $F(x) = 0$ by $\alpha = \alpha_0, \alpha_1, \cdots, \alpha_N$ and let S_m denote $\alpha_0^m + \alpha_1^m + \cdots + \alpha_N^m$. For convenience of printing, we shall occasionally write $\alpha(n)$ for α^n and $\{m\}$ for S_m.

In this paper, I give a number of congruences to the modulus p satisfied by particular solutions of (1.1) and by determinants relating to such solutions. The two main results are as follows:

If $(U)_n$ *is any particular solution of* (1.1), *then*[2]

$$U_{n+m} + U_{n+pm} + U_{n+p^2m} + \cdots + U_{n+p^Nm} \equiv U_n S_m \bmod p. \tag{I}$$

If $N+1$ *is odd, and if* $M(r_0, r_1, \cdots, r_N)$ *denotes the determinant*

$$|\alpha_i^{r_j}|, \qquad (i, j = 0, 1, \cdots, N)$$

where $r_0, r_1, \cdots, r_N$ *are any fixed integers, then*

$$M(r_0, r_1, \cdots, r_N) \equiv \sum_{(j)} (\pm)^j \{r_0 + p\,r_{j_1} + p^2 r_{j_2} + \cdots + p^N r_{j_N}\} \bmod p, \tag{II}$$

[1] Received October 1, 1930, and February 3, 1931.

[2] If μ is the exponent to which α belongs, modulo p, the relations $U_a \equiv U_b$, $S_a \equiv S_b$ mod p if $a \equiv b \bmod \mu$ may be used to reduce the subscripts of U and S to values less than μ.

where the summation is extended over all the $N!$ permutations (j) of the integers $1, 2, \cdots, N$ and the sign $(\pm)^j$ is to be taken positive or negative according as the permutation is of even or odd parity.

For example, if $N+1 = 3$, we have

$$\begin{vmatrix} \alpha_0^{r_0}, & \alpha_0^{r_1}, & \alpha_0^{r_2} \\ \alpha_1^{r_0}, & \alpha_1^{r_1}, & \alpha_1^{r_2} \\ \alpha_2^{r_0}, & \alpha_2^{r_1}, & \alpha_2^{r_2} \end{vmatrix} \equiv S_{r_0+pr_1+p^2r_2} - S_{r_0+pr_2+p^2r_1} \mod p.$$

The proofs of these formulas are given in the next two sections of the paper. The final section contains some special cases of the first formula and some properties of the determinant $M(r_0, r_1, \cdots, r_N)$ regarded as a function of $r_0, r_1, \cdots, r_N$.

2. With a proper choice of notation, we may assume that

$$(2.1) \qquad \alpha_i \equiv \alpha^{p^i} \mod p, \qquad (i = 0, 1, \cdots, N)$$

in the Galois Field[3] of order p^{N+1} associated with the root α of $F(x) = 0$.

Since $F(x)$ is irreducible, the general term of $(U)_n$ may be represented as

$$U_n = A_0\,\alpha_0^n + A_1\,\alpha_1^n + \cdots + A_N\,\alpha_N^n$$

where the constants A are independent of n. We shall take this formula as a definition of U_n when n is a negative integer. Thus

$$(2.2) \qquad U_n \equiv \sum_{r=0}^{N} A_r\,\alpha^{p^r n} \mod p, \qquad S_m \equiv \sum_{s=0}^{N} \alpha^{p^s m} \mod p.$$

To prove formula I, we observe that

$$\sum_{s=0}^{N} \alpha^{p^{r+s} m} \equiv S_m \mod p$$

for any integer r. Hence

$$\sum_{s=0}^{N} U_{n+p^s m} \equiv \sum_{s=0}^{N} \sum_{r=0}^{N} A_r\,\alpha^{p^r(n+p^s m)} \equiv \sum_{r=0}^{N} A_r\,\alpha^{p^r n} \sum_{s=0}^{N} \alpha^{p^{r+s} m} \equiv U_n S_m \mod p.$$

3. Formula II may be proved as follows. With the notation explained in the introduction,

$$M(r_0, r_1, \cdots, r_N) = \sum_{(j)} (\pm)^j\,\alpha_0^{r_{j_0}}\,\alpha_1^{r_{j_1}} \cdots \alpha_N^{r_{j_N}}.$$

Hence by (2.1),

$$(3.1) \quad M(r_0, r_1, \cdots, r_N) \equiv \sum_{(j)} (\pm)^j\,\alpha(r_{j_0} + r_{j_1}p + \cdots + r_{j_N}p^N) \mod p.$$

[3] For the properties of Galois Fields which are assumed, see Dickson, *Linear Groups*, Teubner, (1901).

The $(N+1)!$ permutations (j) of the integers $0, 1, \cdots, N$ which occur in the subscripts of the r on the right hand side of (3.1) may be grouped into $N!$ classes

$$(3.2) \qquad J_1, J_2, \cdots, J_{N!}$$

where each class contains exactly $N+1$ cyclic permutations. Suppose that

$$(3.3) \quad j_0, j_1, \cdots, j_{N-1}, j_N; \quad j_1, j_2, \cdots, j_N, j_0; \quad \cdots; \quad j_N, j_0, \cdots, j_{N-2}, j_{N-1};$$

are the permutations of the class J. These permutations are either all even or all odd; for since $N+1$ is odd, each can be derived from its predescessor by an even number of transpositions.[4] Accordingly, the sign of the general term $\alpha(r_{j_0}+r_{j_1}p+\cdots+r_{j_N}p^N)$ in (3.1) is the same for all the permutations of a given class J.

Furthermore, since any one of the permutations (3.3) completely specifies the class J, we may choose our notation so that $j_0 = 0$. Make a similar change of notation for every other one of the classes (3.2). Then to each of the $N!$ permutations of the integers $1, 2, \cdots, N$ there corresponds a unique class J, and the parity of this permutation determines the parity of all the permutations of J.

The congruence (3.1) can now be written as

$$(3.4) \quad M(r_0, r_1, \cdots, r_N) \equiv \sum_{(j)} (\pm)^j \sum \alpha(r_0+r_{j_1}p+\cdots+r_{j_N}p^N) \mod p$$

where the inner summation is taken over the $N+1$ permutations (3.3), while the outer summation (j) is taken over the $N!$ permutations of $1, 2, \cdots, N$, the sign being plus or minus according as (j) is even or odd.

But since $\alpha(rp^{N+1}) \equiv \alpha(r) \mod p$, the inner summation in (3.4) is congruent modulo p to

$$\begin{aligned} &\alpha(r_0+r_{j_1}p+\cdots+r_{j_N}p^N)+\alpha(p\cdot(r_0+r_{j_1}p+\cdots+r_{j_N}p^N))+\cdots \\ &\qquad\cdots+\alpha(p^N\cdot(r_0+r_{j_1}p+\cdots+r_{j_N}p^N)) \\ &\equiv \{r_0+r_{j_1}p+\cdots+r_{j_N}p^N\} \mod p, \end{aligned}$$

by formula (2.2). On substituting this last expression in (3.4), we obtain formula II.

4. The following special cases of formula I are of interest. First, if we write S for U in I, we obtain a multiplication formula for the function S:

[4] It is at precisely this point that an attempted proof of a similar result for the case when the degree of $F(x)$ is even will break down.

$$S_n S_m \equiv S_{n+m} + S_{n+pm} + \cdots + S_{n+p^N m} \mod p. \tag{4.1}$$

Secondly, let $(Z^0)_n$; $(Z^{(1)})_n, \cdots, (Z^{(N)})_n$ denote the particular solutions of (1.1) with the initial values

$$1, 0, 0, \cdots, 0; \qquad 0, 1, 0, \cdots, 0; \qquad \cdots\cdots; \qquad 0, 0, 0, \cdots, 1.$$

Then if the Kronecker symbol δ_{ij} is defined as usual by

$$\delta_{ij} = 0, \quad i \neq j; \qquad \delta_{ij} = 1, \quad i = j; \qquad (i, j = 0, 1, \cdots, N),$$

we have on taking $Z^{(i)}$ for U in I the curious formulas

$$Z^{(i)}_{j+m} + Z^{(i)}_{j+pm} + \cdots + Z^{(i)}_{j+p^N m} \equiv \delta_{ij} S_m \mod p,$$
$$(i, j = 0, 1, \cdots, N; \; m = 0, \pm 1, \cdots).$$

The function M has a multiplication theorem analogous to that given for S_m in formula (4.1). If for brevity we write $R_{(k)}$ for $r_{k_0} + r_{k_1} p + \cdots + r_{k_N} p^N$, then

$$\begin{aligned} M(r_0, r_1, \cdots, r_N) \cdot M(u_0, u_1, \cdots, u_N) \\ \equiv \sum_{(k)} (\pm)^k M(R_{(k)} + u_0, u_1, \cdots, u_N) \mod p, \end{aligned} \tag{4.2}$$

where the summation (k) extends over all the $(N+1)!$ permutations of the integers $0, 1, \cdots, N$ and the signs are determined as in II by the parity of (k).

To prove (4.2), write $R_{(j)}$ for $r_0 + r_{j_1} p + \cdots + r_{j_N} p^N$. Then by formula II and formula (4.1)

$$\begin{aligned} & M(r_0, r_1, \cdots, r_N) \cdot M(u_0, u_1, \cdots, u_N) \\ & \equiv \sum_{(j)} \sum_{(l)} (\pm)^j (\pm)^l \{R_{(j)}\} \{u_0 + u_{l_1} p + \cdots + u_{l_N} p^N\} \\ & \equiv \sum_{(j)} (\pm)^j \sum_{t=0}^{N} \sum_{(l)} (\pm)^l \{R_{(j)} + p^t u_0 + p^t u_{l_1} p + \cdots + p^t u_{l_N} p^N\} \\ & \equiv \sum_{(j)} (\pm)^j \sum_{t=0}^{N} M(R_{(j)} + p^t u_0, p^t u_1, \cdots, p^t u_N) \mod p. \end{aligned} \tag{4.3}$$

We now reverse the argument in section 3 by which we passed from the $(N+1)!$ permutations of $0, 1, 2, \cdots, N$ to the $N!$ permutations of $1, 2, \cdots, N$. Let $k_0 = j_t$, $k_1 = j_{t+1}$, $\cdots$, $k_N = j_{t-1}$ so that (k): k_0, $k_1, \cdots, k_N$ is a cyclic permutation of the subscripts $0, j_1, \cdots, j_N$ of the r in $R_{(j)}$. Then (k) is a permutation of $0, 1, \cdots, N$ which has the same parity as the permutation (j) of $1, 2, \cdots, N$.

If we now write $R_{(k)}$ for $r_{k_0}+r_{k_1}p+\cdots+r_{k_N}p^N$, then

$$\begin{aligned}(\pm)^j\, M(R_{(j)}+p^t u_0,\, p^t u_1,\, \cdots,\, p^t u_N)\\ \equiv (\pm)^k\, M(p^t R_{(k)}+p^t u_0,\, p^t u_1,\, \cdots,\, p^t u_N)\\ \equiv (\pm)^k\, M(R_{(k)}+u_0,\, u_1,\, \cdots,\, u_N) \quad \operatorname{mod} p.\end{aligned}$$

On substituting this expression into (4.3), we obtain (4.2).

In conclusion, we may note that $M(0, 1, \cdots, N)$ is the square root of the discriminant of $F(x)$. Denoting this discriminant by Δ, we have from II after some obvious simplifications,

$$\sqrt{\Delta} \equiv \sum_{(j)} (\pm)^j \{j_1+j_2 p+\cdots+j_N p^{N-1}\} \quad \operatorname{mod} p.$$

For $N+1=3$, this result assumes the simple form

$$\sqrt{\Delta} \equiv S_{1+2p} - S_{2+p} \quad \operatorname{mod} p.$$

PASADENA,
September, 1930.