AN ENUMERATIVE PROBLEM IN THE ARITHMETIC OF LINEAR RECURRING SERIES*

BY

MORGAN WARD

1. Let m be a fixed positive integer greater than one and let

$$\Omega_{n+k} = c_1\Omega_{n+k-1} + c_2\Omega_{n+k-2} + \cdots + c_k\Omega_n \tag{1.1}$$

be a linear difference equation of order k with rational integral coefficients $c_1, c_2, \cdots, c_k$. If

$$(U): \qquad U_0, U_1, U_2, \cdots, U_n, \cdots$$

is any sequence of rational integers satisfying (1.1), then after a certain point the sequence becomes periodic when considered modulo m. Its least period is called the characteristic number of the sequence (U) modulo m.

In a recent paper in these Transactions†, I have considered the problem of determining this characteristic number given $m, c_1, c_2, \cdots, c_k$ and the k initial values $U_0, U_1, \cdots, U_{k-1}$ of the sequence (U), and I have reduced it to certain basic problems in the theory of higher congruences.‡

In the present paper, I am concerned with the following problem which I shall similarly reduce to a problem in the theory of higher congruences:

Given any positive integer s: to find the number of distinct sequences (U) modulo m whose characteristic number is exactly equal to s.

2. I obtain here the following results.

(i) *It suffices to determine the total number of purely periodic sequences (U) modulu m whose characteristic number is at most equal to s.* (§3.)

(ii) *It suffices to confine ourselves to the case when $m = p^N$ is a power of a prime p, and when the polynomial*

$$f(x) = x^k - c_1x^{k-1} - c_2x^{k-2} - \cdots - c_k \tag{2.1}$$

of degree k associated with the difference equation (1.1) *is of the form*

$$f(x) = B(x) \equiv \{\phi(x)\}^a \pmod{p}$$

where $\phi(x)$ is irreducible modulo p and a is a positive integer. (§4.)

---

* Presented to the Society, December 27, 1934; received by the editors August 1, 1934.

† Vol. 35 (1933), pp. 600–628. I shall refer to this paper as Trans I.

‡ Notably, to finding the least value of n such that $A(x)(x^n-1)\equiv 0 \pmod{p^N, B(x)}$ for any prime p and any assigned polynomials $A(x)$ and $B(x)$.

(iii) *The problem thus delimited is equivalent to determining the total number of distinct polynomials* $U(x)$ *of degree* $\leqq k-1$ *modulo* p^N *such that*

$$U(x)A(x) \equiv 0 \qquad (\text{modd } p^N, B(x)), \tag{2.2}$$

where

$$A(x) \equiv x^s - 1 \qquad (\text{modd } p^N, B(x)).$$

This number can be immediately written down provided that we know the elementary divisors corresponding to the prime p of the matrix $\mathcal{E}$ of the Sylvester eliminant of $A(x)$ and $B(x)$. (§5.)

In another paper in these Transactions* I have made a detailed study of the congruence (2.2) and shown that if $N \leqq \lambda$ (where p^λ is the first elementary divisor of the matrix $\mathcal{E}$ of (iii) corresponding to the prime p) there exists a unique polynomial $U(x) \equiv A_{\lambda-N}(x)$, modulo p^N, satisfying (2.2) of minimal degree in x and leading coefficient unity. Let the degree of $A_{\lambda-N}(x)$ be $\alpha_{\lambda-N}$ $(N=1, 2, \cdots, \lambda)$, and let

$$\sigma_N = \alpha_{\lambda-1} + \alpha_{\lambda-2} + \cdots + \alpha_{\lambda-N} \quad (N = 1, 2, \cdots, \lambda).$$

Then

(iv) *The total number of distinct polynomials modulo* p^N *of degree* $\leqq k-1$ *satisfying* (2.1) *is*

$$p^{Nk-\sigma_N} \text{ if } N \leqq \lambda \text{ and } p^{\lambda k-\sigma_\lambda} \text{ if } N \geqq \lambda.$$

(§6.) In this latter case, the number is therefore independent of N.

3. In the sections which follow, we shall use the German capital $\mathfrak{M}$ for the double modulus $m, f(x)$, writing

$$A(x) \equiv 0 \ (\mathfrak{M}) \text{ for } A(x) \equiv 0 \qquad (\text{modd } m, f(x)).$$

We shall otherwise use the same notation and terminology as in Trans I. In particular, the sequence (U) will be said to be "purely periodic" modulo m if it contains no non-repeating residues when considered modulo m. From Theorem 4.1, Trans I, it suffices to enumerate all the purely periodic sequences (U) with fixed characteristic number s. For if the number of such sequences be denoted by $\psi(s)$, the total number of sequences with characteristic number s may be obtained by multiplying $\psi(s)$ by a factor which is independent of s. (Trans I, part IV.)

By the fundamental theorem on page 606 of Trans I, the enumerative problem for purely periodic sequences is equivalent to the following problem in the theory of congruences to a double modulus:

* Vol. 35 (1933), pp. 254–260. I shall refer to this paper as Trans II.

To determine the total number of distinct polynomials $U(x)$ modulo m of degree $\leqq k-1$ such that

$$U(x)(x^S - 1) \equiv 0 \ (\mathfrak{M}), \tag{3.1}$$

$$U(x)(x^R - 1) \not\equiv 0 \ (\mathfrak{M}) \qquad (1 \leqq R < S). \tag{3.2}$$

We can omit the restriction (3.2). For assume that (3.1) holds, and also that

$$U(x)(x^R - 1) \equiv 0 \ (\mathfrak{M}). \tag{3.3}$$

Then it is easily seen that for any integers L and M,

$$U(x)(x^{LS+MR} - 1) \equiv 0 \ (\mathfrak{M}).$$

Choose L and M so that $LS+MR=D$, the greatest common divisor of S and R. Then

$$U(x)(x^D - 1) \equiv 0 \ (\mathfrak{M}).$$

That is, if (3.3) holds, it must hold for some integer $R=D$ which is a divisor of S. We may therefore replace condition (3.2) by

$$U(x)(x^R - 1) \not\equiv 0 \ (\mathfrak{M}), \ R \text{ any proper divisor of } S. \tag{3.21}$$

Furthermore, if (3.3) holds, there is a smallest value of R for which it holds dividing all other such R.

If $\phi(s)$ is the total number of polynomials $U(x)$ satisfying (3.1) and $\psi(s)$ the total number of polynomials satisfying both (3.1) and (3.21), it is clear then that

$$\phi(s) = \sum_{R \mid S} \psi(R).$$

Therefore by Dedekind's inversion formula,

$$\psi(S) = \sum_{D \mid S} \mu(D)\phi(S/D).$$

The summation here extends over all divisors D of S and $\mu(D)$ denotes Möbius' function. It suffices therefore to determine $\phi(s)$.

4. For the moment, write $u(s;m;f(x))$ for the function $\phi(s)$ defined above. Then first of all, it is readily shown as in Trans I, part III, that if $m=ab$, $(a, b)=1$, then

$$u(s; m; f(x)) = u(s; a; f(x)) \cdot u(s; b; f(x)).$$

That is, $u(s; m; f(x))$ is a multiplicative function of m. *We can assume therefore that*

$$m = p^N, \ p \text{ a prime}, \ N \geqq 1. \tag{4.1}$$

Secondly, it is readily shown that if

$$f(x) \equiv f_1(x) \cdot f_2(x) \pmod{m}, \quad \text{Res } \{f_1(x), f_2(x)\} \text{ prime to } m,$$

then

$$u(s; m; f(x)) = u(s; m; f_1(x))u(s; m; f_2(x)).$$

Since $m = p^N$, we have by Schönemann's second therem* a decomposition of $f(x)$ modulo p^N of the form

$$f(x) \equiv f_1(x)f_2(x) \cdots f_r(x) \pmod{p^N}$$

where $f_i(x)$ is primary and congruent to $\{\phi_i(x)\}^{a_i}$, modulo p, for $i = 1, , \cdots, r$, while the polynomials $\phi_1(x), \phi_2(x), \cdots, \phi_r(x)$ are distinct and irreducible modulo p.

Since

$$\text{Res } \{f_i(x), f_j(x)\} \not\equiv 0 \pmod{p} \quad (i, j = 1, \cdots, r; i \neq j),$$

we can assume that

$$f(x) = B(x) \equiv \{\phi(x)\}^a \pmod{p},$$

$\phi(x)$ *irreducible modulo* p.

5. Let

$$B(x) = x^m + b_1x^{m-1} + \cdots + b_m.$$

Then we have reduced our problem to determining the total number of polynomials $U(x)$ of degree $\leqq m-1$, distinct modulo p^N, such that

$$U(x)A(x) \equiv 0 \quad (\text{modd } p^N, B(x)), \tag{5.1}$$

where p is a prime, while

$$A(x) \equiv x^S - 1 \quad (\text{modd } p^N, B(x)). \tag{5.2}$$

In Trans I, pp. 622–623, I have shown how to determine a polynomial $A(x)$ satisfying (5.2) of degree less than $B(x)$ under the assumption that we know that solution of the difference equation associated with $B(x)$ with the m initial values $0, 0, \cdots, 0, 1$. But here we shall not make any assumption about the degree of $A(x)$. Indeed, we shall show that the number of such polynomials $U(x)$ can be theoretically determined without restricting the form of the polynomial $A(x)$ in any way.

For let

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n.$$

* Fricke, *Algebra*, vol. 2, Braunschweig, 1928, chapter 2.

The congruence (5.1) may be written in the equivalent form

$$A(x)U(x) + B(x)V(x) \equiv 0 \pmod{p^N}, \tag{5.3}$$

where $U(x) = u_0x^{m-1} + \cdots + u_{m-1}$, $V(x) = v_0x^{n-1} + \cdots + v_{n-1}$ are to be determined.

Let $\mathcal{E} = (e_{ij})$ denote the transpose of the matrix corresponding to the Sylvester eliminant of $A(x)$ and $B(x)$. Then if we let

$$z_{i+1} = u_i \ (i = 0, 1, \cdots, m-1), \quad z_{i+1} = v_{i-m} \ (i = m, m+1, \cdots, m+n-1),$$

(5.3) is equivalent to the set of $n+m$ congruences

$$\sum_{j=1}^{m+n} e_{ij}z_j \equiv 0 \pmod{p^N} \quad (i = 1, 2, \cdots, m+n). \tag{5.4}$$

It is clear then *that the number of distinct polynomials* $U(x)$ *satisfying the conditions of* (5.1) *equals the number of distinct solutions* $z_1, z_2, \cdots, z_{m+n}$ *modulo* p^N *of the system* (5.4).

This number was determined by H. J. S. Smith in a classical memoir.* Namely, let $p^{\lambda_1}, p^{\lambda_2}, \cdots, p^{\lambda_k}$ be the successive elementary divisors of the matrix $\mathcal{E}$ corresponding to the prime p. Then if r is so chosen that $\lambda_{r-1} > N \geqq \lambda_r$, *the number of distinct incongruent solutions of* (5.4) *is* $p^{rN+\lambda_r+\lambda_{r+1}+\cdots+\lambda_k}$.

6. We can express the number of solutions of the congruence (5.1) in quite a different manner by using some of the results obtained in my paper Trans II.

Let us assume that $N \geqq \lambda$, where p^λ now denotes the first elementary divisor of the matrix $\mathcal{E}$ defined in §5 corresponding to p. Then (Trans II, p. 255) $U(x)$ must be of the form

$$U(x) = p^{N-\lambda}(Q_0(x)A_0(x) + pQ_1(x)A_1(x) + \cdots + p^{\lambda-1}Q_{\lambda-1}(x)A_{\lambda-1}(x)), \tag{6}$$

where $A_r(x)$ is the unique polynomial of minimal degree and leading coefficient unity such that

$$A_r(x)A(x) \equiv 0 \pmod{p^{\lambda-r}, B(x)}.$$

Let the degree of this polynomial be denoted by α_r.

The procedure by which the polynomials $Q_0(x), Q_1(x), \cdots$ are determined is then as follows:

Let $U(x) = p^{N-\lambda}V_0(x)$. Then $A(x)V_0(x) \equiv 0 \pmod{p^\lambda, B(x)}$ and, as proved in Trans II, $V_0(x) = Q_0(x)A_0(x) + V_1(x)$ where $V_1(x)$ is of lesser degree than

* *On systems of linear indeterminate equations and congruences*, Collected Papers, vol. 1, Oxford, 1894, p. 399.

$A_0(x)$. Then $V_0(x)$ is of degree $\leqq m-1$, $A_0(x)$ is of degree α_0, and $V_1(x)$ of degree $\leqq \alpha_0 - 1$. Hence $Q_0(x)$ is of degree $\leqq m-\alpha_0-1$, so that we can write

$$Q_0(x) = q_1 x^{m-\alpha_0-1} + q_2 x^{m-\alpha_0-2} + \cdots + q_{m-\alpha_0}$$

where $0 \leqq q_j < p^\lambda$ $(j = 1, 2, \cdots, m-\alpha_0)$.

Therefore, there are $p^{\lambda(m-\alpha_0)}$ possible polynomials $Q_0(x)$ for a given $U(x)$.

Next, we have

$$A(x)V_1(x) \equiv 0 \qquad (\text{modd } p^{\lambda-1}, B(x)),$$

$V_1(x) = Q_1(x)A_1(x) + pV_2(x)$ where $V_2(x)$ is of lesser degree than $A_1(x)$. Then $V_1(x)$ is of degree $\alpha_0 - 1$, $A_1(x)$ of degree α_1, and $V_2(x)$ of degree $\leqq \alpha_1 - 1$. Therefore $Q_1(x)$ is of degree $\leqq \alpha_0 - \alpha_1 - 1$, and reasoning as before, we see that there are $p^{(\lambda-1)(\alpha_0-\alpha_1)}$ possible polynomials $Q_1(x)$ for a given $U(x)$.

Continuing in this manner, we see that there are $p^{(\lambda-r)(\alpha_{r-1}-\alpha_r)}$ possible polynomials $Q_r(x)$ $(0 \leqq r \leqq \lambda - 1;\ \alpha_{-1} = m)$. Therefore *there are in all*

$$p^{\lambda(m-\alpha_0)} \cdot p^{(\lambda-1)(\alpha_0-\alpha_1)} \cdot p^{(\lambda-2)(\alpha_1-\alpha_2)} \cdot \cdots \cdot p^{\alpha_{\lambda-2}-\alpha_{\lambda-1}} = p^{\lambda m-(\alpha_0+\alpha_1+\cdots+\alpha_{\lambda-1})}$$

polynomials $U(x)$ satisfying the congruence (5.1); for it easily is seen that each choice of $Q_0(x), \cdots, Q_{\lambda-1}(x)$ in formula (6.1) leads to a distinct polynomial $U(x)$.

If we assume that $N \leqq \lambda$, we have

$$U(x)A(x) \equiv 0 \qquad (\text{modd } p^N, B(x)),$$

$$U(x) = Q_{\lambda-N}(x)A_{\lambda-N}(x) + pV_{\lambda-N+1}(x),$$

$$V_{\lambda-N+1}(x) = Q_{\lambda-N+1}(x)A_{\lambda-N+1}(x) + pV_{\lambda-N+2}(x),$$

and so on.

On determining the degrees of the polynomials $Q_{\lambda-N}(x)$, $Q_{\lambda-N+1}(x), \cdots$, we find that in this case *there are $p^{Nm-(\alpha_{\lambda-N}+\alpha_{\lambda-N+1}+\cdots+\alpha_{\lambda-1})}$ possible polynomials $U(x)$.*

On writing σ_N for $\alpha_{\lambda-1}+\alpha_{\lambda-2}+\cdots+\alpha_{\lambda-N}$ and k for m, we obtain the final result stated in the second section of this paper.

INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.