THE ARITHMETICAL THEORY OF LINEAR RECURRING SERIES*

BY

MORGAN WARD

I. Introduction. The difference equation of order one

1. Let m be an integer greater than one, and let

$$(u): \qquad u_0, u_1, u_2, \cdots, u_n, \cdots$$

be an arithmetical series† of order k; that is, a particular solution of the linear difference equation

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

where $c_1, c_2, \cdots, c_k$ and the k initial values $u_0, u_1, \cdots, u_{k-1}$ of (u) are given integers. Then if a_n is the least positive residue of u_n modulo m, we may associate with (u) a second sequence

$$(a): \qquad a_0, a_1, a_2, \cdots, a_n, \cdots$$

which we call the reduced sequence corresponding to (u) modulo m.

It is easily seen that after a finite number of terms, the sequence (a) repeats itself periodically, and that any one of its periods is a multiple of a certain least period which is called the *characteristic number* of (u) (or (a)) modulo m‡. The number of non-repeating terms in (a) is called the *numeric* of (u) modulo m; if it is zero, (u) is said to be *purely periodic*§ modulo m. If all the terms of (u) after a certain point are divisible by m, so that the repeating part of (a) consists of the single residue zero, (u) is said to be a *null sequence* modulo m.

Three important problems immediately suggest themselves: first, to determine the characteristic number and numeric of the sequence (u) as

* Presented to the Society, August 31, 1932; received by the editors September 6, 1932.

† The literature prior to 1917 is summarized in Dickson's *History*, vol. I, chapter XVII. Among the more recent papers, D. H. Lehmer, Annals of Mathematics, (2), vol. 31 (1930), pp. 419–449, treats the case $k=2$, and the author, these Transactions, vol. 33 (1931), pp. 153–165, the case $k=3$. For general k, see R. D. Carmichael, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 343–372. Certain of Carmichael's results were extended by the use of ideals by H. T. Engstrom, these Transactions, vol. 33 (1931), pp. 210–218. I shall refer to these papers by the authors' name and page number. For the bearing of the problem upon elementary number theory, see R. D. Carmichael, American Mathematical Monthly, vol. 36 (1929), pp. 132–143

‡ This term is due to Carmichael, p. 345.

§ This is always the case if m is prime to c_k in (1.1).

functions of the $2k+1$ integers $c_1, \cdots, c_k, u_0, \cdots, u_{k-1}$ and m*; secondly, given (1.1) and m, to determine least upper bounds for the characteristic number and numeric of any solution of (1.1); and thirdly, given m and k, to determine the least upper bounds for the characteristic number and numeric of any arithmetical series of order k. The bearing of these problems upon the arithmetical properties of such series is evident; nevertheless none of them has as yet been completely solved.†

2. The course of the investigation may best be explained by considering the special case of a difference equation of order one,

$$\Omega_{n+1} = c\Omega_n. \tag{2.1}$$

Any solution (u) of (2.1) is of the form

$$u_n = u_0 c^n$$

where u_0 is an integer. It is possible to express this solution as the sum of two other solutions $v_n = v_0 c^n$, and $w_n = w_0 c^n$ where for the modulus m, (v) is a null sequence with the same numeric as (u), and (w) is a purely periodic sequence with the same characteristic number. The numbers v_0 and w_0 may be determined as soon as u_0 is known.

It readily follows that the numeric and characteristic number of the sequence (u) modulo m are respectively the least values of n such that

$$v_0 c^n \equiv 0 \pmod{m}, \quad w_0(c^n - 1) \equiv 0 \pmod{m}. \tag{2.2}$$

In the special case when m is a prime p and w_0 is not divisible by p, the least value of n for which the second of these congruences is satisfied is simply the exponent to which c belongs modulo p. A complete solution of our fundamental problems is thus at present out of the question even for a difference equation of order one. Nevertheless it is of considerable interest to reduce the general problem to its basic constituents. A short analysis discloses that in order to determine the minimal values of n in (2.2) it is sufficient to know

(i) the decomposition of m, v_0, w_0 and c into their prime factors;

(ii) the least value of n such that

$$c^n \equiv 1 \pmod{p}$$

for every prime factor p of m;

(iii) if λ is the least value of n satisfying (ii), the highest power of p dividing $c^\lambda - 1$.

---

* Compare Carmichael, pp. 345, 346.

† Compare Engstrom, p. 218.

Furthermore, (i) alone suffices for the determination of the numeric of (u), and (i) and (ii) alone for the determination of the characteristic number of (u) for all square-free integers m. (ii) is the unsolved problem of determining the exponent to which a given integer belongs for a given prime modulus, while (iii) is equivalent to the (unsolved) problem of the quotients of Fermat: to find the highest power of p dividing $c^{p-1}-1$.

Let us pass now to the general case of a difference equation of order k. Let

$$F(x) = x^k - c_1x^{k-1} - \cdots - c_k$$

denote the polynomial associated with the difference equation (1.1), and (u) as before any solution of (1.1). Then we can associate with (1.1) and m two congruences analogous to (2.2):

$$V(x)x^n \equiv 0 \pmod{m, F(x)}, \qquad W(x)(x^n - 1) \equiv 0 \pmod{m, F(x)},$$

where $V(x)$ and $W(x)$ are two polynomials whose coefficients may be determined as soon as the k initial values of (u) are known. The numeric and characteristic number of (u) modulo m are respectively the least values of n such that the first and second of these congruences are satisfied.

The central result of this investigation is that these minimal values of n may be determined in general provided that we know the following:

[i] (a) the decomposition of m into its prime factors;

(b) the Schönemann decompositions* of $F(x)$, $V(x)$ and $W(x)$ modulo p^N, where p is a prime factor of m;

[ii] for every prime factor p of m and every irreducible polynomial factor $\phi(x)$ of $F(x)$ to the modulus p, the least value of n such that

$$x^n \equiv 1 \pmod{p, \phi(x)};$$

[iii] if λ is the least value of n satisfying [ii], the polynomial $L(x)$ defined by

$$x^\lambda - 1 \equiv pL(x) \pmod{p^2, \phi^2(x)}.$$

We have then a complete analogy with the case of a difference equation of order one. Corresponding to (ii), [ii] is the unsolved problem of determining the period of a mark in a Galois field, while [iii] is a kind of generalization of the problem of the quotients of Fermat.†

The methods employed are elementary in the sense that no use is made either of the theory of ideals or the "fundamental theorem of algebra." Instead free use is made of polynomial congruences to single and double moduli in the spirit of Kronecker's theory of algebraic fields. The difficulties in the algebraic treatment due to discriminantal divisors are thereby evaded.‡

* See Fricke's *Algebra*, vol. 2, Braunschweig, 1928, chapter 2, and §7 of the present paper.

† Compare Ward, p. 161.

‡ Compare Engstrom, p. 211.

3. We shall adopt the following terminology in this paper. The term polynomial is restricted to mean a polynomial with integral coefficients; if the leading coefficient of the polynomial is unity, it will be said to be primary. We designate polynomials by $A(x)$, $B(x)$, $\cdots$, $U(x)$, $V(x)$, $\cdots$, $\theta(x)$, $\phi(x)$, $\cdots$. A polynomial is said to be divisible by an integer m when and only when all of its coefficients are divisible by m. The notations Res $\{A(x), B(x)\}$ and $(a, b, \cdots)$ will be used for the resultant of two polynomials $A(x)$ and $B(x)$ and the greatest common divisor of two or more integers $a, b, \cdots$.

If (a) is the reduced sequence corresponding to the solution (u) of (1.1) modulo m, and if μ is a period of (a), we shall say that (u) admits the period μ (modd m, $F(x)$) where it will be recalled that $F(x)=x^k-\cdots-c_k$ is the polynomial associated with the difference equation (1.1). In like manner, we shall refer to the characteristic number of (u) as its characteristic number (modd m, $F(x)$) whenever it is necessary to bring m and $F(x)$ in evidence. The notation

$$(u) \equiv (v),\ (u) \equiv (a) \pmod{m},\ 0 \leqq a < m,$$

is self-explanatory.

The following convenient definition was introduced by H. T. Engstrom*: A number π is said to be a general period of the difference equation (1.1) for the modulus m if every sequence of rational integers (u) satisfying (1.1) has the period π. Let τ be the least such general period for the modulus m. Then it is easily seen that every other general period is a multiple of τ, and that the characteristic number of any particular sequence (u) is a divisor of τ. We shall call τ the principal period of the difference equation (1.1) (modd m, $F(x)$). It possesses the following important property:

THEOREM 3.1. *There exist solutions of* (1.1) *whose characteristic number modulo m is the principal period of* (1.1).

Let (u) and (w) be any two solutions of (1.1). Then if we can determine integers $b_1, b_2, \cdots, b_k$ such that

$$u_n \equiv b_1 w_n + b_2 w_{n+1} + \cdots + b_k w_{n+k-1} \pmod{m},\ n = 0, 1, \cdots,$$

the characteristic number of (w) will be a period of (u). Owing to the linearity of (1.1) these congruences will hold for every n provided that they hold for $n=0, 1, 2, \cdots, k-1$. But a sufficient condition that the k congruences

$$\begin{array}{l} b_1 w_0 \quad + \cdots + b_k w_{k-1} \equiv u_0, \\ \quad\vdots \qquad\qquad\qquad\quad \vdots \qquad\quad \vdots \\ b_1 w_{k-1} + \cdots + b_k w_{2k-1} \equiv u_{k-1} \end{array} \pmod{m}$$

* Engstrom, p. 210.

have integral solutions $b_1, \cdots, b_k$ is that their determinant be prime to m. For that particular sequence (w) with the initial values $w_0 = w_1 = \cdots = w_{k-2} = 0$, $w_{k-1} = 1$, this determinant has the value $(-1)^k$.

Hence the characteristic number of (w) is a general period of (1.1). But the characteristic number of (w) must divide the principal period. Hence it is equal to it.

Thus the principal period is the least upper bound of the characteristic numbers of all solutions of (1.1), and the determination of the characteristic number of (w) gives the solution of the second fundamental problem mentioned in the introduction.

COROLLARY. *If* (u) *is any solution of* (1.1) *and if* $\Delta(u)$ *denotes the determinant*

$$\Delta(u) = \begin{vmatrix} u_0, & u_1, \cdots, u_{k-1} \\ u_1, & u_2, \cdots, u_k \\ \cdot & \cdot \quad\quad \cdot \\ \cdot & \cdot \quad\quad \cdot \\ \cdot & \cdot \quad\quad \cdot \\ u_{k-1}, & u_k, \cdots, u_{2k-1} \end{vmatrix},$$

then if $\Delta(u)$ *is prime to* m, *the characteristic number of* (u) *is the principal period of* (1.1).

As an application of this corollary, consider the solution (s) of (1.1) with the initial values $s_0 = k$, $s_1 = c_1$, $s_2 = c_1^2 + 2c_2$ and so on, so that if the discriminant of $F(x)$ does not vanish, s_n is the familiar sum of the nth powers of the roots of $F(x) = 0$. It is well known that $\Delta(s)$ equals the discriminant of $F(x)$. Hence *the characteristic number of* (s) *is the principal period of* (1.1) *provided that* m *is prime to the discriminant of* $F(x)$.

II. THE RELATIONSHIP WITH THE RING ASSOCIATED WITH THE DOUBLE MODULUS

4. We begin by considering the solutions of (1.1) from a group-theoretic stand-point. If we regard any two solutions (u) and (v) of (1.1) as one-rowed matrices we may define their "sum" to be the sequence $(u+v)$:

$$(u) + (v) = (u + v).$$

The set of all solutions of (1.1) form an infinite Abelian group with respect to the operation of vector addition just defined, the identity element of the group being the sequence

$$(0): \qquad 0, 0, \cdots, 0, \cdots.$$

Denote this group by $\mathfrak{U}$ and the corresponding finite group of the reduced sequences (a) by $\mathfrak{A}$. The relationship between these two groups may be conveniently symbolized by writing

$$\mathfrak{U} \equiv \mathfrak{A} \qquad (\text{mod } m).$$

Now the method of attack upon the fundamental problems mentioned in the introduction is *to set up an isomorphism between the group* $\mathfrak{A}$ *and the ring of residue classes associated with the double modulus* m *and* $F(x)$. The problems considered are thus transformed into problems belonging to the theory of congruences to a double modulus which admit of perfectly definite answers.

To set up this isomorphism, it is necessary to define the "product" of two sequences (u) and (v). How this may be done will be explained in §6; for the present, we will confine ourselves to developing the idea of addition of sequences.

THEOREM 4.1. *Every sequence* (u) *may be uniquely represented modulo* m *as the sum of a null sequence and a purely periodic sequence with the same numeric and characteristic number.*

Let λ and μ be respectively the numeric and characteristic number of (u) modulo m, and suppose that $\lambda \equiv -r \pmod{\mu}$, where $0 \leqq r < \mu$, so that $\lambda + r = q\mu$.

Set $v_n = u_{\lambda+r+n}$, $w_n = u_n - v_n$ $(n = 0, 1, \cdots)$.

Then (v) is a purely periodic sequence with the characteristic number μ modulo m, and

$$(u) = (v) + (w).$$

(w) is a null sequence modulo m with the numeric λ. For if $n \geqq 0$,

$$\begin{aligned} w_{n+\lambda} &= u_{n+\lambda} - v_{n+\lambda} = u_{n+\lambda} - u_{q\mu+n+\lambda} \equiv 0, \\ w_{\lambda-1} &= u_{\lambda-1} - v_{\lambda-1} = u_{\lambda-1} - u_{q\mu+\lambda-1} \not\equiv 0 \qquad (\text{mod } m). \end{aligned}$$

Such a representation of (u) is unique modulo m; for if there were a second one

$$(u) = (v') + (w')$$

we would have $(w - w') = (v' - v)$, so that $(w - w')$ would be a purely periodic null sequence. Hence $(w - w') \equiv (0) \pmod{m}$, $(w) \equiv (w')$, $(v) \equiv (v') \pmod{m}$.

It is evident that the set of all null sequences of $\mathfrak{A}$ and the set of all purely periodic sequences of $\mathfrak{A}$ are both sub-groups of $\mathfrak{A}$. If we denote these sub-groups by $\mathfrak{N}$ and $\mathfrak{P}$, we have from Theorem 4.1

THEOREM 4.2. *The group* $\mathfrak{A}$ *is the direct sum of* $\mathfrak{N}$ *and* $\mathfrak{P}$, *where* $\mathfrak{N}$ *is the group of all null sequences of* $\mathfrak{A}$, *and* $\mathfrak{P}$ *is the group of all purely periodic sequences of* $\mathfrak{A}$.

5. If we form from the first n terms of any solution (u) of (1.1) a polynomial of degree $n-1$ in the indeterminate x

$$U_n(x) = u_0x^{n-1} + u_1x^{n-2} + \cdots + u_{n-1},$$

it is easily verified that we have identically in x

$$\begin{aligned} F(x)U_n(x) \doteq\ & x^n\{u_0x^{k-1} + (u_1 - c_1u_0)x^{k-2} + \cdots + (u_{k-1} - c_1u_{k-2} \\ & - \cdots - c_{k-1}u_0)\} - \{u_nx^{k-1} + (u_{n+1} - c_1u_n)x^{k-2} + \cdots \\ & + (u_{n+k-1} - c_1u_{n+k-2} - \cdots - c_{k-1}u_n)\}. \end{aligned}$$

Denote the two polynomials in brackets by $U(x)$ and $U^{(n)}(x)$ respectively. Then on considering the identity modulo m, we obtain the congruence

$$x^nU(x) - U^{(n)}(x) \equiv 0 \qquad (\text{modd } m, F(x)). \tag{5.1}$$

Assume first that (u) is purely periodic modulo m and admits the period n. Then $U^{(n)}(x) \equiv U(x)$ (mod m), so that (5.1) becomes

$$(x^n - 1)U(x) \equiv 0 \qquad (\text{modd } m, F(x)).$$

Conversely if for some n this latter congruence holds, (u) is purely periodic modulo m and admits the period n.

Secondly, assume that (u) is a null sequence modulo m of numeric $\leqq n$. Then $U^{(n)}(x) \equiv 0$ (mod m) and (5.1) becomes

$$x^nU(x) \equiv 0 \qquad (\text{modd } m, F(x)).$$

Conversely if for some n this latter congruence holds, (u) is a null sequence of numeric $\leqq n$. We have thus established the following two basic theorems:

FUNDAMENTAL THEOREM ON PURELY PERIODIC SEQUENCES. *If (u) is any solution of the difference equation* (1.1), *then a necessary and sufficient condition that (u) should be purely periodic and admit the period n* (modd m, $F(x)$) *is that*

$$(x^n - 1)U(x) \equiv 0 \qquad (\text{modd } m, F(x)), \tag{5.2}$$

where

$$U(x) = u_0x^{k-1} + (u_1 - c_1u_0)x^{k-2} + \cdots + (u_{k-1} - c_1u_{k-2} - \cdots - c_{k-1}) \tag{5.3}$$

is a polynomial of degree $k-1$ in x whose coefficients are determined entirely by the k initial values of (u) and the coefficients of (1.1), *while $F(x)$ is the polynomial associated with* (1.1).

We shall call the polynomial $U(x)$ which completely determines the k initial values of (u) and hence (u) itself, the *generator* of (u).

FUNDAMENTAL THEOREM ON NULL SEQUENCES. *If $U(x)$ is the generator of the sequence (u), then a necessary and sufficient condition that (u) should be a null sequence with numeric less than or equal to n is that*

$$x^n U(x) \equiv 0 \qquad (\text{modd } m, F(x)). \tag{5.4}$$

We have the following important corollaries to these theorems.

COROLLARY 1. *If (u) is a purely periodic sequence modulo m, its characteristic number is the least value of n for which the congruence* (5.2) *is satisfied.*

COROLLARY 2. *If (u) is a null sequence modulo m, its numeric is the least value of n for which the congruence* (5.4) *is satisfied.*

The generator of the sequence (w) with the initial values $0, 0, \cdots, 0, 1$ is unity. Hence we have from Theorem 3.1

COROLLARY 3. *The principal period of* (1.1) *modulo m is the least value of n such that*

$$x^n \equiv 1 \qquad (\text{modd } m, F(x)).$$

6. We are now ready to establish the isomorphism between the ring of residue classes associated with the double modulus m, $F(x)$ and the group of reduced sequences defined in §4. The ring may be represented by the set of m^k polynomials

$$L(x) = l_0 x^{k-1} + l_1 x^{k-2} + \cdots + l_{k-1} \qquad (0 \leqq l_i < m).$$

On identifying $U(x)$ of (5.3) modulo m with $L(x)$ we obtain the congruences

$$u_r - c_1 u_{r-1} - c_2 u_{r-2} - \cdots - c_r u_0 \equiv l_r \pmod{m}, \; r = 0, \cdots, k-1. \tag{6.1}$$

These congruences have a unique solution

$$u_i \equiv a_i \pmod{m}, \; 0 \leqq a_i < m; \; i = 0, \cdots, k-1.$$

We associate with $L(x)$ the reduced sequence (a) whose initial values are $a_0, \cdots, a_{k-1}$, and write

$$(a) \sim L(x).$$

Since the congruences (6.1) are solvable for the l_r for any m, given (a), we can determine a unique $L(x)$. The correspondence is therefore a reciprocal one.

Suppose that

$$(b) \sim M(x).$$

Then evidently

$$(a + b) \sim L(x) + M(x).$$

If $L(x)\cdot M(x)\equiv N(x)$ (modd m, $F(x)$), we define the reduced sequence (c) associated with $N(x)$ to be the *product* of the sequences (a) and (b). The exact dependence of the elements of (c) upon those of (a) and (b) need not detain us here. If we write $(a)\cdot(b)$ for the product of the sequences (a) and (b), we have then

$$(a)\cdot(b)\sim L(x)\cdot M(x).$$

It is easily verified that the set $\mathfrak{A}$ with the two operations of addition and multiplication just defined satisfies the postulates for a ring*; hence we have the following result:

THEOREM 6.1. *The set $\mathfrak{A}$ of reduced sequences modulo m forms a commutative ring with respect to the operations of addition and multiplication of sequences defined above which is simply isomorphic with the ring $\mathfrak{R}$ of residue classes associated with the double modulus m, $F(x)$.*

If

$$(a):\qquad a_0,\ a_1,\ a_2,\ \cdots$$

is any sequence of $\mathfrak{A}$, the corresponding element of the ring $\mathfrak{R}$ is

$$L(x)=l_0x^{k-1}+l_1x^{k-2}+\cdots+l_{k-1}$$

where

$$l_r\equiv a_r-c_1a_{r-1}-c_2a_{r-2}-\cdots-c_ra_0\quad(\text{mod } m),\ r=0,\cdots,k-1.$$

To examine the nature of this correspondence further, we need the following lemma.

LEMMA. *If (u) is a solution of the difference equation* (1.1), *and if $\Delta(u)$ denotes the determinant*

$$\Delta(u)=\begin{vmatrix} u_0, & u_1, & \cdots, & u_{k-1}\\ u_1, & u_2, & \cdots, & u_k\\ \cdot & \cdot & & \cdot\\ \cdot & \cdot & & \cdot\\ \cdot & \cdot & & \cdot\\ u_{k-1}, & u_k, & \cdots, & u_{2k-1}\end{vmatrix}$$

and $U(x)$ the polynomial

$$U(x)=u_0x^{k-1}+(u_1-c_1u_0)x^{k-2}+(u_2-c_1u_1-c_2u_0)x^{k-3}+\cdots$$
$$+(u_{k-1}-c_1u_{k-2}-\cdots-c_{k-1}u_0),$$

then $(-1)^k\Delta(u)$ is equal to the resultant of $U(x)$ and $F(x)$, where $F(x)$ is the polynomial associated with the difference equation (1.1).

* van der Waerden, *Algebra*, Berlin, 1930, vol. 1, p. 37.

The nature of the proof is sufficiently indicated by the special case $k=3$. The resultant of $U(x)$ and $F(x)$ may then be expressed as the five-rowed eliminant

$$E = \begin{vmatrix} u_0, & u_1 - c_1u_0, & u_2 - c_1u_1 - c_2u_0, & 0, & 0 \\ 0, & u_0, & u_1 - c_1u_0, & u_2 - c_1u_1 - c_2u_0, & 0 \\ 0, & 0, & u_0, & u_1 - c_1u_0, & u_2 - c_1u_1 - c_2u_0 \\ 1, & -c_1, & -c_2, & -c_3, & 0 \\ 0, & 1, & -c_1, & -c_2, & -c_3 \end{vmatrix}.$$

Now perform upon E the operations

$$\text{row } 1 - u_0 \text{ row } 4 - u_1 \text{ row } 5, \quad \text{row } 2 - u_0 \text{ row } 5.$$

The first two elements in the first three rows of E become zero, so that E reduces to the third-order determinant

$$E = -\begin{vmatrix} u_2, & c_2u_1 + c_3u_0, & c_3u_1 \\ u_1, & u_2 - c_1u_1, & c_3u_0 \\ u_0, & u_1 - c_1u_0, & u_2 - c_1u_1 - c_2u_0 \end{vmatrix}.$$

From the difference equation,

$$u_3 = c_1u_2 + c_2u_1 + c_3u_0, \quad u_4 = c_1u_3 + c_2u_2 + c_3u_1.$$

Hence performing upon E successively the operations

$$\text{col } 2 + c_1 \text{ col } 1, \quad \text{col } 3 + c_2 \text{ col } 1 + c_1 \text{ col } 2,$$

we obtain

$$E = -\begin{vmatrix} u_2, & u_3, & c_3u_1 \\ u_1, & u_2, & c_3u_0 \\ u_0, & u_1, & u_2 - c_1u_1 - c_2u_0 \end{vmatrix} = -\begin{vmatrix} u_2, & u_3, & u_4 \\ u_1, & u_2, & u_3 \\ u_0, & u_1, & u_2 \end{vmatrix} = (-1)^3\Delta(u).$$

THEOREM 6.2. *To the units of the ring $\mathfrak{R}$ correspond those sequences of $\mathfrak{A}$ whose characteristic number is the principal period of the difference equation* (1.1) *modulo m, while to the identity element* 1 *of $\mathfrak{R}$ there corresponds the sequence* (w) *with the initial values* $0, 0, \cdots, 0, 1$.

For the units of $\mathfrak{R}$ are represented by those polynomials $L(x)$ such that the resultant of $L(x)$ and $F(x)$ is prime to m. But if $L(x) = U(x)$ is the generator of the sequence (u), we have just seen that $\Delta(u)$ is numerically

equal to the resultant of $L(x)$ and $F(x)$. By the corollary to Theorem 3.1, the characteristic number of all sequences (u) with $\Delta(u)$ prime to m is the same, and equal to the principal period of (1.1) modulo m. The latter part of the theorem follows from the fact that for the sequence $(w): 0, 0, \cdots, 0, 1, \cdots$ we have $W(x)=1$.

III. Simplification of the form of the modulus and associated polynomial

7. If $m=p_1^{n_1}\cdots p_r^{n_r}$ is the decomposition of m into its prime factors, then it is easy to see that the ring associated with the double modulus m, $F(x)$ is the direct sum of the r rings associated with the double moduli $p_i^{n_i}$, $F(x)$. We have of course a similar dissection of the ring $\mathfrak{A}$ into a sum of simpler rings. The following important theorem gives the corresponding reduction of the problem of determining the characteristic number and numeric of any sequence modulo m to the case when m is a power of a prime.

THEOREM 7.1. *If*

$$m = p_1^{n_1}\cdots p_r^{n_r}$$

is the decomposition of m into its prime factors, then the characteristic number of any sequence modulo m is the least common multiple of its characteristic numbers modulis $p_i^{n_i}$ $(i=1, \cdots, r)$ while its numeric is the maximum of its numerics modulis $p_i^{n_i}$.

It is sufficient to show that if $m=a\cdot b$ where a and b are relatively prime, then the characteristic number of (u) modulo m is the least common multiple of its characteristic numbers modulo a and modulo b, while its numeric modulo m is the greatest of its numerics modulo a and modulo b.

Let

$$(u) \equiv (v) + (w) \pmod{m}$$

be the unique decomposition of (u) into a null sequence (v) and a purely periodic sequence (w). Then since a and b divide m,

$$(u) \equiv (v) + (w) \pmod{a}, \text{ and } (u) \equiv (v) + (w) \pmod{b}.$$

Furthermore (v) is a null sequence modulis a and b and (w) is a purely periodic sequence modulis a and b.

In view of Theorem 4.1, it is sufficient to prove the result for the numeric of (v) and the characteristic number of (w).

Consider first (v), and let $V(x)$ be its generator, ν_m, ν_a and ν_b its numerics modulis m, a and b respectively, and τ the greatest of ν_a and ν_b. Then by the fundamental theorem of §5,

$$x^{\nu_m}V(x) \equiv 0 \pmod{m, F(x)}, \quad x^{\nu_a}V(x) \equiv 0 \pmod{a, F(x)},$$
$$x^{\nu_b}V(x) \equiv 0 \pmod{b, F(x)}.$$

Thus $x^{\nu_m}V(x) \equiv 0 \pmod{a, F(x)}$ (and $\pmod{b, F(x)}$) so that $\nu_m \geqq \tau$. But since a and b are relatively prime,

$$x^{\tau}V(x) \equiv 0 \qquad \pmod{ab, F(x)}$$

so that $\tau \geqq \nu_m$. Hence $\tau = \nu_m$.

The proof for the characteristic number of (w) is similar and will be left to the reader.*

We shall assume hereafter that $m = p^N$, p a prime, N a given integer.

Now suppose that

$$F(x) \equiv \{\phi_1(x)\}^{t_1} \cdot \{\phi_2(x)\}^{t_2} \cdots \{\phi_s(x)\}^{t_s} \qquad \pmod{p}$$

is the unique decomposition of $F(x)$ modulo p into a product of powers of primary irreducible polynomials $\phi(x)$. Then by Schönemann's second theorem† there exists a decomposition of $F(x)$ modulo p^N of the form

$$F(x) \equiv F_1(x) \cdot F_2(x) \cdots F_s(x) \qquad \pmod{p^N} \tag{7.1}$$

where

$$F_i(x) \equiv \{\phi_i(x)\}^{t_i} \qquad \pmod{p}, \; i = 1, 2, \cdots, s,$$

and the polynomials $F_i(x)$ are primary. We shall refer to (7.1) as a Schönemann decomposition of $F(x)$ (modulo p^N).

Corresponding to this decomposition of $F(x)$, we have a decomposition of the ring associated with the double modulus p^N, $F(x)$ into the direct sum of the s rings associated with the moduli p^N, $F_i(x)$. If $U(x)$ is any element of this ring, and

$$U(x) \equiv U^{(i)}(x) \qquad \pmod{p^N, F_i(x)}, \; i = 1, \cdots, s,$$

where $U^{(i)}(x)$ is of degree less than $F_i(x)$, then $U(x)$ may be uniquely represented as

$$U(x) \equiv B^{(1)}(x)U^{(1)}(x) + B^{(2)}(x)U^{(2)}(x) + \cdots + B^{(s)}(x)U^{(s)}(x) \pmod{p^N, F(x)}$$

where the $B^{(i)}(x)$ are of degree less than $F(x)$ and

$$\begin{aligned} B^{(i)}(x) &\equiv 1 \pmod{p^N, F_i(x)}, \\ &\equiv 0 \pmod{p^N, F_j(x)}, \quad j \neq i; \; 1 \leqq j \leqq s; \; i = 1, \cdots, s. \end{aligned}$$

---

* See Ward, p. 155, Theorem 3.11.

† See Fricke, work cited, §11.

If (u) is the sequence generated by $U(x)$, $(u^{(i)})$ and $(b^{(i)})$ the sequences generated by $U^{(i)}(x)$ and $B^{(i)}(x)$, the analogous decomposition of (u) is

$$(u) \equiv (b^{(1)})\cdot(u^{(1)}) + (b^{(2)})\cdot(u^{(2)}) + \cdots + (b^{(s)})\cdot(u^{(s)}) \pmod{p^N}.$$

The corresponding theorem for the characteristic numbers and numeric of (u) is as follows:

THEOREM 7.2. *Suppose that* (7.1) *is a Schönemann decomposition of* $F(x)$ *modulo* p^N, *and that* $U(x)$ *is a polynomial of degree* $\leqq k-1$ *in* x *generating a sequence* (u). *Furthermore suppose that*

$$U(x) \equiv U^{(i)}(x) \qquad (\text{modd } p^N, F_i(x))$$

where $U^{(i)}(x)$ *is a polynomial of degree less than* $F_i(x)$, *and the generator of a sequence* $(u^{(i)})$ *which is a solution of the difference equation whose associated polynomial is* $F_i(x)$.

Then the characteristic number of (u) (modd $p^N, F(x)$) *is the least common multiple of the characteristic numbers of* $(u^{(i)})$ (modd $p^N, F_i(x)$) *and the numeric of* (u) *is the maximum of the numerics of the* $(u^{(i)})$.

Suppose that

$$(u) \equiv (v) + (w) \pmod{p^N} \text{ and } U(x) \equiv V(x) + W(x) \quad (\text{modd } p^N, F(x))$$

are the decompositions of (u) into a null sequence (v) and a purely periodic sequence (w), and the corresponding decomposition of the generator $U(x)$ of (u). Furthermore, suppose that

$$U(x) \equiv U^{(i)}(x),\ V(x) \equiv V^{(i)}(x),\ W(x) \equiv W^{(i)}(x) \quad (\text{modd } p^N, F_i(x))$$

where the polynomials on the right side of the congruences are of lesser degree than $F_i(x)$, and that $(u^{(i)})$, $(v^{(i)})$ and $(w^{(i)})$ are the solutions of the difference equation associated with $F_i(x)$ with the generators $U^{(i)}(x)$, $V^{(i)}(x)$ and $W^{(i)}(x)$ respectively. Then we may write

$$\begin{aligned} (u^{(i)}) &\equiv (v^{(i)}) + (w^{(i)}) && (\text{mod } p^N), \\ U^{(i)}(x) &\equiv V^{(i)}(x) + W^{(i)}(x) && (\text{modd } p^N, F_i(x)). \end{aligned} \tag{7.2}$$

I assert that (7.2) *gives the decomposition of* $(u^{(i)})$ *into its purely periodic and null components*; for if τ and λ are the numeric and characteristic number of (u), we have by the theorems of §§4 and 5

$$x^\tau V(x) \equiv 0, \quad x^\lambda W(x) \equiv W(x) \qquad (\text{modd } p^N, F(x)).$$

Hence

$$x^\tau V^{(i)}(x) \equiv 0,\ x^\lambda W^{(i)}(x) \equiv W^{(i)}(x) \qquad (\text{modd } p^N, F_i(x)) \tag{7.3}$$

so that by the theorems of §5, $(v^{(i)})$ is a null sequence and $(w^{(i)})$ is a purely

periodic sequence. By Theorem 4.1, the numeric of $(v^{(i)})$ and the characteristic number of $(w^{(i)})$ are the numeric and the characteristic number of $(u^{(i)})$. Call this latter number λ_i and let μ be the least common multiple of $\lambda_1, \lambda_2, \cdots, \lambda_s$. From the second congruence in (7.3), $(w^{(i)})$, and hence $(u^{(i)})$, admits the period λ (modd p^N, $F_i(x)$). Hence λ_i divides λ so that μ divides λ. But clearly

$$(x^\mu - 1)W^{(i)}(x) \equiv 0 \qquad (\text{modd } p^N, F_i(x))$$

so that

$$(x^\mu - 1)W(x) \equiv 0 \qquad (\text{modd } p^N, F_i(x)),\ i=1, \cdots, s.$$

Since the resultant of any two distinct $F_i(x)$ is prime to p, these last congruences imply that

$$(x^\mu - 1)W(x) \equiv 0 \qquad (\text{modd } p^N, F(x)).$$

Hence by the fundamental theorem again, λ divides μ so that λ equals μ.

The proof of the result for the numerics is similar and will be omitted here.

8. In the present section, we shall solve completely the problem of determining the null component and the purely periodic component of any sequence (modd p^N, $F(x)$).

Let us assume that the coefficient c_k in (1.1) is divisible by p. Then in the Schönemann decomposition (7.1) one of the $F_i(x)$ must be of the form $x^{t_i}+pV(x)$; let us suppose that it is $F_1(x)$, so that

$$F_1(x) = x^{t_1} + pV(x).$$

The exponent t_1 is simply the number of consecutive coefficients c_k, $c_{k-1}, c_{k-2}, \cdots$ which are divisible by p. Let

$$F'(x) = F_2(x)\cdot F_3(x) \cdots F_s(x),$$

so that Res $\{F_1(x), F'(x)\}$ is prime to p.

By the fundamental theorem of §5, the sequence (u) is a null sequence modulo p^N when and only when the congruence

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

is solvable, $U(x)$ denoting as usual the generator of (u). But this congruence is solvable when and only when the two congruences

$$x^nU(x) \equiv 0 \quad (\text{modd } p^N, F_1(x)), \qquad x^nU(x) \equiv 0 \quad (\text{modd } p^N, F'(x))$$

are solvable. The first of these congruences is solvable for any $U(x)$, for we may take $n=Nt_1$. The second is solvable when and only when $U(x)\equiv 0$ (modd $p^N, F'(x)$) for Res $\{x, F'(x)\}$ is prime to p. We have thus established the following theorem.

THEOREM 8.1. *If in the Schönemann decomposition modulo p^N of the polynomial $F(x)$ associated with the difference equation* (1.1),

$$F(x) \equiv F_1(x)\cdot F_2(x)\cdots F_s(x) \pmod{p^N}, \tag{7.1}$$

we have $F_1(x)=x^{t_1}+pV(x)$, then a necessary and sufficient condition that a given solution (u) of (1.1) *be a null sequence modulo p^N is that its generator $U(x)$ satisfy the relation*

$$U(x) \equiv 0 \qquad (\text{modd } p^N, F_2(x)\cdots F_s(x)).$$

In this case its numeric is the least value of n such that

$$x^n\, U(x) \equiv 0 \qquad (\text{modd } p^N, F_1(x)). \tag{8.1}$$

We can prove the following result in very much the same manner.

THEOREM 8.2. *With the hypotheses of Theorem* 8.1, *a necessary and sufficient condition that a given solution (u) of* (1.1) *be purely periodic modulo p^N is that its generator $U(x)$ satisfy the relation*

$$U(x) \equiv 0 \qquad (\text{modd } p^N, F_1(x)).$$

The decomposition of (u) into its purely periodic and null components is now easily effected. For since Res $\{F_1(x), F'(x)\}$ is prime to p, we can determine two polynomials $S_1(x)$, $S_2(x)$ such that

$$S_1(x)F_1(x) + S_2(x)F'(x) \equiv U(x) \qquad (\text{modd } p^N, F(x)).$$

Suppose that

$$S_2(x)F'(x) \equiv V(x), \quad S_1(x)F_1(x) \equiv W(x) \qquad (\text{modd } p^N, F(x))$$

where the degrees of $V(x)$ and $W(x)$ do not exceed $k-1$, and let (v) and (w) be the sequences generated by $V(x)$ and $W(x)$ respectively. Then

$$U(x) \equiv V(x) + W(x) \quad (\text{modd } p^N, F(x)), \quad (u) \equiv (v) + (w) \pmod{p^N},$$

and (v) is a null sequence and (w) a purely periodic sequence modulo p^N.

IV. THE DETERMINATION OF THE NUMERIC

9. If (u) is a null sequence modulo p^N, we have just seen that its generator is of the form

$$U(x) \equiv U'(x)\cdot F_2(x)\cdots F_s(x) \pmod{p^N}$$

and that its numeric is the least value of n such that

$$x^n U'(x) \equiv 0 \qquad (\text{modd } p^N, F_1(x)).$$

$F_1(x)$ it will be recalled is of the form $x^{t_1}+pV(x)$. It may happen that $V(x)$ is also divisible by p. To conserve generality, we therefore assume that

$$F_1(x) = x^{t_1} - p^{\sigma_1}\theta(x); \qquad \theta(x) \not\equiv 0 \pmod{p}; \qquad \theta(x) \text{ of degree less than } t_1.$$

By Schönemann's theorems,* $U'(x)$ has a decomposition modulo p^N of the form

$$U'(x) \equiv p^M G_1(x) U''(x) \qquad \pmod{p^N}$$

where

$$M \geqq 0, \qquad G_1(x) = x^{\alpha_1} + p^{\beta_1}\zeta_1(x);$$
$$\text{Res}\,\{G_1(x), U''(x)\} \text{ prime to } p; \qquad \zeta_1(x) \not\equiv 0 \pmod{p}.$$

It follows immediately that the numeric of (u) is the least value of n such that

$$x^n G_1(x) \equiv 0 \qquad (\text{modd } p^{N-M}, F_1(x)). \tag{9.1}$$

This minimal value may always be calculated in view of the following two theorems:

THEOREM 9.1. *Suppose that a set of polynomials $U(x)$, $G(x)$, $\zeta(x)$ are defined recursively by*

$$\begin{aligned} U_{r-1}(x) &\equiv G_r(x)\overline{U}_{r-1}(x) && (\text{mod } p^{L_{r-1}}),\ r = 1, 2, \cdots, \\ x^{t_1-\alpha_r}G_r(x) &\equiv p^{\rho_r}U_r(x) && (\text{mod } F_1(x)), \\ G_r(x) &= x^{\alpha_r} + p^{\beta_r}\zeta_r(x), \\ L_r &= N - M - (\rho_1 + \rho_2 + \cdots + \rho_r), \end{aligned}$$

where $U_r(x)$ is not divisible by p, $\overline{U}_{r-1}(x)$ is not divisible by x modulo p, and $\zeta_r(x)$ is a polynomial of degree less than α_r not divisible by p, while $U_0(x) = G_1(x)U''(x)$, $\overline{U}_0(x) = U''(x)$. Then the numbers ρ are all positive, and after a finite number of steps, say l, we will either have

$$N \leqq M + \rho_1 + \rho_2 + \cdots + \rho_l \text{ or } \text{Res}\,\{U_l(x), F_1(x)\} \text{ prime to } p.$$

Let l now denote the first time one of these alternatives occurs. Then in the first case, the numeric of (u) is $lt_1-(\alpha_1+\alpha_2+\cdots+\alpha_l)$ and in the second case, the numeric is $lt_1-(\alpha_1+\alpha_2+\cdots+\alpha_l)+\nu_l$, where ν_l is the least value of n such that

$$x^n \equiv 0 \qquad (\text{modd } p^{L_l}, F_1(x)). \tag{9.2}$$

* Fricke, work cited, p. 59, p. 65.

THEOREM 9.2. *Suppose that a set of polynomials $\theta(x)$, $\bar{\theta}(x)$ are defined recursively by*

$$\theta_r(x) \equiv (x^{\tau_r} + p^{\gamma_r}\phi_r(x))\bar{\theta}_r(x) \pmod{p^{L_k}},$$
$$x^{t_1-\tau_r}\theta_r(x) \equiv p^{\sigma_r}\theta_{r+1}(x) \pmod{F_1(x)}, \quad r = 1, 2, \cdots,$$

where $\theta_r(x)$ is not divisible by p, and $\bar{\theta}_r(x)$ is not divisible by x modulo p, $\phi_r(x)$ is a polynomial of degree less than τ_r not divisible by p, while τ_r is the number of consecutive coefficients of the zeroth, first, second, $\cdots$ powers of x in $\theta_r(x)$ which are divisible by p. Then after a finite number of steps, say h, we will either have $L_l \leqq \sigma_1+\sigma_2+\cdots+\sigma_h$ or $\tau_h=0$ and Res $\{\theta_h(x), F_1(x)\}$ *prime to p.*

Let h denote the first time one of these alternatives occurs. Then in the first case, the least value of n for which the congruence (9.2) *is satisfied is $\bar{\tau}_h = ht_1-(\tau_1+\tau_2+\cdots+\tau_h)$. In the second case it is $q_h\bar{\tau}_h$, where q_h is the integer next greater than or equal to L_l divided by $\sigma_1+\sigma_2+\cdots+\sigma_h$.*

The proofs of these theorems are by induction, and are perfectly straightforward though rather lengthy. They will be omitted here, as the important result is that *the numeric may be calculated if we merely know the Schönemann decompositions of $U(x)$ and $F(x)$ quite independently of the calculation of the characteristic number.*

The following results are immediate corollaries of Theorems 9.1 and 9.2.

COROLLARY 1. *If*

$$F(x) \equiv F_1(x)\cdots F_s(x) \pmod{p^N},$$
$$F_1(x) \equiv x^{t_1} - p^{\sigma_1}\theta_1(x) \qquad (\theta_1(x) \not\equiv 0 \bmod p)$$

is the Schönemann decomposition of the polynomial $F(x)$ mod p^N *associated with the difference equation* (1.1), *the least upper bound of the numerics of all solutions of* (1.1) *modulo p^N is qt_1, where q is the integer next greater than or equal to N/σ_1.*

COROLLARY 2.* *The least upper bound for the numerics of all difference equations* (1.1) *modulo p^N whose t_1 last coefficients are divisible by p is Nt_1.*

COROLLARY 3. *The least upper bound for the numeric of all difference equations* (1.1) *of order k modulo p^N is Nk.*

V. THE DETERMINATION OF THE CHARACTERISTIC NUMBER

10. In this division of the paper we shall reduce the problem of determining the characteristic number of any solution of (1.1) to its constituents in the sense explained in the introduction. In view of the results of §7, we may

* Due to Engstrom, p. 218, Theorem 9.

assume that $m=p^N$ where p is a prime, and that the associated polynomial $F(x)$ is of the form

$$F(x) = \{\phi(x)\}^a - p\theta(x) \tag{10.1}$$

where it will be recalled that $\phi(x)$ is primary and irreducible modulo p, while $\theta(x)$ is of lesser degree than $F(x)$.

The results of §8 allow us to assume that (u) is purely periodic. Hence by the fundamental theorem of §5, the characteristic number of (u) is the least value of n such that

$$(x^n - 1)U(x) \equiv 0 \qquad (\text{modd } p^N, F(x)), \tag{10.2}$$

where $U(x)$ is the generator of (u).

The following easily established theorem* justifies us in assuming that $U(x)$ is not divisible by p.

THEOREM 10.1. *If (u) is any solution of the difference equation* (1.1), *the form of $F(x)$ being unrestricted, and if the integer d is a common factor of the k initial values of (u), then the characteristic number of (u) to any modulus m is the characteristic number of $d^{-1}(u)$ modulo (m/l), where l is the greatest common divisor of m and d.*

Suppose that λ is the characteristic number of (u) (modd p^N, $F(x)$), so that

$$(x^\lambda - 1)U(x) \equiv 0 \qquad (\text{modd } p^N, F(x)) \tag{10.21}$$

and let p^K be the first elementary divisor of the matrix of the eliminant of $U(x)$ and $F(x)$ corresponding to the prime p. Then I have shown elsewhere† that (10.21) implies that

$$x^\lambda - 1 \equiv 0 \qquad (\text{modd } p^{N-K}, F(x)).$$

Thus λ is a multiple of the principal period of (1.1) modulo p^{N-K}.

THEOREM 10.2. *If the first elementary divisor of the matrix of the eliminant of $U(x)$ and $F(x)$ corresponding to the prime p is p^K, then the characteristic number of (u)* (modd p^N, $F(x)$), $N>K$, *is a multiple of the principal period of* (1.1) *modulo p^{N-K}.*

This theorem is of some practical importance, as it gives us a lower limit to the characteristic number of any sequence. The extension to composite m and $F(x)$ unrestricted is obvious in view of the results of §7.

* Ward, p. 157, Theorem 5.2.

† These Transactions, vol. 35 (1933), p. 258.

Since $U(x)$ in (10.2) is not congruent to zero modulo p, we may assume that

$$U(x) \equiv \{\phi(x)\}^b \psi(x) \qquad (\text{mod } p),\ a > b \geqq 0,$$

where Res $\{\psi(x), \phi(x)\}$ is prime to p. Then by Schönemann's second theorem,† we have

$$U(x) \equiv U^*(x)V(x) \qquad (\text{mod } p^N)$$

where

$$U^*(x) = \{\phi(x)\}^b + p\xi(x), \qquad \xi(x) \text{ of lower degree than } U^*(x), \tag{10.3}$$

and $V(x) \equiv \psi(x)$, mod p.

It follows that *the characteristic number of* (u) *is the least value of* n *such that*

$$(x^n - 1)U^*(x) \equiv 0 \qquad (\text{modd } p^N, F(x)). \tag{10.4}$$

To avoid circumlocutions, we shall refer to this number as the characteristic number of the congruence (10.4).

If $N = 1$, we may replace (10.4) by

$$x^n - 1 \equiv 0 \qquad (\text{modd } p, \{\phi(x)\}^{a-b}). \tag{10.5}$$

Suppose that the polynomial $\phi(x)$ is of degree t in x. Then the characteristic number of

$$x^n - 1 \equiv 0 \qquad (\text{modd } p, \phi(x))$$

is a well known quantity in the Galois field theory‡; for it is simply the exponent to which belongs the mark associated with a root of $\phi(x) = 0$ in the Galois field of order p^t. We shall regard this number as known to us§; it is a divisor of $p^t - 1$ and hence prime to p and at most equal to $p^t - 1$. Let us denote it by λ. Then there exist polynomials $\phi(x)$ of degree t for which the corresponding λ equals $p^t - 1$; in other words, $p^t - 1$ is not only an upper bound for λ, but it is the least upper bound for λ.

We have then

$$x^\lambda - 1 = \psi(x)\phi(x) + p\zeta(x) \tag{10.6}$$

where $\psi(x)$ and $\zeta(x)$ are polynomials and $\zeta(x)$ is of lower degree than $\phi(x)$. Since the discriminant of $x^\lambda - 1$ is prime to p,

$$\psi(x) \not\equiv 0 \qquad (\text{modd } p, \phi(x)). \tag{10.7}$$

† Fricke, work cited, pp. 65–66.

‡ See Dickson, *Linear Groups*, Teubner, 1901, Part I.

§ Compare the remarks in §2 of the introduction.

From (10.6),

$$x^{r\lambda} \equiv 1 + r\psi(x)\phi(x) \qquad (\text{modd } p, \phi^2(x)).$$

Hence the characteristic number of

$$x^n \equiv 1 \qquad (\text{modd } p, \phi^2(x))$$

is $p\lambda$. But since

$$x^{p\lambda} \equiv 1 + \{\psi(x)\}^p\{\phi(x)\}^p \qquad (\text{mod } p),$$

$p\lambda$ is also the characteristic number of (10.5) if $2 \leqq a-b \leqq p$.

Proceeding in this manner, we obtain the following result:

THEOREM 10.3. *If $U(x)$ is the generator of a purely periodic solution (u) of the difference equation* (1.1) *whose associated polynomial is of the form*

$$F(x) \equiv \{\phi(x)\}^a \ (\text{mod } p), \textit{ while } U(x) \equiv \{\phi(x)\}^b V(x) \qquad (\text{mod } p),$$

where Res $\{V(x), \phi(x)\}$ *is prime to p and $\phi(x)$ is irreducible modulo p, then the characteristic number of (u) modulo p is $p^q\lambda$ where the integer q is such that*

$$p^{q-1} < a - b \leqq p^q$$

and λ is the least value of n such that

$$x^n \equiv 1 \qquad (\text{modd } p, \phi(x)).$$

THEOREM 10.4. *Under the hypothesis of Theorem* 10.3, *the principal period of* (1.1) *modulo p is $p^r\lambda$ where the integer r is determined by the condition*

$$p^{r-1} < a \leqq p^r$$

and the least upper bound for the principal period is $p^r(p^t-1)$, where t is the degree of the polynomial $\phi(x)$ in x.

We leave the formulation of the corresponding theorems when $F(x)$ is unrestricted in form and m any square-free integer to the reader.

11. We are now in a position to attack (10.4) in the general case when N is greater than one. We have, with the notation of Theorem 10.4,

$$x^{p^r\lambda} - 1 \equiv p^\sigma V(x) \qquad (\text{mod } F(x)) \tag{11.1}$$

where σ is a positive integer, and $V(x)$ is of lesser degree than $F(x)$. If $V(x) = 0$, we shall think of σ as arbitrarily large. If $V(x) \neq 0$, the value of σ is fixed by the condition $V(x) \not\equiv 0 \ (\text{mod } p)$. Then

$$U^*(x)V(x) \equiv p^\rho W(x) \qquad (\text{mod } F(x)) \tag{11.2}$$

where ρ is a positive integer or zero, and $W(x)$ is of lesser degree than $F(x)$. If $W(x) = 0$, we assign an arbitrarily large value to ρ. Otherwise, the value of ρ is fixed by the condition $W(x) \not\equiv 0 \ (\text{mod } p)$.

ρ may be equally well defined as the largest whole number M such that

$$U(x)V(x) \equiv 0 \qquad (\text{modd } p^M, F(x)).$$

Unless $V(x)$ divides $F(x)$ (when $U(x)$ may be taken so that $W(x)=0$), ρ has a definite upper bound† depending only on $V(x)$, $F(x)$ and p.

From (11.1), we deduce that

$$x^{\lambda p^{r+t}} \equiv (1+p^\sigma V(x))^{p^t} \equiv 1 + p^{\sigma+t}V(x) + \frac{p^{2\sigma+t}(p^t-1)}{1\cdot 2}V^2(x) + \cdots \pmod{F(x)}.$$

Hence from (11.2),

$$U^*(x)(x^{\lambda p^{r+t}}-1) \equiv p^{\sigma+\rho+t}W(x) + p^{2\sigma+\rho+t}W(x)\frac{(p^t-1)}{1\cdot 2}V(x) + \cdots \pmod{F(x)},$$

$$U^*(x)(x^{\lambda p^{r+t}}-1) \equiv p^{\sigma+\rho+t}W(x) \qquad (\text{modd } p^{\rho+\sigma+t+1}, F(x)),$$

save possibly in the case $p=2$, $\sigma=1$, which we shall exclude. From this last congruence, we deduce the following theorems:

THEOREM 11.1. *If p is an odd prime, $N>1$, the characteristic number of the congruence* (10.4) *is $p^r\lambda$ if $N \leqq \rho+\sigma$ and $\lambda p^{r+N-\rho-\sigma}$ if $N \geqq \rho+\sigma$, where ρ and σ are determined by the congruences* (11.1) *and* (11.2).

THEOREM 11.2. *If p is an odd prime, the least upper bound for the characteristic number of the congruence* (10.4) *for all choices of $U^*(x)$ is $p^r\lambda$ if $N \leqq \rho$ and $\lambda p^{r+N-\rho}$ if $N \geqq \rho$, where ρ is determined by the congruence* (11.2).

The fundamental problem of finding the characteristic number of any linear recursive sequence to any modulus m has thus finally reduced to determining the exponents σ and ρ in (11.1) and (11.2). We shall first seek to determine ρ in the case when p is odd and the exponent a in (10.1) is greater than unity.

If u is an indeterminate, and if we let

$$H(u) = u - \frac{u^2}{2} + \cdots - \frac{u^{p-1}}{p-1},$$

$$K(u) = -\frac{u}{2} + \left(1+\frac{1}{2}\right)\frac{u^2}{3} - \left(1+\frac{1}{2}+\frac{1}{3}\right)\frac{u^3}{4} + \cdots$$
$$+\left(1+\frac{1}{2}+\cdots+\frac{1}{p-2}\right)\frac{u^{p-1}}{p-1},$$

$$L(u) = 1 - u + u^2 - \cdots + u^{p-1},$$

$$H^{(r)}(x) = H((\phi\psi)^{p^r}),\ K^{(r)}(x) = K((\phi\psi)^{p^r}),\ L^{(r)}(x) = L((\phi\psi)^{p^r}),$$

† These Transactions, vol. 35 (1933), p. 258.

and, for uniformity of notation,

$$H^{(-1)}(x) = \zeta(x),$$

then it follows by induction on r from (10.6) that for any positive integral value of r,

$$x^{p^r\lambda} \equiv 1 + p\Theta_1(x) + p^2\Theta_2(x) + \{\psi(x)\}^{p^r}\{\phi(x)\}^{p^r} \pmod{p^3},$$

where

$$\Theta_1(x) = H^{(r-1)}(x),\ \Theta_2(x) = K^{(r-1)}(x) + H^{(r-2)}(x)L^{(r-1)}(x). \tag{11.3}$$

Now by (10.1),

$$\phi^{p^r} = \phi^a \cdot \phi^{p^r-a} = \phi^{p^r-a}(F + p\theta) \equiv p\theta\phi^{p^r-a} \pmod{F(x)}.$$

Therefore

$$x^{p^r\lambda} \equiv 1 + p(\theta\psi^{p^r}\phi^{p^r-a} + \Theta_1) + p^2\Theta_2 \quad (\text{modd } p^3, F(x)). \tag{11.4}$$

On comparing (11.4) and (11.1), we have

$$p^{\sigma-1}V(x) \equiv \theta\psi^{p^r}\phi^{p^r-a} + \Theta_1 + p\Theta_2 \quad (\text{modd } p^2, F(x)). \tag{11.41}$$

Therefore a necessary and sufficient condition that σ be greater than one is that $\theta\psi^{p^r}\phi^{p^r-a}+\Theta_1\equiv 0$ (modd p, $F(x)$). This congruence is equivalent to

$$\theta\psi^{p^r}\phi^{p^r-a} + \psi^{p^{r-1}}\phi^{p^{r-1}} - \tfrac{1}{2}\psi^{2p^{r-1}}\phi^{2p^{r-1}} + \cdots \equiv 0 \quad (\text{modd } p, \{\phi(x)\}^a), \tag{11.5}$$

which may be looked upon as a condition upon $\theta(x)$.

If $p^r-a>p^{r-1}$ or $\theta(x)\equiv 0$ (mod p), the congruence has no solutions. For if it had a solution, we would have

$$\psi^{p^{r-1}} \equiv 0 \quad (\text{modd } p, \phi(x))$$

contradicting (10.7). If $p^r-a\leqq p^{r-1}$ and $\theta(x)\not\equiv 0$ (mod p), (11.5) implies that

$$\theta(x) \equiv 0 \ (\text{modd } p, \{\phi(x)\}^c), \text{ where } c = p^{r-1} - p^r + a.$$

If $\theta(x)\equiv 0$ (modd p, $\{\phi(x)\}^{c+1}$), we again obtain a contradiction of (10.7). Hence

$$\theta(x) \equiv \kappa(x)\{\phi(x)\}^c \pmod{p}, \qquad \kappa(x) \not\equiv 0 \quad (\text{modd } p, \phi(x)).$$

On substituting in (11.5), we find that

$$\kappa\psi^{p^r-p^{r-1}} + 1 \equiv 0 \quad (\text{modd } p, \{\phi(x)\}^{p^{r-1}}). \tag{11.6}$$

This criterion can be greatly simplified. For if $y=x^{p^{r-1}}$,

$$\{\psi(x)\}^{p^r-p^{r-1}} \equiv \{\psi(y)\}^{p-1},\ \{\phi(x)\}^{p^{r-1}} \equiv \phi(y) \pmod{p}.$$

Hence (11.6) is equivalent to

$$\kappa(x)\{\psi(y)\}^{p-1}+1\equiv 0 \qquad (\text{modd } p,\ \phi(y)).$$

Since $\psi(y)\not\equiv 0$ (modd p, $\phi(y)$), there exists a polynomial $\vartheta(y)$ of degree less than $\phi(y)$ such that

$$\vartheta(y)\{\psi(y)\}^{p-1}+1\equiv 0 \qquad (\text{modd } p,\ \phi(y)).$$

Hence $\kappa(x)\equiv\vartheta(y)$ (modd p, $\phi(y)$), so that we may take

$$\kappa(x)=\vartheta(x^{p^{r-1}}),$$

where

$$\vartheta(x)\{\psi(x)\}^{p-1}+1\equiv 0 \qquad (\text{modd } p,\ \phi(x)). \tag{11.7}$$

If we let

$$\theta_1(x)=\vartheta(x^{p^{r-1}})\{\phi(x)\}^c,\ F_1(x)=\{\phi(x)\}^a-p\theta_1(x),$$

the results we have obtained may be summarized in the following theorem:

THEOREM 11.3. *If p is an odd prime, $a>1$, the exponent σ in* (11.1) *is generally unity. It is always unity if $p^r-a>p^{r-1}$, or if $\theta(x)\equiv 0$* (mod p) *or if $p^r-a>p^{r-1}$, $\theta(x)\not\equiv 0$* (modd p, $\phi(x)$). *It is greater than unity only when $F(x)\equiv F_1(x)$* (mod p^2) *where the polynomial $F_1(x)$ has been defined above.*

The further study of the exceptional case when $F(x)\equiv F_1(x)$ (mod p^2) would take us too far afield and will not be embarked upon here. The theorems of §13 on the determination of ρ when $a=1$ will give the reader an idea of the considerations which apply. We do however gain additional insight into the close relationship between recurring series and higher congruences if we seek to determine the polynomial $\psi(x)$ in (11.7) which must be known (modd p, $\phi(x)$) for $F_1(x)$ to be well defined. It will be recalled that $\psi(x)$ was originally defined as the quotient obtained on dividing $x^\lambda-1$ by $\phi(x)$. Hence if

$$x^\lambda-1\equiv pL(x)\ (\text{modd } p^2,\ \phi^2(x)),\ L(x) \text{ of lesser degree than } \phi^2(x),$$

$\psi(x)$ satisfies the congruence

$$\psi(x)\equiv L(x) \qquad (\text{modd } p,\ \phi(x)).$$

It is sufficient then for our purpose to determine $L(x)$.

Now if we set

$$\phi^2(x)=x^l-d_1x^{l-1}-\cdots-d_l,$$

$$x^n\equiv\sum_{k=1}^{l}w_{n,k}x^{l-k} \qquad (\text{mod } \phi^2(x)),$$

$$w_{n,l+1}=0 \qquad (n=0,1,2,\cdots),$$

then it is easily verified that the constants $w_{n,k}$ satisfy the following relations:

$$w_{n+1,k} = w_{n,k+1} + d_k w_{n,1} \quad (k = 1, \cdots, l;\ n = 0, 1, 2, \cdots),$$
$$w_{n,k} = \delta_{n,l-k} \qquad (n < l)$$

where $\delta_{n,l-k}$ is the Kronecker δ. It follows without much difficulty that $w_{0,k}, w_{1,k}, w_{2,k}, \cdots$ is a particular solution of the difference equation

$$\Omega_{n+l} = d_1\Omega_{n+l-1} + \cdots + d_l\Omega_n. \tag{11.8}$$

For convenience denote the sequence $w_{0,l-1}, w_{1,l-1}, w_{2,l-1}, \cdots$ whose initial values are $0, 0, \cdots, 0, 1$ simply by (w). Then we may write for a fixed k

$$w_{n,k} = \sum_{j=1}^{l} c_{kj} w_{n+l-j}$$

where the c_{kj} are integers determined by the l equations

$$\sum_{j=1}^{l} c_{kj} w_{n+l-j} = \delta_{n,l-k} \qquad (n = 0, 1, \cdots, l-1).$$

Thus if

$$W_j(x) = \sum_{k=1}^{l} c_{kj} x^{l-k},$$

$W_j(x)$ is a polynomial of degree $l-1$ in x with integral coefficients, which we may regard as known to us. Then

$$x^n = \sum_{k=1}^{l} w_{n,k} x^{l-k} = \sum_{k=1}^{l}\sum_{j=1}^{l} c_{kj} w_{n+l-j} x^{l-k}$$
$$= \sum_{j=1}^{l} w_{n+l-j} W_j(x).$$

Hence

$$pL(x) \equiv w_{\lambda+l-1}W_1(x) + w_{\lambda+l-2}W_2(x) + \cdots + w_\lambda W_l(x) + 1 \pmod{\phi^2(x)}$$

so that $L(x)$ is determined if we know the residues modulo p^2 of the l terms $w_{\lambda+l-1}, w_{\lambda+l-2}, \cdots, w_\lambda$ of the solution $0, 0, \cdots, 0, 1, d_1, \cdots$ of (11.8). There seems to be no way of obtaining these residues short of calculating the whole sequence (w) modulo p^2 step by step out to $\lambda+l$ terms. Such a calculation will at the same time determine λ after at most p^t-1 terms have been found.

12. We are now in a position to study the value of ρ in (11.2) in the general case when $\sigma=1$. We have from (10.3) and (11.41)

$$(12.1)\quad U^*(x)V(x) \equiv \theta\psi^{p^r}\phi^{p^r-a+b} + \phi^b\Theta_1 + p(\xi\psi^{p^r}\phi^{p^r-a} + \xi\Theta_1 + \phi^b\Theta_2) \pmod{p^2, F(x)}.$$

Hence ρ is greater than zero when and only when

$$\theta\psi^{p^r}\phi^{p^r-a+b} + \phi^b\Theta_1 \equiv 0 \pmod{p, F(x)};$$

that is, when and only when

$$(12.2)\quad \theta\psi^{p^r-a+b} + \phi^{p^{r-1}+b}\psi^{p^{r-1}}(1 - \tfrac{1}{2}\phi^{p^{r-1}}\psi^{p^{r-1}} + \cdots) \equiv 0 \pmod{p, \{\phi(x)\}^a}.$$

If $p^r-a+b \geqq a$, $p^{r-1}+b \geqq a$, (12.2) is satisfied for any choice of $\theta(x)$. In the contrary case, it is either insolvable or imposes a condition upon $\theta(x)$. We find in fact that there are no solutions in any one of the five following cases:

(i) $$p^r - a + b \geqq a,\ p^{r-1} + b < a;$$

(ii) $$p^r - a + b < a,\ p^{r-1} + b < a,\ p^r - a > p^{r-1};$$

(iii) $$\theta(x) \equiv 0 \pmod{p},\ p^{r-1} + b < a;$$

(iv) $$p^r - a + b < a,\ p^{r-1} + b < a,\ p^{r-1} \geqq p^r - a,$$
$$\theta(x) \not\equiv \kappa(x)\{\phi(x)\}^{p^{r-1}-p^r+a} \pmod{p},$$

where $\kappa(x)\{\psi(x)\}^{p^r-p^{r-1}}+1 \equiv 0 \pmod{p, \{\phi(x)\}^{2a-p^r-b}}$;

(v) $$p^r - a + b < a,\ p^{r-1} + b \geqq a,\ \theta(x) \not\equiv 0 \pmod{p, \{\phi(x)\}^{2a-p^r-b}}.$$

Thus generally speaking, if $\sigma=1$, $\rho=0$ unless $b \geqq a-p^{r-1}$, $b \geqq 2a-p^r$. Passing to this case, we have from (10.1), (11.21) and (12.1)

$$\begin{aligned} U^*(x)V(x) \equiv p\{&\theta^2\psi^{p^r}\phi^d + \theta\psi^{p^{r-1}}\phi^e(1 - \tfrac{1}{2}\psi^{p^{r-1}}\phi^{p^{r-1}} + \cdots) + \xi\psi^{p^r}\phi^{p^r-a} \\ &+ \xi\psi^{p^{r-1}}\phi^{p^{r-1}}(1 - \tfrac{1}{2}\psi^{p^{r-1}}\phi^{p^{r-1}} + \cdots) \\ &+ \phi^{b+p^{r-1}}\psi^{p^{r-1}}(-\tfrac{1}{2} + \tfrac{1}{2}\phi^{p^{r-1}}\psi^{p^{r-1}} - \cdots) \\ &+ \phi^{b+p^{r-2}}\psi^{p^{r-2}}(1 - \tfrac{1}{2}\psi^{p^{r-2}}\phi^{p^{r-2}} + \cdots)\} \pmod{p^2, F(x)}, \end{aligned}$$

where the last group of terms within the bracket must be replaced by $\phi^b\zeta(x)(1-\psi\phi+\cdots)$ if $r=1$, and the exponents d and e in the first two groups of terms are $\geqq 0$ and have the values p^r-2a+b, $p^{r-1}+b-a$.

Hence $\rho=1$ unless the expression in brackets above is congruent to zero (modd p, $F(x)$) or

$$(12.3)\quad \begin{aligned} &\theta^2\psi^{p^r}\phi^d + \theta\psi^{p^{r-1}}\phi^e + \xi\psi^{p^r}\phi^{p^r-a} + \xi\psi^{p^{r-1}}\phi^{p^{r-1}} + \phi^{b+p^{r-1}}\psi^{p^{r-1}} + \phi^{b+p^{r-2}}\psi^{p^{r-2}} \\ &\quad + \phi^{b+2p^{r-2}}E + \xi\phi^{2p^{r-1}}F + \phi^{b+2p^{r-1}}G + \theta\phi^{e+p^{r-1}}H \equiv 0 \pmod{p, \phi^a}, \end{aligned}$$

where E, F, G, H denote polynomials in x which are not congruent to zero (modd p, $\phi(x)$) with integral coefficients modulo p. The terms $\phi^{b+2p^{r-2}}E + \phi^{b+p^{r-2}}\psi^{p^{r-2}}$ must be replaced by $\phi^b\zeta + \phi^{b+1}\zeta E$ if $r=1$.

It is not difficult to show that the lowest exponent of ϕ occurring in (12.3) is either d or e so that (12.3) imposes a condition upon $\theta(x)$ of the type appearing under (12.2),

$$\theta(x) \equiv \{\phi(x)\}^g \kappa(x) \qquad (\text{mod } p).$$

The exponent g here depends upon the relative magnitudes of a, b, p^r, p^{r-1}, p^{r-2} but may be shown to be positive. We may therefore state the following theorem:

THEOREM 12.1. *If p is an odd prime, $F(x) = \{\phi(x)\}^a + p\theta(x)$, $a>1$, $\theta(x) \not\equiv 0$ (modd p, $\phi(x)$), then ρ in* (11.2) *is unity if $p^r+b \geqq 2a$, $p^{r-1}+b \geqq a$ and zero otherwise. If $\theta(x) \equiv 0$ (mod p), ρ is zero if $p^{r-1}+b<a$, and if $p^{r-1}+b \geqq a$ it is unity unless both p^r-a and p^{r-1} are $\leqq b+p^{r-2}$ and $\theta(x)$ satisfies a special condition. If $\theta(x) \equiv 0$ (modd p, $\phi(x)$) $\not\equiv 0$ (mod p), the same results usually apply unless $F(x)$ is of a special form similar to that of $F_1(x)$ in Theorem* 11.4.

13. We shall conclude by discussing the case when the exponent a in (10.1) is unity so that

$$F(x) = \phi(x) - p\theta(x). \tag{13.1}$$

A necessary condition for this to hold is that p should not divide the discriminant of $F(x)$. Hence if this discriminant is not zero, the results of this section will apply to the powers of all primes save a finite number.

If the sequence (u) is not divisible by p, Res $\{U(x), F(x)\}$ is necessarily prime to p, so that the characteristic number of (u) modulo p^N is the principal period of (1.1), and hence the characteristic number of the congruence

$$x^n \equiv 1 \qquad (\text{modd } p^N, F(x)).$$

With the notation of §10, let λ be the characteristic number of the congruence

$$x^n \equiv 1 \qquad (\text{modd } p, \phi(x)),$$

so that we have identically in x

$$\begin{aligned} x^\lambda - 1 &= \psi(x)\phi(x) + p\zeta(x), \\ \psi(x) &\not\equiv 0 \end{aligned} \qquad (\text{modd } p, \phi(x)). \tag{13.2}$$

We shall now establish the following comprehensive theorem:

THEOREM 13.1. *Let p be an odd prime, $\phi(x)$ an irreducible polynomial modulo p, and suppose that the polynomial $F(x)$ associated with the difference equation* (1.1) *is of the form* (13.1). *Furthermore, let*

$$F_2(x) = \phi(x) - p\theta_1(x)$$

where $\xi(x) = \theta_1(x)$ is a solution of the congruence

$$\psi(x)\xi(x) + \zeta(x) \equiv 0 \qquad (\text{modd } p, \phi(x)),$$

$\psi(x)$ and $\zeta(x)$ being given† *by* (13.2) .

Then if $F(x) \not\equiv F_2(x)$ (mod p^2), *the characteristic number modulo p^N of any solution of* (1.1) *which is not divisible by p is $p^{N-1}\lambda$, where λ is the least value of n such that*

$$x^n \equiv 1 \qquad (\text{modd } p, \phi(x)).$$

On the other hand, if $F(x) \equiv F_2(x)$, mod p^2, *there exists a set of polynomials $F_2(x), F_3(x), \cdots, F_T(x), \cdots$, depending only upon p, $\phi(x)$, $\psi(x)$ and $\zeta(x)$, such that if $F(x) \equiv F_T(x)$* (mod p^T), $\not\equiv F_{T+1}(x)$ (mod p^{T+1}), *the characteristic number is λ or $p^{N-T}\lambda$ according as $N \leqq T$ or $N \geqq T$.*

We have

$$x^\lambda - 1 = \psi(x)F(x) + p(\theta(x)\psi(x) + \zeta(x)).$$

Suppose first that $\theta(x)\psi(x) + \zeta(x) \not\equiv 0$ (modd p, $\phi(x)$). Then

$$x^\lambda \equiv 1 + pK(x) \qquad (\text{mod } F(x))$$

where $K(x)$ is of lesser degree than $F(x)$ and not divisible by p. On raising this last congruence to the p^rth power, we obtain

$$x^{p^r\lambda} \equiv 1 + p^{r+1}K(x) + \frac{p^r(p^r-1)}{1\cdot 2}p^2K(x) + \cdots \qquad (\text{mod } F(x)). \tag{13.3}$$

Hence if p is an odd prime,

$$x^{p^r\lambda} \equiv 1 + p^{r+1}K(x) \qquad (\text{modd } p^{r+2}, F(x)).$$

But clearly

$$x^{p^{r+1}\lambda} \equiv 1 \qquad (\text{modd } p^{r+2}, F(x)).$$

Since the characteristic number of (13.1) for $N = r+2$ is a multiple of its characteristic number for $N = r+1$, it is exactly equal to $p^{N-1}\lambda$.

Now let us assume that

† They may be determined sufficiently to define $F_2(x)$ by the procedure sketched in §11.

$$\psi(x)\theta(x) + \zeta(x) \equiv 0 \qquad (\text{modd } p, \phi(x)).$$

This congruence has a unique solution modulo p of degree less than $\phi(x)$. Let us denote it by $\theta_1(x)$, and set

$$F_2(x) = \phi(x) - p\theta_1(x).$$

Then if $F(x) \not\equiv F_2(x) \pmod{p^2}$, $\theta(x) \not\equiv \theta_1(x) \pmod{p}$. Consequently $\psi(x)\theta(x) + \zeta(x) \not\equiv 0$ (modd p, $\phi(x)$) and the argument just given is applicable. Assume then that

$$F(x) \equiv F_2(x) \qquad (\text{mod } p^2).$$

Consider the polynomials

$$F_1(x), F_2(x), F_3(x), \cdots, F_k(x), \cdots$$

defined by the recursive relations†

$$\begin{aligned} &F_k(x) = \phi(x) - p\Theta_{k-1}(x), \quad \Theta_k(x) = \Theta_{k-1}(x) + p^{k-1}\theta_k(x), \quad \Theta_0(x) = 0, \\ &\psi(x)\Theta_{k-1}(x) + \zeta(x) \equiv p^{k-1}r_k(x) \qquad (\text{modd } p^k, F_k(x)), \\ &\psi(x)\theta_k(x) + r_k(x) \equiv 0 \qquad (\text{modd } p, \phi(x)), \; k = 1, 2, 3, \cdots. \end{aligned} \tag{13.4}$$

These relations are consistent with one another; for if $k=1$ they give $F_1(x) = \phi(x)$ and for $k=2$ they give the polynomial $F_2(x)$ defined above. If we assume that they are consistent for $k=1, 2, 3, \cdots, s$ it easily follows that they are consistent for $k=s+1$.

Now suppose that

$$F(x) \equiv F_T(x) \pmod{p^T}, \not\equiv F_{T+1}(x) \pmod{p^{T+1}}, \; T \geqq 2.$$

Then

$$x^\lambda - 1 \equiv 0 \; (\text{modd } p^T, F(x)), \not\equiv 0 \; (\text{modd } p^{T+1}, F(x)).$$

For by (13.2) and the relations (13.4),

$$\begin{aligned} x^\lambda - 1 &= \psi(x)\phi(x) + p\zeta(x) = \psi(x)\{F_T(x) + p\Theta_{T-1}(x)\} + p\zeta(x) \\ &= \psi(x)F_T(x) + p(\psi(x)\Theta_{T-1}(x) + \zeta(x)) \\ &\equiv p(\psi(x)\Theta_{T-1}(x) + \zeta(x)) \qquad (\text{mod } F_T(x)) \\ &\equiv p \cdot p^{T-1}r_{T-1}(x) \qquad (\text{modd } p^T, F_T(x)) \\ &\equiv 0 \qquad (\text{modd } p^T, F_T(x)), \qquad \equiv 0 \qquad (\text{modd } p^T, F(x)). \end{aligned}$$

In like manner it can be shown that

$$x^\lambda - 1 \not\equiv 0 \qquad (\text{modd } p^{T+1}, F(x)).$$

† The $\Theta(x)$ here have no connection with those of §11.

Hence we have

$$x^{\lambda} \equiv 1 + p^{T}K(x) \qquad (\operatorname{mod} F(x)),$$

where $K(x) \not\equiv 0$ (modd p, $F(x)$). On raising this congruence to the appropriate power, we find that whether p be even or odd the characteristic number is $p^{N-T}\lambda$ or λ according as $N \geqq T$ or $N \leqq T$.

The case $p=2$, $T=1$ demands separate treatment. If $\theta(x)\psi(x)+\zeta(x) \equiv K(x) \not\equiv 0$ (modd 2, $\phi(x)$), we obtain from (12.3), on putting $p=2$,

$$x^{2^r\lambda} = 1 + 2^{r+1}K(x)(1 + (2^r - 1)K(x) + \cdots) \equiv 1 + 2^{r+1}K(x)(1 - K(x)) \qquad (\text{modd } 2^{r+2}, F(x)).$$

If $K(x) \not\equiv 1$ (mod 2), the previous argument for p odd is applicable. But in case $K(x) \equiv 1$ (mod 2), the characteristic number is a divisor of $2^r\lambda$.

Since $K(x)$ is of lesser degree than $F(x)$, the most general assumption is that

$$K(x) + 1 = 2^s L(x) \text{ where } L(x) \not\equiv 0 \qquad (\text{mod } 2).$$

Then

$$x^{\lambda} \equiv -1 + 2^{s+1}L(x) \qquad (\operatorname{mod} F(x)), \tag{13.5}$$

$$x^{2\lambda} \equiv 1 \qquad (\text{modd } 2^{s+2}, F(x)).$$

Hence if $N=1$, the characteristic number is λ, while if $s+2 \geqq N > 1$, the characteristic number is 2λ. On raising (13.5) to a power of 2, we find that if $N \geqq s+2$, the characteristic number is $2^{N-s-1}\lambda$.

These results determine the characteristic number in the excluded case of (11.1) when $\sigma=1$ and $p=2$ for all $F(x)$ of the form $\phi(x)-2\theta(x)$. The further discussion of the characteristic number for powers of 2 demands a special treatment which will be given elsewhere.

California Institute of Technology,
Pasadena, Calif.