THE DISTRIBUTION OF RESIDUES IN A SEQUENCE SATISFYING A LINEAR RECURSION RELATION*

BY
MORGAN WARD

I. INTRODUCTION

1. Statement of problem. Let

$(W)_n$: $\qquad W_0, W_1, \cdots, W_n, \cdots$

denote a sequence of integers satisfying the linear difference equation of order $r=3$,

$$\Omega_{n+3} = P\Omega_{n+2} - Q\Omega_{n+1} + R\Omega_n, \quad R \neq 0, \tag{1.1}$$

where P, Q, R, W_0, W_1, W_2 are fixed integers.†

If m is a positive integer, and if

$$W_n \equiv A_n \bmod m, \quad 0 \leqq A_n \leqq m-1,$$

we shall call

$(A)_n$: $\qquad A_0, A_1, \cdots, A_n, \cdots$

the *reduced sequence corresponding to* $(W)_n$, *modulo* m.

It is easily shown the $(A)_n$ is periodic; following Carmichael,‡ we shall call its smallest period, τ, the *characteristic number* of $(W)_n$ modulo m.

The object of this memoir is to attack the following fundamental distribution problem:§

Given the numerical values of the integers P, Q, R, W_0, W_1, W_2, m *and* τ, *to determine the distribution of the residues* $0, 1, 2, \cdots, m-1$ *among any* τ *terms of the reduced sequence* $(A)_n$.

There are really two distinct problems involved here: the determination of the particular place a given residue occurs in $(A)_n$ and the determination of the number of times a given residue occurs in any τ terms of $(A)_n$. Both

* Presented to the Society, November 29, 1929; received by the editors in January, 1930.

† For references to investigations of (1.1) see Dickson's *History*, vol. 1, chapter 17. For a general discussion of the problems in number theory connected with (1.1), see Carmichael, American Mathematical Monthly, vol. 36 (1929), pp. 132–143.

‡ Carmichael, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 344–345.

§ As far as I am aware, this problem has not been explicitly considered for difference equations of order greater than two. In a paper which has already appeared in these Transactions I have considered the problem of determining τ, given P, Q, R, W_0, W_1, W_2 and m.

problems may be readily solved in particular cases. Consider for example the difference equation $\Omega_{n+3}=\Omega_{n+2}+\Omega_{n+1}-\Omega_n$ with $W_0=0$, $W_1=1$, $W_2=2$. But the general solution of either problem presents considerable difficulties.*

I shall confine myself here almost entirely to the second, simpler, distribution problem for the special case when m is a prime p and the characteristic function of (1.1),

$$F(x) = x^3 - Px^2 + Qx - R, \tag{1.2}$$

is irreducible modulo p. A discussion of this case is a necessary preliminary to the more complicated cases when m is composite or when the characteristic function (1.2) is reducible modulo p.

2. **Plan of paper and principal results.** Let $k(i)=k_i$ denote the number of times the least positive residue $i \pmod p$ occurs in the first τ terms

$$(A): \qquad A_0, A_1, \cdots, A_{\tau-1}$$

of any reduced sequence $(A)_n \pmod p$.† Regarding k_i as a function of i, we shall speak of it as the *distribution function for the cycle* (A) *of* $F(x)$ *associated with* $(A)_n$ *and* $(W)_n$.

If we know the distribution function for the cycle (A), then we will know it for the cycle (B) if the three initial values B_0, B_1, B_2 of (B) happen to be three consecutive elements of (A). It is thus important to be able to tell from the initial values of two sequences whether or not their cycles are distinct. This problem is dealt with in §§6 and 7, where it is reduced to the problem of determining whether or not any given three consecutive residues appear in a *fixed* cycle (K) of $F(x)$. The preliminary definitions and results needed there and in the body of the paper are developed in §§3, 4, and 5. In §8 I digress slightly to give some results connected with the first distribution problem.

In §9 I prove that the number of zeros that can occur in each cycle of $F(x)$ are not independent of one another, but must satisfy two simple diophantine equations. In §10, I apply this result to determine completely the number of zeros which can occur in any cycle of $F(x)$ when $\tau=(p^2+p+1)/3$. In §11 I prove that if $\tau=p^2+p+1$, then every residue occurs in every cycle at least once.

In §12 it is proved that the distribution problem is essentially the same for all difference equations (1.1) with the same characteristic number τ

* In connection with the first problem, probably the best known result is that if $W_0=3$, $W_1=P$, $W_2=P^2-2Q$ and p is a prime, then $W_n\equiv W_{np}\equiv W_{np^2} \bmod p$. In §8 of this paper I shall give several new results of a similar character.

† We shall omit the words "modulo p" when no confusion can arise.

modulo p, and that it can be reduced to the case when τ divides p^2+p+1 and is prime to 3.

In §13, I show that the distribution function $k(n)$ for any cycle (A) is known as soon as we know the least positive residues of k_i modulis p and 3. In particular, k_0 is known as soon as its residue modulo p is known.

In §15, I give an explicit formula which determines k_i modulo p as the residue of a summation taken over the solutions of a certain diophantine system. This system is discussed fully in §14, and a general method of solving it is given. I have been unable to determine the residue of k_i modulo 3 save in special cases.

In §16, I apply my results to various special cases, obtaining theorems like the following:

If $p=3N+1$, $3\tau=p^2+p+1$, *and* k_0 *is the number of terms divisible by* p *in the first* τ *terms of* $(S)_n$, *where* $S_0=3$, $S_1=P$, $S_2=P^2-2Q$, *then* k_0 *is the least positive residue modulo* p *of* $(2N+1)(1+3N!/(N!)^3)$.

Finally in §17, I give a method for obtaining an upper limit to the size of k_i for any (A) and τ.

3. **Preliminary definitions. Triads.** Let the roots of $F(x)=0$ in the Galois field of order p^3 associated with $F(x)$ be denoted by* α, α^p, α^{p^2}, and suppose that

$$\alpha^n + \alpha^{pn} + \alpha^{p^2 n} \equiv S_n \mod p \quad \begin{pmatrix} 0 \leqq S_n \leqq p-1, \\ n = 0, \pm 1, \pm 2, \cdots \end{pmatrix}.$$

Then

$$S_1 \equiv P, \quad RS_{-1} \equiv Q, \quad \alpha^{1+p+p^2} \equiv R \mod p.$$

We shall refer to the p numbers

$$0, 1, 2, \cdots, p-1$$

which form a sub-field in the Galois field as *residues*. The characteristic number τ is simply the exponent to which α belongs in the Galois field; we shall also refer to it as the *period* of $F(x)$ (modulo p).

The τ residues $A_0, A_1, \cdots, A_{\tau-1}$ of any reduced sequence $(A)_n$ will be said to form a *cycle belonging to* $F(x)$. The cycle (S), where S_n is defined above, will be called the *principal cycle* of $F(x)$.

An ordered set of three residues (or more generally, of three rational integers) A', B', C' will be called a *triad*, and denoted by $[A', B', C']$. The τ triads

$$[A_0, A_1, A_2], \ [A_1, A_2, A_3], \cdots, [A_{\tau-2}, A_{\tau-1}, A_0], \ [A_{\tau-1}, A_0, A_1]$$

will be called the *triads belonging to the cycle* (A).

* For the properties of Galois fields which are assumed here, see Dickson, *Linear Groups*, Leipzig, 1901.

Two triads are equal when and only when they are identical modulo p; two cycles are equal if one may be derived from the other by a cyclic permutation of its elements. It is clear that any cycle is completely specified by any one of its triads; furthermore, two given cycles have either all or none of their triads in common.

The cycles whose initial triads are [1, 0, 0], [0, 1, 0], and [0, 0, 1] will be denoted by (X), (Y), and (Z) respectively.*

4. **Multipliers and blocks.** If L is any residue such that the cycles

$$LA_0, LA_1, \cdots, LA_{\tau-1} \text{ and } A_0, A_1, \cdots, A_{\tau-1}$$

are equal (modulo p), L is called a *multiplier* of (A).

In the paper previously referred to, I have shown that every cycle of $F(x)$ has the same multipliers, and that there exists a unique "basic multiplier" M such that every other multiplier is congruent to some power of M.

It follows that if $e=\epsilon(M)$ denotes the exponent to which M belongs modulo p, then there are exactly e distinct multipliers. e moreover divides τ and the quotient divides p^2+p+1. If we write $\tau=\epsilon(M)\mu$, $\mu \mid p^2+p+1$, then μ is called the restricted period† of $F(x)$.

Let

$$et = p - 1, \quad \mu\kappa = p^2 + p + 1.$$

Then there are exactly t distinct cycles modulo p among the $p-1$ cycles

$$XA_0, XA_1, \cdots, XA_{\tau-1} \qquad (X = 1, 2, \cdots, p - 1).$$

These t cycles will be said to form a *block* of cycles. There are in all exactly κ distinct blocks of cycles; we shall denote them by the capital German letters $\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_\kappa$.

In particular, it will be understood that $\mathfrak{B}_1$ is the block containing the principal cycle (S).

The number of times a given residue appears in a given block is given by the following easily established theorem.

THEOREM 4.1. *If b_0 denotes the number of times the residue 0 appears in the first μ terms of any cycle of a given block $\mathfrak{B}$, then every residue other than zero appears in $\mathfrak{B}$ exactly $\mu-b_0$ times, while the residue zero appears $(p-1)b_0$ times.*

5. **Illustration.** In order to clarify the definitions of the preceding two sections, we give all the cycles of $F(x)=x^3+3x^2+4x+1$ for $p=7$, and a list of the notations introduced.

* For a number of algebraic properties of the associated sequences, see Bell, Tôhoku Mathematical Journal, vol. 24 (1924), pp. 169–184. The terms of the principal cycle (S) and (X), (Y), (Z) are connected by the simple relation $S_n \equiv X_n+Y_{n+1}+Z_{n+2} \bmod p$.

† This term is due to Carmichael, who uses it in a slightly more general sense. See Quarterly Journal paper, p. 354.

COMPLETE CYCLES, GROUPED BY BLOCKS

$\mathfrak{B}_1$

$$\begin{matrix}3, & 4, & 1, & 6, & 2, & 4, & 2, & 4, & 4, & 5, & 0, & 4, & 4, & 0, & 1, & 0, & 3, & 4, & 4,\\ 4, & 3, & 6, & 1, & 5, & 3, & 5, & 3, & 3, & 2, & 0, & 3, & 3, & 0, & 6, & 0, & 4, & 3, & 3.\end{matrix}$$

$$\begin{matrix}6, & 1, & 2, & 5, & 4, & 1, & 4, & 1, & 1, & 3, & 0, & 1, & 1, & 0, & 2, & 0, & 6, & 1, & 1,\\ 1, & 6, & 5, & 2, & 3, & 6, & 3, & 6, & 6, & 4, & 0, & 6, & 6, & 0, & 5, & 0, & 1, & 6, & 6.\end{matrix}$$

$$\begin{matrix}2, & 5, & 3, & 4, & 6, & 5, & 6, & 5, & 5, & 1, & 0, & 5, & 5, & 0, & 3, & 0, & 2, & 5, & 5,\\ 5, & 2, & 4, & 3, & 1, & 2, & 1, & 2, & 2, & 6, & 0, & 2, & 2, & 0, & 4, & 0, & 5, & 2, & 2.\end{matrix}$$

$\mathfrak{B}_2$

$$\begin{matrix}0, & 0, & 1, & 4, & 5, & 3, & 2, & 5, & 2, & 0, & 1, & 2, & 4, & 0, & 3, & 1, & 6, & 3, & 1,\\ 0, & 0, & 6, & 3, & 2, & 4, & 5, & 2, & 5, & 0, & 6, & 5, & 3, & 0, & 4, & 6, & 1, & 4, & 6.\end{matrix}$$

$$\begin{matrix}0, & 0, & 2, & 1, & 3, & 6, & 4, & 3, & 4, & 0, & 2, & 4, & 1, & 0, & 6, & 2, & 5, & 6, & 2,\\ 0, & 0, & 5, & 6, & 4, & 1, & 3, & 4, & 3, & 0, & 5, & 3, & 6, & 0, & 1, & 5, & 2, & 1, & 5.\end{matrix}$$

$$\begin{matrix}0, & 0, & 3, & 5, & 1, & 2, & 6, & 1, & 6, & 0, & 3, & 6, & 5, & 0, & 2, & 3, & 4, & 2, & 3,\\ 0, & 0, & 4, & 2, & 6, & 5, & 1, & 6, & 1, & 0, & 4, & 1, & 2, & 0, & 5, & 4, & 3, & 5, & 4.\end{matrix}$$

$\mathfrak{B}_3$

$$\begin{matrix}0, & 1, & 3, & 1, & 5, & 6, & 3, & 4, & 5, & 1, & 1, & 2, & 3, & 3, & 5, & 5, & 4, & 5, & 6,\\ 0, & 6, & 4, & 6, & 2, & 1, & 4, & 3, & 2, & 6, & 6, & 5, & 4, & 4, & 2, & 2, & 3, & 2, & 1.\end{matrix}$$

$$\begin{matrix}0, & 2, & 6, & 2, & 3, & 5, & 6, & 1, & 3, & 2, & 2, & 4, & 6, & 6, & 3, & 3, & 1, & 3, & 5,\\ 0, & 5, & 1, & 5, & 4, & 2, & 1, & 6, & 4, & 5, & 5, & 5, & 3, & 1, & 4, & 4, & 6, & 4, & 2.\end{matrix}$$

$$\begin{matrix}0, & 3, & 2, & 3, & 1, & 4, & 2, & 5, & 1, & 3, & 3, & 6, & 2, & 2, & 1, & 1, & 5, & 1, & 4,\\ 0, & 4, & 5, & 4, & 6, & 3, & 5, & 2, & 6, & 4, & 4, & 1, & 5, & 5, & 6, & 6, & 2, & 6, & 3.\end{matrix}$$

For this case, $p-1=6$, $p^2+p+1=57$, $M=6$, $e=2$, $t=3$, $\mu=19$, $\kappa=3$, $\tau=38$ and in $\mathfrak{B}_1$, $b_0=3$.

LIST OF NOTATION

Characteristic number, period of $F(x)$; Number of elements or triads in a cycle: τ

Number of cycles in a block: t

Number of blocks: κ

Restricted period of $F(x)$: μ

Basic multiplier: M

Exponent to which M belongs modulo p: $e=\epsilon(M)$.

Connecting relations: $\mu\kappa=p^2+p+1$, $et=p-1$, $\tau=e\mu$.

Triad: $[U, V, W]$

Cycle: (A)

Block: $\mathfrak{B}$

II. The distribution of triads

6. **Invariant of a cycle.** Let us assume that we know the distribution functions of the cycles $(U), (V), \cdots, (W)$ and that we are given the initial values $A_0=K, A_1=L, A_2=M$ of some cycle (A). Then if the triad $[K, L, M]$ occurs in one of the cycles $(U), (V), \cdots, (W)$, the distribution function of (A) is also known. We are thus led to consider the problem of determining to what cycle any given triad belongs. In this section we shall restrict ourselves to the simplest case, when we know beforehand that the triad belongs to a certain block.

First, if α, β, γ are the roots of

$$F(x) = x^3 - Px^2 + Qx - R = 0 \tag{6.1}$$

and

$$W_n = \sum_{(\alpha)}(K_0 + K_1\alpha + K_2\alpha^2)\alpha^n \qquad (n = 0, 1, \cdots)$$

is the general term of any sequence $(W)_n$ satisfying (1.1), then it is easily shown that the determinant

$$D_n(W) = \begin{vmatrix} W_n, & W_{n+1}, & W_{n+2} \\ W_{n+1}, & W_{n+2}, & W_{n+3} \\ W_{n+2}, & W_{n+3}, & W_{n+4} \end{vmatrix}$$

has the value

$$D_n(W) = R^n\Delta N(w), \tag{6.11}$$

where R is the constant term of the characteristic equation (6.1), Δ is the discriminant of $F(x)$, and $N(w)$ the norm of the algebraic number $w=K_0+K_1\alpha+K_2\alpha^2$.

Consequently, if $\epsilon(R)$ denotes the exponent to which R belongs modulo p, and if (A) is the cycle corresponding to $(W)_n$ modulo p, then the value of

$$J(A) \equiv [\Delta_n(A)]^{\epsilon(R)} \mod p$$

is independent of n. We shall call this residue the *invariant* of the cycle (A).

By means of (1.1), we can express the determinant $\Delta_n(W)$ as a polynomial in W_n, W_{n+1}, W_{n+2}. If we define $\Lambda(K, L, M)$ for all values of its arguments to be the polynomial

$$\begin{aligned}\Lambda(K, L, M) = &- R^2K^3 + 2QRK^2L - PRK^2M - (PR + Q^2)KL^2 \\ &+ (PQ + 3R)KLM - QKM^2 + (PQ - R)L^3 - (P^2 + Q)L^2M \\ &+ 2PLM^2 - M^3,\end{aligned}$$

then

$$\Delta_n(W) = \Lambda(W_n, W_{n+1}, W_{n+2}). \tag{6.12}$$

Thus if A_0, A_1, A_2 are the initial values of any cycle (A), the invariant $J(A)$ is determined by the congruence

$$J(A) \equiv [\Lambda(A_0, A_1, A_2)]^{\epsilon(R)} \mod p.$$

Now if L is any constant residue, $\Delta_n(L\cdot W) = L^3\Delta_n(W)$. Hence if $(L\cdot A)$ denotes the cycle $LA_0, LA_1, \cdots, LA_{\tau-1}$,

$$J(L\cdot A) \equiv L^{3\epsilon(R)}J(A) \mod p. \tag{6.2}$$

In the work previously referred to, I have shown that either $\epsilon(M) = \epsilon(R)$ or $\epsilon(M) = 3\epsilon(R)$, where it will be recalled that $\epsilon(M)$ is the exponent to which the basic multiplier M belongs modulo p. If $p \equiv 2 \mod 3$, then $\epsilon(M)$ necessarily equals $\epsilon(R)$. Moreover, $L^{3\epsilon(M)} \equiv 1 \mod p$ when and only when $L^{\epsilon(M)} \equiv 1 \mod p$; hence, from (6.2) $J(L\cdot A) \equiv J(A) \mod p$ when and only when L is a multiplier of (A). A precisely similar result holds if $p \equiv 1 \mod 3$ and $\epsilon(M) = 3\epsilon(R)$.*

It follows that in these two cases if $(A^{(1)}), \cdots, (A^{(t)})$ are the t distinct cycles of a given block $\mathfrak{B}$, the invariants $J(A^{(1)}), \cdots, J(A^{(t)})$ are all incongruent to one another modulo p. We thus obtain the following theorem.

THEOREM 6.1. *If $p \equiv 2 \mod 3$ or $p \equiv 1 \mod 3$, and $\epsilon(M) = 3\epsilon(R)$, and if $[K, L, M]$ is any triad of the block $\mathfrak{B}$, then a necessary and sufficient condition that $[K, L, M]$ belong to the cycle (A) of $\mathfrak{B}$ is that*

$$\{\Lambda(K, L, M)\}^{\epsilon(R)} \equiv J(A) \mod p. \tag{6.3}$$

If $p \equiv 1 \mod 3$ and $\epsilon(M) = \epsilon(R)$ (which implies that $\epsilon(M) \not\equiv 0 \mod 3$), we cannot go quite so far. For if ω is a primitive cube root of unity modulo p, then

$$\Delta_n(\omega\cdot A) = \omega^3\Delta_n(A) \equiv \Delta_n(A) \mod p.$$

Consequently, since ω is not a multiplier, the three cycles (A), $(\omega\cdot A)$, $(\omega^2\cdot A)$ are distinct, and will have the same invariant. (6.3) must then be replaced by

$$\{\Lambda(K, L, M)\}^{\epsilon(R)} \equiv J(A) = J(\omega\cdot A) = J(\omega^2\cdot A),$$

and for any given triad $[K, L, M]$ of the block $\mathfrak{B}$, we can ascertain merely that it must be in one of three cycles of $\mathfrak{B}$.

* If $p = 3^lN+1$ sufficient conditions for $\epsilon(M) = 3\epsilon(R)$ are $\epsilon(R) \equiv 0 \mod 3$, $\not\equiv 0 \mod 3^k$; or R not a cubic residue of p.

7. Distribution of triads in cycles. Let

$$(K): \qquad K_0, K_1, \cdots, K_{\tau-1}$$

denote a fixed cycle of $F(x)$. We shall show that we can determine whether or not two triads $[A, B, C]$ and $[A', B', C']$ belong to the same cycle if we know all the triads which belong to (K).

If L_0, L_1, L_2 are determined by the congruences

$$\begin{aligned} A &\equiv L_0K_0 + L_1K_1 + L_2K_2, \\ B &\equiv L_0K_1 + L_1K_2 + L_2K_3, \\ C &\equiv L_0K_2 + L_1K_3 + L_2K_4, \end{aligned} \tag{7.1}$$

then a necessary and sufficient condition that $[A', B', C']$ should belong to the same cycle as $[A, B, C]$ is that for some value of m there should exist congruences of the form

$$\begin{aligned} A' &\equiv L_0K_m + L_1K_{m+1} + L_2K_{m+2}, \\ B' &\equiv L_0K_{m+1} + L_1K_{m+2} + L_2K_{m+3}, \\ C' &\equiv L_0K_{m+2} + L_1K_{m+3} + L_2K_{m+4}. \end{aligned} \tag{7.2}$$

Now, by means of the difference equation (1.1), we can express K_{m+3} and K_{m+4} in (7.2) linearly in terms of K_m, K_{m+1}, K_{m+2}. Write A'', B'', C'' for K_m, K_{m+1}, K_{m+2}. Then if we introduce the abbreviations $[LU]_i$ $(U=X, Y, Z;$ $i=1, 2, 3)$ for the sums $L_0U_i+L_1U_{i+1}+L_2U_{i+2}$, the equations (7.2) give the following values for A'', B'', C'':

$$A'' \equiv \frac{|A', [LY]_1, [LZ]_2|}{|[LX]_0, [LY]_1, [LZ]_2|}, \text{ etc.}, \tag{7.3}$$

where $|A', [LY]_1, [LZ]_2|$ stands for the determinant

$$\begin{vmatrix} A', & [LY]_0, & [LZ]_0 \\ B', & [LY]_1, & [LZ]_1 \\ C', & [LY]_2, & [LZ]_2 \end{vmatrix},$$

and so on.

If we treat (7.1) in a similar manner, letting $\{KX\}_i$ stand for the sum $K_0X_i+K_1Y_i+K_2Z_i$ $(i=0, 1, 2, 3, 4)$ we find that

$$L_0 \equiv \frac{|A, \{KX\}_2, \{KX\}_4|}{|\{KX\}_0, \{KX\}_2, \{KX\}_4|}, \text{ etc.}, \tag{7.4}$$

where $|A, \{KX\}_2, \{KX\}_4|$ stands for the determinant

$$\begin{vmatrix} A, & \{KX\}_1, & \{KX\}_2 \\ B, & \{KX\}_2, & \{KX\}_3 \\ C, & \{KX\}_3, & \{KX\}_4 \end{vmatrix}$$

and so on.

We thus obtain the following theorem.

THEOREM 7.1. *A necessary and sufficient condition that the triads* $[A, B, C]$ *and* $[A', B', C']$ *should belong to the same cycle is that the triad* $[A'', B'', C'']$ *determined by* (7.3) *and* (7.4) *should belong to the cycle* (K).

We have thus reduced the problem of determining to what cycle any triad belongs to the problem of determining whether or not a triad belongs to some fixed cycle, say the principal cycle of $F(x)$.

8. The distribution of zeros in a cycle. We shall assume in this section that the cycles of $F(x)$ have no multiplier other than the trivial multiplier unity which implies that τ divides p^2+p+1. The distribution of zeros in an arbitrary cycle (U) of $F(x)$ then depends in a remarkable manner upon the distribution of residues in the principal cycle (S), as is shown by the following theorem:

THEOREM 8.1. *Let* (U) *denote a definite cycle of* $F(x)$ *in which it is known that*

$$U_a \equiv U_b \equiv 0 \mod p \qquad (a \not\equiv b). \tag{8.1}$$

Then a necessary and sufficient condition that $U_c \equiv 0 \mod p$ *is that**

$$S_{a+bp+cp^2} \equiv S_{a+bp^2+cp} \mod p. \tag{8.2}$$

Let

$$U_n \equiv K_0 S_n + K_1 S_{n+1} + K_2 S_{n+2} \mod p. \tag{8.3}$$

Then (8.1) gives

$$K_0 : K_1 : K_2 = \begin{vmatrix} S_{a+1}, & S_{a+2} \\ S_{b+1}, & S_{b+2}. \end{vmatrix} : \begin{vmatrix} S_{a+2}, & S_a \\ S_{b+2}, & S_b \end{vmatrix} : \begin{vmatrix} S_a, & S_{a+1} \\ S_b, & S_{b+1} \end{vmatrix}.$$

Hence by (8.3)

$$U_n \equiv LD(a, b, n) \mod p,$$

where $D(a, b, n)$ denotes the determinant

$$\begin{vmatrix} S_a, & S_{a+1}, & S_{a+2} \\ S_b, & S_{b+1}, & S_{b+2} \\ S_n, & S_{n+1}, & S_{n+2} \end{vmatrix}$$

and L is a constant residue.

* In numerical cases the subscripts of the S are reduced modulo τ.

On expanding this determinant and substituting for S_a, S_b, etc.,

$$\alpha^a + \alpha^{pa} + \alpha^{p^2a}, \quad \alpha^b + \alpha^{pb} + \alpha^{p^2b} \text{ etc.},$$

we find that

$$D(a, b, n) \equiv S_{a+bp+np^2} - S_{a+bp^2+np} \pmod{p},$$

so that

$$U_n \equiv L(S_{a+bp+np^2} - S_{a+bp^2+np}) \qquad (n = 0, 1, \cdots, \tau - 1). \tag{8.31}$$

This proof would fail if

$$\begin{vmatrix} S_{a+1}, & S_{a+2} \\ S_{b+1}, & S_{b+2} \end{vmatrix}, \quad \begin{vmatrix} S_{a+2}, & S_a \\ S_{b+2}, & S_b \end{vmatrix}, \quad \begin{vmatrix} S_a, & S_{a+1} \\ S_b, & S_{b+1} \end{vmatrix}$$

should all be congruent to zero modulo p. But in this case

$$S_a \equiv MS_b, \quad S_{a+1} \equiv MS_{b+1}, \quad S_{a+2} \equiv MS_{b+2}$$

where M is a constant residue. Since the only multiplier of (S) is unity, $M = 1$ and $a = b$ contrary to hypothesis.

The following two theorems are direct corollaries of Theorem 8.1.

THEOREM 8.11. *If (Z) denotes the cycle* 0, 0, 1, $\cdots$, *then a necessary and sufficient condition that $Z_n \equiv 0 \bmod p$ is that $S_{n+p} \equiv S_{n+p^2} \bmod p$.*

THEOREM 8.12. *If (Y) denotes the cycle* 0, 1, 0, $\cdots$, *then a necessary and sufficient condition that $Y_n \equiv 0 \bmod p$ is that $S_{n+2p} \equiv S_{n+2p^2} \bmod p$.*

We have several times used the fact that if (S) is the principal cycle, $S_n \equiv S_{np} \equiv S_{np^2} \bmod p$. The following limited converse of this result is a direct consequence of Theorem 8.1.

THEOREM 8.2. *Let (U) be any cycle of $F(x)$. If for any $m \neq 0$ it is known that $U_m \equiv U_{pm} \equiv U_{p^2m} \equiv 0 \bmod p$, then $U_n \equiv KS_n$ $(n = 0, 1, \cdots, \tau - 1)$.*

The following congruences, which are all special cases of the easily established general formula

$$U_{n+m} + U_{n+pm} + U_{n+p^2m} \equiv U_nS_m \pmod{p},$$

give some curious arithmetical properties of cycles:

$$\begin{aligned} U_n + U_{pn} + U_{p^2n} &\equiv U_0S_n, \\ U_0 + U_{(p-1)n} + U_{(p^2-1)n} &\equiv U_{-n}S_n, \\ S_{n+m} + S_{n+pm} + S_{n+p^2m} &\equiv S_nS_m, \\ X_n + X_{pn} + X_{p^2n} &\equiv S_n, \\ Y_n + Y_{pn} + Y_{p^2n} &\equiv 0, \\ Z_n + Z_{pn} + Z_{p^2n} &\equiv 0 \pmod{p}. \end{aligned} \tag{8.4}$$

From Theorem 8.2, we see that it is impossible for Y_n, Y_{pn}, Y_{p^2n} or Z_n, Z_{pn}, Z_{p^2n} to be all congruent to zero modulo p simultaneously. From the last two formulas of (8.4), we see that it is also impossible for Y_n and Y_{pn} or Z_n and Z_{pn} to be congruent to zero simultaneously. In the succeeding section we shall prove a much more precise result of this character, which will enable us to obtain valuable information about the number of zeros in any cycle.

9. **Diophantine relations for the number of zeros in a cycle.** If the cycles of $F(x)$ have no multiplier save unity, each block of cycles contains $p-1$ distinct cycles. Let $\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_\kappa$ be the separate blocks, and let $(p-1)b_i$ be the number of zeros in $\mathfrak{B}_i$, so that each cycle of $\mathfrak{B}_i$ contains b_i zeros. Clearly, $\sum_{i=1}^{\kappa}(p-1)b_i = p^2-1$; hence

$$b_1 + b_2 + \cdots + b_\kappa = p + 1. \tag{9.1}$$

In this section I shall establish the additional formula

$$b_1^2 + b_2^2 + \cdots + b_\kappa^2 = \tau + p. \tag{9.2}$$

THEOREM 9.1. *Let a, b be any two distinct numbers $\geqq 0$, $< \tau$. Then there exists a cycle $U_0, U_1, \cdots, U_{\tau-1}$ such that*

$$U_a \equiv U_b \equiv 0 \mod p.$$

The τ residues

$$U_n \equiv \begin{vmatrix} S_n, & S_a, & S_b \\ S_{n+1}, & S_{a+1}, & S_{b+1} \\ S_{n+2}, & S_{a+2}, & S_{b+2} \end{vmatrix} \mod p$$

clearly form a cycle satisfying the conditions of the theorem.

THEOREM 9.2. *Let (U), (V) be any two cycles of $F(x)$, in which it is known that*

$$U_a \equiv U_b \equiv 0, \quad V_c \equiv V_d \equiv 0 \mod p.$$

Then a sufficient condition that (U) and (V) should belong to the same block is that $a-b \equiv c-d \bmod \tau$.

Let $V_n = W_{n+a-c}$ $(n = 0, 1, \cdots, \tau-1)$. Then $W_a \equiv W_b \equiv 0 \bmod p$. Hence if

$$U_n \equiv K_0S_n + K_1S_{n+1} + K_2S_{n+2}, \quad W_n \equiv L_0S_n + L_1S_{n+1} + L_2S_{n+2},$$

then

$$K_0S_a + K_1S_{a+1} + K_2S_{a+2} \equiv 0, \qquad L_0S_a + L_1S_{a+1} + L_2S_{a+2} \equiv 0,$$
$$K_0S_b + K_1S_{b+1} + K_2S_{b+2} \equiv 0, \qquad L_0S_b + L_1S_{b+1} + L_2S_{b+2} \equiv 0.$$

Hence* $L_0:L_1:L_2=K_0:K_1:K_2$, so that

$$V_{n+c-a} \equiv W_n \equiv MU_n \mod p \quad (n = 0, 1, \cdots, \tau - 1),$$

and (V) and (W) belong to the same block.

THEOREM 9.3. *If the cycle (U) has no multiplier save unity, and if U_{a_1}, $U_{a_2}, \cdots, U_{a_b}$ are the b residues of (U) congruent to zero modulo p, then the $b(b-1)$ differences $a_i-a_j (i, j=1, \cdots, b; i\neq j)$ are all incongruent modulo τ.*

If $a_i-a_j\equiv a_k-a_l \mod \tau$, then, by the previous theorem,

$$U_{a_i-a_k+n} \equiv MU_n \qquad (n = 0, 1, \cdots, \tau - 1).$$

Hence $M=1$ and $a_i-a_k\equiv 0 \mod \tau; i=k, j=l$.

THEOREM 9.4. *Let $(U^{(1)}), \cdots, (U^{(\kappa)})$ be κ cycles belonging to the blocks $\mathfrak{B}_1, \cdots, \mathfrak{B}_\kappa$, respectively, so that $(U^{(i)})$ contains exactly b_i zeros. Then*

$$\sum_{i=1}^{k} b_i(b_i - 1) = \tau - 1. \tag{9.21}$$

If $b_i<2$, $b_i(b_i-1)=0$. If $b_i\geqq 2$, then as in Theorem 9.3 the cycle $(U^{(i)})$ furnishes $b_i(b_i-1)$ differences a_i-a_j which are all incongruent modulo τ. But by Theorems 9.1 and 9.2, to each of the $\tau-1$ distinct differences a_k-a_l modulo τ there corresponds exactly one block such that for every cycle (U) of this block $U_{a_k}\equiv U_{a_l}\equiv 0 \mod p$. Hence (9.21) follows.

Formula (9.2) now follows from (9.21) and (9.1) by addition.

10. **Application to the case $\tau=(p^2+p+1)/3$.** We shall now apply the formulas of §9 to the case when $p=3N+1$ and when the characteristic number τ equals $(p^2+p+1)/3$. There are then only three blocks of cycles and no multipliers, so that (9.1) and (9.2) become

$$\begin{aligned} b_1 + b_2 + b_3 &= p + 1, \\ b_1^2 + b_2^2 + b_3^2 &= (p^2 + 4p + 1)/3. \end{aligned} \tag{10}$$

Moreover, since $\mathfrak{B}_1$ contains the principal cycle (S), $b_1\equiv 0 \mod 3$; for $S_n\equiv 0 \mod p$ implies that $S_{np}\equiv S_{np^2}\equiv 0 \mod p$. Thus we have the additional restrictions

$$b_1 \equiv 0 \mod 3, \quad 0 \leqq b_1, \ b_2, \ b_3 \leqq p + 1. \tag{10.1}$$

The theory of the diophantine system (10) and (10.1) is a special case of a theory of simultaneous quadratic and linear representation given by Dr. Gordon Pall in a forthcoming paper. I am indebted to Dr. Pall for the following result:

* It is impossible for the ratios to be indeterminate; see the proof of Theorem 8.1.

The system (10), (10.1) *always has a unique solution in positive integers. If* (ξ, η) *is that solution of* $\xi^2+3\eta^2=p$ *satisfying the condition* $\xi \equiv 2 \bmod 3$, *then the solution of* (10) *is given by*

$$b_1 = N + \tfrac{2}{3}(\xi + 1),\ b_2 = N + \eta - \tfrac{1}{3}(\xi - 2),\ b_3 = N - \eta - \tfrac{1}{3}(\xi - 2).$$

It should be noted that b_2 and b_3 are both congruent to 1 modulo 3, and distinct.

In §17, we shall return to this case and obtain the values of b_1, b_2, b_3 by quite a different method.

The next simplest case is when $\tau=(p^2+p+1)/7$. Pall's theory allows us to reduce the solution of (9.1) and (9.2) to a single equation in six variables, but unfortunately this new equation has a large number of possible solutions.

11. **Minimum number of residues of a cycle.** I shall conclude this part of the paper by proving the following theorem:

THEOREM. *If the characteristic number* τ *equals* p^2+p+1, *then every residue appears in every cycle of* $F(x)$ *at least once.*

Under the hypothesis of the theorem, there are $p-1$ cycles grouped in a single block $\mathfrak{B}$; hence it is sufficient to prove that every residue appears in the cycle (S) at least once.

Consider the $(p-1)^3-1$ triads which do not contain a particular residue K. If U, V, W stand for distinct residues, these triads may be grouped into five classes; namely,

$$\begin{aligned}
m_1 &= (p-1)(p-2)(p-3) && \text{triads of type } [U, V, W];\\
m_2 &= (p-1)(p-2) && \text{“ } [U, V, U];\\
m_3 &= (p-1)(p-2) && \text{“ } [U, U, V];\\
m_4 &= (p-1)(p-2) && \text{“ } [U, V, V];\\
m_5 &= (p-2) && \text{“ } [U, U, U].
\end{aligned}$$

Let μ_i be the number of triads of type i which appear in (S). To each triad of type 1 there correspond $p-4$ distinct triads of type 1 in the block of cycles $L(S)$; namely, those for which

$$LU \not\equiv K,\ LV \not\equiv K,\ LW \not\equiv K \mod p \quad (L = 1, 2, \cdots, p-1).$$

Therefore,

$$(p-4)\mu_1 \leqq m_1, \text{ or } \mu_1 < (p-1)(p-2).$$

Similarly,

$$\mu_2 < p-1;\ \mu_3 < p-1;\ \mu_4 < p-1;\ \mu_5 < 1.$$

Accordingly, if the residue K does not appear in (S),

$$\tau = \mu_1 + \mu_2 + \mu_3 + \mu_4 + \mu_5 < (p-1)(p-2) + 3(p-1) + 1 = p^2,$$

giving a contradiction.

III. Determination of distribution function

12. **Reduction to the case when τ is prime to 3 and divides p^2+p+1.** We shall now show that it is sufficient to determine the distribution functions for difference equations whose characteristic number is prime to 3 and divides p^2+p+1.

Let $F(x)$ and $F'(x)$ be two irreducible cubics modulo p with the periods τ and τ', where $F'(x)$ is so chosen that τ' divides τ. Write

$$\tau = \tau' k'. \tag{12.1}$$

Let the roots of $F(x)=0$ and $F'(x)=0$ be denoted by α, β, γ; α', β', γ' respectively. We then have in the Galois field associated with $F(x)$ a congruence of the form

$$\alpha' \equiv \alpha^{k's} \mod p. \tag{12.2}$$

s here is a fixed integer prime to τ depending on our choice of $F'(x)$.

Now let (U') be any cycle of $F'(x)$. Then

$$U_n' \equiv \sum_{(\alpha')} (K_0 + K_1\alpha' + K_2\alpha'^2)\alpha'^n \qquad (n = 0, 1, \cdots, \tau'-1).$$

Hence by (12.2)

$$U_n' \equiv \sum_{(\alpha)} (L_0 + L_1\alpha + L_2\alpha^2)\alpha^{nk's}$$

where

$$\begin{aligned} &L_0 \equiv X_0K_0 + X_{k's}K_1 + X_{2k's}K_2;\ L_1 \equiv Y_0K_0 + Y_{k's}K_1 + Y_{2k's}K_2; \\ &L_2 \equiv Z_0K_0 + Z_{k's}K_1 + Z_{2k's}K_2. \end{aligned} \tag{12.3}$$

L_0, L_1, L_2 cannot moreover all be congruent to zero modulo p, for if Δ and Δ' are the discriminants of $F(x)$ and $F'(x)$,

$$\begin{vmatrix} X_0, & X_{k's}, & X_{2k's} \\ Y_0, & Y_{k's}, & Y_{2k's} \\ Z_0, & Z_{k's}, & Z_{2k's} \end{vmatrix} \equiv \Delta'/\Delta \not\equiv 0 \mod p.$$

Write

$$\begin{aligned} A &\equiv L_0S_0 + L_1S_1 + L_2S_2, \\ B &\equiv L_0S_1 + L_1S_2 + L_2S_3, \\ C &\equiv L_0S_2 + L_1S_3 + L_2S_4. \end{aligned} \tag{12.31}$$

Then A, B, C are the initial values of the sequence (U) where

$$U_n \equiv \sum_{(\alpha)}(L_0 + L_1\alpha + L_2\alpha^2)\alpha^n \quad (n = 0, 1, \cdots, \tau - 1)$$

and we have the formula

$$U_n' \equiv U_{nk's} \mod p \qquad (n = 0, 1, \cdots, \tau' - 1). \tag{12.4}$$

The process by which we obtained (U) from (U') fixed the initial elements of (U); if we remove this restriction, then if we are given (U), τ' and s, by letting $[A, B, C]$ in (12.31) equal successively the triads $[U_0, U_1, U_2]$, $[U_1, U_2, U_3], \cdots, [U_{k'-1}, U_{k'}, U_{k'+1}]$, K_0, K_1, K_2 are obtained from (12.3), so that (U') is known, and (12.4) is replaced by the more general relation

$$U_n' \equiv U_{nk's+r} \qquad (n = 0, 1, \cdots, \tau' - 1; 0 \leqq r < k'). \tag{12.41}$$

Since ns in (12.4) or (12.41) runs through a complete residue system modulo τ', the result we have obtained may be formulated as follows:

THEOREM 12.1. *Any cycle (U') of $F'(x)$ can be obtained from some cycle (U) of $F(x)$ by selecting from (U) terms whose subscripts lie in an arithmetical progression of constant difference k', and arranging them in a suitable order.*

A cycle (U') obtained in this manner from some cycle (U) of $F(x)$ will be called a *derived* cycle of (U). On taking $\tau' = \tau$, we obtain the following:

THEOREM 12.2. *If $F(x)$ and $F'(x)$ are two irreducible cubics modulo p with the same characteristic number τ, and if (U') is any cycle of $F'(x)$, then there exists a cycle (U) of $F(x)$ with the same distribution function as (U').*

Thus in a certain sense the distribution function of a cycle is independent of the characteristic function to which the cycle belongs. For example, the distribution functions of the derived cycles (U') of (U) defined in (12.41) are independent of the value of s, provided only that s is prime to τ.

Now let us take* $\tau = e\mu$ where e denotes as usual the period modulo p of the basic multiplier, and take $\tau' = \mu$. We shall show that the distribution function of any cycle (U) of $F(x)$ is determined if we know the distribution function for a single one of its derived cycles (U') of period μ.

Let

$$\begin{array}{llll} a_0M, & a_0M^2, & \cdots, & a_0M^e; \\ a_1M, & a_1M^2, & \cdots, & a_1M^e; \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ a_{t-1}M, & a_{t-1}M^2, & \cdots, & a_{t-1}M^e \end{array}$$

* It can be shown that $(e, \mu) = 1$ save when $p = 3^kN+1$, $\epsilon(R) \equiv 0 \mod 3^k$. We shall exclude this case from consideration here.

represent the separation of the multiplicative group $\{1, 2, \cdots, p-1\}$ of the $p-1$ non-zero residues of p into co-sets with respect to its cyclic sub-group $\{M\}$. Then if $k(n)$ is the distribution function of (U), and $l(n)$ the distribution function of the first μ terms of (U),

$$k(a_iM^s) = [l(a_iM) + l(a_iM^2) + \cdots + l(a_iM^e)]$$
$$(i = 0, 1, \cdots, \tau; s = 1, 2, \cdots, e).$$

Now let $k'(n)$ be the distribution function of any derived cycle (U') of (U) with the period μ. From the properties of multipliers, it is evident that if $a \equiv b \bmod \mu$, then $U_a \equiv M^\sigma U_b \bmod p$, the exponent σ depending of course on our choice of U_a and U_b. Now the subscript $n\kappa's+r(\kappa'=e)$ of (U) in (12.41) runs through a complete residue system modulo μ, for $(e, \mu)=1$; hence to each term U_a' of (U') there corresponds a unique term U_b in the first μ terms of (U) such that

$$U_a' \equiv M^\sigma U_b \pmod p.$$

Consequently, U_a' and U_b always lie in the same co-set, and

$$k'(a_iM) + k'(a_iM^2) + \cdots + k'(a_iM^e) = l(a_iM) + l(a_iM^2) + \cdots + l(a_iM^e).$$

Thus we have the formula

$$k(a_iM^s) = [k'(a_iM) + k'(a_iM^2) + \cdots + k'(a_iM^e)]$$
$$(i = 0, 1, \cdots, \tau; s = 0, 1, \cdots, e).$$

In a similar manner, we find that

$$k(0) = ek'(0).$$

These two formulas express the distribution function of (U) in terms of the distribution function of any one of its derived cycles (U') of period μ. It can be readily shown that μ divides p^2+p+1 and is prime to 3.

If we assume that the period τ of $F(x)$ is p^2+p+1 while the period τ' of $F'(x)$ is a divisor of p^2+p+1, we can deduce the following important result from Theorem 12.1.

THEOREM 12.3. *If τ divides p^2+p+1, then no residue can appear in any cycle of period τ more times than it appears in any cycle of period p^2+p+1.*

13. **Reduction to determination of residues modulis P and 3.** Consider an irreducible cubic $F(x)=x^3-Px^2+Qx-R$ with the period $\tau=p^2+p+1$, modulo p, so that its cycles are grouped into a single block $\mathfrak{B}$, and let $k_n=k(n)$ be the distribution function of the principal cycle (S).

Then since

$$S_n \equiv S_{np} \equiv S_{np^2} \pmod p,$$

we see that if $p=3N+2$, then

$$k_i \equiv 0 \ (i \not\equiv 3), \ k_3 \equiv 1 \qquad \text{mod } 3.$$

If $p=3N+1$, it is easily verified that $p\tau/3 \equiv \tau/3 \bmod \tau$. Furthermore, if ω denotes a primitive cube root of unity modulo p,

$$S_0 \equiv 3, \ S_{\tau/3} \equiv 3\omega, \ S_{2\tau/3} \equiv 3\omega^2 \qquad \text{mod } p.$$

Hence

$$k_i \equiv 0 \mod 3 \qquad (i \not\equiv 3, 3\omega, 3\omega^2),$$
$$k_3 \equiv k_{3\omega} \equiv k_{3\omega^2} \equiv 1 \qquad \text{mod } 3.$$

Consequently,

$$k_i = 3l_i \ (i \not\equiv 3), \ k_3 = 3l_3 + 1, \ p = 3N + 2,$$

(13.1)
$$k_i = 3l_i \ (i \not\equiv 3, 3\omega, 3\omega^2),$$
$$k_{3\omega^a} = 3l_{3\omega^a} + 1 \ (a = 0, 1, 2), \qquad p = 3N + 1.$$

Now all of the cubics

$$x^3 - S_n x^2 + S_{-n} x - 1, \ 0 < n < \tau \qquad \left(n \not\equiv \frac{\tau}{3}, \ \frac{2\tau}{3} \text{ if } p = 3N + 1\right)$$

are irreducible modulo p and have periods which divide τ; thus l_i is the number of irreducible cubics modulo p among the p cubics

$$x^3 - ix^2 + ux - 1 \qquad (u = 0, 1, \cdots, p - 1).$$

Hence

(13.2)
$$0 \leqq l_i \leqq p - 2,$$

for the cubics x^3-ix^2+ix-1, $x^3-ix^2-(i+2)x-1$ are obviously reducible for any p.

Consequently, for $p>3$, k_i is completely determined if we know its residues modulis p and 3.

Since the other cycles of $F(x)$ are obtained simply by multiplying the cycle (S) by some constant residue, their distribution functions are merely permutations of the distribution function of (S), so that (13.2) holds for all the cycles of $F(x)$.

Now let $F'(x)$ be any other irreducible cubic with the period τ', a divisor of p^2+p+1, and let $k'(n)$ be the distribution function of some cycle (U') of $F'(x)$. If $k(n)$ is the distribution function of the cycle (U) of $F(x)$ from which (U') is derived in accordance with Theorem 12.1, then by Theorem 12.2,

$$k'(n) \leqq k(n) \qquad (n = 0, 1, \cdots, p - 1).$$

We thus have the following important result.

THEOREM 13.1. *If $k(n)$ is the distribution function of any cycle (U) whose characteristic number divides p^2+p+1, then $k(n)$ is completely determined if we know its residues modulo p and modulo 3.*

Since by (9.1), $k(0) \leqq p+1$, we merely need to know the residue of $k(0)$ modulo p.

14. Digression on diophantine systems. The diophantine system

$$(D) \qquad r_1 + r_2 + r_3 = m, \quad r_1 + pr_2 + p^2 r_3 = s\tau,$$

where the integers m, p, τ are given, plays such an important part in the developments which are to follow, that it is necessary to discuss its solution rather fully.

The parameters p and τ are defined as follows. Let κ be any fixed integer of the sequences 1, 3, 7, 13, 19, 21, 31, 39, $\cdots$, of all possible divisors of the form x^2+x+1, and let p be a prime such that p^2+p+1 is exactly divisible by κ.

If $p=k\kappa+\rho$, $1<\rho<\kappa$, then ρ is zero if $\kappa=1$ and unity if $\kappa=3$. In all other cases, ρ is a primitive cube root of unity modulo κ. p is thus restricted to certain linear forms $n\kappa+\rho$.

τ is defined to be the quotient obtained by dividing p^2+p+1 by κ. If $\rho^2+\rho+1=\sigma\kappa$, then

$$(14.1) \qquad \tau = k(k\kappa+\rho) + (\rho+1)k + \sigma, \quad 0 < (\rho+1)k + \sigma < 2p.$$

Finally m is restricted to be less than p, and the solutions r_1, r_2, r_3 must all be $\geqq 0$. There are no restrictions on s other than that it be an integer.

Since $p^3 \equiv 1 \bmod \tau$, if $r_1=u$, $r_2=v$, $r_3=w$, or for short (u, v, w) is a solution of (D), (v, w, u) and (w, u, v) are also solutions. We can accordingly restrict ourselves to finding those solutions of (D) for which $r_3 \leqq r_1, r_2$.

Now

$$r_1 + pr_2 + p^2 r_3 - r_3\kappa\tau = (k\kappa+\rho)(r_2 - r_3) + (r_1 - r_3) \equiv 0 \pmod{\tau}.$$

Thus if we let $r_2-r_3=s_1$, $r_1-r_3=s_2$, we obtain

$$(14.2) \qquad (k\kappa+\rho)s_1 + s_2 = u\tau \quad (s_1, s_2, u \geqq 0; \quad 0 \leqq s_1, s_2 < p).$$

Moreover, it is easily shown that $0 \leqq u < \kappa$, $s_1+s_2<p$, and

$$(14.21) \qquad m \geqq s_1 + s_2; \quad m \equiv s_1 + s_2 \pmod 3.$$

The method for solving (D) is then as follows: For a given value of κ, ρ and σ are determined, so that τ is known as a function of k from (14.1). For

each value of u between 0 and $\kappa-1$ we can determine from (14.2) a pair of values for s_1 and s_2 in terms of k. We reject all solutions of (14.2) for which $s_1+s_2 \geqq p$. (14.21) then gives the restrictions upon m, and the corresponding solution of (D) is

$$\left(\frac{m-s_1+2s_2}{3}, \frac{m+2s_1-s_2}{3}, \frac{m-s_1-s_2}{3}\right).$$

The following theorems for the cases $\kappa=1$ and $\kappa=3$ will serve to illustrate the method.

THEOREM 14.1. *If* $\kappa=1$, *there is no solution of* (D) *unless* $m\equiv 0 \bmod 3$. *If* $m=3M$, *there is the single solution* (M, M, M).

We have $\rho=0$, $p=k$, so that (14.5) becomes

$$ps_1+s_2 = u(p^2+p+1);\ u=0 \text{ giving } s_1=s_2=0,\ m\equiv 0 \bmod 3;$$
$$(r_1, r_2, r_3) = (M, M, M).$$

THEOREM 14.2. *If* $\kappa=3$, *there is no solution of* (D) *unless* $p\equiv 1$, $m\equiv 0 \bmod 3$. *If* $m=3M$, *there is the single solution* (M, M, M).

Since $p^2+p+1\equiv 0 \bmod 3$, $p\equiv 1 \bmod 3$. Let $p=3k+1$. Then $\tau=k(3k+1)+2k+1$, and (14.2) becomes

$$(3k+1)s_1+s_2 = uk(3k+1)+u(2k+1) \qquad (u=0, 1, 2).$$

Case (i) $u=0$. We have $s_1=s_2=0$, so that from (14.2), $m=3M$, giving the solution (M, M, M).

Case (ii) $u=1$. Then $s_1=k$, $s_2=2k+1$ so that $s_1+s_2=p$ and there is no solution.

Case (iii) $u=2$. From (14.5) $s_2\equiv 4k+2\equiv k+1 \bmod p$. Since $s_2<p$, $s_2=k+1$ and consequently $s_1=2k+1$. Hence $s_1+s_2>p$ and there is no solution.

In general, if $p\equiv 1 \bmod 3$, we see from (14.2) and (14.21) that $m\equiv\tau\equiv 0 \bmod 3$.

When $\kappa=7$, which requires that p be of the form $7n+2$ or $7n+4$, we find by the same method the following solutions of (D).

SOLUTIONS FOR $p\equiv 2, 4 \bmod 7$, $7\tau=p^2+p+1$

Form of p	Form of m	Restriction on m	Solution
$21L+2$	$3M$	$\geqq 0$	(M, M, M)
	$3M+1$	$\geqq 12L+1$	$(M+5L+1, M-L, M-4L)$
	$3M+2$	$\geqq 15L+2$	$(M+L+1, M+4L+1, M-5L)$
	$3M$	$\geqq 18L+3$	$(M-3L, M+9L+1, M-6L-1)$

SOLUTIONS FOR $p \equiv 2, 4 \bmod 7$, $7\tau = p^2+p+1$ (continued)

Form of p	Form of m	Restriction on m	Solution
$21L+16$	$3M$	$\geqq 0$	(M, M, M)
	$3M$	$\geqq 12L+9$	$(M+5L+4, M-L-1, M-4L-3)$
	$3M$	$\geqq 15L+12$	$(M+L+1, M+4L+3, M-5L-4)$
	$3M$	$\geqq 18L+15$	$(M-3L-2, M+9L+7, M-6L-5)$
$21L+4$	$3M$	$\geqq 0$	(M, M, M)
	$3M$	$\geqq 12L+3$	$(M-L, M+5L+1, M-4L-1)$
	$3M$	$\geqq 15L+3$	$(M+4L+1, M+L, M-5L-1)$
	$3M$	$\geqq 18L+3$	$(M+9L+2, M-3L-1, M-6L-1)$
$21L+11$	$3M$	$\geqq 0$	(M, M, M)
	$3M+1$	$\geqq 12L+5$	$(M-L, M+5L+3, M-4L-2)$
	$3M+2$	$\geqq 15L+8$	$(M+4L+3, M+L+1, M-5L-2)$
	$3M$	$\geqq 18L+9$	$(M+9L+5, M-3L-2, M-6L-3)$

For other small values of k the explicit solution of (D) may be obtained in a similar manner without undue labor.

15. **Determination of distribution function modulo p.** Let $k(n) = k_n$ be the distribution function modulo p of any cycle (U) whose characteristic number τ divides p^2+p+1. We shall determine the residue of k_n modulo p.

Let i be any residue of p. Then by Fermat's theorem

$$(U_n - i)^{p-1} \equiv 1 \mod p, \quad U_n \not\equiv i;$$
$$\equiv 0 \mod p, \quad U_n = i.$$

Hence

$$\sum_{n=0}^{\tau-1} (U_n - i)^{p-1} \equiv \tau - k_i \mod p \quad (i = 0, 1, \cdots, p-1).$$

On expanding $(U_n - i)^{p-1}$ by the binomial theorem, we obtain after a few easy reductions

$$\tau - k_i \equiv \sum_{n=0}^{\tau-1} \sum_{m=0}^{p-1} (i)^{-m} U_n{}^m \tau - k_0 \equiv \sum_{n=0}^{\tau-1} U_n{}^{p-1} \mod p. \tag{15.1}$$

Suppose that

$$U_n \equiv A\alpha^n + B\beta^n + C\gamma^n,$$

where $A = K_0 + K_1\alpha + K_2\alpha^2$, etc., so that

$$N(u) = ABC \equiv N(K_0 + K_1\alpha + K_2\alpha^2) \mod p.$$

Then by the multinomial theorem

$$U_n{}^m \equiv \sum_{(r)} \frac{m!}{r_1!r_2!r_3!} A^{r_1}B^{r_2}C^{r_3}\alpha^{n(r_1+pr_2+p^2r_3)} \mod p.$$

Since

$$\sum_{n=0}^{\tau-1}\alpha^{nR} \equiv 0 \mod p \text{ if } \tau \text{ does not divide } R,$$

$$\equiv \tau \mod p \text{ if } \tau \text{ divides } R,$$

we obtain, on substituting in (15.1), the fundamental formulas

$$k_i \equiv -\tau \sum_{m=1}^{p-1}\sum_{(r)} \frac{m!}{r_1!r_2!r_3!}\,\frac{A^{r_1}B^{r_2}C^{r_3}}{i^m} \mod p,$$

(15.2)

$$k_0 \equiv \tau\left(1 + \sum_{(r)} \frac{A^{r_1}B^{r_2}C^{r_3}}{r_1!r_2!r_3!}\right) \mod p,$$

where in the expression for k_i the summation variables satisfy the conditions

(D) $$r_1 + r_2 + r_3 = m,\ r_1 + pr_2 + p^2r_3 \equiv 0 \mod \tau,$$

while in the expression for k_0,

$$r_1 + r_2 + r_3 = p - 1,\ r_1 + pr_2 + p^2r_3 \equiv 0 \mod \tau.$$

For the principal cycle (S), $A = B = C = 1$ and the formulas (15.2) assume the simpler form

$$k_i \equiv \tau \sum_{m=1}^{n-1}\sum_{(r)} \frac{m!}{r_1!r_2!r_3!i^m} \mod p,$$

(15.3)

$$k_0 \equiv \tau\left(1 + \sum_{(r)} \frac{1}{r_1!r_2!r_3!}\right) \mod p.$$

The problem of determining the residue of k_i modulo 3 offers very serious difficulties, principally because $U_0, U_1, \cdots, U_{\tau-1}$ do not satisfy a difference equation when taken modulo 3. The only cases in which I have succeeded in determining the residue are given in the formulas (13.1) for the distribution function of the principal cycle (S), and their obvious extension to the remaining cycles of the block $\mathfrak{B}_1$ to which (S) belongs.

16. **Applications.** By applying the results of §14 on the solutions of the diophantine equations (D) to formulas (15.2) and (15.3), we obtain a number of interesting special cases. Throughout this section, (U) denotes a fixed cycle of $F(x)$ whose general term is $U_n \equiv A\alpha^n + B\beta^n + C\gamma^n \mod p$, $A = K_0 + K_1\alpha + K_2\alpha^2$ etc., and whose distribution function is $k(n)$.

From formulas (6.11), (6.13),

(16.1) $$ABC \equiv \Lambda(U_0, U_1, U_2)/\Delta \mod p,$$

where Λ is the polynomial defined in formula (6.12), and Δ is the discriminant of $F(x)$.

If $p \equiv 2 \bmod 3$ and $\tau = p^2+p+1$, then by Theorem 14.1 formulas (15.2) become

$$k_i \equiv \sum_{n=1}^{(p-2)/3} \frac{(3n)!}{(n!)^3} \left(\frac{\Lambda(U_0, U_1, U_2)}{\Delta i^3}\right)^n \bmod p,$$

$$k_0 \equiv 1 \bmod p.$$

Since in this case the residues of k_i modulo 3 are known, these formulas determine the distribution function $k(n)$ completely.

If $p \equiv 1 \bmod 3$ and $\tau = (p^2+p+1)/3$, then on writing $p = 3N+1$, $\tau \equiv 2N+1 \bmod p$, and by Theorem 14.2, formulas (15.2) become

$$k_i \equiv N \sum_{n=1}^{N} \frac{(3n)!}{(n!)^3} \left(\frac{\Lambda(U_0, U_1, U_2)}{\Delta i^3}\right)^n \bmod p,$$

(16.2)

$$k_0 \equiv (2N+1)\left(1 + \frac{(\Lambda(U_0, U_1, U_2))^N}{(N!)^3}\right) \bmod p.$$

These formulas will determine the distribution function $k(n)$ for any cycle (U) belonging to the block $\mathfrak{B}$, since the residues of k_i modulo 3 are known. For the other blocks, the residues of k_i modulo 3 are unknown.

Formula (16.2) has some important consequences. We have seen in §10 that if $k_0^{(1)}$, $k_0^{(2)}$, $k_0^{(3)}$ are the number of zeros in three cycles $(U^{(1)})$, $(U^{(2)})$, $(U^{(3)})$ belonging to the blocks $\mathfrak{B}_1$, $\mathfrak{B}_2$, $\mathfrak{B}_3$ respectively, then $h_0^{(1)}$, $h_0^{(2)}$, $h_0^{(3)}$ are all distinct from one another. Hence if (U) is allowed to range over all the cycles of $F(x)$, we see from (16.1), (16.2) that $(ABC)^N$ must take three distinct values modulo p.

Since $(ABC)^{3N} \equiv 1 \bmod p$, $(ABC)^N \equiv \omega^a \bmod p$ where ω is a primitive cube root of unity modulo p, and the exponent a of ω depends on the block to which (U) belongs. In particular, for (S), $ABC = 1$ so that $a = 0$. We thus obtain from (16.1) and formulas (6.11), (6.12) the following simple criterion to decide whether or not two triads belong to the same block.

THEOREM 16.1. *If* $[A', B', C']$ *and* $[A'', B'', C'']$ *are any two triads of* $F(x)$ *and if* $F(x)$ *has the period* $(p^2+p+1)/3$, *then a necessary and sufficient condition that* $[A', B', C']$ *and* $[A'', B'', C'']$ *belong to the same block is that* $\Lambda(A', B', C')$ *and* $\Lambda(A'', B'', C'')$ *have the same cubic character modulo* p.

For the cycle (Z): 0, 0, 1, $\cdots$, $ABC \equiv (-1/\Delta) \bmod p$. Hence (Z) lies in $\mathfrak{B}_1$ when and only when $\Delta^N \equiv 1 \bmod p$. But obviously (Z) lies in $\mathfrak{B}_1$ when and

only when the cycle (S) contains two consecutive zeros; we thus obtain the following interesting theorem:

THEOREM 16.2. *If $p \equiv 1 \bmod 3$ and $F(x)$ is any irreducible cubic with the period $\tau = (p^2+p+1)/3 \bmod p$, then the sequence $(S)_n$ of $F(x)$ will contain pairs of consecutive elements divisible by p when and only when the discriminant of $F(x)$ is a cubic residue of p.*

Formulas (15.1) serve to determine the distribution function for all the cycles of $\mathfrak{B}_1$, regardless of the value of τ, but if the period τ is less than $(p^2+p+1)/3$, they become increasingly complicated as τ is taken smaller. The table at the close of §14 allows us to give explicit formulas for the residues of $k(n)$ modulo p when $\tau = (p^2+p+1)/7$. The simplest of these results is contained in the following theorem.

THEOREM 16.3. *If $\tau = (p^2+p+1)/7$, $p \equiv 2 \bmod 3$ and if b_0 denotes the number of zeros in the principal cycle (S), then*

$$b_0 \equiv (9L+1)\left(1 + \frac{3}{(12L+1)!6L!3L!}\right) \bmod p$$

or

$$b_0 \equiv (15L+8)\left(1 + \frac{3}{(6L+3)!(12L+6)!(3L+1)!}\right) \bmod p$$

according as p is of the form $21L+2$ or $21L+11$.

17. **Determination of upper limit to distribution function.** On account of the great increase in complexity in the formulas (15.2) as τ is taken smaller, it is desirable to have an upper limit to the number of times a given residue can appear in a given cycle. The results I have obtained in this connection are incomplete in the same sense as those I have obtained to determine $k(n)$; it is necessary to know this upper limit modulis p and 3, whereas I have determined it only modulo p. They suffice nevertheless to give an upper limit to the number of times the residue zero can appear in any cycle, and the number of times any residue can appear in the principal cycle.

We have seen, in §13, that if (U') is any sequence of $F'(x)$ of period τ', where $\tau'\kappa' = \tau$, the period of $F(x)$, then the terms of (U') consist of the rth, $(\kappa'+r)$th, $(2\kappa'+r)$th, $\cdots$, $((\tau'-1)\kappa'+r)$th terms of some definite sequence (U) of $F(x)$ written usually in a different order. We shall now regard (U), τ, and r as given, but τ' as unknown, and endeavor to obtain an upper limit to $k'(n)$, the distribution function of (U'). Let us take U_r, U_{r+1}, U_{r+2} as the initial values of (U), which amounts to replacing (U) by the cycle (W), where

$$W_n = U_{n+r} \qquad (n = 0, 1, \cdots, \tau - 1).$$

This change does not affect the distribution function $k(n)$ of (U). Then if m_i denotes the number of times the residue i appears in those terms of (U) whose indices are prime to τ, it is apparent that

$$k_i' \leqq k_i - m_i \qquad (i = 0, 1, \cdots, p-1). \tag{17.1}$$

m_i is determined if we know its residues modulis p and 3, in particular, m_0 is determined if we know its residue modulo p. Moreover, it is easily shown that if (W) belongs to the block of the principal cycle, $m_i \equiv 0 \bmod 3$. We shall now determine m_i modulo p.

By Fermat's theorem, we have the fundamental formula

$$\phi(\tau) - m_i \equiv \sum_{(n,\tau)=1} (W_n - i)^{p-1} \qquad \bmod p,$$

where the summation extends over all the terms of (W) whose subscripts are prime to τ, and $\phi(\tau)$ denotes as usual the totient of τ.

On proceeding as in §17, we find that, if $i \neq 0$,

$$\sum_{(n,\tau)=1} (W_n - i)^{p-1} \equiv \sum_{(n,\tau)=1} \sum_{m=0}^{p-1} \sum_{(r)} \frac{(i)^{-m} m!}{r_1! r_2! r_3!} A^{r_1} B^{r_2} C^{r_3} \alpha^{(r_1 + p r_2 + p^2 r_3) n},$$

where $r_1 + r_2 + r_3 = m$ and $W_n \equiv A\alpha^n + B\beta^n + C\gamma^n \bmod p$.

Now if $\mu(n)$ denotes Möbius' function, it is easily shown that

$$\sum_{(n,\tau)=1} \alpha^{Rn} \equiv \mu(\tau) \quad \bmod p, \quad \tau \text{ does not divide } R,$$

$$\equiv \phi(\tau) \quad \bmod p, \quad \tau \text{ divides } R.$$

Hence after a slight transformation, we find that

$$\phi(\tau) - m_i \equiv \mu(\tau) \sum_{m=0}^{p-1} \sum_{(r)} \frac{(i)^{-m} m!}{r_1! r_2! r_3!} A^{r_1} B^{r_2} C^{r_3} + (\phi(\tau) - \mu(\tau)) \sum_{m=0}^{p-1} \sum_{(r)} \frac{(i)^{-m} m!}{r_1! r_2! r_3!} A^{r_1} B^{r_2} C^{r_3},$$

where in the first summation $r_1 + r_2 + r_3 = m$, but in the second summation

$$r_1 + r_2 + p^2 r_3 \equiv 0 \quad \bmod \tau, \quad r_1 + r_2 + r_3 = m. \tag{D}$$

By the multinomial theorem, the first sum is found to be congruent modulo p to $\mu(\tau)[W_0(W_0 - i)]^{p-1}$.

Referring back to the formulas (15.2), the second sum is congruent to $(\phi(\tau) - \mu(\tau))(1 - k_i/\tau)$. Thus using the fact that $\kappa\tau = p^2 + p + 1 \equiv 1 \bmod p$, we obtain

$$m_i \equiv \kappa(\phi(\tau - \mu(\tau))k_i + \epsilon\mu(\tau) \mod p, \tag{17.2}$$

where $\epsilon = -1$, if $W_0 = 0$ or i, $\epsilon = 0$, otherwise.

In a similar manner, we find that

$$m_0 \equiv \kappa(\phi(\tau) - \mu(\tau))k_0 + \epsilon'\mu(\tau) \mod p, \tag{17.3}$$

where $\epsilon' = 1$, $W_0 = 0$, $\epsilon' = 0$ otherwise.

Thus if τ has a square factor, we have the simple formula*

$$m_i \equiv \kappa\phi(\tau)h_i \mod p \qquad (i = 0, 1, \cdots, p-1).$$

For $\tau = p^2+p+1$ or $(p^2+p+1)/3$, these formulas give a practicable determination of m_i for any given p.

---

* It is perhaps worth noting that p never divides $\phi(\tau)$.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.