THE CHARACTERISTIC NUMBER OF A SEQUENCE OF INTEGERS SATISFYING A LINEAR RECURSION RELATION*

BY

MORGAN WARD

1. Introduction. Let

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

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

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

where P, Q, R, W_0, W_1, W_2 are fixed integers,† and let $m>1$ be any positive integer. If

$$W_n \equiv A_n \pmod{m;\ 0 \leqq A_n \leqq m-1;\ n = 0, 1, \cdots}$$

we shall call $(A)_n$ the *reduced sequence* corresponding to $(W)_n$ modulo m.

If after s terms in the reduced sequence, a cycle of t terms keeps repeating itself indefinitely, $(W)_n$ will be said to *admit the period t, modulo m.* The least period that $(W)_n$ admits (modulo m) is called its *characteristic number.*‡

In this paper, I give a number of new results on the form of the characteristic number of a sequence. The principal result is the following:

If $m = p_1^{a_1} \cdots p_k^{a_k}$ is the resolution 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 $p_1^{a_1}, \cdots, p_k^{a_k}$.

The restriction to the case of a difference equation of order 3 is mainly for convenience of notation and ease of illustration. The theorems in the first seven sections of the paper, which include my main result, may be immediately extended to the general case of a difference equation of order r.

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

† The arithmetical properties of such sequences do not seem to have been extensively investigated. Besides the references in Dickson's *History*, there is an important paper by Carmichael on the linear recursion relation (1.1) for general r (Quarterly Journal of Mathematics, vol. 48 (1920), pp. 343–372). We shall refer to this paper as Carmichael I, giving page reference. Many of Carmichael's results are summarized in a more recent paper (American Mathematical Monthly, vol. 36 (1929), pp. 132–143). Draeger (*Ueber rekurrente Reihen von höherer, insbesondere von der dritten Ordnung*, Dissertation, Jena, 1919) has discussed (1.1) in detail and given some arithmetical results for the cases $m=2, 3$ and $P \equiv 0 \pmod{m}$.

‡ Carmichael I, p. 345. We shall omit the phrase "modulo m" when no confusion can arise.

2. **Periodicity of sequences.** We shall employ the notation

$$A_0, A_1, \cdots, A_{\lambda-1}; \dot{A}_\lambda, A_{\lambda+1}, \cdots, \dot{A}_{\lambda+\mu-1}$$

for a reduced sequence $(A)_n$ having λ non-repeating terms $A_0, A_1, \cdots, A_{\lambda-1}$ and μ repeating terms* $A_\lambda, A_{\lambda+1}, \cdots, A_{\lambda+\mu-1}$. If $\lambda=0$, $(W)_n$ is said to be *purely periodic* modulo m.

If μ is the characteristic number of $(W)_n$, then a necessary and sufficient condition that $(W)_n$ admit the period r is that† $\mu \mid r$.

THEOREM 2.1. *Every sequence $(W)_n$ becomes periodic,‡ modulo m. Moreover, if μ is the characteristic number of $(W)_n$ and λ the maximum number of non-repeating terms in the reduced sequence $(A)_n$ corresponding to $(W)_n$, then*

$$\lambda \leqq m^3 - 1; \quad 1 \leqq \mu \leqq m^3 - \lambda.$$

Call an ordered set of three consecutive elements of $(A)_n$ a triad. Then the first m^3+3 terms of $(A)_n$ contain the m^3+1 triads

$$A_0, A_1, A_2; A_1, A_2, A_3; \cdots; A_{m^3}, A_{m^3+1}, A_{m^3+2} \tag{2.1}$$

of which at most m^3 are distinct, since $0 \leqq A_n \leqq m-1$. Hence if λ, μ are the least values of s, t such that

$$A_s = A_{s+t}, A_{s+1} = A_{s+t+1}, A_{s+2} = A_{s+t+2}$$

in (2.1), the first part of the theorem follows from the linearity of (1.1). The remainder of the theorem follows from the inequalities

$$s \leqq m^3 - 1; \quad s + t + 2 \leqq m^3 + 2.$$

3. **Reduction to prime powers.** We shall now show that there is no loss of generality in supposing that m is a power of a prime.

THEOREM 3.1. *Let $(W)_n$ be any particular solution of the difference equation (1.1), and assume that $m = a \cdot b$ where $(a, b) = 1$; $a, b > 1$. Then the characteristic number of $(W)_n$ modulo m is the L.C.M. of its characteristic numbers modulis a and b.*

Let $\mu(x) \equiv \mu_x$ denote the characteristic number of $(W)_n$ modulo x, and let κ denote the L.C.M. of μ_a and μ_b where, by hypothesis, $a \cdot b = m$; $(a, b) = 1$.

$(W)_n$ admits the period μ_m modulis a and b; therefore $\mu_a \mid \mu_m$, $\mu_b \mid \mu_m$, so that $\kappa \mid \mu_m$.

* It is understood that λ is the greatest number of non-repeating terms, and μ the smallest number of repeating terms in the reduced sequence.

† We use the customary abbreviations (a, b) for the greatest common divisor of the integers a and b, $a \mid b$ for a divides b, and L.C.M. of a and b for the least common multiple of a and b.

‡ For another proof, see Carmichael I, p. 344.

$(W)_n$ also admits the period κ modulis a and b; therefore

$$(3.1)\quad W_{\lambda+\kappa+n} - W_{\lambda+n} \equiv 0 \pmod{a},\ W_{\lambda+\kappa+n} - W_{\lambda+n} \equiv 0 \pmod{b}\ (n = 0, 1, \cdots)$$

where λ is the number of non-repeating terms in the reduced sequence $(A)_n$ corresponding to $(W)_n$ modulo $m = a \cdot b$.

Since $(a, b) = 1$, (3.1) implies that

$$W_{\lambda+\kappa+n} - W_{\lambda+n} \equiv 0 \pmod{m;\ n = 0, 1, \cdots}.$$

Hence $(W)_n$ admits the period κ modulo m and $\mu_m \mid \kappa$. Since $\kappa \mid \mu_m$, $\kappa = \mu_m$.

The following fundamental result is a direct corollary of this theorem.

THEOREM 3.11. *Let $(W)_n$ be any particular solution of the difference equation* (1.1) *and let*

$$m = p_1^{a_1} \cdots p_k^{a_k}$$

be the resolution of m into its prime factors. Then the characteristic number of $(W)_n$ modulo m is the L.C.M. of its characteristic numbers modulis $p_1^{a_1}, \cdots, p_k^{a_k}$.

To illustrate this theorem, consider the difference equation

$$\Omega_{n+3} = \Omega_{n+2} + \Omega_{n+1} + \Omega_n$$

with the particular solution $(U)_n$ whose first few terms are

$$1, 0, 0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, 927, \cdots.$$

Let $\mu(m)$ denote the characteristic number of $(U)_n$ modulo m. Taking $(U)_n$ modulis 2, 3, 4, 5, 6, 7, 9, 42, we find that $\mu(2) = 4$, $\mu(3) = 13$, $\mu(4) = 8$, $\mu(6) = 52$, $\mu(7) = 48$, $\mu(9) = 39$, and $\mu(42) = 624$. Thus $\mu(42)$, for example, equals $3 \cdot 13 \cdot 16$ which is the L.C.M. of $\mu(2)$, $\mu(3)$ and $\mu(7)$; and $\mu(6)$ is the L.C.M. of $\mu(2)$ and $\mu(3)$.

4. Purely periodic sequences. We shall now give some conditions that a sequence $(W)_n$ be purely periodic, modulo m. It is easily shown that a sufficient condition* that the sequence $(W)_n$ be purely periodic is that $(R, m) = 1$. This condition is not, however, a necessary one. On the other hand, we shall prove

THEOREM 4.1. *A necessary condition that the sequence $(W)_n$ be purely periodic modulo m is that*

$$(4.1)\quad W_2 \equiv PW_1 - QW_0 \pmod{d},$$

where d is the greatest common divisor of R and m.

* Carmichael, I, p. 344, §2.

Assume that $(W)_n$ is purely periodic modulo m, and has the characteristic number μ. Then if $(m, R)=d$, $d \mid m$ and $d \mid R$, so that

$$W_{\mu+2} \equiv PW_{\mu+1} - QW_\mu + RW_{\mu-1} \equiv PW_{\mu+1} - QW_\mu \pmod{d},$$

giving (4.1) immediately.

Unfortunately, this condition is not sufficient for pure periodicity. Consider for example the difference equation

$$\Omega_{n+3} = 2\Omega_{n+2} + \Omega_{n+1} + 3\Omega_n, \text{ with } m = 9.$$

Here $d=3$, and if we take $W_0=0$, $W_1=0$, $W_2=3$, then $W_2 \equiv 2W_1+W_0 \pmod 3$. Nevertheless, in this case $(A)_n$ is $0; \dot{0}, 3, 6, 6, 0, 6, 3, \dot{3}$.

We can, however, prove as in Theorem 3.1 that if $(W)_n$ is purely periodic modulis a and b, where $(a, b)=1$, then $(W)_n$ is purely periodic modulo $a \cdot b$. Consequently, we have the following criterion for pure periodicity:

THEOREM 4.2. *If $m=p_1^{a_1} \cdots p_k^{a_k}$ is the decomposition of m into its prime factors, then a necessary and sufficient condition that $(W)_n$ be purely periodic modulo m is that it be purely periodic modulis $p_1^{a_1}, \cdots, p_k^{a_k}$.*

We shall consider henceforth only purely periodic solutions of (1.1).

5. **Singular and non-singular sequences.** Let $(W)_n$ stand as usual for a particular solution of (1.1), and let $D=D(W)$ denote the determinant

$$\begin{vmatrix} W_0, & W_1, & W_2 \\ W_1, & W_2, & W_3 \\ W_2, & W_3, & W_4 \end{vmatrix}.$$

The solution $(W)_n$ is said to be non-singular (modulo m) if $(D, m)=1$ and singular if $(D, m)=d>1$.

THEOREM 5.1. *All purely periodic non-singular sequences satisfying* (1.1) *have the same characteristic number, τ, modulo m. Moreover, the characteristic number modulo m of any singular sequence is a divisor of τ.*

Let $(W)_n$ be any solution of (1.1), and $(T)_n$ any non-singular solution, and let the characteristic numbers of $(W)_n$ and $(T)_n$ modulo m be μ and τ respectively. Then we can determine integers K_0, K_1, K_2 such that

$$W_n \equiv K_0T_n + K_1T_{n+1} + K_2T_{n+2} \pmod{m;\ n = 0, 1, \cdots} \tag{5.1}$$

where

$$0 \leqq K_0, K_1, K_2 \leqq m - 1. \tag{5.2}$$

For on account of the linearity of (1.2), (5.1) will be true provided that it is true for $n=0$, 1, and 2.

But a sufficient condition that the congruences

$$W_i \equiv K_0T_i + K_1T_{i+1} + K_2T_{i+2} \qquad (\text{mod } m;\ i = 0, 1, 2)$$

have a solution satisfying the conditions (5.2) is that $(D(T), m)=1$.

From (5.1), we see that $(W)_n$ admits all the periods of $(T)_n$, so that $\mu \mid \tau$. If $(W)_n$ is also non-singular, a repetition of the argument shows that $\tau \mid \mu$, so that $\tau = \mu$.

The characteristic number τ is called the *principal period of* (1.1) modulo m.

It is easily shown that if $(m, c)=1$, the sequences $(W)_n$ and cW_0, cW_1, $\cdots$ or for short $c(W)_n$, have the same characteristic number* modulo m. If $(m, c)>1$, this is not usually the case.

For instance, consider the difference equation and particular solution given to illustrate Theorem 3.11. The characteristic number of $(U)_n$ modulo 6 is 52. Nevertheless, the characteristic number of $3(U)_n$ modulo 6 is only 4.† Now 4 is the characteristic number of $(U)_n$ modulo $2=6/3$. We have here an illustration of the following theorem:

THEOREM 5.2. *If $(W)_n$ is any particular solution of* (1.1) *and c is any integer, the characteristic number of $c(W)_n$ modulo m equals the characteristic number of $(W)_n$ modulo m/d, where d is the greatest common divisor of m and c.*

Let $c=c'\cdot d$, $m=m'\cdot d$; $(m', c')=1$. From the congruences

$$cW_{n+3} \equiv cPW_{n+2} - cQW_{n+1} + cRW_n \qquad (\text{mod } m),$$

we obtain

$$(5.3) \qquad c'W_{n+3} \equiv c'PW_{n+2} - c'QW_{n+1} + c'RW_n \qquad (\text{mod } m';\ n = 0, 1, \cdots).$$

Since $(c', m')=1$, the characteristic number of $c'(W)_n$ modulo m' is the same as the characteristic number, κ, of $(W)_n$ modulo m'. Let μ denote the characteristic number of $c(W)_n$ modulo m. From (4.3), $(W)_n$ admits the period μ modulo m', so that $\kappa \mid \mu$.

But we also have

$$W_{k+\kappa} - W_k \equiv 0 \qquad (\text{mod } m';\ k = 0, 1, \cdots).$$

Hence $c'W_{k+\kappa} - c'W_k \equiv 0 \pmod{m'}$, $cW_{k+\kappa} - cW_k \equiv 0 \pmod{m}$, so that $c(W)_n$ admits the period κ, modulo m. Thus $\mu \mid \kappa$, so that $\mu = \kappa$.

* If the periodic parts of $(A)_n$ and $c(A)_n$ are merely cyclic permutations of each other, c is called a multiplier of $(W)_n$. The theory of the multipliers of a sequence is considered in §9, for m a prime p.

† Note that $D(3U)=27$, which is not prime to the modulus 6.

We can derive the following important consequence from Theorem 5.2.

THEOREM 5.3. *Let* $(S)_n$ *be any singular solution of* (1.1) *and let* d *be the greatest common divisor of* $D(S)$ *and* m. *Then the characteristic number of* $(S)_n$ *modulo* m *is a multiple of the principal period of* (1.1) *modulo* m/d.*

If $(T)_n$ is any non-singular solution and if $(D(S), m) = d$, then it is easily shown that we can determine constants K_0, K_1, K_2 such that

$$dT_n \equiv K_0S_n + K_1S_{n+1} + K_2S_{n+2} \qquad (\text{mod } m;\ n = 0, 1, \cdots),$$

where $0 \leqq K_0, K_1, K_2 \leqq m-1$. Hence $d(T)_n$ admits the periods of $(S)_n$. The theorem now follows immediately from Theorem 5.2, since $(T)_n$ is also a non-singular solution of (1.1) modulo m/d.

6. **The binomial congruence.** Consider the binomial congruence

$$x^n \equiv 1 \qquad (\text{modd } m, F(x)) \tag{6.1}$$

where it should be noted that

$$F(x) = x^3 - Px^2 + Qx - R$$

is the characteristic function of the difference equation (1.1).

The problem which immediately suggests itself is to find those values of n for which (6.1) is an identity in x. We shall see that they are the periods of the non-singular sequences of (1.1), modulo m.

If

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

denotes that particular solution of

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

with the initial values $U_0 = 1/R$, $U_1 = 0$, $U_2 = 0$, then it may be shown by induction that

$$x^n = U_{n+1}x^2 + (U_{n+2} - PU_{n+1})x + RU_n + Q_n(x)F(x), \tag{6.2}$$

where

$$Q_0(x) = 0; \qquad Q_n(x) = \sum_{r=1}^{n} U_r x^{n-r} \qquad (n = 1, 2, \cdots).$$

Suppose that

$$U_n \equiv H_n \qquad (\text{mod } m;\ 0 \leqq H_n \leqq m - 1;\ n = 0, 1, \cdots).$$

* One might conjecture from Theorem 4.3 that all singular solutions $(S)_n$ for which the greatest common divisor of $D(S)$ and m has the same value would have the same characteristic number, but it is easy to construct examples showing that this is not the case.

(6.2) then gives us the fundamental formula

$$x^n \equiv H_{n+1}x^2 + (H_{n+2} - PH_{n+1})x + RH_n \pmod{m, F(x)}.$$

Hence $x^n \equiv 1 \pmod{m, F(x)}$ identically in x when and only when $U_{n+1} \equiv U_{n+2} \equiv 0 \pmod{m}$ and $RU_n \equiv 1 \pmod{m}$. Thus we have the following theorem:

THEOREM 6.1. *Necessary and sufficient conditions that* (6.1) *hold identically in x for $n = \mu$ are that R be prime to m, and that the sequence $(U)_n$ admit the period μ modulo m.*

We shall assume henceforth that $(R, m) = 1$. Since

$$D(U) = \begin{vmatrix} R^{-1}, & 0, & 0 \\ 0, & 0, & 1 \\ 0, & 1, & P \end{vmatrix} = (-R)^{-1},$$

the characteristic number of $(U)_n$ is the principal period τ of (1.2) modulo m. It then follows from Theorem 6.1 that the least value of n for which (6.1) is an identity in x is τ.*

If we put $x = \alpha$ in the identity (6.2), where α is a root of $F(x) = 0$, we have the congruence

$$\alpha^n \equiv 1 \pmod{m}.$$

Thus τ is divisible by the exponent to which α belongs modulo m, which gives us the following theorem:

THEOREM 6.2. *The principal period of* (1.1) *modulo m is divisible by the L.C.M. of the exponents to which the roots of $F(x) = 0$ belong, modulo m.*

7. **Characteristic number for powers of a prime.** Assume now that

$$m = p^t \ (t \geqq 1) \text{ is a power of a prime, } p.$$

THEOREM 7.1. *If $(W)_n$ is any solution of* (1.1) *and $\mu^{(t)} = \mu(p^t)$, $\mu = \mu(p)$ the characteristic numbers of $(W)_n$ modulo $m = p^t$ and modulo p respectively, then*

$$\mu^{(t)} = p^b\mu \tag{7.1}$$

where† $0 \leqq b \leqq t-1$.

By Theorem 6.1, $x^{\mu^{(t)}} \equiv 1 \pmod{p^t, F(x)}$, so that $x^{\mu^{(t)}} \equiv 1 \pmod{p, F(x)}$ and $\mu \mid \mu^{(t)}$. Also,

* Compare the relationship between the binomial congruence $x^n \equiv 1 \pmod{m}$ and the difference equation $\Omega_{n+1} \equiv R\Omega_n \pmod{m}$; $(R, m) = 1$. The characteristic number of any solution of the difference equation is an admissible value of n for the congruence.

† Carmichael (I, p. 352) gives the limits $0 \leqq b \leqq t$ for b.

$$x^{\mu} = 1 + pP(x) + F(x)Q(x) \tag{7.2}$$

where $P(x)$ and $Q(x)$ are polynomials in x with integral coefficients. On raising both sides of (7.2) to the p^{t-1} power, we see that $x^{\mu p^{t-1}} \equiv 1 \pmod{p^t, F(x)}$. By Theorem 6.1, $\mu^{(t)} \mid \mu p^{t-1}$; since $\mu \mid \mu^{(t)}$, (7.1) follows.

For illustrations of this theorem, see the examples following Theorem 3.11.*

By the same method of proof used in Theorem 7.1, we can establish the following result:

THEOREM 7.2. *If* $\sigma \geqq 1$ *and* $x^{\mu(p)} \equiv 1 \pmod{p^{\sigma}, F(x)}$ *but* $x^{\mu(p)} \not\equiv 1 \pmod{p^{\sigma+1}, F(x)}$, *then*

$$\mu(p^t) = \mu(p) \quad \text{if} \quad \sigma \geqq t \geqq 1,$$
$$\mu(p^t) = p^{t-\sigma}\mu(p) \quad \text{if} \quad t \geqq \sigma.$$

The problem of determining the exponent b in (7.1) is thus a generalization of Abel's famous problem† of finding the highest power of p which will divide $a^{p-1}-1$.

8. **Characteristic number for prime modulus.** Assume now that m is a prime, p. The factorization of $F(x)$ modulo p may be described by a partition of three; for example, if $F(x)$ is irreducible, we shall say it is of "type [3]", if it can be factored into an irreducible quadratic factor and a linear factor, we shall say that it is of "type [2, 1]" and so on. In any case, the factorization is unique; denote the roots which correspond to linear factors by small italic letters a, b, c and the roots which correspond to irreducible quadratic or cubic factors by small greek letters α, β, γ.

Let $L(\alpha)$; $L(a)$ denote the exponents to which the roots α; a belong modulo p and $L(\alpha, b)$; $L(\alpha, \beta, c)$, etc., the L.C.M. of the exponents to which α, b; α, β, c etc. belong modulo p.

Finally, let Δ denote the discriminant of $F(x)$, and W the matrix

$$\begin{pmatrix} W_0, & W_1, & W_2 \\ W_1, & W_2, & W_3 \\ W_2, & W_3, & W_4 \end{pmatrix}.$$

Then it is easily shown from the known algebraic theory of (1.1) that the characteristic number of $(W)_n$ is given by the following table:

---

* b in (7.2) may be zero; for example, take $F(x) = x^3 - 2x^2 + x - 1$ and $p = 2$. The first few terms of $(U)_n$ are $1, \dot{0}, \dot{0}, 1, \dot{2}, 3, 5, 9, 16, 28, \cdots$. Taking the sequence modulo 2 and modulo 4, we obtain $\dot{1}, 0, 0, 1, 0, 1, \dot{1}$, and $\dot{1}, 0, 0, 1, 2, 3, 1$ so that $\mu(2^2) = \mu(2) = 7$.

† Crelle's Journal, vol. 3 (1828), p. 212. See also Dickson's *History*, Chapter IV.

CHARACTERISTIC NUMBERS MODULO p

Case	Type of $F(x)$	Quadratic character* of Δ modulo p	Algebraic form of W_n in terms of roots of $F(x)\equiv 0 \pmod p$	Rank of W	Characteristic number
I	[3]	$+1$	$A\alpha^n+B\beta^n+C\gamma^n$	3	$L(\alpha)=L(\beta)=L(\gamma)$.
II	[2, 1]	-1	$A\alpha^n+B\beta^n+C\gamma^n$	3	$L(\alpha, c)=L(\beta, c)$,
			$A\alpha^n+B\beta^n$	2	$L(\alpha)=L(\beta)$,
			Cc^n	1	$L(W_1/W_0)$.
III	[1, 1, 1]	$+1$	$Aa^n+Bb^n+Cc^n$	3	$L(a, b, c)$,
			Aa^n+Bb^n Bb^n+Cc^n Cc^n+Aa^n	2	$L(a, b)$, $L(b, c)$, $L(c, a)$,
			Aa^n; Bb^n; Cc^n	1	$L(W_1/W_0)$.
IV	[1^2, 1]	0 $PQ-9R\neq 0$	$(A+Bn)a^n+Cc^n$ Bna^n+Cc^n	3	$pL(a, c)$,
			Bna^n $(A+Bn)a^n$	2	$pL(a)$,
			Aa^n+Cc^n	2	$L(a, c)$,
			Aa^n; Cc^n	1	$L(W_1/W_0)$.
V	[1^3]	0 $PQ-9R\equiv 0$	$(A+Bn+Cn^2)a^n$ $(Bn+Cn^2)a^n$ $(A+Cn^2)a^n$ Cn^2a^n	3	$pL(a)$,
			$(A+Bn)a^n$	2	$pL(a)$,
			Aa^n	1	$L(W_1/W_0)$.

The problem of determining the characteristic number for a prime modulus is thus equivalent to the problem of determining the exponent to which a given element in a Galois field of order p^3, p^2 or p belongs.†

* There exists no convenient criterion for distinguishing the cases when $F(x)$ is of type [3], and of type [1, 1, 1]. See Dickson's *History*, vol. I, pp. 252–256.

† If we call a difference equation *primitive* (modulo p) when there is only one sequence belonging to it, then, just as in the allied theory of primitive marks in a Galois field, or primitive roots of p^n, we can show that for every prime p, there exist primitive difference equations of any order r.

We shall devote the concluding two sections of the paper to studying case I. The characteristic number modulo p of all sequences satisfying (1.1) is then the same, and equals the exponent to which any root of $F(x)=0$ belongs in the Galois field $[p^3]$ associated with $F(x)$. We shall call this number the *period* of $F(x)$, and denote it by τ. It is of course a divisor of p^3-1.

If α, β, γ are the roots of $F(x)=0$, and $S_n=\alpha^n+\beta^n+\gamma^n$, then*

$$\beta \equiv \alpha^p,\ \gamma \equiv \alpha^{p^2};\ R \equiv \alpha^{1+p+p^2};\ S_n \equiv \alpha^n + \alpha^{pn} + \alpha^{p^2 n}. \tag{8.1}$$

9. **Multipliers of cycles.** If $(A)_n$ is any reduced sequence of residues, so that

$$A_{n+3} \equiv PA_{n+2} - QA_{n+1} + RA_n \qquad (0 \leqq A_n \leqq p-1,\ n = 0, \pm 1, \cdots)$$

the τ residues $A_0, \cdots, A_{\tau-1}$ are said to form a cycle (A) belonging to $F(x)$. Two such cycles are said to be equal if either can be obtained from the other by a cyclic permutation of its elements.

Let L be any residue. If the cycle $LA_0, \cdots, LA_{\tau-1}$ equals the cycle (A), then L is called a multiplier of (A); we have

$$LA_n \equiv A_{n+l} \qquad (n = 0, \cdots, \tau-1). \tag{9.1}$$

Since any other cycle (B) of $F(x)$ may be expressed in the form

$$B_n \equiv K_0 A_n + K_1 A_{n+1} + K_2 A_{n+2} \qquad (n = 0, \cdots, \tau-1),$$

where K_0, K_1, K_2 are residues, the following theorem is apparent:

THEOREM 9.1. *If L is a multiplier of one cycle of $F(x)$, it is a multiplier of all the cycles of $F(x)$, and the integer l in equation* (9.1) *does not depend on the particular cycle (A) used in defining L.*

We shall call l the span of L.

The following three theorems are easily established:

THEOREM 9.2. *The multipliers of the cycles of $F(x)$ form a group with respect to multiplication modulo p.*

THEOREM 9.3. *Two multipliers with the same span are identical modulo p.*

THEOREM 9.4. *The group of the multipliers of the cycles of $F(x)$ is cyclic, and a generator is the unique multiplier of least span.*

Let M denote this unique multiplier. From Theorem 9.4, there follows:

* It is understood that all congruences in which the modulus is not indicated are to be taken to the modulus p over the field of the p residues $0, 1, \cdots, p-1$. For the properties of Galois fields which are assumed, see Dickson, work cited.

THEOREM 9.41. *The span of M divides the span of every other multiplier.*

THEOREM 9.5. *If $p^2+p+1\equiv\pi \pmod{\tau}$, then R is a multiplier of span π.*

Since $p^3\equiv 1 \pmod{\tau}$,

$$p^2\pi \equiv p\pi \equiv \pi \pmod{\tau}.$$

By (8.1),

$$RS_n \equiv \alpha^\pi(\alpha^n + \alpha^{pn} + \alpha^{p^2n}) \equiv \alpha^{n+\pi} + \alpha^{p(n+\pi)} + \alpha^{p^2(n+\pi)} \equiv S_{n+\pi}.$$

Hence by Theorem 9.1, R is a multiplier of span π.

As an immediate consequence of these theorems, we see that R is congruent to a power of M, modulo p, and that the span of M divides π.

THEOREM 9.6. *If $\epsilon(M)$ is the exponent to which the multiplier M belongs modulo p, and if μ is its span, then*

$$\tau = \epsilon(M)\mu \tag{9.2}$$

*where τ is the period of $F(x)$.**

$\mu \mid \tau$; for if $\tau = s\mu + t$ $(0 \leqq t \leqq \mu - 1)$, then by (9.1)

$$M^{\tau-s}A_n \equiv A_{n+(\tau-s)\mu} \equiv A_{n+t} \qquad (n=0, \cdots, \tau-1)$$

so that $\mu \mid t$; $t=0$. Similarly, $\epsilon(M) \mid \tau$ so that $\epsilon(M)\cdot\mu \mid \gamma\tau$ where $\gamma = (\epsilon(M), \mu) =$ 3 or 1. But

$$A_n \equiv M^{\epsilon(M)}A_n \equiv A_{n+\epsilon(M)\mu} \qquad (n = 0, \cdots, \tau-1).$$

Hence $\tau \mid \epsilon(M)\mu$, so that either $\tau = \epsilon(M)\mu$ or $3\tau = \epsilon(M)\mu$.

The latter case can occur only when $(\epsilon(M), \mu) = 3$; but then

$$A_{n+\tau} \equiv A_n \equiv M^{\epsilon(M)/3}\cdot A_n$$

so that $M^{\epsilon(M)/3} \equiv 1$, contradicting the definition of $\epsilon(M)$.

We shall call μ the *restricted period* of $F(x)$; since it is a divisor of p^2+p+1, we may write

$$p^2 + p + 1 = \kappa\cdot\mu. \tag{9.3}$$

We easily find that

$$M^\kappa \equiv R, \quad M^3 \equiv R^\mu, \tag{9.31}$$

---

* (9.2) is a special case of a theorem given in Carmichael I, p. 355. Carmichael calls μ the restricted period of the sequence whose characteristic number is τ.

so that

$$\epsilon(R) \mid \epsilon(M) \mid 3\epsilon(R), \tag{9.32}$$

where $\epsilon(R)$ is the exponent to which R belongs, modulo p.

If $p \equiv 2 \pmod 3$, then $p^2+p+1 \equiv 1 \pmod 3$ and it follows from Theorem 9.6 and equation (9.32) that $\tau = \epsilon(R)\mu$ where $\mu \mid p^2+p+1$ and $(\mu, 3) = 1$. The concluding section of the paper is devoted to the more interesting case when $p \equiv 1 \pmod 3$.

10. **Period for primes of form $3m+1$.** We shall assume throughout this section that

$$p = 3^k n + 1, \ (n, 3) = 1; \ k \geqq 1. \tag{10.1}$$

Then $p^2+p+1 \equiv 0 \pmod 3$, $\not\equiv 0 \pmod 9$, and from (9.3),

$$\kappa\mu/3 \equiv 1 \pmod{\epsilon(M)} \equiv 1 \pmod{\epsilon(R)}. \tag{10.2}$$

THEOREM 10.1. *If p is of the form $3^k n+1$, and μ denotes the restricted period of $F(x)$, then $\mu \equiv 0 \pmod 3$ when and only when $\epsilon(R) \equiv 0 \pmod{3^k}$.*

If this last condition holds, then

$$\tau = \epsilon(R)\mu, \ M \equiv R^{\mu/3} \pmod p. \tag{10.3}$$

Let $\mu = 3\mu'$. Then $(\mu', 3) = 1$, $(\kappa, 3) = 1$, and from (10.2) $\kappa\mu' \equiv 1 \pmod{\epsilon(M)}$. From (9.31), $R \equiv M^{\kappa} \pmod p$ and

$$M \equiv R^{\mu'} \pmod p. \tag{10.31}$$

Hence by (9.32), $\epsilon(M) = \epsilon(R)$. Assume that

$$\epsilon(M) = 3^s \cdot \sigma, \ (\sigma, 3) = 1; \ s \leqq k;$$

then by (9.2), $\tau = 3^{s+1}\tau'$;

$$\tau'; \quad (\tau', 3) = 1.$$

Now it is easily seen that $\alpha^{\tau'}$ is a primitive 3^{s+1} root of unity, modulo p, and hence a residue of p if and only if $s < k$. Assume that $s < k$. Then if $\alpha^{\tau'} \equiv Q$, $\alpha^{p\tau'} \equiv \alpha^{p^2\tau'} \equiv Q$, so that by (8.1),

$$QS_n \equiv S_{n+\tau'},$$

and by Theorem 9.1, Q is a multiplier. By Theorem 9.4, $3^{s+1} = \epsilon(Q)$; but $\epsilon(Q) \mid \epsilon(M)$. Hence $s = k$ and

$$\epsilon(R) = \epsilon(M) \equiv 0 \pmod{3^k}. \tag{10.32}$$

Conversely, if $\epsilon(R)\equiv 0 \pmod{3^k}$, then (10.32) follows from (9.32). If $\mu\not\equiv 0 \pmod 3$, then $\kappa\equiv 0 \pmod 3$, and (9.32) gives

$$M^{\kappa\epsilon(M)/3} \equiv 1 \equiv R^{\epsilon(M)/3} \equiv R^{\epsilon(R)/3} \pmod p,$$

contrary to the definition of $\epsilon(R)$. Equation (10.3) now follows from Theorem 9.6, (10.32) and (10.31).

THEOREM 10.2. *If* $\epsilon(R)\equiv 0 \pmod 3$, $\not\equiv 0 \pmod{3^k}$, *then* $\tau = 3\epsilon(R)\mu$, *where* $\mu \mid (p^2+p+1)/3$.

The last part of the theorem follows immediately from Theorem 10.1, so that it is sufficient, in view of Theorem 9.6, to prove that $\epsilon(M) = 3\epsilon(R)$. But this equality follows from (9.31), (9.32), since $(\mu, \epsilon(R)) = 1$.

THEOREM 10.21. *If* R *is not a cubic residue of* p, τ *is of the form* $3\epsilon(R)\sigma$, *where* $\sigma \mid (p^2+p+1)/3$.

If R is not a cubic residue of p, $\epsilon(R)\equiv 0 \pmod 3$, and the theorem follows from Theorems 10.1 and 10.2.

If $\epsilon(R)\not\equiv 0 \pmod 3$, then $(\mu, 3) = 1$, but I have not found a criterion to distinguish whether $\tau = 3\epsilon(R)\mu$ or $\tau = \epsilon(R)\mu$. The discovery of such a criterion would fill a serious lacuna in the theory. To illustrate the two cases possible, take $p = 7$. Then $p^2+p+1 = 57 = 3\cdot 19$, so that $\mu = 19$. For the irreducible polynomial modulo 7, $F(x) = x^3+x-1$, $\epsilon(R) = 1$ and we find by direct computation that the period τ is $57 = 3\epsilon(R)\mu$. However, for x^3-3x^2+4x-1, the period is only $19 = \epsilon(R)\mu$.

Finally, the case $p = 3$ may be easily treated by a direct enumeration of the possible cases.*

---

* Draeger's Thesis contains such an enumeration for certain forms of $F(x)$.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.