ON SEQUENCES DEFINED BY LINEAR RECURRENCE RELATIONS*

BY

H. T. ENGSTROM†

I. INTRODUCTION

A sequence of rational integers

$$u_0, u_1, u_2, \cdots \tag{1}$$

is defined in terms of an initial set $u_0, u_1, \cdots, u_{k-1}$ by the recurrence relation

$$u_{n+k} + a_1 u_{n+k-1} + \cdots + a_k u_n = a, \quad n \geqq 0, \tag{2}$$

where $a, a_1, a_2, \cdots, a_k$ are given rational integers. The purpose of this paper is to investigate the periodicity of such sequences with respect to a rational integral modulus m. Carmichael‡ has studied the period for a modulus m whose prime divisors exceed k and are prime to a_k. In this paper, I give a solution to the problem without restriction on m. If m is prime to a_k the sequence (1) is periodic from the start; otherwise, it is periodic after a definite number of initial terms.

DEFINITION 1. *We say that π is a general period of the recurrence* (2) *for the modulus m if every sequence of rational integers satisfying* (2) *has the period π* (mod m).

THEOREM 1. *The minimum period μ* (mod m) *of a sequence* (1) *satisfying* (2) *is a divisor of any general period π* (mod m) *of* (2).

For, since (1) has the period π, $\pi \geqq \mu$. Suppose μ does not divide π, that is, $\pi = q\mu + \rho$, where $0 < \rho < \mu$. Then $u_{i+q\mu+\rho} \equiv u_i$ (mod m), that is, $u_{i+\rho} \equiv u_i$ (mod m) and (1) has the period ρ, which is contradictory.

The algebraic equation

$$F(x) = x^k + a_1 x^{k-1} + \cdots + a_k = 0 \tag{3}$$

is said to be associated with the recurrence (2). We obtain general periods (mod m) of (2) in terms of the decompositions

$$F(x) \equiv \phi_1(x)^{e_1} \phi_2(x)^{e_2} \cdots \phi_r(x)^{e_r} \pmod{p} \tag{4}$$

---

* Presented to the Society, September 11, 1930; received by the editors in August, 1930.

† National Research Fellow, California Institute of Technology.

‡ R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quarterly Journal of Mathematics, vol. 41 (1920), pp. 343–372.

for the prime divisors p of m, where the $\phi_i(x)$ are prime functions (mod p) whose degrees we denote by k_i.

For the case of periodicity (mod p) it is shown in Section II that we may choose a polynomial $f(x) \equiv F(x)$ (mod p) so that p is not a divisor of the index* of $f(x)$ and hence, by the theorem of Dedekind, (4) implies a corresponding prime ideal decomposition of p in the field generated by a root of $f(x) = 0$. General periods of (2) (mod p) are obtained directly from the general solution of (2) by use of the theorem of Fermat in an algebraic field.

The results for the prime power modulus p^α are obtained directly from those (mod p) by the theorem of Section IV. In Section V the solution for a composite modulus m is expressed in terms of the solutions for the prime divisors of m.

The theorems obtained include those given by Carmichael for primes greater than k. The methods may be readily extended to the study of periodicity for an ideal modulus of algebraic sequences defined by linear recurrence relations.

II. Periodicity (mod p)

2.1. It is seen that any change of $F(x)$ (mod p) such that the new polynomial is of degree k with leading coefficient unity does not change the associated sequences (mod p). We prove the following lemma:

Lemma 1. *We may choose a polynomial* $f(x) \equiv F(x)$ (mod p) *with the following properties*:

(i) $f(x)$ *is irreducible of degree* k *with leading coefficient unity.*

(ii) p *does not divide the index of* $f(x)$.

(iii) If θ *is a root of* $f(x) = 0$ *and* p *contains precisely the* α*th power of a prime ideal* $\mathfrak{p}$ *in* $K(\theta)$, *then* $f'(\theta)$ *contains precisely* $\mathfrak{p}^{\alpha-1+\rho}$ *where* $\rho = 1$ *or* 0 *according as* α *is or is not divisible by* p.

(iv) $1 - \theta \not\equiv 0 \pmod{\mathfrak{p}^2}$ *for any prime ideal divisor* $\mathfrak{p}$ *of* p *in* $K(\theta)$.

If, in (4), $e_i > 1$, we write

$$f_i(x) = \phi_i(x)^{e_i} + p(1 + \phi_i(x)). \tag{5}$$

If $e_i = 1$ we write

$$f_i(x) = \phi_i(x) + p. \tag{6}$$

The discriminant of the product

* If θ is any root of the irreducible equation $f(x) = 0$, d the discriminant of the field $K(\theta)$, and D the discriminant of $f(x)$, then $D = \kappa^2 d$, where κ is a rational integer which is called the index of θ or of $f(x)$.

$$P(x) = \prod_{i=1}^{r} f_i(x)$$

is not zero. For the discriminant of each $f_i(x)$ is not zero since the $f_i(x)$ are algebraically irreducible* and the resultant of $f_i(x)$ and $f_j(x)$ is not zero for $i \neq j$. Suppose the discriminant of $P(x)$ contains precisely p^δ. We set

$$f(x) = P(x) + p^{\delta+2}R(x), \tag{7}$$

where $R(x)$ is a polynomial of degree $k-1$ chosen so that $f(x)$ satisfies the Eisenstein irreducibility criterion for another prime q. Then $f(x)$ is irreducible and of degree k with leading coefficient unity.

Since

$$f(x) = \phi_1(x)^{e_1}\phi_2(x)^{e_2} \cdots \phi_r(x)^{e_r} + pM(x), \tag{8}$$

where $M(x) \not\equiv 0 \pmod{p, \phi_i(x)}$, $i = 1, 2, \cdots, r$, it follows by the criterion of Dedekind that p is not a divisor of the index of $f(x)$.

Hence, by the theorem of Dedekind, (4) implies the prime ideal decomposition

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}, \quad N(\mathfrak{p}_i) = p^{k_i} \tag{9}$$

in the field defined by a root θ of $f(x) = 0$. Furthermore,

$$\mathfrak{p}_i = (p, \phi_i(\theta)) \qquad (i = 1, 2, \cdots, r). \tag{10}$$

From (10), $f_j(\theta)$ is prime to $\mathfrak{p}_i$ for $i \neq j$. Hence, from (7), since $f(\theta) = 0$, $f_i(\theta) \equiv 0 \pmod{\mathfrak{p}_i^{e_i(\delta+2)}}$, and

$$f'(\theta) \equiv f_i'(\theta)Q(\theta) \pmod{\mathfrak{p}_i^{e_i(\delta+2)}}, \tag{11}$$

where $Q(\theta)$ is prime to $\mathfrak{p}_i$. Hence $f'(\theta)$ contains the same power of $\mathfrak{p}_i$ as $f_i'(\theta)$. If $e_i = 1$, $f_i'(\theta) = \phi_i'(\theta)$ is prime to $\mathfrak{p}_i$. If $e_i > 1$,

$$f_i'(\theta) = [e_i\phi_i(\theta)^{e_i-1} + p]\phi_i'(\theta).$$

But since $\phi_i(x)$ is a prime function (mod p), $\phi_i'(\theta)$ is prime to $\mathfrak{p}_i$. Hence $f'(\theta)$ contains $\mathfrak{p}_i^{e_i}$ or $\mathfrak{p}_i^{e_i-1}$ according as e_i is or is not divisible by p, and (iii) is proved.

If $F(1) \equiv 0 \pmod{p}$ we choose $\phi_1(x) = x - 1$. Then, from (8), $f(1) \not\equiv 0 \pmod{p^2}$. Suppose $1 - \theta \equiv 0 \pmod{\mathfrak{p}_i^2}$ for some i. We have the contradiction $N(1-\theta) = f(1) \equiv 0 \pmod{p^2}$. Hence (iv) is proved. Furthermore, by (10), the only prime ideal divisor of p which divides $1-\theta$ is the ideal $\mathfrak{p} = (p, \theta - 1)$.

* Cf. Ö. Ore, *Zur Theorie der Irreduzibilitätskriterien*, Mathematische Zeitschrift, vol. 18 (1923), p. 287.

2.2. We shall consider the sequence

$$v_0, v_1, v_2, \cdots \tag{12}$$

associated with $f(x)$ such that $v_i = u_i$, $i = 0, 1, 2, \cdots, k-1$. Then $v_i \equiv u_i \pmod{p}$ for all i. If $\theta_1, \theta_2, \cdots, \theta_k$ are the roots of $f(x) = 0$, the general term of the sequence (12) is given by

$$v_n = \frac{a}{f(1)} + \beta_1\theta_1^n + \beta_2\theta_2^n + \cdots + \beta_k\theta_k^n, \tag{13}$$

where the β_j are algebraic constants, that is, independent of n. If we set $n = 0, 1, 2, \cdots, k-1$ and insert the initial values $v_0, v_1, \cdots, v_{k-1}$, on solving for the β_j we obtain

LEMMA 2. *The general term of the sequence* (12) *is given by* (13), *where*

$$\beta_j = \frac{\gamma_j}{f'(\theta_j)} + \frac{a\delta_j}{(1-\theta_j)f'(\theta_j)} \tag{14}$$

and γ_j, δ_j *are integers in* $K(\theta_j)$.

2.3. We shall develop some modifications of the theorem of Fermat. Let p have the decomposition (9) in $K(\theta)$. If ω is an integer of $K(\theta)$ prime to p, and $P_i = p^{k_i} - 1$, then by the theorem of Fermat

$$\omega^{P_i} \equiv 1 \pmod{\mathfrak{p}_i} \qquad (i = 1, 2, \cdots, r), \tag{15}$$

or

$$\omega^{P_i} = 1 + \pi,$$

where π is an integer in $K(\theta)$ divisible by $\mathfrak{p}_i$. Taking the pth power we have

$$\omega^{pP_i} \equiv 1 \pmod{\mathfrak{p}_i^{e_i+1}} \text{ or } \pmod{\mathfrak{p}_i^{p}} \tag{16}$$

according as $p > e_i$ or $p \leqq e_i$. Suppose $p^{\epsilon_i} \leqq e_i < p^{\epsilon_i+1}$. Taking successive pth powers of (15) and writing $E_i = p^{\epsilon_i}$, we obtain

$$\omega^{E_iP_i} \equiv 1 \pmod{\mathfrak{p}^{E_i}}, \tag{17}$$

and hence, if ω is prime to p,

$$\omega^{pE_iP_i} \equiv 1 \pmod{\mathfrak{p}^{e_i+E_i}} \text{ or } \pmod{\mathfrak{p}^{pE_i}} \tag{18}$$

according as $e_i + p^{\epsilon_i} < p^{\epsilon_i+1}$ or $\geqq p^{\epsilon_i+1}$.

2.4. From (4) and Lemma 1, p has the prime ideal decomposition

$$p = \mathfrak{p}_{1j}^{e_1}\mathfrak{p}_{2j}^{e_2} \cdots \mathfrak{p}_{rj}^{e_r}, \quad N\mathfrak{p}_{ij} = p^{k_i}$$

in the field $K(\theta_j)$. Let G denote the Galois field formed by composition of the fields $K(\theta_j), j=1, 2, \cdots, k-1$. We have

LEMMA 3. *The ideals* $\prod_{i=1}^{r}\mathfrak{p}_{ij}$, $j=1, 2, \cdots, k$, *have a common ideal divisor* $\mathfrak{P}$ *in* G.

For if $\mathfrak{P}$ is a prime ideal divisor of p in G, then for each j there exists an i such that $\mathfrak{p}_{ij}$ is divisible by $\mathfrak{P}$.

2.5. Let e denote the maximum e_i in (4) and l the least common multiple of $p^{k_i}-1, i=1, 2, \cdots, r$. We consider first the case $(a_k, p)=1, a\equiv 0 \pmod{p}$. Then the roots θ_j are prime to p. If $e=1$, the denominators in (14) are prime to p by Lemma 1. Hence, by (15),

$$\theta_j^{\,l} \equiv 1 \left(\mod \prod_{i=1}^{r}\mathfrak{p}_{ij}\right) \qquad (j = 1, 2, \cdots, k),$$

and, by Lemma 3,

$$v_{n+l} \equiv v_n \pmod{\mathfrak{P}} \qquad (n = 0, 1, 2, \cdots).$$

Since the v_i are rational integers and congruent (mod p) to the u_i, we have

$$u_{n+l} \equiv u_n \pmod{p} \qquad (n = 0, 1, 2, \cdots),$$

and hence obtain

THEOREM 2. *If* $(a_k, p)=1, a\equiv 0 \pmod{p}$ *in* (2) *and* $e=1$ *in* (4), *then* (2) *has the general period* l, *where* $e=\max e_i$ *in* (4) *and* l *is the least common multiple of* $p^{k_i}-1, i=1, 2, \cdots, r$.

Consider the case $(a_k, p)=1, a\equiv 0 \pmod{p}$ and $e>1$. From (18) we have

$$\theta_j^{\,p^{\epsilon+1}l} \equiv 1 \pmod{\mathfrak{p}_{ij}^{\,e_i+1}}. \tag{19}$$

Since the denominators in (14) contain at most $\mathfrak{p}_{ij}^{\,e_i}$ we have the following theorem:

THEOREM 3. *If* $(a_k, p)=1, a\equiv 0 \pmod{p}$, $p^\epsilon \leqq e < p^{\epsilon+1}$, $\epsilon \geqq 0$, *then* (2) *has the general period* $p^{\epsilon+1}l$.

2.6. We shall now consider the periodicity in the non-homogeneous case $a\not\equiv 0 \pmod{p}$. If $F(1)\not\equiv 0 \pmod{p}$ as in Lemma 1, it is seen that $1-\theta_j$ is prime to $p, j=1, 2, \cdots, k$. Hence, as above, we have the following theorem:

THEOREM 4. *If* $(a_k, p)=1, a\not\equiv 0 \pmod{p}$ *and* $F(1)\not\equiv 0 \pmod{p}$, *then if* $e=1$, *the recurrence* (2) *has the period* l; *if* $e>1$, *the recurrence* (2) *has the period* $p^{\epsilon+1}l$.

Suppose $a\not\equiv 0 \pmod{p}$ and $F(1)\equiv 0 \pmod{p}$. Let $\phi_1(x)=x-1$ and hence $\mathfrak{p}_{ij}=(p, \theta_j-1), j=1, 2, \cdots, k$. Suppose $p^\epsilon \leqq e < p^{\epsilon+1}$, $e=\max e_i$, $\epsilon \geqq 0$. If

$(e, p)=1$, the denominators in (14) contain at most $\mathfrak{p}_{ij}^{e_i}$, $i=1, 2, \cdots, r$. Hence it follows from (19) that (2) has the period $p^{\epsilon+1}l$. If p divides e_1, then $\epsilon \geqq 1$ and $p^{\epsilon+1} \geqq e_1+2$. Hence (18) gives

$$\theta_j^{p^{\epsilon+1}l} \equiv 1 \pmod{\mathfrak{p}_{ij}^{e_1+2}}$$

while (19) holds for $i \neq 1$. But the denominators in (14) contain at most $\mathfrak{p}_{ij}^{e_i}$ for $i \neq 1$ and $\mathfrak{p}_{ij}^{e_1+1}$. Hence we have the following theorem:

THEOREM 5. *If* $(a_k, p)=1$, $a \not\equiv 0 \pmod{p}$ *and* $p^\epsilon \leqq e < p^{\epsilon+1}$, *then* (2) *has the general period* $p^{\epsilon+1}l \pmod{p}$ *where* $e=\max e_i$ *in* (4) *and* l *is the least common multiple of* $p^{k_i}-1$, $i=1, 2, \cdots, r$.

We state a corollary of these theorems:

COROLLARY. *If* $(a_k, p)=1$ *and* $p>e$ *then* (2) *has the general period* $l \pmod{p}$ *when* $e=1$ *and* $F(1) \not\equiv 0 \pmod{p}$, *otherwise it has the general period* $pl \pmod{p}$.

The results of Carmichael for $p>k$ are contained in Theorems 1 to 4.

2.7. We now consider the case where p divides a_k, that is, $f(x)$ contains the factor $x \pmod{p}$. Suppose that $f(x)$ contains precisely $x^{e_2} \pmod{p}$, that is, $a_{k-i} \equiv 0 \pmod{p}$, $i=0, 1, \cdots, e_2-1$ and $a_{k-e_2} \not\equiv 0 \pmod{p}$. We may write $\mathfrak{p}_{2j}=(p, \theta_j)$, $j=1, 2, \cdots, k$. Then $(\mathfrak{p}_{ij}, \theta_j)=1$ for $i \neq 2$. Hence $\theta_j^\beta \equiv \theta_j^{e_2} \pmod{\mathfrak{p}_{2j}^{e_2}}$ for all $\beta > e_2$ while the results of §2.5 hold for the ideals $\mathfrak{p}_{ij}$, $i \neq 2$. Furthermore $1-\theta_j$ is not divisible by $\mathfrak{p}_{2j}$ and the denominators in (14) contain at most $\mathfrak{p}_{2j}^{e_2}$. Hence we have the following theorem:

THEOREM 6. *If* p *divides* a_k *and the last* s *coefficients of* (2) *are divisible by* p, $a_{k-s} \not\equiv 0 \pmod{p}$, *the sequence* (1) *is periodic* (mod p) *except for the initial terms* $u_0, u_1, \cdots, u_{s-1}$, *and* (2) *has the general period given by Theorems* 2 *to* 5 *inclusive.*

III. PERIODICITY (mod p). A SECOND METHOD

3.1. We consider again in this section the periodicity of (2) (mod p) for $(a_k, p)=1$ and $a=0$ and obtain an improved result for the case $e=p$. Instead of the $f(x)$ of II we consider the associate polynomial

$$\pi(x) = \prod_{i=1}^{r} \phi_i(x)^{e_i}. \tag{20}$$

Let ρ_{ij}, $j=1, 2, \cdots, k_i$, be the roots of $\phi_i(x)=0$. Then the general solution of a homogeneous recurrence associated with (20) is given by

$$v_n = \sum_{i,j} \left\{ c_{ij}^{(1)} + c_{ij}^{(2)} \binom{n}{1} + \cdots + c_{ij}^{(e_i)} \binom{n}{e_i - 1} \right\} \rho_{ij}^n. \tag{21}$$

If we set $n=0, 1, \cdots, k-1$ and insert the initial terms $v_0, v_1, \cdots, v_{k-1}$, it is seen that the determinant Δ of the coefficients of the c's is precisely a determinant of Bonolis* whose value is

$$\Delta = \pm \left[\prod_{i,j} \rho_{ij}^{(1/2)e_i(e_i-1)} \right] \prod (\rho_{\alpha\beta} - \rho_{\gamma\delta})^{e_\alpha e_\gamma}, \tag{22}$$

where the second product extends over all differences of distinct roots ρ_{ij}, only one permutation of a given pair being included. We prove

LEMMA 4. *If* $(a_k, p)=1$, *then* Δ *is prime to* p.

For since $(a_k, p)=1$, the roots ρ_{ij} are all prime to p. If $\alpha \neq \gamma$, since the resultant of $\phi_\alpha(x)$ and $\phi_\beta(x)$ is prime to p, the differences $\rho_{\alpha\beta}-\rho_{\gamma\delta}$ are prime to p. If $\alpha=\gamma$ the differences $\rho_{\alpha\beta}-\rho_{\alpha\delta}$ are prime to p since the discriminant of a prime function $\phi_\alpha(x)$ is prime to p.

By the theorem of Dedekind, p is a prime ideal of degree k_i in the fields $K(\rho_{ij})$, $j=1, 2, \cdots, k$. Hence by the theorem of Fermat

$$\rho_{ij}^{P_i} \equiv 1 \pmod{p}, \tag{23}$$

where $P_i=p^{k_i}-1$. We obtain the following theorem directly from (2) since the denominators of the c's are prime to p by Lemma 4.

THEOREM 7. *If* $p \geqq e$ *and* $(a_k, p)=1$, $a=0$, *then* (2) *has the general period* l *or* pl (mod p) *according as* $e=1$ *or* $e>1$.

The period given by Theorem 7 is less than that of II for the single case $p=e$. The denominators in (21) contain, in general, a higher power of p than those in (14). It is possible, however, that the results of II may be obtained from (21) by an analysis of the minors of Δ.

IV. PERIODICITY (mod p^α)

4.1. In this section we prove a theorem which gives a general period of (2) (mod p^α) directly from the results already obtained (mod p). Let us first consider the case $(a_k, p)=1$. We prove the following lemmas:

LEMMA 5. *If a non-homogeneous recurrence* (2) *has the general period* π (mod m), *then* π *is a period* (mod m) *of the corresponding homogeneous recurrence.*

For if $[u_i]$ is a sequence satisfying (2) for $a \neq 0$, then $[u_i]$ has the period π (mod m). If $[v_i]$ is any sequence satisfying (2) for $a=0$, then $[u_i-v_i]$ is a sequence satisfying (2) for $a \neq 0$. Hence $[u_i-v_i]=[w_i]$ has the period π (mod m). It follows that $[u_i-w_i]=[v_i]$ has the period π (mod m).

* A. Bonolis, *Sviluppi di alcuni determinanti*, Giornale di Matematiche, vol. 15 (1877), p. 133.

LEMMA 6. *If the recurrence* (2) *has the general period* $\pi \pmod{p^\beta}$ *then it has the period* $p\pi \pmod{p^{\beta+1}}$, $\beta \geqq 1$.

For, replacing n by $n+\pi$ in (2) and subtracting (2), we obtain

$$(u_{n+\pi+k} - u_{n+k}) + a_1(u_{n+\pi+k-1} - u_{n+k-1}) + \cdots + a_k(u_{n+\pi} - u_n) = 0. \tag{24}$$

Hence, since π is a period of (2) $\pmod{p^\beta}$,

$$U_i = (u_{i+\pi} - u_i)/p^\beta \qquad (i = 1, 2, \cdots) \tag{25}$$

is a sequence of integers satisfying (2) with $a=0$. By Lemma 5, (25) has the period $\pi \pmod{p^\beta}$. Consider the subsequence $U_{i+j\pi}$ where i is fixed but arbitrary and j has the range 0, 1, 2, $\cdots$. The first differences of this subsequence and hence the $(p-1)$th differences are divisible by p^β. If Δ_j^γ denotes the γth difference for variable j, we have

$$\Delta_j^{p-1}U_{i+j\pi} = \Delta_j^p u_{i+j\pi}/p^\beta \equiv 0 \pmod{p^\beta}. \tag{26}$$

Hence

$$[\Delta_j^p u_{i+j\pi}]_{j=0} \equiv 0 \pmod{p^{2\beta}},$$

that is,

$$u_{i+p\pi} - \binom{p}{1}u_{i+(p-1)\pi} + \binom{p}{2}u_{i+(p-2)\pi} + \cdots + (-1)^p u_i \equiv 0 \pmod{p^{2\beta}}. \tag{27}$$

If p is odd we may group the terms in (27) and obtain

$$(u_{i+p\pi} - u_i) + \binom{p}{1}(u_{i+(p-1)\pi} - u_{i+\pi}) + \cdots + \binom{p}{(p+1)/2}(u_{i+(p+1)\pi/2} - u_{i+(p-1)\pi/2}) \equiv 0 \pmod{p^{2\beta}}. \tag{28}$$

But the differences on the left are divisible by p^β, and the binomial coefficients are divisible by p. Hence

$$u_{i+p\pi} - u_i \equiv 0 \pmod{p^{\beta+1}}. \tag{29}$$

If $p=2$, (27) becomes

$$u_{i+2\pi} - 2u_{i+\pi} + u_i \equiv 0 \pmod{p^{2\beta}},$$

or

$$(u_{i+2\pi} - u_i) - 2(u_{i+\pi} - u_i) \equiv 0 \pmod{2^{2\beta}}.$$

Hence (29) follows for $p=2$ and the lemma is proved.

The following theorem is obtained directly from Lemma 6 and is sufficient to determine a period $\pmod{p^\alpha}$ of (2) from the results $\pmod{p}$ of II.

THEOREM 8.* *If* $(a_k, p)=1$, *and the recurrence* (2) *has the general period* $\pi \pmod{p}$, *then it has the general period* $p^{\alpha-1}\pi \pmod{p^\alpha}$.

Let $e=\max e_i$ in (4) and l the least common multiple of $p^{k_i}-1$, $i=1, 2, \cdots, r$. We state an immediate corollary:

COROLLARY. *If* $p>e$, *then* (2) *has the general period* $p^{\alpha-1}l$ *or* $p^\alpha l \pmod{p^\alpha}$ *according as* $e=1$ *or* $e>1$.

4.2. Suppose $(a_k, p)\neq 1$ and $F(x)\equiv x^s F_1(x) \pmod{p}$, where $F_1(x)$ does not contain $x \pmod{p}$. We have shown in §2.7 that (1) is periodic (mod p) after s terms. We shall show by induction that (1) is periodic (mod p^α) after αs terms. For suppose (2) has the general period $\pi \pmod{p^\beta}$ after βs terms, $\beta \geqq 1$. Then (25) defines a sequence of integers for $i \geqq \beta s$; namely, $U_{\beta s}, U_{\beta s+1}, \cdots$. This sequence has the period $\pi \pmod{p}$ after s terms, that is, for $i \geqq (\beta+1)s$. Hence we obtain the congruence (27) for the modulus $p^{\beta+1}$ for $i \geqq (\beta+1)s$ and as above

$$u_{i+p\pi} - u_i \equiv 0 \pmod{p^{\beta+1}}, \quad i \geqq (\beta+1)s.$$

By induction we obtain the following theorem:

THEOREM 9. *If the last* s *coefficients of* (2) *are divisible by* p, $a_{k-s}\not\equiv 0 \pmod{p}$, *then* (1) *is periodic* (mod p^α) *after* αs *terms and a period* (mod p^α) *is determined by Theorem* 8.

V. PERIODICITY (mod m)

For the general rational integral modulus m the following theorem suffices for obtaining a general period of (2) (mod m) from the previous results.

THEOREM 10. *If* $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ *the least common multiple* L *of a set of general periods* λ_i *of* (2) $\pmod{p_i^{\alpha_i}}$, $i=1, 2, \cdots, t$, *is a general period of* (2) (mod m).

For $u_{n+L}\equiv u_n \pmod{p_i^{\alpha_i}}$, $i=1, 2, \cdots, t$, and hence $u_{n+L}\equiv u_n \pmod{m}$.

We have obtained in this paper general periods of the recurrence (2), that is, periods of (1) for arbitrary initial values. Whether or not there exists a set of initial values for which the sequence has the general period obtained has not been discussed. Furthermore, it is possible that improved results may be obtained for sequences with special initial values such as the fundamental sequences of Lucas.

* For $e=1$, $(a_k, p)=1$, $F(1)\not\equiv 0 \pmod{p}$, this theorem gives the period $p^{\alpha-1}l \pmod{p^\alpha}$. The period obtained by Carmichael for the same case with $p>k$ is $p^\alpha l$.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.