AN ISOMORPHISM BETWEEN LINEAR RECURRING SEQUENCES AND ALGEBRAIC RINGS*

BY
MARSHALL HALL

I. INTRODUCTION

1. The Thirteenth Century was in but its second year when Fibonacci (or Pisano) proposed a problem on the number of offspring of a pair of rabbits, whose solution led to the sequence of numbers now named after him. There is reason to believe that Fermat derived many of his arithmetic theorems from a knowledge of recurrences and, certainly, his celebrated Last Theorem may be stated as a problem on sequences. Lucas† was the first to make any extended researches on sequences, establishing a great many properties of certain second order sequences. Carmichael [1]‡ in 1920 made the first attack on sequences in general, and established their fundamental property of modular periodicity.

This paper undertakes a general survey of the modular properties of linear recurring sequences, beginning from the results of a paper by H. T. Engstrom and two by Morgan Ward.§ No problems on sequences are considered here which are not strictly modular, though questions on divisibility sequences|| and their remarkable factorization properties are closely related.

The mechanism which the author uses for examining the properties of sequences is an isomorphism between the set of all sequences satisfying a fixed recurrence and a polynomial ring of operators. The isomorphism is not with the abstract ring but with a particular realization of it, and this is not especially surprising as a linear sequence is essentially an exponential function. This isomorphism may be derived from the theory of generating functions, and includes the fundamental identity used in Ward [11].

In Chapter II the isomorphism is set up and the basic properties of the ring are examined and their interpretation is given for the sequences. For example, the zero divisors of the ring correspond to the sequences which satisfy recurrences of lower order.

---

* Presented to the Society, September 3, 1936; received by the editors August 27, 1937.

† For the early bibliography see Dickson's *History of the Theory of Numbers*.

‡ Numbers in square brackets refer to the bibliography at the end of this paper.

§ Engstrom [3] and Ward [11], [12].

|| Lucas [7], Lehmer [6], Hall [4], Ward [14].

Chapter III considers in some detail the periods modulus $p^j, (j=1, 2, \cdots)$, of a fixed sequence and of all sequences. The structure of possible periods is thoroughly investigated and a method is given for its complete determination. The period patterns are shown to be dependent upon the ideal structure (or lattice) of the ring.

Chapter IV gives a similar dissection of the numeric patterns of sequences, and their relation to null sequences. Necessary and sufficient conditions that a sequence be null modulo m are found, and a very elegant criterion for "p-adically null" sequences is given.

Chapter V treats some questions on the distribution of modular residues in sequences. It is shown that the internal modular structure of sequences is intimately bound up with residual groups. A diophantine equation on distribution numbers which Ward found for third order sequences is shown to be one of a family of equations, and it is also shown that similar equations hold for sequences of any order.

Whereas Chapters III and IV would seem to exhaust the possibilities of the problems considered, Chapter V is only the introduction to some extremely recondite questions. The author will consider these further in another paper.

II. The isomorphism

2. Consider a linear recurrence of kth order

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n \tag{2.1}$$

in which $a_1, a_2, \cdots, a_k$ are rational integers. Two operations on sequences (v_n) satisfying (2.1) may be defined:

I. *Sum*:

$$(v_n) + (w_n) = (v_n + w_n).$$

II. *Scalar product*:

$$t(v_n) = (tv_n), \qquad \text{any rational integer.}$$

In addition an operator x is defined:

III. $x(v_n) = (v_{n+1})$.

These three operations may be combined to yield a ring $R(x)$ of polynomial operators on the sequences, under which the sequences satisfying (2.1) are closed. This ring is easily shown to be associative, commutative, and distributive.

The characteristic polynomial of the recurrence (2.1), $f(x) = x^k - a_1 x^{k-1} - \cdots - a_k$, has the property that

$$f(x)(v_n) = (0) \tag{2.2}$$

for all sequences (v_n) satisfying (2.1). We may set up an isomorphism between the sequences satisfying (2.1) and the ring $R(x)$ by the correspondences:

Primary isomorphism:

$$1 \rightleftarrows (w_n), \qquad h(x) \rightleftarrows h(x)(w_n), \tag{2.3}$$

where (w_n) is the sequence defined by $w_0 = w_1 = \cdots = w_{k-2} = 0$, $w_{k-1} = 1$, which shall be called the unit sequence. It is a simple matter to verify that (2.3) actually defines a one-to-one correspondence between the sequences satisfying (2.1) and the ring $R(x)$ of polynomials modulo $f(x)$. In fact

$$(v_n) \rightleftarrows V(x) = v_0 x^{k-1} + (v_1 - a_1 v_0) x^{k-2} + \cdots + (v_{k-1} - \cdots - a_{k-1} v_0) \tag{2.4}$$

for any sequence (v_n). This polynomial $V(x)$ is the (unique) polynomial of degree less than k in the residue class modulo $f(x)$ corresponding to (v_n) by the isomorphism (2.3). We note in passing that the sequence (v_n) is integral if and only if the coefficients of the corresponding canonical polynomial $V(x)$ are integral.

It is sometimes convenient to use a secondary form of the isomorphism in considering single terms of the sequence (v_n).

Secondary isomorphism:

$$\begin{aligned} V(x) &\to v_0, \\ xV(x) &\to v_1, \\ &\cdots\cdots, \\ x^i V(x) &\to v_i. \end{aligned} \tag{2.5}$$

The secondary isomorphism is simply a correspondence between an element $h(x)$ of the ring $R(x)$ and the coefficient of x^{k-1} in the canonical representative of the residue class $h(x)$ modulo $f(x)$. The relations of (2.5) are justified by the definition III of the operator x and by (2.4).

3. If $f(x)$ is reducible, then $R(x)$ contains zero divisors, and if $f(x)$ has multiple factors, then $R(x)$ contains nilpotent elements. Hence the theory of fields may not be applied to $R(x)$ although a number of theorems on fields hold true. Again, $R(x)$ is not in general a maximal order, and the arithmetic of algebras is not directly applicable to the arithmetic of $R(x)$. But we may apply many theorems on algebraic number fields to $R(x)$ without reproving them because of the following theorem:

THEOREM 3.1. PRESERVATION OF IDENTITIES. *If $F(a_1, \cdots, a_k)$ is a polynomial in $a_1, \cdots, a_k$ with rational integral coefficients and if $F = 0$ whenever $a_1, \cdots, a_k$ are rational integers such that $f(x) = x^k - a_1 x^{k-1} - \cdots - a_k$ is irreducible, then $F \equiv 0$.*

If we take $f(x)$ arbitrary modulo p and irreducible modulo q, then $F=0$. Hence $F\equiv 0 \pmod{p}$ for $a_1, \cdots, a_k$ arbitrary modulo any p and $F\equiv 0$.

If we define the *norm* of $(v_n)\rightleftarrows V(x)$ by $N(v_n)=N[V(x)]$, then we have

$$N(v_n) = (-1)^{[k/2]} \begin{vmatrix} v_0, & v_1, \cdots, & v_{k-1} \\ v_1, & v_2, \cdots, & v_k \\ v_2, & v_3, \cdots, & v_{k+1} \\ \cdots & \cdots & \cdots \\ v_{k-1}, & v_k, \cdots, & v_{2k-2} \end{vmatrix}. \tag{3.1}$$

Similarly for the *spur* (or *trace*)

$$S(v_n) = kv_{k-1} - (k-1)a_1v_{k-2} - \cdots - a_{k-1}v_0. \tag{3.2}$$

It is easily verified that the norm of the unit sequence is unity and that its trace is k.

A classical result of interest here is the following:

THEOREM OF KRONECKER. *A necessary and sufficient condition that* (v_n) *satisfy a recurrence of lower order than* (2.1) *is that* $N(v_n)=0$.

Hence, with respect to the recurrence of lowest order which (v_n) satisfies, $N(v_n)\neq 0$.

Another rational integer associated with a sequence (v_n) is its *container*. For some purposes this is more useful than the norm.

DEFINITION. *If* $(v_n)\rightleftarrows g(x)$ *then the container of* (v_n) *is the least positive rational integer which* $g(x)$ *divides.*

Since the rational integers which $g(x)$ divides form a modulus, they are all multiples of the container. There is a very close relationship between the container and the norm given by the following theorem:

THEOREM 3.2. *Precisely the same primes divide the container and the norm.*

If m is the container of $(v_n)\rightleftarrows g(x)$, then $h(x)g(x)=m$. Hence $N(h(x))\,N(g(x))=N(m)=m^k$ and so $N(v_n)\,|\,m^k$. But from the definition of the container $m\,|\,N(v_n)$. Hence every prime dividing m divides $N(v_n)$ and conversely.

III. PERIOD PATTERNS

4. If for a fixed τ and all $n\geqq n_0$

$$u_{n+\tau} \equiv u_n \pmod{m}, \tag{4.1}$$

then the least τ is said to be the period* of (u_n) modulo m and the least n_0

* The notation and terminology of this paper are in agreement with Ward [11] for the most part. I use "period" following Engstrom rather than Ward's "characteristic number."

the numeric. The principal results on periods and numerics are given in Carmichael [1], Engstrom [3], and Ward [11]. Here we shall not consider periods individually. We shall study the period patterns of sequences satisfying (2.1), where two sequences are said to have the same period pattern modulo p if their periods modulo p^j, $(j=1, 2, 3, \cdots)$, are the same.

Following Ward [11], we reduce the determination of periods to the solution for τ_i of congruences

$$(x^{\tau_i} - 1)g(x) \equiv 0 \pmod{p^j, F_i(x)}, \tag{4.2}$$

where $(u_n) \rightleftarrows g(x)$, and

$$f(x) \equiv F_1(x)F_2(x) \cdots F_r(x) \pmod{p^j}, \quad F_i(x) \equiv h_i(x)^{e_i} \pmod{p}, \tag{4.3}$$

the $h_i(x)$ being irreducible and distinct modulo p.*

THEOREM 4.1. *The partial period τ_i of $(u_n) \rightleftarrows g(x)$ modulo p^j is the exponent to which x belongs modulo the ideal A_i of all y satisfying $yg(x) \equiv 0$ (modd p^j, $F_i(x)$).*

This theorem and its proof are obvious, but it seems desirable to emphasize from the start the relation of periods to ideal theory.

As we shall confine our attention to a single component $F_i(x)$, the subscript i will be omitted hereafter. Moreover we may whenever desirable restrict ourselves to *ordinary* sequences for which $g(x) \not\equiv 0$ (modd p, $F(x)$). If (u_n) is not ordinary, then $g(x) \equiv p^s k(x)$ (modd p^j, $F(x)$), where $(v_n) \rightleftarrows k(x)$ is ordinary, and the period of (u_n) modulo p^j is the period of (v_n) modulo p^{j-s}.

If λ is the exponent to which x belongs modulo p, $h(x)$,† that is, the least solution of

$$x^n \equiv 1 \pmod{p, h(x)}, \tag{4.4}$$

and if r is determined by

$$p^{r-1} < e \leqq p^r, \tag{4.5}$$

then $\nu = p^r\lambda$ is the principal period of (2.1) modulo p (Ward [11], Theorem 10.4). The principal period (by definition the period of the unit sequence) modulo p is a fortiori a period of any sequence modulo p. But no writer has considered the possibility that a sequence may have a period which is a proper divisor of ν. This can indeed happen and we shall later see that such periods appear in period patterns in a special role.

---

* This is the well known Schönemann decomposition. The $F_i(x)$ are unique and p-adically determinate.

† Information on the value of λ is given by a law of higher reciprocity due to F. K. Schmidt [9], pp. 165–166. For a particularly simple proof of this relation see O. Ore [8], pp. 272–273.

THEOREM 4.2. *The period of any ordinary sequence modulo p^i is of the form $p^i\lambda$.*

Since $p^{i-1}\nu = p^{r+i-1}\lambda$ is a general period modulo p^i (Engstrom [3], p. 217), it is sufficient to show that the period of an ordinary (u_n) is a multiple of λ. If the ideal A_j of Theorem 4.1 is the unit ideal, then $g(x) \equiv 0$ $(p^i, F(x))$ and (u_n) is not ordinary. Otherwise, since A_j contains the primary ideal $[p^i, F(x)]$, A_j must be contained in the prime ideal $[p, h(x)]$. Hence we must have

$$x^\tau \equiv 1 \text{ (modd } p, h(x)), \tag{4.6}$$

and τ is a multiple of λ.

Now ν may be the principal period not only modulo p, but also modulo p^σ, where the greatest σ will be called the *defect.** Again, for a particular sequence $(u_n) \rightleftarrows g(x)$, ν may be a period not only modulo p^σ but also modulo $p^{\sigma+\rho}$, where ρ is called the initial defect as it depends on the initial values. The values of ρ and σ determine all periods which are multiples of ν as given in the following:

THEOREM 4.3. *If $p^\sigma \neq 2$, and ν is a period of (u_n) modulo $p^{\rho+\sigma}$, then the period of (u_n) modulo p^j for $j > \rho+\sigma$ is $p^{j-\rho-\sigma}\nu$; when $p^\sigma = 2$, if 2ν is a period modulo exactly 2^s, then the period of (u_n) modulo 2^j is 2^{j-s+1} for $j > s$.*

For the method of proof see Ward [11], pp. 619–620. The statement of his Theorem 11.1 is inaccurate as it does not consider the possibility of periods which are proper divisors of ν. Note that ν is not said to be the period of (u_n) modulo $p^{\rho+\sigma}$ but merely one of the periods. Examples can be given in which the period of (u_n) modulo $p^{\rho+\sigma}$ is a proper divisor of ν.

Example. $u_{n+3} = 3u_{n+1} - u_n$ with $u_0 = 1$, $u_1 = 2$, $u_2 = 4$. Here $\nu = 6$ is a period of (u_n) modulo 3 but not modulo 9. The period of (u_n) modulo 3 is, however, 2.

5. From Theorem 4.2 the periods of (u_n) modulo p^i are among the numbers λ, $p\lambda$, $p^2\lambda$, $\cdots$. Let $p^{j(i)}$ be the highest power of p for which $p^i\lambda$ is a period of (u_n). Then the period of (u_n) modulo p^i is $p^i\lambda$, where i is the least number for which $j(i) \geqq j$. And from Theorem 4.3 the period pattern of (u_n) is completely determined given $j(0), \cdots, j(r)$. We may represent a period pattern graphically if, in the cartesian plane, we plot the points $(i, j(i))$ and connect successive points with straight lines. The resulting graph will be called the *period path* of (u_n).

In congruences (modd p^i, $F(x)$), the *partial container* plays the role of the container in $R(x)$. The partial container is zero or the least positive rational

* Ward [11], p. 622, gives some information which shows that the defect can be greater than unity only in certain rare cases. The determination of the defect is the generalization of the (unsolved) problem of the Fermat quotients $(a^{p-1}-1)/p$.

number which $g(x)$ divides modulo p^j $F(x)$. Evidently the partial container must be p^{δ_1}, with $\delta_1 \leqq \delta$ if p^δ is the highest power of p dividing the container of $g(x)$. It may be shown without difficulty that the exponent δ_1 is the same whatever the value of j.

THEOREM 5.1. *If p^{δ_h} is the partial container of $x^{p^h\lambda}-1$ (modd p^j, $F(x)$) then $p^h\lambda$ is a period of some ordinary (v_n) modulo p^{δ_h}, but of no ordinary (u_n) modulo p^j for $j > \delta_h$.*

Let $h(x)(x^{p^h\lambda}-1) \equiv p^{\delta_h}$ (modd p^j, $F(x)$). If $h(x) \equiv 0$ $(p, F(x))$, then $h(x) \equiv pk(x)$ (modd p^j, $F(x)$) and $k(x)(x^{p^h\lambda}-1) \equiv p^{\delta_h - 1}$ $(p^{j-1}, F(x))$ and p^{δ_h} is not the partial container of $x^{p^h\lambda}-1$ contrary to the assumption. Hence $h(x) \not\equiv 0$ $(p, F(x))$ and $(v_n) \rightleftarrows h(x)$ is ordinary. Moreover $p^h\lambda$ is a period of (v_n) modulo p^{δ_h} since $h(x)(x^{p^h\lambda}-1) \equiv 0$ $(p^{\delta_h}, F(x))$. Suppose that $p^h\lambda$ is a period of some $(u_n) \rightleftarrows g(x)$ modulo p^{δ_h+1}. Then $g(x)(x^{p^h\lambda}-1) \equiv 0$ $(p^{\delta_h+1}, F(x))$ and so $g(x)h(x)(x^{p^h\lambda}-1) \equiv 0$ $(p^{\delta_h+1}, F(x))$ or $g(x)p^{\delta_h} \equiv 0$ $(p^{\delta_h+1}, F(x))$, whence $g(x) \equiv 0$ $(p, F(x))$ and (u_n) is not ordinary.

If $f(x)$ has a root of unity among its roots, the container of some $x^n - 1$ is zero and this theorem is without content in the form here given. In §6 it will be shown in what way the theory may be modified to cover this case.

The complete set of (ordinary) period paths modulus 3^j belonging to the recurrence

$$u_{n+4} = -u_{n+3} - 3u_{n+2} + 5u_{n+1} - u_n \tag{5.1}$$

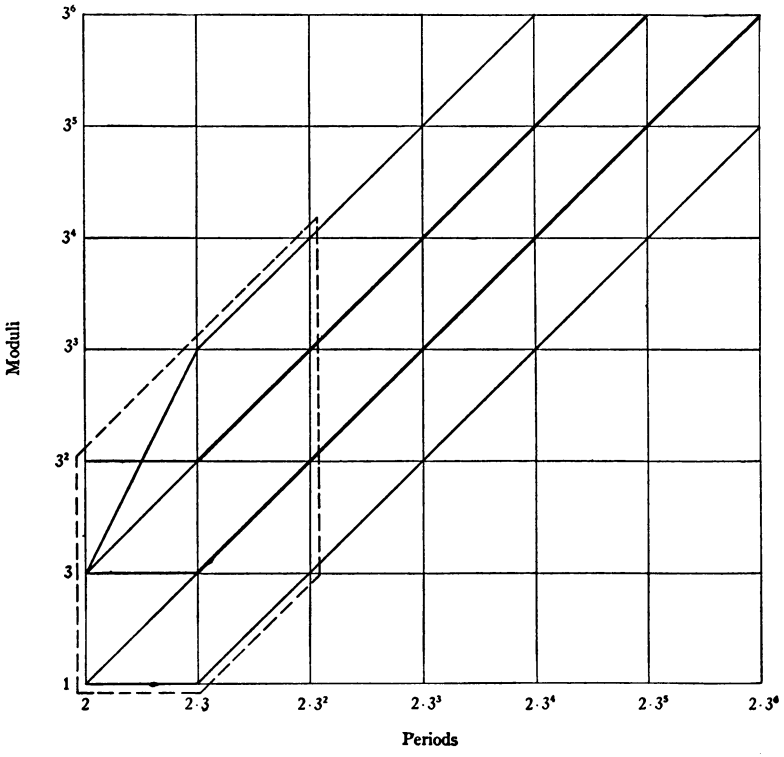
is given here.

There are six different period paths:

$(0, 0, 0, 1, \cdots) \rightleftarrows 1$ passing through	$(0, 0); (1, 0); (2, 1),$
$(0, 0, 1, 0, \cdots) \rightleftarrows x + 1$	$(0, 0); (1, 1); (2, 2),$
$(1, -1, -2, 11, \cdots) \rightleftarrows x^3 + 1$	$(0, 1); (1, 1); (2, 2),$
$(1, -1, -2, 8, \cdots) \rightleftarrows x^3 - 2$	$(0, 1); (1, 2); (2, 3),$
$(1, 2, -5, -1, \cdots) \rightleftarrows x^3 + 3x^2 - 5$	$(0, 1); (1, 3); (2, 4),$
$(1, -1, 1, 8, \cdots) \rightleftarrows x^3 + 3x + 1$	$(0, 2); (1, 2); (2, 3).$

Here, as $f(x) \equiv (x+1)^4 \pmod 3$, we have $\lambda = 2$, $r = 2$, and $\nu = 18$. Theorem 4.3 shows that the period paths to the right of the line whose abscissa r corresponds to ν, are straight lines of inclination $\pi/4$.

The *period polygon* (dotted in the following figure) is defined as that polygon bounded on the left by the line $x = 0$, on the right by $x = r$, above by the line segments passing through the points (i, δ_i) in order, and below by the segments joining $(0, 0)$, $(r-1, 0)$, and (r, σ). Theorems 4.3 and 5.1 dispose of all period paths except those parts of ordinary period paths lying within the period polygon.



Principle of addition of paths. If the path of $g(x)$ passes through (i, j_1) and the path of $k(x)$ passes through (i, j_2), then the path of $g(x)+k(x)$ passes through (i, j'), where $j'=\min(j_1, j_2)$ when $i \neq j_2$ and $j' \geqq j_1$ when $j_1=j_2$.

Proof. Suppose $j_1<j_2$. Then $(x^{p^{2\lambda}}-1)g(x) \equiv 0 \ (p^{i_1}, F(x)) \not\equiv 0 \ (p^{i_1+1}, F(x))$ and $(x^{p^{2\lambda}}-1)k(x) \equiv 0 \ (p^{i_2}, F(x))$. Hence $(x^{p^{2\lambda}}-1)(g(x)+h(x)) \equiv 0 \ (p^{i_1}, F(x)) \equiv (x^{p^{2\lambda}}-1)g(x) \not\equiv 0 \ (p^{i_1+1}, F(x))$. For $j_1=j_2$ the proof is obvious.

All $A(x)$ which satisfy $A(x)(x^{p^{i\lambda}}-1) \equiv 0 \ (p^i, F(x))$ form an ideal $A_{i,j}$. The path of an element belonging to $A_{i,j}$ will pass through or above (i, j). The path of (u_n) shows clearly to which $A_{i,j}$ $g(x)$ belongs and to which it does not belong.

An ideal is said to be ordinary if it contains an ordinary element.

Inclusion principle. If A is an ordinary ideal and is not included in the ideal B, then A contains an ordinary element which is not contained in B.

Proof. Choose an ordinary $h(x)$ from A. If $h(x)$ is in B, then we choose a $k(x)$ from A which is not in B. If $k(x)$ is ordinary, it satisfies our requirements. If $k(x)$ is not ordinary, then $h(x)+k(x)$ is ordinary and is in A but not in B.

Since the period of (u_n) modulo p^{i+1} is a multiple of the period modulo p^i, any period path must remain horizontal or go upward as we move to the right. We shall find further properties of the paths and give some existence theorems.

THEOREM 5.2. *There is an ordinary path passing through an arbitrary point of the period polygon.*

The lower boundary of the period polygon is the period path of the unit sequence. By Theorem 5.1 there is an ordinary path through an arbitrary point of the upper boundary. Note that as in the example of (5.1) the upper boundary is not necessarily a period path itself. If a point is s units above the lower boundary, then $(u_n) \rightleftarrows p^s$ passes through this point, and if we add this to the ordinary path passing through the point on the upper boundary immediately above it, we find an ordinary path passing through this point.

COROLLARY. $A_{i,j+1}$ *is properly contained in* $A_{i,j}$.

By actual calculation $A_{i,1} = [p,\ h(x)^{e-p^i}]$ for $i = 0, \cdots, r-1$. Also $p^{j-1}h(x)^{e-p^i}$ is in $A_{i,j}$ but not in $A_{i-1,j}$; hence $A_{i-1,j}$ is properly included in $A_{i,j}$. Using these simple facts, the principle of inclusion, and the principle of addition of paths, we may prove the existence of a variety of paths.

THEOREM 5.3. *There is an ordinary path through the following points of the period polygon*: (a) $(i-1, j)$, (i, j), *and* $(i+1, j)$ *provided that the last is not on the right boundary*; (b) $(i-1, j-1)$, (i, j), *and* $(i+1, j)$ *if all are interior points*; (c) $(i-1, j)$, (i, j), *and* $(i+1, j+1)$ *if all are interior points.* (d) *There is a path going up from every point on the lower boundary.* (e) *There is a horizontal path to the right from every point on the left or upper boundary.* (f) *There is an upward path from every point on the left boundary except possibly at the upper corner.* (g) *There is a path coming from below to every point on the right boundary, with one possible exception when* $p^\sigma = 2$, *and* $[p, h(x)] = [2, x+1]$.

The method of proof is the same in all cases, and only (g) will be proved here. Let the ordinary path (v_n) through (r, δ_r) pass through $(r-1, t)$. The unit sequence is ordinary and passes through $(r-1, 0)$ and (r, σ). If $(u_n) \rightleftarrows p^{j-\sigma}$, $(\sigma < j \leqq \delta_r)$, then $(u_n + v_n)$ is ordinary and passes through (r, j) and through $(r-1, j-\sigma)$ if $j-\sigma < t$, through $(r-1, t)$ if $j-\sigma > t$. Hence there is an exception only if $j-\sigma = t$ and (u_n+v_n) passes through $(r-1, j)$ and (r, j), that is, $(r-1, t+\sigma)$ and $(r, t+\sigma)$. If $\sigma > 1$, then $(w_n) \rightleftarrows p^{t+\sigma-1}$ passes through $(r-1, t+\sigma-1)$ and $(r, t+2\sigma-1)$; whence $(u_n+v_n+w_n)$ passes through $(r-1, t+\sigma-1)$ and $(r-1, t+\sigma)$. If $\sigma = 1$, it may happen that $(u_n+v_n+w_n)$ passes through $(r-1, t+\sigma-1)$ and (r, s) with $s > t+\sigma = t+1$. We now have an ordinary path $(y_n) \rightleftarrows y(x)$ through $(r-1, t+1)$ and $(r, t+1)$ and another

$(z_n)\rightleftarrows z(x)$ through $(r-1, t)$ and (r, s) with $s>t+1$ and no path to $(r, t+1)$ from below. (y_n+z_n) passes through $(r-1, t)$ and $(r, t+1)$ but may not be ordinary. If it is not ordinary, take $c\not\equiv 0$, 1 $(p, h(x))$; then the path of $y(x)+cz(x)$ is ordinary and passes through $(r-1, t)$ and $(r, t+1)$ as we wished. It is impossible to find such a c only if $[p, h(x)]=[2, x+1]$. In this case there may be an exception.

Example. If $F(x)=x^2+2x+5$, $p=2$, there is no ordinary path from below to (1, 3).

6. When $f(x)$ has one of its roots a root of unity, Theorem 5.1 may be without content, but all period paths may nevertheless be predicted by a finite process if we modify of the theory as in the following example:

$$u_{n+4} = -u_{n+3} + 3u_{n+2} - 4u_{n+1} + 2u_n. \tag{6.1}$$

Here $f(x)=x^4+x^3-3x^2+4x-2=(x^2-x+1)(x^2+2x-2)$, and if we take $p=3$, then $\lambda=2$ and $\nu=18$.

$$\begin{aligned}(x^2-1)(5x^3+9x^2-6x+17) &= -9,\\ (x^6-1)(x^2+2x-2) &= 0,\\ (x^{18}-1)(x^2+2x-2) &= 0.\end{aligned} \tag{6.2}$$

Hence 2 may be a period modulo 1, 3, or 9, but 6 may be a period modulo 3^i for any i. Let $(u_n)\rightleftarrows g(x)$ be any sequence satisfying (6.1). Then we may write $g(x)=g_1(x)(x^2+2x-2)+g_2(x)$, where $g_2(x)=ax+b$. If (u_n) does not satisfy a recurrence of order lower than (6.1), then by the Theorem of Kronecker, $g_2(x)$ may not vanish since $N[g_1(x)(x^2-2x-2)]=0$.

Let $g_2(x)=3^ig_3(x)$, where $g_3(x)\not\equiv 0 \pmod 3$. Then $(x^6-1)g(x) = 3^i(x^6-1)g_3(x)$ or $(x^6-1)g(x)\equiv 3^i(x^2-x+1)(x^4+x^3-x-1)g_3(x) \pmod{(x^2-x+1)(x^2+2x-2)}$. Hence we may reduce $(x^4+x^3-x-1)g_3(x)$ modulo x^2+2x-2, that is, to $(-11x+7)g_3(x)$, and as the partial container of $-11x+7 \pmod{3^i, x^2+2x-2}$ is 3, we find that $(x^6-1)g(x)$ is divisible either by 3^i or 3^{i+1}. Similarly the partial container of $(x^{18}-1)/(x^2-x+1) \pmod{3^i, x^2+2x-2}$ is 9. We may summarize these results by saying that 2 is a period modulo 1, 3, or 9; 6 is a period modulo 3^i or 3^{i+1}; and 18 is a period modulo 3^{i+1} or 3^{i+2}. For periods greater than 18, we may apply Theorem 4.3.

The methods used in this example are perfectly general and may be applied to any case in which the characteristic has roots of unity.

THEOREM 6.1. *If the greatest common divisor of $x^{p^h\lambda}-1$ and $F(x)$ is $r(x)$, then $p^h\lambda$ is a period of $(u_n)\rightleftarrows g(x)$ modulo p^t, $(i\leqq t\leqq i+\delta_h)$, where $g(x)\equiv p^ig_1(x) \pmod{p^i, F(x)/r(x)}$ and p^{δ_h} is the partial container of $(x^{p^h\lambda}-1)/r(x) \pmod{p^i, F(x)/r(x)}$.*

7. If $p^\sigma = 2$, we have not only the possibility of an exception to Theorem 5.3, but Theorem 4.3 is applicable only to periods greater than 2ν. Closer study of this case yields some interesting results.

In this case we will have

$$x^\nu - 1 \equiv 2M(x) \pmod{2^i, F(x)}, \tag{7.1}$$

where $M(x) \not\equiv 0\ (2, F(x))$. By direct calculation we obtain

$$x^{2\nu} - 1 \equiv 4M(x)[M(x) + 1] \quad (2^i, F(x)). \tag{7.2}$$

If $g(x)M(x)[M(x)+1] \equiv 2^t S(x)\ (2^i, F(x))$, then 2ν is a period of $(u_n) \rightleftarrows g(x)$ modulo 2^{t+2}. But of the two quantities $M(x)$, $M(x)+1$, one or the other must be relatively prime to the modulus. Suppose $M(x)+1$ is relatively prime to the modulus. Then $g(x)M(x) \equiv 2^t S(x)/(M(x)+1) \equiv 2^t S_1(x)\ (2^i, F(x))$, and from (7.1) $g(x)(x^\nu - 1) \equiv 2^{t+1} S_1(x)\ (2^i, F(x))$, whence ν is a period of (u_n) modulo 2^{t+1}. In this case the period paths to the right of $x = r$ (corresponding to period ν) are straight lines of inclination $\pi/4$, that is, Theorem 4.3 may be applied for all periods greater than ν, as in the case of paths when $p^\sigma \neq 2$.

Suppose, on the other hand, that $M(x)+1$ is not relatively prime to the modulus. In this case $M(x)$ is relatively prime and its partial container is 1. Hence from (7.1) every ordinary period path goes through $(r, 1)$. Let $M(x)+1 \equiv 2^\kappa T(x)$, $T(x) \not\equiv 0\ (2, F(x))$, and let 2^λ be the partial container of $T(x)$ (modd $2^i, F(x)$). Then it is easily shown by previous methods that there are ordinary paths passing through $(r+1, i)$ with $2 + \kappa \leqq i \leqq 2 + \kappa + \lambda$. An example of this is given by $F(x) = x^4 + 3x^2 + 4x - 3$. Here $\nu = 6$,

$$x^6 - 1 = 2(-2x^3 + 6x^2 + 6x - 5) = 2M(x). \tag{7.3}$$

Here $M(x)+1 = 2T(x)$, where the partial container of $T(x)$ is 2. The graph of the period paths has a curious "elbow" in it.

IV. Numerics and null sequences

8. The numeric of a sequence (u_n) modulo m is the least integer $n(m)$ for which $u_{n+\tau} \equiv u_n \pmod{m}$, $n \geqq n(m)$, where τ is the period of (u_n) modulo m. The null index (if it exists) of a sequence (u_n) modulo m is the least integer $n_1(m)$ for which $u_n \equiv 0 \pmod{m}$, $n \geqq n_1(m)$ and is of course also the numeric. Theorem 4.1 of Ward [11] shows that the existence of a sequence with a prescribed numeric implies the existence of another sequence with the same null index. This theorem may be extended to include a prescribed set of numerics for a finite number of moduli.

Let $f(x) \equiv F(x)G(x) \pmod{p^i}$, where $F(x) \equiv x^e \pmod{p}$ and $G(x) \not\equiv 0\ (p, x)$. This is the Schönemann decomposition of $f(x)$ with the factors $F_2(x) \cdots F_r(x)$

combined into the single term $G(x)$. The congruence for the numeric of (u_n) modulo p^j is

$$x^n g(x) \equiv 0 \ (\text{modd } p^j, F(x)). \tag{8.1}$$

THEOREM 8.1. *A necessary and sufficient condition that* $(u_n) \rightleftarrows g(x)$ *be null modulo* p^j *is that* $g(x) \equiv 0$ (modd $p^j, G(x)$).

This theorem is given in Ward [11], pp. 613–614.

Let us call a sequence *p-adically null* if it is null modulo p^j for all j.

THEOREM 8.2. *If* p^δ *is the highest power of* p *dividing the container of* $(u_n) \rightleftarrows g(x)$, *then* (u_n) *cannot be null modulo* p^j *for* $j > \delta$ *unless* $G(x) = 1$, *in which case* (u_n) *is p-adically null.*

Let $g(x)h(x) \equiv p^\delta r \pmod{f(x)}$ where $r \not\equiv 0 \pmod{p}$. Then a fortiori $g(x)h(x) \equiv p^\delta r$ (modd $p^j, G(x)$) and hence $g(x) \not\equiv 0$ $(p^j, G(x))$ for $j > \delta$ unless $G(x) = 1$, in which case $g(x) \equiv 0$ (modd $p^j, G(x)$) for all j.

A less precise but more striking way of stating the same theorem is the following:

THEOREM 8.3. *If* (2.1) *is the recurrence of lowest order which* (u_n) *satisfies, then* (u_n) *is p-adically null if and only if p divides all of* $a_1, \cdots, a_k$.

It is possible to graph numeric paths of sequences in a way similar to that in which period paths were graphed. If n is a numeric of (u_n) modulo p^j but not modulo p^{j+1}, we plot the point (n, j). The broken line joining these points for $n = 0, 1, 2, \cdots$ is the numeric path of (u_n). There is an analogue to Theorem 5.1 for numeric paths, but not to Theorem 4.3. We note that a sequence is ordinary $[g(x) \not\equiv 0 \ (p, F(x))]$ if it is *not* purely periodic modulo p.

THEOREM 8.4. *The numeric path of the unit sequence is the lower boundary of all numeric paths, and the segments joining the points* (i, δ_i), *where* p^{δ_i} *is the partial container of* x^i *modulo* $p^j, F(x)$, *form the upper boundary of ordinary numeric paths.*

The proof is straightforward and parallels that of Theorem 5.1. The portion of the plane included between the lower and upper boundaries of ordinary numeric paths will be called the numeric sector.

THEOREM 8.5. *Let* $F(x) = x^e + b_1 x^{e-1} + \cdots + b_e$, *and let* p^{α_i} *be the highest power of* p *dividing* b_i. *If we define* $\alpha = \alpha_i/i = \min(\alpha_1, \alpha_2/2, \cdots, \alpha_e/e)$, *then a point on the lower boundary of the numeric sector is either on or within a distance* $e\alpha_i$ *below the ray through the origin whose slope is* α. *If* $\beta = \beta_j/j = \min(\alpha_{e-1}, (\alpha_{e-2} + \alpha_e)/2, \cdots, (e-1)\alpha_e/e)$, *then any point on the upper boundary is either on or within a distance* $e\beta_j$ *above the ray through the origin whose slope is* $\alpha_e - \beta$.

We may define a commutative algebra $\mathfrak{A}(x)$ over the field of all algebraic numbers by taking $1, x, \cdots, x^{e-1}$ as basis elements and putting $F(x)=0$. The element $y=p^{-\gamma}x$ is integral in the sense of Deuring [2] (p. 68) if γ is a rational number less than or equal to α, but not for any γ greater than α. Hence $z=p^{-\alpha i}x^i=y^i$ satisfies an equation

$$z^s + c_1 z^{s-1} + \cdots + c_s = 0 \tag{8.2}$$

of degree not greater than e, where the c's are rational since z is a rational function of x, and are integral since z is an integral element of $\mathfrak{A}(x)$. Not all c's are divisible by p, for if they were, then $p^{-1/s}z$ would be an integral element of $\mathfrak{A}(x)$ and so also would be some $p^{-\gamma}x$ with $\gamma > \alpha$.

If (u_n) is the unit sequence satisfying a recurrence of characteristic $F(x)$, then by the secondary isomorphism (2.5)

$$x^{ni+\rho} \rightarrow u_{ni+\rho}. \tag{8.3}$$

Hence since $p^{\alpha i}z=x^i$, we may write

$$p^{n\alpha i}z^n x^\rho \rightarrow u_{ni+\rho}. \tag{8.4}$$

The elements $(x^\rho z^n)$, $n=0, 1, 2, \cdots$ and ρ fixed as one of $0, 1, \cdots, i-1$, satisfy the recurrence

$$v_{n+s} = -c_1 v_{n+s-1} - \cdots - c_s v_n. \tag{8.5}$$

Hence the leading coefficients in their minimal residues modulo $F(x)$ must also satisfy the same recurrence. But from (8.4) these are the sequence $(u_{ni+\rho}/p^{n\alpha i})$, $(n=0, 1, \cdots)$. Now the coefficients of (8.5) are rational integers and hence the denominators of a sequence satisfying this recurrence cannot exceed the denominators of the initial values. Hence the denominator of any one of the sequences $(u_{ni+\rho}/p^{n\alpha i})$, $(\rho=0, 1, \cdots, i-1)$, cannot exceed $p^{(e-1)\alpha i}$ and a fortiori $p^{(e-1)\alpha i}$. Hence $u_{ni+\rho}=p^{n\alpha i}v_n=p^{n\alpha i-\sigma}v_n^*$, where v_n^* is integral and $\sigma \leqq (e-1)\alpha_i$. As this relation holds for $\rho=0, \cdots, i-1$, we have $x^{ni+\rho}\equiv 0 \ (p^{n\alpha i-\sigma})$. Hence the lower boundary passes through or above the points $(ni+\rho, n\alpha_i-\sigma)$, and as $\rho<i$, $\sigma<(e-1)\alpha_i$, these points are not more than $e\alpha_i$ below the ray through the origin with slope $\alpha=\alpha_i/i$. On the other hand, no point of the lower boundary can lie above this ray, for if $x^n\equiv 0 \ (p^j)$ with $j>n\alpha$, then $p^{-j}x^n$ is an integral element of $\mathfrak{A}(x)$ and so also is $(p^{-j}x^n)^{1/n}$ or $p^{-j/n}x$. But $p^{-\gamma}x$ cannot be an integral element of $\mathfrak{A}(x)$ with $\gamma>\alpha$.

From Theorem 8.4 to determine the upper boundary it is necessary only to find the partial container of x^n (modd $p^i, F(x)$). We have

$$x(x^{e-1} + b_1 x^{e-2} + \cdots + b_{e-1}) = -b_e = p^{\alpha e}b \tag{8.6}$$

where $p \nmid b$. We may write this

$$xw = p^{\alpha_e} b. \tag{8.7}$$

Hence if $w^n = p^\kappa \bar{w}$ with $p \nmid w$, then $p^{n\alpha_e - \kappa}$ is the partial container of x^n. It remains to find the greatest power of p dividing w^n. But $w = b_e/x$ satisfies the rank equation

$$w^e + b_{e-1}w^{e-1} + \cdots + b_e^{e-2}b_1 w + b_e^{e-1} = 0. \tag{8.8}$$

Reasoning for w^n from this equation as for x^n from $F(x) = 0$, we find that $w^n \equiv 0 \pmod{p^{n\beta - \sigma}}$, where $0 \leqq \sigma \leqq e\beta_j$. Hence the partial container of x^n is $p^{n\alpha - n\beta + \sigma}$. This shows that a point on the upper boundary of the numeric sector is either on or within $e\beta_j$ units above the ray through the origin with slope $\alpha_e - \beta$. This completes the proof of the theorem, which incidentally justifies the use of the term "sector" for the portion of the plane containing ordinary numeric paths.

9. We now calculate the numeric paths.

THEOREM 9.1. *If p^δ is the partial container of $(u_n) \rightleftarrows g(x)$ modulo $p^i, F(x)$, then the numeric of (u_n) modulo p^i is at least as great as the numeric of the unit sequence modulo $p^{i-\delta}$.*

COROLLARY. *The numeric path of (u_n) remains within a distance δ above the lower boundary of the numeric sector.*

Proof. If n is the numeric of (u_n) modulo p^i, then by (8.1)

$$x^n g(x) \equiv 0 \ (\text{modd } p^i, F(x)), \tag{9.1}$$

and if $g(x)h(x) \equiv p^\delta \ (\text{modd } p^i, F(x))$, then multiplying (9.1) by $h(x)$ we obtain

$$x^n p^\delta \equiv 0 \ (\text{modd } p^i, F(x)), \tag{9.2}$$

whence $x^n \equiv 0 \ (\text{modd } p^{i-\delta}, F(x))$ and n must be at least as great as the numeric of the unit sequence modulo $p^{i-\delta}$, which is the least solution of this congruence.

In consequence of (9.1) we consider the coefficients of

$$[x^{ni+\rho}g(x)]/p^{n\alpha_i}, \qquad \rho = 0, \cdots, i-1; \ n = 0, 1, 2, \cdots, \tag{9.3}$$

which for ρ fixed, by a previous argument, satisfy recurrence (8.5). As before, the denominators cannot exceed $p^{e\alpha_i}$. The coefficients of

$$x^{ni+\rho}/p^{n\alpha_i} \tag{9.4}$$

cannot for any single value of n all be divisible by p, since then the path of the unit sequence would come above the ray through the origin with slope α. Similarly, by the corollary to Theorem 9.1 the coefficients of (9.3) cannot for

a single value of n all be divisible by $p^{\delta+1}$. Hence to determine the numeric path of (u_n), we need only know the values of the coefficients of (9.3) modulo p^{δ}. But this is equivalent to knowing the values of the coefficients of $p^{e\alpha_i}[x^{n_i+\rho}g(x)]/p^{n\alpha_i}$ modulo $p^{e\alpha_i+\delta}$ and these are sequences of integers satisfying (8.5). We are thus reduced to a finite problem, since the numeric and period of a sequence modulo $p^{e\alpha_i+\delta}$ are finite. But in general δ is not bounded for the set of all ordinary sequences satisfying the recurrence.

10. The following properties of period paths may easily be verified to hold for numeric paths:

(a) As we move to the right, the path never moves downward.

(b) Every non-ordinary numeric path is an upward translation of an ordinary path.

(c) The sum path of two paths passes through the lower of the two and through or above points of intersection.

(d) The elements corresponding to paths passing through or above a point (n, j) form an ideal $B_{n,j}$.

Using these properties and Theorem 8.4, we easily deduce the following theorem:

THEOREM 10.1. *Through an arbitrary point of the numeric sector there is an ordinary path.*

There is no analogue to Theorem 4.3 for numeric paths, but there is an important relation of another sort.

THEOREM 10.2. *If any finite section at the beginning of a numeric path is cut off, the remainder is a translation of an entire ordinary numeric path.*

Suppose the numeric path of $(u_n) \rightleftarrows g(x)$ passes through the point (n, j). We have

$$x^n g(x) = p^j h(x), \tag{10.1}$$

where $h(x) \not\equiv 0 \pmod{p}$. The section of the numeric path of (u_n) beyond (n, j) is the numeric path of $(v_n) \rightleftarrows h(x)$. For if

$$x^{n+m} g(x) = p^{j+i} t(x), \tag{10.2}$$

where $t(x) \not\equiv 0 \ (p)$, then $x^m[x^n g(x)] = x^m[p^j h(x)] = p^{j+i} t(x)$ or

$$x^m h(x) = p^i t(x), \tag{10.3}$$

and conversely.

One consequence of this theorem is that no small section of a numeric path can have peculiarities not exhibited by a path in the neighborhood of the origin. For example, no path may at any point rise more rapidly than the first

segments of the upper boundary or more slowly than the first segments of the lower boundary. The existence of a variety of path structures may be deduced from these two fundamental theorems by adding appropriate paths.

11. In one particular instance we may by a finite process predict all numeric paths. By Theorem 8.5 and the corollary to Theorem 9.1 there will certainly be infinitely many numeric paths when the upper ray is distinct from the lower ray. But when these coalesce there are only a finite number of paths. This happens only when $\alpha+\beta=\alpha_e$. But $\alpha\leqq\alpha_e/e$ and $\beta\leqq(e-1)\alpha_e/e$. Hence we must have $\alpha=\alpha_e/e$ and $\beta=(e-1)\alpha_e/e$. We may take $z=x^e/p^{\alpha_e}$ and we find that $N(z)=(b_e)^e/p^{e\alpha_e}\not\equiv 0\ (p)$. Hence in the recurrence (8.5) $c_e\not\equiv 0\ (p)$ and the (v_n) sequences are purely periodic modulo p^i. Consequently the lower boundary of the numeric sector must touch the ray infinitely often. If it passes through a point (n, j) on the ray,

$$x^n \equiv p^j h(x)\ (F(x)), \tag{11.1}$$

where $h(x)\not\equiv 0\ (p, F(x))$ and $j/n=\alpha$. If $h(x)\equiv 0\ (p, x)$, then $h(x)^e\equiv 0\ (p, x^e)\equiv 0\ (p, F(x))$. Then $x^{ne}\equiv p^{je}h(x)^e\equiv p^{je+1}s(x)\ (F(x))$. But $(je+1)/ne>\alpha$ and this would mean that the lower path goes above the ray. Hence $h(x)\not\equiv 0\ (p, x)$ and the partial container of x^n must be p^j, and the upper boundary must also pass through (n, j). Similarly the lower boundary must pass through every point on the ray through which the upper boundary passes. The boundaries form a series of sausage-like loops about the ray.

Let (r, i) be a point on the numeric path of $(u_n)\rightleftarrows g(x)$. Then

$$x^r g(x) \equiv p^i t(x)\ (F(x)), \tag{11.2}$$

where $t(x)\not\equiv 0\ (p, F(x))$. Multiplying (11.1) by $x^r g(x)$ we obtain

$$x^{n+r}g(x) \equiv p^{j+i}t(x)h(x)\ (F(x)), \tag{11.3}$$

and here $t(x)h(x)\not\equiv 0\ (p, F(x))$ since $h(x)$ is relatively prime to the modulus and $t(x)\not\equiv 0\ (p, F(x))$. Hence $(n+r, j+i)$ is on the numeric path of (u_n) and similarly $(2n+r, 2j+i)$ and so on. Consequently the entire path structure is given by that in the first loop.

12. In the study of both period and numeric patterns, it has been shown that the pattern of $(u_n)\rightleftarrows g(x)$ depends on which ideals of the $A_{i,j}$ (or $B_{n,j}$) contain $g(x)$ and which do not. These are a subset of the primary ideals contained in a single prime ideal $[p, h(x)]$. Hence the following equivalence criterion is of interest:

THEOREM 12.1. *A necessary and sufficient condition that elements y and z of $R(x)$ belong to the same primary ideals contained in $[p, h(x)]$ is that they have the same partial container p^δ (modd $p^i, F(x)$) and that*

$$z \equiv yu \ (p^\delta, F(x)), \qquad y \equiv zv \ (p^\delta, F(x)). \tag{12.1}$$

Necessity. Let the partial containers of y and z be p^{δ_1} and p^{δ_2}, respectively. If $\delta_1 \neq \delta_2$, suppose $\delta_1 < \delta_2$. Then $[p^{\delta_2}, z, F(x)]$ does not contain y. For if it does, then

$$y \equiv bz \ (p^{\delta_2}, F(x)). \tag{12.2}$$

There exist $w \not\equiv 0 \ (p, F)$ with $yw \equiv p^{\delta_1} \ (p^i, F)$ and $s \not\equiv 0 \ (p, F)$ with $zs \equiv p^{\delta_2} \ (p^i, F)$. Hence $swy \equiv bswz \ (p^{\delta_2}, F)$ and so

$$p^{\delta_1} s \equiv 0 \ (p^{\delta_2}, F); \qquad s \equiv 0 \ (p^{\delta_1 - \delta_2}, F) \tag{12.3}$$

contradicting $s \not\equiv 0 \ (p, F)$. Consequently $\delta_1 = \delta_2 = \delta$. Now the supposition that z is in $[p^\delta, y, F(x)]$ and that y is in $[p^\delta, z, F(x)]$ leads to the congruences (12.1).

Sufficiency. Any primary ideal A contained in $[p, h(x)]$ must contain some ideal $[p^i, F(x)]$ with a sufficiently large j. From (12.1) and $yw \equiv p^\delta \ (p^i, F(x))$

$$\begin{aligned} z &\equiv yu + p^\delta r \ (p^i, F(x)) \\ &\equiv yu + ywr \\ &\equiv y(u + wr) \\ &\equiv yu^*. \end{aligned} \tag{12.4}$$

Similarly $y \equiv zv^* \ (p^i, F(x))$. A fortiori

$$z \equiv yu^* \pmod{A}, \qquad y \equiv zv^* \pmod{A}; \tag{12.5}$$

hence $y \equiv 0 \pmod{A}$ implies $z \equiv 0 \pmod{A}$, and conversely.

V. Cycles and residual groups

13. The residues of a sequence (u_n) modulo m consist of a numeric section, $u_0, u_1, \cdots, u_{n_0-1}$, where n_0 is the numeric modulo m, and a periodic section $u_{n_0}, \cdots$. The periodic section consists of infinitely many repetitions of the *cycle* $u_{n_0}, \cdots, u_{n_0+\tau-1}$, where τ is the period modulo m. Any set of τ consecutive terms from the periodic section will be called a cycle. Each cycle is a cyclic permutation of any other. For most purposes it is convenient not to consider these cycles as distinct, and in this sense a sequence (u_n) has but one cycle modulo m. Whenever it is important to distinguish these, we shall call any particular one of them an *ordered cycle*. For the rest of the terminology used in this section, see Ward [12].

Here we shall restrict ourselves to the case in which the modulus is a prime p. If $p \nmid a_{k-r}$, $p \mid a_{k-r-1}, \cdots, p \mid a_k$, then the numeric section is included in $u_0, \cdots, u_{r-1}$ and these terms, being initial values, are arbitrary. Hence, without loss of generality, (u_n) may be supposed purely periodic, as the periodic section is independent of the numeric section. In addition, as the Theo-

rem of Kronecker holds true modulo p, with respect to the recurrence of lowest order which (u_n) satisfies modulo p, p is not a divisor of $N(u_n)$. Hence (Ward [11], p. 604) the period of (u_n) modulo p is the principal period.

In this section we shall always use the secondary isomorphism

$$x^n g(x) \rightarrow u_n, \tag{13.1}$$

and a cycle will correspond to the elements $x^n g(x)$, $(n=0, \cdots, \tau-1)$.

THEOREM 13.1. *The elements corresponding to a cycle of (u_n) form a coset of the cyclic group $\{x\}$ in the group of residues relatively prime to the modulus $p, f(x)$.*

Proof. The elements relatively prime to the modulus p, $f(x)$ form an abelian multiplicative group. As we are assuming (u_n) to be purely periodic, $p \nmid a_k$ and the element x is in this group, and so the cyclic group $\{x\}$ is also in this group. *As* $p \nmid N(u_n)$, $g(x)$ is relatively prime to the modulus. $x^\tau \equiv 1$ (modd $p, f(x)$) is the congruence for the (principal) period modulo p. Hence $\{x\}$ consists of the elements $1, x, \cdots, x^{\tau-1}$, and the elements $g(x)$, $xg(x), \cdots, x^{\tau-1}g(x)$ form a coset of this subgroup.

As a finite abelian group, the residues relatively prime to p, $f(x)$ are characterized completely by the generators and order invariants of the group. By a slight modification of the methods used in T. Takenouchi [10] these may be found explicitly. A knowledge of the generators and invariants will be presupposed here. Except when $f(x)$ has factors modulo p of high multiplicity they are very simple.

THEOREM 13.2. *If $y^n g(x) \rightarrow v_n$ by the secondary isomorphism, then (v_n) satisfies a recurrence whose characteristic is the minimal polynomial of y.*

For let

$$F(y) = y^s - b_1 y^{s-1} - \cdots - b_s = 0. \tag{13.2}$$

Certainly y, as a polynomial in x, satisfies an equation of degree k, but it may possibly satisfy an equation of lower degree. The elements $y^n g(x)$, $(n=0, 1, \cdots)$, satisfy

$$v_{n+s} = b_1 v_{n+s-1} + \cdots + b_s v_n \tag{13.3}$$

and hence their leading coefficients (v_n) must also satisfy it.

In studying cycles and the distribution of residues therein, we shall use not only the group G of residues prime to $p, f(x)$ (Theorem 13.1) and auxiliary recurrences (Theorem 13.2) but also theorems on the existence of sequences with zeros in prescribed positions, of which the two following are typical.

THEOREM 13.3. *There exists a sequence (u_n) satisfying* (2.1) *and not identically zero modulo p for which $u_n \equiv 0 \pmod{p}$ for $k-1$ arbitrary values of n.*

Proof. Write $(u_n) = (c_0 w_n + c_1 w_{n+1} + \cdots + c_{k-1} w_{n+k-1})$, where (w_n) is the unit sequence and the c's are to be determined by the following $k-1$ congruences:

$$u_{n_1} \equiv u_{n_2} \equiv \cdots \equiv u_{n_{k-1}} \equiv 0 \pmod{p}. \tag{13.4}$$

These are $k-1$ linear homogeneous congruences in k variables, and so there must exist a solution in which not all the c's vanish, and in turn (u_n) does not vanish identically. To know the exact number of solutions, we must know the rank of the w-matrix involved, and in general this is not known.

The following notation and terminology are almost exactly those of Ward [12], p. 170:

τ = period; μ = reduced period;
e = exponent to which basic multiplier m belongs mod p;
$\phi(f)$ = number of residues prime to $p, f(x)$;
κ = number of blocks.

$$\begin{aligned} x^{\mu} &\equiv m(p, f(x)); \\ \tau &= e\mu; \qquad et = p - 1; \\ \phi(f) &= (p-1)\mu\kappa = t\tau\kappa. \end{aligned} \tag{13.5}$$

THEOREM 13.4. *Let $0 < a < \mu$. Then among the representative reduced cycles, one from each block, there are precisely $(p^{k-2}-1)/(p-1)$ pairs of zeros in positions differing by a.*

Proof. In an unordered cycle there are as many pairs of zeros differing in position by a as there are ordered cycles made from it with zeros u_n and u_{n+a}, n fixed. In the block there will be $p-1$ times as many pairs of zeros differing in position by a as there are in a representative reduced cycle. Hence we must find the number of solutions of

$$u_n \equiv u_{n+a} \equiv 0 \pmod{p} \tag{13.6}$$

not vanishing identically and then divide by $p-1$. If we write $(u_n) = (c_0 w_n + \cdots + c_{k-1} w_{n+k-1})$, where (w_n) is the unit sequence, then the number of solutions of (13.6) will depend on the rank of the matrix

$$\begin{pmatrix} w_n, & w_{n+1}, & \cdots, & w_{n+k-1} \\ w_{n+a}, & w_{n+a+1}, & \cdots, & w_{n+a+k-1} \end{pmatrix}. \tag{13.7}$$

The rank of this matrix is two. It cannot be zero, for k consecutive terms of the unit sequence may not vanish. It cannot be one, for then the two rows would be proportional and a would be a multiple of the reduced period. Hence (13.6) has p^{k-2} solutions, of which one vanishes identically.

We are now in a position to prove the very interesting theorem:

THEOREM 13.5. *If $f(x)$ is irreducible modulo p, and b_i is the number of zeros in a reduced cycle of the ith block (the blocks having been appropriately ordered), then we have the following equations**

$$\begin{aligned} \sum b_i &= (p^{k-1}-1)/(p-1), \\ \sum (b_i^2 - b_i) &= (\mu-1)(p^{k-2}-1)/(p-1), \\ \sum b_i b_{i+r} &= (p^{k-2}-1)/(p-1), \qquad r = 1, \cdots, \kappa-1. \end{aligned} \tag{13.8}$$

LEMMA 1. *If $f(x)$ is irreducible modulo p, then*

$$e = (\tau, p-1). \tag{13.9}$$

Let $s=(\tau, p-1)$. From (13.5) both τ and $p-1$ are multiples of e, and hence s is a multiple of e. Let $\tau=ws$, where w must be a divisor of μ. From the congruence for the period we have

$$(x^w)^s \equiv 1 \text{ (modd } p, f(x)) \tag{13.10}$$

or, writing $x^w=z$,

$$z^s \equiv 1 \text{ (modd } p, f(x)). \tag{13.11}$$

Now as s is a divisor of $p-1$ this congruence must have s rational solutions, namely those of $z^s \equiv 1 \pmod{p}$. But since $f(x)$ is irreducible, the residues modd $p, f(x)$ form a Galois field and no equation can have more solutions than its degree. Hence all the possible values of z in (13.11) must be rational and we have

$$x^w \equiv \text{rational (modd } p, f(x)); \tag{13.12}$$

whence w must be a multiple of μ. But as w is also a divisor of μ, we must have

$$w = \mu, \qquad e = r = (\tau, p-1), \tag{13.13}$$

and the lemma is proved.

From the properties of the group of residues modulo $p, f(x)$ we may find a primitive root y (modd $p, f(x)$) such that

$$y^{\kappa t} \equiv x \text{ (modd } p, f(x)). \tag{13.14}$$

The period of y is p^k-1 and by application of Lemma 1 to y-cycles (Theorem 13.2) the reduced y-period is $\mu\kappa=(p^k-1)/(p-1)$. There is but one y-cycle

* In this theorem it is tacitly assumed that the recurrence is at least of third order. There can be no zeros in a cycle of a first order recurrence. In a second order sequence there is only one reduced cycle which contains any zeros, and this contains only one zero. A partial criterion for the appearance of a multiple of p in a second order sequence was given in Ward [13] and a complete criterion in Hall [5].

and the x-cycles, cosets of $\{x\}$ in G are obtained by starting from any term of the y-cycle and taking every κtth term after that. The reduced x-cycles form the terms $y^{n\kappa t+i}$, where $n=0, 1, \cdots, \mu-1$, and different (ordered) reduced cycles will correspond to different values of i.

LEMMA 2. *Two reduced x-cycles corresponding to i_1 and i_2 will belong to the same block if and only if $i_1 \equiv i_2 \pmod{\kappa}$.*

The number of blocks is κ, and hence it is sufficient to show that multiplying a reduced x-cycle by y^κ takes it into another reduced cycle of the same block. From (13.9) and (13.13)

$$e = (\tau, p-1) = (\mu e, et), \tag{13.15}$$

whence

$$(\mu, t) = 1. \tag{13.16}$$

Hence the equation $\mu s + tq = 1$ has integral solutions s and q. Multiplying we get $\mu\kappa s + \kappa tq = \kappa$. Thus $y^\kappa = y^{\mu\kappa s} y^{\kappa tq}$. But $\mu\kappa$ is the reduced period of y and hence

$$y^{\mu\kappa} \equiv g \pmod{p, f(x)}, \tag{13.17}$$

where g is rational. From (13.14) and (13.17) we now have

$$y^\kappa \equiv g^s x^q \pmod{p, f(x)}, \tag{13.18}$$

and multiplication of a reduced x-cycle by such a quantity takes it into another reduced cycle of the same block.

In consequence of this lemma, we may choose as representative reduced cycles, one from each block, the terms

$$y^{n\kappa t+i}, \qquad n = 0, 1, \cdots, \mu-1; \; i = 0, 1, \cdots, \kappa-1. \tag{13.19}$$

LEMMA 3. *There are as many zeros in the terms $y^{n\kappa+i}$ as there are in the terms $y^{n\kappa t+i}$, where $n=0, 1, \cdots, \mu-1$.*

In any cycle, two terms which differ in position by a multiple of the reduced period are both zeros or neither. Applying this to the y-cycle, as $n=0, 1, \cdots, \mu-1$, $n\kappa t+i$ and $n\kappa+i$ take on the same residues modulo $\mu\kappa$ and hence must contain the same number of zeros.

From Lemma 3, b_i is the number of zeros in the terms $y^{n\kappa+i}$, $(n=0, \cdots, \mu-1)$. From Lemma 2 we shall have enumerated one cycle from each block if we take $i=0, 1, \cdots, \kappa-1$. Together all these terms form a single reduced y-cycle. By Theorem 13.4 in this reduced y-cycle there will be $(p^{k-2}-1)/(p-1)$ pairs of zeros differing by a in position for every a from 1 to $\mu\kappa-1$. Two zeros

belong to the same x-cycle if and only if they differ in position in the y-cycle by a multiple of κ. Among the differences $1, \cdots, \mu\kappa-1$ there are $\mu-1$ multiples of κ. Hence $(\mu-1)(p^{k-2}-1)/(p-1)$ differences arise from pairs of zeros in the same x-cycle. But from the cycle of the ith block there are $b_i(b_i-1)$ differences. The second of equations (13.8) arises from equating the two methods of enumerating these differences. Two zeros of the y-cycle differing in position by a number congruent to r modulo κ, will be in blocks i and $i+r$. Enumerating these differences we obtain the final equations of (13.8). The first of equations (13.8) states merely that there are a total of $(p^{k-1}-1)/(p-1)$ zeros in the reduced y-cycle or $p^{k-1}-1$ zeros in the complete y-cycle. Or in other words, there are $p^{k-1}-1$ residues modulo p, $f(x)$ whose leading coefficient vanishes, excluding the residue zero.

If we consider the third order recurrence

$$u_{n+3} = 3u_{n+2} - 2u_{n+1} - u_n \tag{13.20}$$

and its cycles modulo 11, we find that $\mu=19$ and $\kappa=7$. The b's in order are 3, 3, 1, 3, 1, 1, 0 and it is easily verified that these numbers satisfy equations (13.8). Similarly for the fourth order recurrence

$$u_{n+4} = -u_{n+3} + u_{n+2} + u_{n+1} - u_n \tag{13.21}$$

considered modulo 5, we find that $\mu=13$ and $\kappa=12$, and that the b's in order are 3, 4, 5, 2, 3, 0, 3, 2, 1, 4, 3, 1.

In both these instances there are sequences satisfying the recurrence which contain no multiples of p, namely those belonging to the block whose $b=0$. It is interesting to ask if there must be zeros in every cycle if the reduced period is large enough. This is answered by the following theorem:

THEOREM 13.6. *A sequence will contain multiples of a prime p if $f(x)$ is irreducible modulo p and $\mu > p^{k/2}$.*

This theorem is proved by obtaining $\mu < p^{k/2}$ as a consequence of the assumption that some $b=0$. Suppose that one of the b's is zero. We observe that if the sum of a fixed number of real numbers is fixed, then the sum of their squares is a minimum when all are equal. Hence

$$\sum b_i^2 \geqq (\kappa - 1)\left(\frac{\sum b_i}{\kappa - 1}\right)^2. \tag{13.22}$$

Substituting the known value of $\sum b_i$ and $\sum b_i^2$ from (13.8), we obtain after some calculation

$$\mu \leqq p^{k/2} - (p-1) + \frac{(p-1)(p^{(k-2)/2}-1)}{p^{k-2}-1}; \tag{13.23}$$

whence certainly μ is less than $p^{k/2}$.

BIBLIOGRAPHY

1. R. D. Carmichael. *On sequences of integers defined by recurrence relations*, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 343–372.

2. M. Deuring. *Algebren*, Ergebnisse der Mathematik, Berlin, Springer, 1935.

3. H. T. Engstrom. *On sequences defined by linear recurrence relations*, these Transactions, vol. 33 (1931), pp. 210–218.

4. M. Hall. *Divisibility sequences of third order*, American Journal of Mathematics, vol. 58 (1936), pp. 577–584.

5. ———, *Divisors of second order sequences*, Bulletin of the American Mathematical Society, vol. 43 (1937), pp. 78–80.

6. D. H. Lehmer. *An extended theory of Lucas' functions*, Annals of Mathematics, (2), vol. 31 (1930), pp. 419–448.

7. E. Lucas. *Théorie des fonctions numériques simplement périodiques*, American Journal of Mathematics, vol. 1 (1878), pp. 184–239, 289–321.

8. O. Ore. *Contributions to the theory of finite fields*, these Transactions, vol. 36 (1934), pp. 243–274.

9. F. K. Schmidt. *Zur Zahlentheorie in Körpern von der Charakteristik p*, Erlangen Sitzungsberichte, vol. 58 (1928), pp. 159–172.

10. T. Takenouchi. *On the classes of congruent integers in an algebraic Körper*, Journal of the College of Science, Tokyo, vol. 36 (1913), pp. 1–18.

11. Morgan Ward. *The arithmetical theory of linear recurring series*, these Transactions, vol. 35 (1933), pp. 600–628.

12. ———, *The distribution of residues in a sequence satisfying a linear recursion relation*, these Transactions, vol. 33 (1931), pp. 166–190.

13. ———, *An arithmetical property of recurring series of the second order*, Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 825–828.

14. ———, *Arithmetical properties of sequences in rings*, Annals of Mathematics, (2), vol. 39 (1938), pp. 210–219.

YALE UNIVERSITY,
NEW HAVEN, CONN.