ANNALS OF MATHEMATICS
Vol. 39, No. 1, January, 1938

ARITHMETICAL PROPERTIES OF SEQUENCES IN RINGS

BY MORGAN WARD

(Received February 1, 1937; Revised June 21, 1937)

INTRODUCTION

1. Let S be the set of numbers 0, 1, 2, $\cdots$, $\mathfrak{O}$, a commutative ring of elements $A, B, \cdots, Z, \cdots$ containing a unit element, and let U_n be a one-valued function on S to $\mathfrak{O}$; that is, a sequence

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

of elements of $\mathfrak{O}$. The object of this paper is to study the periodicity and divisibility of such sequences relative to ideals of $\mathfrak{O}$. If we extend[1] U_n over the ring of rational integers by letting $U_{-n} = U_n$, we have a special instance of a correspondence between a commutative ring and a structure (lattice) studied in a previous paper in these Annals (Ward [1][2]).

The less general hypotheses of the present paper allow us to prove as theorems many of the axioms assumed in W. A. The results of the paper are however of a quite different character from those in W. A., and the paper may be read independently.

In conjunction with W. A. this paper gives a general theory of the arithmetic properties of sequences which renders any half-hearted generalizations of the ordinary theory of linear sequences of rational integers[3] such as to linear sequences of algebraic integers, to a large extent superfluous. In addition, we obtain many results for the special case of linear sequences of rational integers under much less restrictive hypotheses than heretofore.[4]

The existence of a smaller period for the places of apparition of a divisor of a linear divisibility sequence than the restricted period of the sequence which we prove here abstractly[5] is a fact of some arithmetical interest which does not seem to have been observed previously.

---

[1] We include the case when U_n is defined over a sub-set T of S by letting U_n be the zero of $\mathfrak{O}$ over the complementary set $S - T$. For example a function defined merely for $n = 0$, 1 and 2 is regarded as a sequence in which all terms vanish after the third.

[2] The bracketed numerals refer to the reference listed at the close of the paper. I shall refer to this particular paper as W. A.

[3] See W. A. for references to recent papers.

[4] See for example theorems 3.2, 4.1, 4.2 and 4.3. Theorem 3.2 is given in Ward [2] for a very special case. See also Carmichael [1]. Theorems 4.1–4.3 are closely connected with Marshall Hall's Theorem III (Hall [1], p. 579).

[5] Numerical examples over the ring of rational integers can be constructed without much difficulty, but unfortunately satisfy difference equations of quite high order.

2. We shall adhere to the following scheme of notation based on van der Waerden [1] and used in W. A. Elements of $\mathfrak{O}$ are denoted by roman capitals; small italic and Greek letters denote ordinary integers. The ideals of $\mathfrak{O}$ are denoted by German letters $\mathfrak{A}, \mathfrak{B}, \cdots$ $(\mathfrak{A}, \mathfrak{B})$ and $[\mathfrak{A}, \mathfrak{B}]$ denote the union and cross-cut of the ideals $\mathfrak{A}$ and $\mathfrak{B}$; (a, b) and $[a, b]$ the greatest common divisor and least common multiple of the numbers a and b; (A, B) the union of the principal ideals $[A]$ and $[B]$. The letters U and V are reserved to denote sequences. Thus (U) stands for a function. If the ideals $\mathfrak{A}$ and $[A]$ are co-prime ("teilerfremd," van der Waerden [1], §85), we write $(\mathfrak{A}, A) = \mathfrak{O}$. a divides b is written as usual $a \mid b$.

II. Modular Periodicity and Divisibility Sequences

3. We begin with some definitions. The sequence (U) is said to be *finite* if it contains only a finite number of non-vanishing terms. It is said to be *linear over* $\mathfrak{O}$ if its terms satisfy a recursion relation

$$U_{n+k} = C_1 U_{n+k-1} + \cdots + C_k U_n, \qquad (n = 0, 1, 2, \cdots) \tag{3.1}$$

with coefficients C_i in $\mathfrak{O}$.

(U) is said to be a *divisibility sequence* (M. Hall [1], Ward [1], [4]) if U_n divides U_m in $\mathfrak{O}$ whenever n divides m. If (U) is both a linear sequence and a divisibility sequence we shall call (U) "Lucasian"[6] in honor of the French mathematician E. Lucas who first systematically studied a special class of such sequences. (Lucas [1], [2], Dickson [1].)

It may happen that the terms of (U) become periodic when taken to a fixed ideal modulus $\mathfrak{A}$ of $\mathfrak{O}$; that is, there exist numbers λ and ν such that

$$U_{n+\lambda} \equiv U_n \pmod{\mathfrak{A}}, \; n \geqq \nu. \tag{3.2}$$

The least such λ and ν are called the *period* and *numeric* of (U) for the modulus $\mathfrak{A}$. This minimal period is easily seen to divide every other period. If $\nu = 0$, (U) is said to be *purely periodic* modulo $\mathfrak{A}$.

If there exists at least one term U_k of (U) such that $U_k \equiv 0 \pmod{\mathfrak{A}}$ then $\mathfrak{A}$ is called a divisor of (U). If all terms of (U) are divisible by $\mathfrak{A} \neq \mathfrak{O}$ from a certain point on, then $\mathfrak{A}$ is called a *null divisor* of (U), and (U) a null sequence modulo $\mathfrak{A}$. Every finite sequence is thus a null sequence for any modulus.

A positive integer μ is said to be a *restricted period* of (U) modulo $\mathfrak{A}$ if there exists an element A of $\mathfrak{O}$ such that

$$U_{n+\mu} \equiv A U_n \pmod{\mathfrak{A}}, \text{ all large } n.[7] \tag{3.3}$$

Here A depends on μ. We call A a multiplier of (U) modulo $\mathfrak{A}$. The least μ for which (3.3) holds is called *the* restricted period of (U).

---

[6] The more euphonious term "Lucas sequence" already has a precise meaning in the literature.

[7] It usually suffices to consider (3.3) for n greater than the numeric of (U) modulo $\mathfrak{A}$.

THEOREM 3.1. *Let (U) be a sequence of $\mathfrak{O}$, and $\mathfrak{A}$ any ideal of $\mathfrak{O}$ such that no divisor of $\mathfrak{A}$ is a null divisor of (U). Then if (U) is periodic modulo $\mathfrak{A}$, the minimal restricted period μ of (U) modulo $\mathfrak{A}$ exists, and divides every other restricted period, and in particular the actual period λ. Furthermore the multipliers of (U) modulo $\mathfrak{A}$ are all prime to $\mathfrak{A}$,[8] and form a group with respect to multiplication modulo $\mathfrak{A}$.*

PROOF. If $\mathfrak{A}$ is a null divisor of (U), (3.3) becomes a triviality. In any event, if (U) is periodic modulo $\mathfrak{A}$, the actual period λ is a restricted period with $A = I$. Hence a minimal μ exists $\leqq \lambda$, and we may write $\lambda = s\mu - t$ where $s \geqq 1$, $0 \leqq t < \mu$. Then for all large n,

$$U_{n+t} \equiv U_{n+t+\lambda} \equiv U_{n+s\mu} \equiv A^s U_n \pmod{\mathfrak{A}}$$

Hence $t = 0$ by the minimal property of μ, and

$$(A^s - 1)U_n \equiv 0 \pmod{\mathfrak{A}}, \text{ all large } n. \tag{3.4}$$

I say that

$$(A, \mathfrak{A}) = \mathfrak{O}. \tag{3.41}$$

For if $(A, \mathfrak{A}) = \mathfrak{B} \neq \mathfrak{O}$, then $(A^s - 1, \mathfrak{B}) = \mathfrak{O}$ so that by (3.4), $U_n \equiv 0 \pmod{\mathfrak{B}}$, all large n, contradicting the hypothesis that no divisor of $\mathfrak{A}$ is a null divisor of (U).

Let ϕ be any other restricted period with multiplier B, and write $\phi = u\mu + \theta$, $u \geqq 1$, $0 \leqq \theta < \mu$. Then by (3.3)

$$A^u U_{n+\theta} \equiv U_{n+\theta+u\mu} \equiv U_{n+\phi} \equiv BU_n \pmod{\mathfrak{A}}. \tag{3.5}$$

Therefore

$$(B, \mathfrak{A}) = \mathfrak{O}. \tag{3.51}$$

For if $(B, \mathfrak{A}) = \mathfrak{B} \neq \mathfrak{O}$, then by (3.5) and (3.41) $U_{n+\theta} \equiv 0 \bmod \mathfrak{B}$ for all large n, contradicting the hypothesis that no divisor of $\mathfrak{A}$ is a null divisor of (U).

Now the set of all elements of $\mathfrak{O}$ which are prime to $\mathfrak{A}$ form a group with respect to multiplication modulo $\mathfrak{A}$. (van der Waerden [1], Chapter XII.) Hence by (3.41) there exists an element A' of $\mathfrak{O}$ such that $A'A \equiv I \pmod{\mathfrak{A}}$ Thus by (3.5)

$$U_{n+\theta} \equiv (A'A)^u U_{n+\theta} \equiv A'^u BU_n \pmod{\mathfrak{A}}.$$

Therefore $\theta = 0$ by the minimal property of μ, and μ divides ϕ.

It remains to prove the group property of the multipliers. It follows from (3.51) that the multipliers of (U) form a semi-group. All that remains is to show the existence of an inverse for each multiplier B.

---

[8] This statement is taken as an axiom in the discussion of the restricted period in part IV of W. A.

Since $(B, \mathfrak{A}) = \mathfrak{O}$, there exists an element B' of $\mathfrak{O}$ such that $BB' \equiv 1 \pmod{\mathfrak{A}}$ while $U_{n+\phi} \equiv BU_n \pmod{\mathfrak{A}}$, $n \geqq \nu$. On replacing n by $n - \phi$, we obtain for $n \geqq \nu + \phi$

$$U_{n-\phi} \equiv (B'B)U_{n-\phi} \equiv B'U_n \pmod{\mathfrak{A}}.$$

Determine positive integers x, y such that $x\phi = y\lambda$ where λ as usual is the period of (U). Then

$$U_{n+(x-1)\phi} \equiv U_{n-\phi+y\lambda} \equiv U_{n-\phi} \equiv B'U_n \pmod{\mathfrak{A}}.$$

Hence B' is a multiplier. This proof fails if $x = 1$. But then $\phi = \lambda$, $B \equiv I \pmod{\mathfrak{A}}$ so that $B' \equiv I \pmod{A}$ directly.

THEOREM 3.2. *Let $\mathfrak{O}$ be a ring in which the chain condition ("Teilerkettenforderung") holds for ideals. Let (U) be a sequence of $\mathfrak{O}$ and $\mathfrak{A}$ an ideal such that (U) is periodic modulo $\mathfrak{A}$, but such that no divisor of $\mathfrak{A}$ is a null divisor of (U). Then if λ is the period and μ the restricted period of (U) modulo $\mathfrak{A}$, the multipliers of (U) form a cyclic group of order λ/μ. Furthermore the multiplier A of (3.3) associated with the restricted period is a generator of this group.* (Ward [2].)

PROOF. Consider the sequence of ideals

$$\mathfrak{A}_0 = (\mathfrak{A}, U_r), \quad \mathfrak{A}_1 = (\mathfrak{A}, U_r, U_{r+1}), \quad \mathfrak{A}_2 = (\mathfrak{A}, U_r, U_{r+1}, U_{r+2}), \cdots$$

where r is a fixed number greater than the numeric of (U). Then $\mathfrak{A}_{i+1} \supset \mathfrak{A}_i$, $(i = 0, 1, 2, \cdots)$. Therefore by the chain condition, all the $\mathfrak{A}_i$ are equal from a certain point on. This resulting ideal $\mathfrak{T}$ divides both $\mathfrak{A}$ and every term of (U) beyond a certain point. Since (U) has no null divisors dividing $\mathfrak{A}$, $\mathfrak{T} = \mathfrak{O}$. Thus for some number l,

$$(\mathfrak{A}, U_r, U_{r+1}, \cdots U_{r+l-1}) = \mathfrak{O}.$$

It follows that the ideal $(U_{r+1}, U_{r+1}, \cdots U_{r+l-1})$ contains a number

$$W = X_1U_r + \cdots + X_lU_{r+l-1}, \qquad X \text{ in } \mathfrak{O} \tag{3.6}$$

such that $(W, \mathfrak{A}) = \mathfrak{O}$.

With the notation of the previous theorem, choose r so that the congruences (3.4) and (3.5) hold for $n \geqq r$. Then by (3.6) $(A^s - 1)W \equiv (B - A^u)W \equiv 0 \pmod{\mathfrak{A}}$, or $A^s \equiv 1$, $B \equiv A^u \pmod{\mathfrak{A}}$. Now if we define s as the *least* integer such that $A^s \equiv 1 \pmod{\mathfrak{A}}$ the multipliers are seen to form a cyclic group of order s with A as a generator. From the minimal property of λ, $\lambda = \mu s$ and $s = \lambda/\mu$.

4. The following easily proved theorem on the divisors of any sequence extends a previous theorem of mine (Ward [1] theorem 5.3) and is the basis for the study of divisors of divisibility sequences.

THEOREM 4.0. *Let (U) be a sequence over $\mathfrak{O}$, and $\mathfrak{M}$ any divisor of (U). Then if $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$, the set of places of apparition of $\mathfrak{M}$ in (U) is the cross-cut of the sets of places of apparition of $\mathfrak{A}$ and $\mathfrak{B}$ in (U).*

If in particular (U) is a divisibility sequence, the places of apparition of any divisor of (U) have the property of being closed under multiplication by positive integers. Furthermore, for any place of apparition s of a divisor $\mathfrak{A}$ of (U) there will exist a number r dividing s and such that

$$U_r \equiv 0 \pmod{\mathfrak{A}}, \qquad U_x \not\equiv 0 \pmod{\mathfrak{A}} \text{ if } x \mid r. \tag{4.1}$$

Following M. Hall [1], we call such a number r a *rank of apparition*[9] of $\mathfrak{A}$ in (U). Of paramount interest and simplicity are the cases when a divisor of (U) has only a *finite* number of ranks of apparition. We then say the ranks of apparition constitute a *multiplicative set*. The theory of such sets is developed in part III of this paper. In the present section, we give a series of theorems on the finiteness of the ranks of apparition.

THEOREM 4.1. *If $\mathfrak{A}$ is a divisor of the divisibility sequence (U) and if (U) is also periodic modulo $\mathfrak{A}$, then a necessary and sufficient condition that $\mathfrak{A}$ shall have only a finite number of ranks of apparition are that all its ranks of apparition divide the restricted period of (U) modulo $\mathfrak{A}$.*

PROOF. The sufficiency of this condition is obvious. To establish its necessity, let r be a rank of apparition of $\mathfrak{A}$ which does not divide the restricted period μ, and let $(r, \mu) = d \neq r$. For any positive integer t, we can choose positive integers x_t, y_t such that $td = y_t r - x_t \mu$. Then if $t \geqq \nu/d$ (where ν is the numeric of (U)),

$$U_{x_t \mu + td} \equiv A^{x_t} Y_{td} \equiv U_{y_t r} \equiv 0 \pmod{\mathfrak{A}},$$

for (U) is a divisibility sequence and $U_r \equiv 0 \pmod{\mathfrak{A}}$. By theorem 3.2, $(A, \mathfrak{A}) = \mathfrak{O}$, so that $U_{td} \equiv 0 \pmod{\mathfrak{A}}$. Hence td is a place of apparition of $\mathfrak{A}$ in (U) and is hence divisible by one or more ranks of apparition r' of $\mathfrak{A}$. If t is a prime number, r' must be divisible by t. For otherwise $r' \mid td$ implies $r' \mid d$, so that $r' \mid r$, $r' = r$, $d = r$. Hence

$$td \geqq r' \geqq t \qquad t \text{ a prime.} \tag{4.2}$$

Since the number of primes is infinite, we may choose an infinite sequence of primes $t_0, t_1, t_2, \cdots$ such that $t_{n+1} > t_n d$, $t_0 d \geqq \nu$. Then the inequality (4.2) implies the existence of an infinity of ranks of apparition.

THEOREM 4.2. *Let (U) be a divisibility sequence, and $\mathfrak{A}$ a divisor of (U) such that (U) is purely periodic modulo $\mathfrak{A}$. Then $\mathfrak{A}$ has only a finite number of ranks of apparition and each such rank divides the restricted period of (U) modulo $\mathfrak{A}$.*

PROOF. Let r be a rank of apparition of $\mathfrak{A}$ in (U). In view of the previous theorems we need only show that r divides μ. Let $(r, \mu) = d$. Then it suffices to show that d is a place of apparition of $\mathfrak{A}$, for then since $d \mid r$, $r = d$ and $r \mid \mu$.

---

[9] In Ward [1], [3], [4], a rank of apparition was defined by the stricter requirement $U_r \equiv 0 \pmod{\mathfrak{A}}$, $U_x \not\equiv 0 \pmod{\mathfrak{A}}$ if $0 < x < r$, or in the case considered in Ward [1], the places of apparition were required to form an ideal. Although such a definition leads to many interesting results and is apparently met with frequently in the numerical cases of the Lucasian sequences from which the theory springs, (4.1) appears preferable.

Now there exist positive integers x, y such that $d = rx - \mu y$. Then by (3.3) and our hypotheses on r and (U),

$$A^{y}U_d \equiv U_{d+\mu y} \equiv U_{rx} \equiv 0 \pmod{\mathfrak{A}}.$$

But $(A, \mathfrak{A}) = \mathfrak{O}$. Hence $U_d \equiv 0 \pmod{\mathfrak{A}}$.

III. Multiplicative Sets

5. Let $r_1, r_2, \cdots, r_n$ be n fixed numbers. The set M consisting of all their integral multiples will be called the *multiplicative set based on* $r_1, r_2, \cdots, r_n$. If r_i divides r_j only for $i = j$, $(i, j = 1, \cdots, n)$, the r_i will be called the *generators* of the set. A generator is thus any element of the set which is irreducible in the set. Henceforth we assume that $r_1, \cdots, r_n$ are a set of generators of M.

The multiplicative set based on $r_1, \cdots, r_n$ is thus the maximal multiplicative semi-group containing $r_1, \cdots, r_n$ as its only irreducible elements.

The number $r = [r_1, r_2, \cdots, r_n]$ (where here and later $[x, \cdots, z]$ denotes the least common multiple or L.C.M. of the numbers $x, \cdots, z$) is called the *rank* of the set M.

Theorem 5.1. *If r is the rank of the multiplicative set M, every element of M is congruent modulo r to an element of the set greater than or equal to zero and less than r.*

Proof. If x lies in M, there exists a generator r_i dividing x: $x = yr_i$. Also $r = zr_i$ by the definition of L.C.M. Hence if $x = qr + t$ where $0 \leqq t < r$, then $t \equiv 0 \pmod{r_i}$ so that t lies in M and $x \equiv t \pmod{r}$.

We call a set of distinct elements of M which lie in a complete residue system modulo r a *representative set* of M.

Theorem 5.2. *The number of elements in a representative set of M is given by the formula*

$$r \sum_{s=1}^{n} (-1)^{s-1} \sum_{(i)} \frac{1}{[r_{i_1}, r_{i_2}, \cdots r_{i_s}]}.$$

Here the inner summation is taken over all the $\binom{n}{s}$ distinct combinations $i_1, \cdots, i_s$ of the subscripts 1 to n of the generators r_i taken s at a time. We omit the (simple) proof of this theorem here.[10]

Theorem 5.3. *The cross-cut of any two multiplicative sets is a multiplicative set, and each generator of the cross-cut is the* L.C.M. *of generators of the component sets.*

Proof. Let the sets be M_1 and M_2 and let $M_3 = [M_1, M_2]$ be their cross-cut. M_3 is obviously a multiplicative set. Every element of M_3 lies both in M_1

[10] For example take $r_1 = 6$, $r_2 = 10$, $r_3 = 15$. Then $r = 30$. A representative set consists of the eight numbers 0, 6, 10, 12, 15, 18, 20 and 24. The formula gives

$$30\left\{\left(\frac{1}{6} + \frac{1}{10} + \frac{1}{15}\right) - \left(\frac{1}{30} + \frac{1}{30} + \frac{1}{30}\right) + \left(\frac{1}{30}\right)\right\} = 5 + 3 + 2 - 3 + 1 = 8.$$

and M_2 and is hence divisible by a generator r_i of M_1 and a generator r_j' of M_2 and hence by their L.C.M. $[r_i, r_j']$. Therefore M_3 is based on the set of nm elements $[r_1, r_1'], \cdots, [r_n, r_m']$ where the r_i and r_j' are respectively the generators of M_1 and M_2. Hence the generators of M_3 consist of the irreducible elements in the set $[r_i, r_j']$.

In like manner it is easy to prove

THEOREM 5.4. *The union of two multiplicative sets is a multiplicative set. If $r_1, \cdots, r_n$; $r_1', \cdots, r_m'$ are the generators of the two sets, the generators of their union consist of the irreducible elements in the set of $n + m$ elements $r_1, \cdots, r_m'$.*

THEOREM 5.5. *The aggregate of all multiplicative sets forms an arithmetic structure* (O. Ore [1])——or (distributive) C-lattice—(G. Birkoff [1]) *with respect to the operations of forming the union and cross-cut.*[11]

PROOF. Let M_1, M_2, M_3 be any three multiplicative sets with generators $r_1, \cdots, r_n$; $r_1', \cdots, r_m'$; $r_1'', \cdots, r_p''$. Let $[M_i, M_j]$, (M_i, M_j) stand for cross-cut and union respectively. Then it suffices to show that

$$[M_1, (M_2, M_3)] = ([M_1, M_2], [M_1, M_3]).$$

But this equality is obvious, since by the preceding two theorems, both sets are based upon the numbers $[r_1, r_1'], \cdots, [r_n, r_m'], [r_1, r_1''], \cdots [r_n, r_p'']$.

It is evident that the theorems of this section will also be true with slight changes of wording for multiplicative sets defined over a principal ideal ring $\mathfrak{O}$ all of whose quotient rings $\mathfrak{O}/\mathfrak{A}$ are finite.

IV. LINEAR SEQUENCES

6. THEOREM 6.1. *Let (U) be a linear sequence, and let $\mathfrak{A}$ be an ideal of $\mathfrak{O}$ whose quotient ring $\mathfrak{O}/\mathfrak{A}$ is of finite order. Then (U) is periodic modulo $\mathfrak{A}$. Furthermore, if $\mathfrak{A}$ is relatively prime to the last term C_k in the recursion* (3.1) *defining (U), then (U) is purely periodic modulo $\mathfrak{A}$.*

PROOF. (Ward [2].) The sequence (U) will become periodic modulo $\mathfrak{A}$ if any set of k residues of k consecutive terms of (U) modulo $\mathfrak{A}$ occurs more than once. Now the first $n + k - 1$ terms of (U) contain the $n + 1$ sets of k consecutive terms $U_0, \cdots, U_{k-1}$; $\cdots$; $U_n, \cdots U_{n+k-1}$. Let T be the order of the finite ring $\mathfrak{O}/\mathfrak{A}$, so that a complete residue system modulo $\mathfrak{A}$ contains T distinct elements. Then the period λ of (U) modulo $\mathfrak{A}$ is at most $T^k - 1$. Thus (3.2) holds with $\lambda \leqq T^k - 1$, $\nu \leqq T^k - 1$.

---

[11] No simple relation appears to exist between the rank of two sets and the ranks of their cross-cut and union. For example, let $M_1 = \{36, 54\}$, $M_2 = \{18, 24\}$. Then $[M_1, M_2] = M_1$, $(M_1, M_2) = M_2$ so that M_2 contains M_1. The rank of M_1 is 108, while the rank of M_2 is 72. Thus, the L. C. M. of the ranks of M_1 and M_2 is not the rank of their cross-cut, the G. C. D. of their ranks is not the G. C. D. of their union, nor does one rank divide the other.

Now assume that $(\mathfrak{A}, C_k) = \mathfrak{O}$. If (3.2) holds for $n \geqq n_0 > 0$ we have from the recursion relation

$$U_{n_0+k-1+\lambda} = C_1 U_{n_0+k-2+\lambda} + \cdots + C_k U_{n_0-1+\lambda}$$
$$U_{n_0+k-1} = C_1 U_{n_0+k-2} + \cdots + C_k U_{n_0-1}.$$

But by (3.2), $U_{n_0+k-r+\lambda} \equiv U_{n_0+k-r} \pmod{\mathfrak{A}}$, $(r = 1, 2, \cdots, k)$. Hence by subtraction

$$C_k(U_{n_0-1+\lambda} - U_{n_0-1}) \equiv 0 \pmod{\mathfrak{A}}.$$

Since $(C_k, \mathfrak{A}) = \mathfrak{O}$, (3.2) holds for $n \geqq n_0 - 1$. Therefore (3.2) holds for $n \geqq 0$ and (U) is purely periodic.

THEOREM 6.2.[12] *Let $\mathfrak{O}$ be a domain of integrity, K a finite extension of its quotient field. Let $\Phi = \Phi(x_1, \cdots, x_r ; y)$ be a polynomial in the $r + 1$ indeterminates $x_1, \cdots, x_r, y$ with coefficients in K and let $\omega_1, \omega_2, \cdots, \omega_r$ be r fixed integers of K. Define a sequence (V) over K by*

$$V_n = \Phi(\omega_1^n, \omega_2^n, \cdots, \omega_r^n ; n), \qquad (n = 0, 1, 2, \cdots).$$

Then (V) is linear, and satisfies a recursion of the form (3.2) with coefficients in $\mathfrak{O}$. Every sequence which is linear over $\mathfrak{O}$ may be thus obtained by a suitable choice of the extension field K and polynomial Φ.

PROOF. Let N be the maximum degree of Φ in the x, and M the maximum degree of Φ in y. Suppose that the polynomial Φ when written in the form

$$\Phi = \sum_{(k)} \Gamma_{(k)}(p) x_1^{k_1} x_2^{k_2} \cdots x_r^{k_r} \qquad 0 \leqq k_1 + k_2 + \cdots + k_r \leqq N$$

has precisely s terms $X_{(k)} = x_1^{k_1} \cdots x_r^{k_r}$. Here the $\Gamma_{(k)}(y)$ are polynomials in y of degree $\leqq M$ with coefficients in K. Let $\Omega_k = \omega_1^{k_1} \cdots \omega_r^{k_r}$. Then there exists a polynomial $f(x) = x^t - c_1 x^{t-1} - \cdots - c_t$ with coefficients in $\mathfrak{O}$ such that $f_{T-1}(\Omega_{(k)}) = 0$, $(k = 1, \cdots, s)$. Let

$$F(x) = f(x)^M = x^T - D_1 x - \cdots - D_T.$$

Then each $\Omega_{(k)}$ is a root of $F(x) = 0$ of multiplicity at least M, and $D_1, \cdots D_T$ lie in $\mathfrak{O}$. But

$$V_n = \sum_{h=1}^{s} \Gamma_{(h)}(n) \Omega_{(k)}^n. \tag{6.1}$$

Hence (V) satisfies the recurrence

$$Y_{n+T} = D_1 Y_{n+T-1} + \cdots + D_T Y_n \tag{6.2}$$

associated with $F(x)$.

Now let (V) be a linear sequence of $\mathfrak{O}$ defined by (6.2) and assume that the

[12] We discard the scheme of notation explained in section 2 for the statement and proof of this theorem.

distinct roots of the associated polynomial $F(x)$ are $\Omega_{(1)}, \cdots, \Omega_{(s)}$. The Ω then lie in a finite extension K of the quotient field of $\mathfrak{O}$. Furthermore let each Ω be of multiplicity $\leqq M$. Then every solution of (6.2) in $\mathfrak{O}$ is of the form (6.1) if the coefficients of the polynomials $\Gamma_{(k)}(n)$ are suitably chosen in K. It suffices then to take $\Phi = \sum_{k=1}^{s} \Gamma_{(k)}(y)X_{(k)}$ where $X_{(1)}, \cdots, X_{(s)}$ and y are now our indeterminates.

THEOREM 6.21. *If $\mathfrak{O}$ is a domain of integrity and (U), (V) are linear over $\mathfrak{O}$, then the sequence (UV) whose general term is U_nV_n is also linear over $\mathfrak{O}$.*

PROOF. It suffices to observe that the product of two polynomials Φ_1 and Φ_2 with different indeterminates x but the same y with coefficients in the finite extension fields K_1 and K_2 is again a polynomial of the same form whose coefficients lie in the union of K_1 and K_2.

We shall call (UV) the *product* of the sequences (U) and (V) writing $(U)\cdot(V) = (UV)$. The operation of obtaining (UV) from (U) and (V) will be called *multiplication* of sequences. If we define the sum of two sequences as in Ward [5] by $(U) + (V) = (U + V)$, the following theorem is evident.

THEOREM 6.3. *The set of all sequences linear over a domain of integrity forms a commutative ring with respect to the operations of addition and multiplication defined above.*

This ring contains as its unit element the sequence $1, 1, 1, \cdots$ satisfying the recursion $Y_{n+1} = Y_n$. It in general has no finite basis and is not a domain of integrity.

We may apply the operation of multiplication to divisibility sequences. The following theorem has important applications (Ward [6]).

THEOREM 6.4. *The product $(U)\cdot(V)$ of two divisibility sequences (U) and (V) is again a divisibility sequence. The set of places of apparition of any prime divisor $\mathfrak{P}$ of $(U)\cdot(V)$ is the union of the sets of places of apparition of $\mathfrak{P}$ in (U) and (V). The ranks of apparition of $\mathfrak{P}$ in $(U)\cdot(V)$ are contained among the ranks of apparition of $\mathfrak{P}$ in (U) and (V).*

The proof is simple, and will be omitted here. It is essential that the ideal divisor be a prime.

V. LUCASIAN SEQUENCES

7. We lose little generality[13] by assuming that a given divisibility sequence is *normal*; that is, $U_0 = 0$, $U_1 = 1$. (Ward [1], section 11.) If in addition (U) is Lucasian, the results of part III and IV of the paper yield at once a great deal of information about the divisors of (U) and their places of apparition. For any ideal $\mathfrak{A}$ prime to C_k and such that the quotient ring $\mathfrak{O}/\mathfrak{A}$ is finite is at

[13] Since any number divides zero, every divisor of a divisibility sequence divides U_0. This fact restricts the divisors at the outset unless $U_0 = 0$. Since 1 divides every number, U_1 divides every term of (U). If U_1 is not zero, we can divide it out of the sequence obtaining a new divisibility sequence in which $U_1 = 1$.

once a divisor of (U), and all its ranks of apparition divide the restricted period of (U). The least common multiple r of these ranks of apparition gives us the period of the places of apparition of $\mathfrak{A}$ in the sequence. In contrast to the behavior of the period and restricted period of (U) modulo $\mathfrak{A}$, the rank r modulo $\mathfrak{A}$ does not appear to be effectively calculable merely from a knowledge of the ranks of constituent factors of $\mathfrak{A}$. However if $\mathfrak{A} = [\mathfrak{B}, \mathfrak{C}]$, the set of places of apparition of $\mathfrak{A}$ are effectively calculable from the places of apparition of $\mathfrak{B}$ and $\mathfrak{C}$ by virtue of theorems 4.0 and 5.3.

I hope to discuss the theory of Lucasian sequences in relation to the operation of multiplication of sequences defined in part IV in some detail elsewhere.

CALIFORNIA INSTITUTE OF TECHNOLOGY

REFERENCES

G. BIRKHOFF, 1 Bulletin American Math. Soc. vol. 45 (1934) pp. 613-619.
R. D. CARMICHAEL, 1. Quarterly Journal of Mathematics, vol. 48 (1920) pp. 343-372.
L. E. DICKSON, 1. *History*, volume 1, chapter XVII.
MARSHALL HALL, 1. American Journal of Mathematics, vol. 47 (1936) pp. 577-584.
E. LUCAS, 1. American Journal of Mathematics, vol. 1 (1878) pp. 184-240, pp. 289-321.
2. *Theorie des Nombres*, Paris 1891.
O. ORE, 1. These Annals, (2) vol. 36 (1935) pp. 406-437.
B. L. VAN DER WAERDEN, *Modern Algebra*, vol. 2, Berlin 1931.
M. WARD, 1. These Annals, vol. 38 (1937) pp. 725-732.
2. Transactions of the American Math. Soc., vol. 33 (1931) pp. 162-164.
3. Bulletin of the American Math. Soc., vol. 42 (1936) pp. 843-845.
4. Transactions of the American Math. Soc., vol. 41 (1937), pp. 276-286.
5. Transactions of the American Math. Soc., vol. 35 (1933) pp. 600-628.
6. To appear in the Transactions of the American Math. Soc.