ANNALS OF MATHEMATICS
Vol. 38, No. 3, July, 1937

ARITHMETIC FUNCTIONS ON RINGS

BY MORGAN WARD

(Received September 1, 1936)

I. INTRODUCTION

1. The classic arithmetic properties of the Lucas[1] [1] function

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad \alpha + \beta \quad \alpha\beta \quad \text{rational integers},$$

can be shown to depend ultimately upon its periodicity to any integral modulus and its divisibility property: u_n divides u_m if n divides m. While the first property extends to any recurring series of integers[2], [3], [4] and the second may be similarly generalized,[5], [6], [7] the divisibility property is shared by numerous functions bearing no evident relation to recurring series, such as the totient function and its generalizations[8] and the polynomials γ_n of Halphen[9] associated with the rational multiplication of the Weierstrass $\mathfrak{P}$ and σ functions.

I show here that a much more extensive generalization is possible which not only reveals inner connections between the arithmetical properties of the Lucas function, but also appears to be of some independent interest.

The generalization consists in systematically developing the divisibility properties and modular periodicity of a function $y = \phi_x$ where x lies in an abstract commutative ring[2] while y lies in a structure[3] (usually another ring).

2. Let $\mathfrak{o}$ be a commutative ring, Σ a structure. We assume that to each element x of $\mathfrak{o}$ there corresponds a unique element

$$X = \phi(x) = \phi_x$$

of Σ. In the phraseology of general analysis, we call ϕ *a function on* $\mathfrak{o}$ *to* Σ. ϕ_a, ϕ_b are *values* of ϕ, a, b specific elements of $\mathfrak{o}$. We call ϕ *arithmetic* if ϕ_a divides ϕ_b in Σ whenever a divides b in $\mathfrak{o}$.

If $\mathfrak{o}$ and Σ are both the ring of rational integers, and $\phi_{-n} = -\phi_n$, an arithmetic function is equivalent to M. Hall's[6] divisibility sequence.[4] If $\mathfrak{o}$ itself is a structure, say a principal ideal ring, any homomorphism between $\mathfrak{o}$ and

---

[1] The [1] refers to the list of references concluding this paper.

[2] The Lucas function is brought within the scope of this generalization by letting $u_n = -u_n$.

[3] We use the term recently introduced by O. Ore[10] in these Annals. Equivalent terms are dual group, lattice.

[4] See the references in Hall[6] for earlier work on these sequences.

the values of ϕ in Σ with respect to cross-cut or union (O. Ore[10] pp. 416–419) defines an arithmetic function.[5]

3. We use the following notation: $\tilde{\sigma}$ denotes the structure of all ideals of $\mathfrak{o}$, $a, \cdots, z$ elements of $\mathfrak{o}$, $\mathfrak{a}, \cdots, \mathfrak{z}$ ideals of $\mathfrak{o}$, $(a), \cdots, (z)$ principal ideals. We use $x \mid y$, $\mathfrak{x} \supseteq \mathfrak{y}$, $\mathfrak{y} \subseteq \mathfrak{x}$ for division in $\mathfrak{o}$ and $\tilde{\sigma}$, xy, $\mathfrak{x}\mathfrak{y}$ for product, and $(\mathfrak{x}, \mathfrak{y})$, $[\mathfrak{x}, \mathfrak{y}]$ for union and cross-cut respectively.[6]

Corresponding entities in Σ are denoted by capital letters. We use $A, \cdots, Z$ for values of ϕ in Σ. These are on occasion imbedded in a ring $\mathfrak{O}$. Σ then denotes the structure of all ideals of $\mathfrak{O}$. We use $\mathfrak{A}, \cdots \mathfrak{Z}$ for elements of Σ and write $\mathfrak{X} \supseteq \mathfrak{Y}$, $\mathfrak{Y} \subseteq \mathfrak{X}$ for $\mathfrak{X}$ divides $\mathfrak{Y}$, $(\mathfrak{X}, \mathfrak{Y})$, $[\mathfrak{X}, \mathfrak{Y}]$ for union and cross-cut. If $\mathfrak{X}$ divides $X = \phi_x$, we write $X \equiv 0 \pmod{\mathfrak{X}}$ even when the X are not imbedded in a ring.

Ordinary Greek letters ϕ, ρ, μ, τ stand for functions.

4. Following Ore,[10] we define the structure Σ by means of its division relation $\supset$ and not by postulates on the cross-cut and union.

(4.1) $\mathfrak{X} \supset \mathfrak{X}$; if $\mathfrak{X} \supset \mathfrak{Y} \supset \mathfrak{Z}$ then $\mathfrak{X} \supset \mathfrak{Z}$. $\mathfrak{X} = \mathfrak{Y}$ if and only if $\mathfrak{X} \supset \mathfrak{Y}$ and $\mathfrak{Y} \supset \mathfrak{X}$. We write $\mathfrak{X} \supset \mathfrak{Y}$ or $\mathfrak{Y} \subseteq \mathfrak{X}$ if $\mathfrak{X} \supset \mathfrak{Y}$ or $\mathfrak{X} = \mathfrak{Y}$.

The cross-cut $[\mathfrak{X}, \mathfrak{Y}]$ is defined by

(4.2) $\mathfrak{X} \supseteq [\mathfrak{X}, \mathfrak{Y}]$, $\mathfrak{Y} \supseteq [\mathfrak{X}, \mathfrak{Y}]$; if $\mathfrak{X} \supseteq \mathfrak{Z}$ and $\mathfrak{Y} \supseteq \mathfrak{Z}$, then $[\mathfrak{X}, \mathfrak{Y}] \supseteq \mathfrak{Z}$.

The union is defined by

(4.3) $(\mathfrak{X}, \mathfrak{Y}) \supseteq \mathfrak{X}$, $(\mathfrak{X}, \mathfrak{Y}) \supseteq \mathfrak{Y}$; if $\mathfrak{Z} \supseteq \mathfrak{X}$ and $\mathfrak{Z} \supseteq \mathfrak{Y}$ then $\mathfrak{Z} \supseteq (\mathfrak{X}, \mathfrak{Y})$.

Let Ω be any sub-set of Σ. Since the division relation in Σ determines that in Ω, a pair of elements $\mathfrak{A}$, $\mathfrak{B}$ of Ω may have a cross-cut and union satisfying definitions (4.2), (4.3) for all elements of Ω. We write then $[\mathfrak{A}, \mathfrak{B}]_\Omega$, $(\mathfrak{A}, \mathfrak{B})_\Omega$ denoting the set relative to which we consider the cross-cut or union by a sub-script. Obviously

$$(4.4) \qquad (\mathfrak{A}, \mathfrak{B}) \supseteq (\mathfrak{A}, \mathfrak{B})_\Omega \supseteq [\mathfrak{A}, \mathfrak{B}] \supseteq [\mathfrak{A}, \mathfrak{B}]_\Omega .$$

We call a set closed in this sense with respect to cross-cut and union *a structure within* Σ. If $(\mathfrak{A}, \mathfrak{B})_\Omega = (\mathfrak{A}, \mathfrak{B})$, $[\mathfrak{A}, \mathfrak{B}]_\Omega = [\mathfrak{A}, \mathfrak{B}]$ for every pair of elements of Ω, we call Ω *a sub-structure of* Σ. (Ore[10] p. 409.)

If any set of elements of Σ, finite or infinite have a unique cross-cut and union, we shall say that Σ is a *completely closed structure.*

II. Divisors of Arithmetical Functions and Their Ranks of Apparition

5. Let ϕ be an arithmetical function on $\mathfrak{o}$ to Σ. An element of Σ dividing one or more values of ϕ is said to divide ϕ or to be a *divisor of* ϕ. Obviously any factor of a divisor of ϕ divides ϕ. Hence:

---

[5] An arithmetic function need not however determine any structure homomorphism.

[6] The meaning of the symbols $(\ldots)$ and $[\ldots]$ is reversed in Ore's paper[10]. See section 4.

THEOREM 5.1. *The set of all divisors of an arithmetical function is closed under union.*

We denote this set by Δ.

Let $\mathfrak{A}$ be any divisor of ϕ. If $\mathfrak{A} \supseteq \phi_a$, we call a a *place of apparition of* $\mathfrak{A}$ *in* ϕ. We now assume

AXIOM 1.[7] *The places of apparition of every divisor of* ϕ *form an ideal of* $\mathfrak{o}$.

The ideal $\mathfrak{r}$ corresponding to a divisor $\mathfrak{Y}$ is called the *rank of apparition of* $\mathfrak{Y}$ *in* ϕ. We write $\mathfrak{r} = \rho(\mathfrak{Y})$. The set of all ranks of apparition is denoted by δ. The following theorem is now obvious.

THEOREM 5.2. *The correspondence between divisors and ranks of apparition defines an arithmetical function* ρ *on* Δ *to* $\bar{\sigma}$.

We cannot prove that the set Δ is closed under cross-cut as well as union. We assume:

AXIOM 2. *The set* Δ *of all divisors of* ϕ *is a completely closed sub-structure of* Σ.

THEOREM 5.3. *If* $\mathfrak{A}$, $\mathfrak{B}$ *are divisors of* ϕ *and* $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$, *then* $[\rho(\mathfrak{A}), \rho(\mathfrak{B})] = \rho(\mathfrak{M})$.

PROOF. By axiom 2, $\mathfrak{M}$ is a divisor of ϕ and by (4.2) $\mathfrak{A} \supseteq \mathfrak{M}$. Hence $\rho(\mathfrak{A}) \supseteq \rho(\mathfrak{M})$ by theorem 5.2. Similarly $\rho(\mathfrak{B}) \supseteq \rho(\mathfrak{M})$ so that $[\rho(\mathfrak{A}), \rho(\mathfrak{B})] \supseteq \rho(\mathfrak{M})$ by (4.2).

Assume that m lies in $[\rho(\mathfrak{A}), \rho(\mathfrak{B})]$. Then $m \equiv 0 \pmod{\rho(\mathfrak{A})}$, $m \equiv 0 \pmod{\rho(\mathfrak{B})}$ by (4.2). Hence $\phi_m \equiv 0 \pmod{\mathfrak{A}}$, $\phi_m \equiv 0 \pmod{\mathfrak{B}}$ or by (4.2) again, $\phi_m \equiv 0 \pmod{\mathfrak{M}}$. Hence $m \equiv 0 \pmod{\rho(\mathfrak{M})}$ so that $\rho(\mathfrak{M}) \supseteq [\rho(\mathfrak{A}), \rho(\mathfrak{B})]$.

THEOREM 5.31. "DECOMPOSITION THEOREM." *If the values of* ϕ *lie in a commutative ring* $\mathfrak{D}$ *with a unit element and if* $\mathfrak{A}$, $\mathfrak{B}$ *are any two divisors of* ϕ *such that* $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, *then* $\rho(\mathfrak{AB}) = [\rho(\mathfrak{A}), \rho(\mathfrak{B})]$.

PROOF. If $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, then $[\mathfrak{A}, \mathfrak{B}] = \mathfrak{AB}$ (van der Waerden,[11] p. 45).

If $\mathfrak{o}$ is a principal ideal ring, the following theorem allows us to replace axiom 1 by a simple structure condition. The result is independent of axiom 2.

THEOREM 5.4.[8] *If* $\mathfrak{o}$ *is a principal ideal ring, the places of apparition of every divisor of* ϕ *form an ideal if and only if* ϕ *defines a homomorphism with respect to union between* $\mathfrak{o}$ *and the values of* ϕ *in* Σ.

PROOF. If $\mathfrak{o}$ is a principal ideal ring, the union (m, n) of (m) and (n) is a principal ideal (d): we write $d = (m, n)$. Let $\mathfrak{A}$ be a divisor of ϕ, and assume that $\phi_m \equiv 0 \pmod{\mathfrak{A}}$, $\phi_n \equiv 0 \pmod{\mathfrak{A}}$. Also assume that $(m, n) = d$ in $\mathfrak{o}$ implies that $(\phi_m, \phi_n) = \phi_d$ in Σ. Then by (4.3) $\phi_d \equiv 0 \pmod{\mathfrak{A}}$. Now $d \mid m$, $d \mid n$. Hence $d \mid m - n$ so that $\phi_d \supseteq \phi_{m-n}$. Hence by (4.1) $\phi_{m-n} \equiv 0 \pmod{\mathfrak{A}}$. Thus if m and n are places of apparition of $\mathfrak{A}$, so is $m - n$. But since ϕ is arithmetical, if a is a place of apparition so is xa, x any element of $\mathfrak{o}$. Hence the places of apparition of $\mathfrak{A}$ form an ideal.

Assume conversely that $\mathfrak{o}$ is a principal ideal ring and that the places of

---

[7] It suffices to assume the places of apparition form a module, since ϕ is arithmetical.

[8] Given by Ward[12] for the case $\mathfrak{o}$ and Σ the ring of rational integers.

apparition of any divisor $\mathfrak{A}$ of ϕ form an ideal $\mathfrak{a} = (a)$. Let $(\phi_m, \phi_n) = D$, and let (d') be the rank of apparition of D in ϕ (Theorem 5.1). Since m, n lie in (d'), $d' \mid m$, $d' \mid n$. Hence if $(m, n) = d$, $d' \mid d$ by (4.3). Hence $\phi_d \equiv 0 \pmod{D}$. But since $d \mid m$, $d \mid n$, $\phi_d \supseteq \phi_m$, $\phi_d \supseteq \phi_n$ so that $\phi_d \supseteq D$ by (4.3). Thus $\phi_d = D$.

6. It is possible to have divisors $\mathfrak{A}$, $\mathfrak{B}$ of ϕ for which $\rho(\mathfrak{A}) = \rho(\mathfrak{B})$ $\mathfrak{A} \neq \mathfrak{B}$. Let $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$. Then by Theorem 5.3, $\rho(\mathfrak{M}) = [\rho(\mathfrak{A}), \rho(\mathfrak{B})] = \rho(\mathfrak{A})$. Thus the set of all elements $\mathfrak{Z}$ of Δ such that $\rho(\mathfrak{Z}) = n$ is closed under cross-cut. Hence by axiom 2, for every rank of apparition $\mathfrak{n}$ there exists a divisor $\mathfrak{N}$ of ϕ such that

(6.1) $\rho(\mathfrak{N}) = \mathfrak{n}$; if $\mathfrak{C}$ divides ϕ and $\rho(\mathfrak{C}) = \mathfrak{n}$ then $\mathfrak{C} \supseteq \mathfrak{N}$.

We call such a divisor a *maximal* divisor of ϕ.[9] We denote the set of all maximal divisors of ϕ by $\tilde{\mu}$.

THEOREM 6.1. *Let $\mathfrak{A}$ be any divisor of ϕ and $\mathfrak{a}$ its rank of apparition. If $\mathfrak{N}$ is a maximal divisor of ϕ such that $\mathfrak{a} \supseteq \rho(\mathfrak{N})$, then $\mathfrak{A} \supseteq \mathfrak{N}$.*

PROOF. Let $[\mathfrak{A}, \mathfrak{N}] = \mathfrak{B}$. $\mathfrak{B}$ is a divisor of ϕ by axiom 2. Hence $\rho(\mathfrak{B})$ exists, and by theorem 5.3, $\rho(\mathfrak{B}) = [\rho(\mathfrak{A}), \rho(\mathfrak{N})] = \rho(\mathfrak{N})$ since $\rho(\mathfrak{A}) \supseteq \rho(\mathfrak{N})$. Since $\mathfrak{N}$ is maximal, $\mathfrak{B} \supseteq \mathfrak{N}$. But $\mathfrak{A} \supseteq \mathfrak{B}$.

As a corollary, we have

THEOREM 6.11. *If $\mathfrak{A}$ and $\mathfrak{B}$ are maximal divisors of ϕ with ranks of apparition $\mathfrak{a}$ and $\mathfrak{b}$ respectively, then $\mathfrak{A} \supseteq \mathfrak{B}$ when and only when $\mathfrak{a} \supseteq \mathfrak{b}$.*

THEOREM 6.2. *The set $\tilde{\mu}$ of all maximal divisors of ϕ is closed under union.*

PROOF. Let $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$. By (4.3),

(i) $\mathfrak{D} \supseteq \mathfrak{A}$, $\mathfrak{D} \supseteq \mathfrak{B}$;

(ii) If $\mathfrak{C} \supseteq \mathfrak{A}$, $\mathfrak{C} \supseteq \mathfrak{B}$ then $\mathfrak{C} \supseteq \mathfrak{D}$.

By theorem 5.1, $\mathfrak{D}$ divides ϕ. Let $\mathfrak{d}$ be its rank of apparition and $\mathfrak{C}$ any divisor of ϕ such that $\rho(\mathfrak{C}) = \mathfrak{d}$. By (i) and theorem 5.2, $\rho(\mathfrak{C}) \supseteq \rho(\mathfrak{A})$. Hence since $\mathfrak{A}$ is maximal, $\mathfrak{C} \supseteq \mathfrak{A}$. Similarly $\mathfrak{C} \supseteq \mathfrak{B}$. Hence $\mathfrak{C} \supseteq \mathfrak{D}$ by (ii) so that $\mathfrak{D}$ is maximal.

THEOREM 6.21. *If $\mathfrak{A}$ and $\mathfrak{B}$ are maximal divisors of ϕ and $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$ then $(\rho(\mathfrak{A}), \rho(\mathfrak{B})_\delta$ exists and equals $\rho(\mathfrak{D})$.*

PROOF. By theorem 6.2, $\mathfrak{D}$ is maximal. Hence by theorem 6.11, if $\mathfrak{a} = \rho(\mathfrak{A})$, $\mathfrak{b} = \rho(\mathfrak{B})$, $\mathfrak{c} = \rho(\mathfrak{C})$ and $\mathfrak{d} = \rho(\mathfrak{D})$, (i) $\mathfrak{d} \supseteq \mathfrak{a}$, $\mathfrak{d} \supseteq \mathfrak{b}$; (ii) if $\mathfrak{c} \supseteq \mathfrak{a}$, $\mathfrak{c} \supseteq \mathfrak{b}$ then $\mathfrak{c} \supseteq \mathfrak{d}$. (i) and (ii) are the definition of union.

Since to every rank of apparition corresponds a maximal divisor, in view of theorem 6.21 and 5.3, we can state

THEOREM 6.211. *The ranks of apparition of the divisors of ϕ form a structure within $\tilde{\sigma}$.*

---

[9] For example let ϕ_n denote the n^{th} of the Fibonacci numbers 1, 1, 2, 3, 5, 8, $\cdots$. Then $\phi_{19} = 4181 = 37 \times 113$. Hence for $\mathfrak{A} = (37)$, $\mathfrak{B} = (113)$, $\mathfrak{n} = \rho(\mathfrak{A}) = \rho(\mathfrak{B}) = (19)$ while $\mathfrak{N} = (4181)$.

THEOREM 6.3. *If $\mathfrak{A}$ and $\mathfrak{B}$ are maximal divisors of ϕ, then the cross-cut $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]_\mu$ within $\bar{\mu}$ exists, and $\rho(\mathfrak{M}) = [\rho(\mathfrak{A}), \rho(\mathfrak{B})]$.*

PROOF. Let $[\mathfrak{A}, \mathfrak{B}] = \mathfrak{N}$. By axiom 2, $\mathfrak{N}$ divides ϕ. Let $\mathfrak{m} = \rho(\mathfrak{N})$ and let $\mathfrak{M}$ be the corresponding maximal divisor such that $\mathfrak{m} = \rho(\mathfrak{M})$. Then $\mathfrak{N} \supseteq \mathfrak{M}$. I say that $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]_\mu$. For $\mathfrak{A} \supseteq \mathfrak{M}$, $\mathfrak{B} \supseteq \mathfrak{M}$ by (4.4), (4.2). Let $\mathfrak{C}$ be any other maximal divisor such that $\mathfrak{A} \supseteq \mathfrak{C}$, $\mathfrak{B} \supseteq \mathfrak{C}$. Then $\mathfrak{N} \supseteq \mathfrak{C}$ by (4.2). Hence $\rho(\mathfrak{N}) \supseteq \rho(\mathfrak{C})$ by theorem 6.2, so that $\rho(\mathfrak{M}) \supseteq \rho(\mathfrak{C})$. Since $\mathfrak{M}$ and $\mathfrak{C}$ are maximal, $\mathfrak{M} \supseteq \mathfrak{C}$ by theorem 6.1, so that $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]_\mu$ by (4.2).

THEOREM 6.31. *The maximal divisors of ϕ form a structure within Σ isomorphic* (Ore,[10] pp. 416–418) *to the structure of ranks of apparition within $\bar{\sigma}$.*

PROOF. Theorems 6.3, 6.2, 6.11.

III. MODULAR PERIODICITY

7. We assume henceforth that the values of ϕ lie in a commutative ring $\mathfrak{O}$. Σ now denotes the structure of all ideals of $\mathfrak{O}$, so that the values of ϕ *quâ* elements of Σ are principal ideals of $\mathfrak{O}$.

For the present ϕ is any function on $\mathfrak{o}$ to $\mathfrak{O}$, not necessarily arithmetical, and $\bar{\sigma}$ denotes the structure of all *modules* of $\mathfrak{o}$. We use small German letters now for modules instead of ideals. If $\mathfrak{m}$ is a module, $m \equiv 0 \pmod{\mathfrak{m}}$ means $\mathfrak{m}$ contains m.

Let $\mathfrak{S}$ be any element of Σ. If there exists an element $m \neq 0$ of $\mathfrak{o}$ such that

$$\phi_{x+m} \equiv \phi_x \pmod{\mathfrak{S}}, \qquad \text{every } x \text{ of } \mathfrak{o},^{10} \tag{7.1}$$

$\mathfrak{S}$ is called a *modulus* of ϕ, and m a *period* of ϕ modulo $\mathfrak{S}$. The periods (0 included) obviously form a module, $\mathfrak{s}$ *the characteristic module of ϕ modulo $\mathfrak{S}$*. We shall also call $\mathfrak{s}$ the module of $\mathfrak{S}$, writing

$$\mathfrak{s} = \mu(\mathfrak{S}). \tag{7.2}$$

Let Π denote the set of all moduli of ϕ in Σ, and $\bar{\pi}$ the set of all characteristic modules in $\bar{\sigma}$. Clearly as in section 5, we have

THEOREM 7.1. *Π is closed under union.*

THEOREM 7.2. *μ is an arithmetic function on Π to $\bar{\sigma}$.*

We cannot prove in general that Π is closed under cross-cut. We assume:

AXIOM 3. *The set of all moduli of ϕ is a completely closed sub-structure of Σ.*

Then the following theorems follow precisely as in section 5.

THEOREM 7.3. *If $\mathfrak{A}$, $\mathfrak{B}$ are moduli of ϕ and if $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$, then $\mu(\mathfrak{M}) = [\mu(\mathfrak{A}), \mu(\mathfrak{B})]$.*

THEOREM 7.31. "DECOMPOSITION THEOREM."[11] *If $\mathfrak{A}$, $\mathfrak{B}$ are moduli of ϕ and $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{O}$, then $\mu(\mathfrak{AB}) = [\mu(\mathfrak{A}), \mu(\mathfrak{B})]$.*

---

[10] We shall omit this phrase henceforth, reserving the letter x exclusively to denote every element of $\mathfrak{o}$.

[11] Stated in Ward[13] for linear recurring series. The analogous theorems 5.31 and 10.31 appear to be new.

8. The theory of maximal moduli exactly parallels the theory of maximal divisors.

For every possible module of periods $\mathfrak{n}$ there exists a maximal modulus $\mathfrak{N}$ such that

$$\mu(\mathfrak{N}) = \mathfrak{n}; \quad \text{if} \quad \mu(\mathfrak{S}) = \mathfrak{n}, \ \mathfrak{S} \text{ a module}, \ \mathfrak{S} \supseteq \mathfrak{N}. \tag{8.1}$$

THEOREM 8.1. *Let $\mathfrak{A}$ be any modulus of ϕ, $\mathfrak{a}$ its characteristic module. Then if $\mathfrak{N}$ is a maximal modulus such that $\phi \supseteq \mathfrak{a}(\mathfrak{N})$, $\mathfrak{A} \supseteq \mathfrak{N}$.*

THEOREM 8.11. *If $\mathfrak{A}$ and $\mathfrak{B}$ are maximal moduli of ϕ with characteristic modules $\mathfrak{a}$ and $\mathfrak{b}$ respectively, then $\mathfrak{A} \supseteq \mathfrak{B}$ when and only when $\mathfrak{a} \supseteq \mathfrak{b}$.*

THEOREM 8.2. *The set of all maximal moduli of ϕ is closed under union.*

THEOREM 8.21. *If $\mathfrak{A}$ and $\mathfrak{B}$ are maximal moduli of ϕ and $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, then $(\mu(\mathfrak{A}), \mu(\mathfrak{B}))_r$ exists and equals $\mu(\mathfrak{D})$.*

THEOREM 8.211. *The characteristic modules of the moduli of ϕ form a structure within $\tilde{\sigma}$.*

THEOREM 8.3. *If $\mathfrak{A}$ and $\mathfrak{B}$ are maximal moduli of ϕ then $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]_r$ exists, and $\mu(\mathfrak{M}) = [\mu(\mathfrak{A}), \mu(\mathfrak{B})]$.*

THEOREM 8.31. *The maximal moduli of ϕ form a structure within Σ isomorphic to the structure of characteristic modules within $\tilde{\sigma}$.*

It is easily seen that if we assume in analogy with axiom 1,

AXIOM 4. *The periods of any modulus of ϕ form an ideal.*

Then all the theorems of this section and the preceding one hold if the word module is everywhere replaced by ideal, and the notation $\mathfrak{a}, \cdots, \mathfrak{z}$ is understood to mean ideals instead of modules.

IV. Restricted Periods. Relationships between Divisors and Moduli of an Arithmetic Function

9. The concept of "restricted period" which we formulate abstractly here is very important in the theory of the Lucas function and linear recurring series in general. (Carmichael,[2] Ward[4].) As in sections 7, 8 we assume that the values of ϕ lie in a commutative ring $\mathfrak{O}$ containing a unit element. Let $\mathfrak{S}$ be an ideal of $\mathfrak{O}$. If there exist elements M and m of $\mathfrak{O}$ and $\mathfrak{o}$ such that

$$\phi_{x+m} \equiv M\phi_x \pmod{\mathfrak{S}} \text{ all } x \text{ in } \mathfrak{o} \tag{9.1}$$

$$((M), \mathfrak{S}) = \mathfrak{O} \tag{9.11}$$

then m is called a *restricted period* of ϕ modulo $\mathfrak{S}$, and M a *multiplier* of ϕ modulo $\mathfrak{S}$.

THEOREM 9.1. *The multipliers of ϕ modulo $\mathfrak{S}$ are closed under multiplication. The restricted periods of ϕ modulo $\mathfrak{S}$ form an additive semi-group.*

PROOF. Assume that $\phi_{x+m_i} \equiv M_i\phi_x \pmod{\mathfrak{S}}$, $((M_i), \mathfrak{S}) = \mathfrak{O}$, $i = 1, 2$. Then $\phi_{x+m_1+m_2} \equiv M_1\phi_{x+m_2} \equiv M_1M_2\phi_x \pmod{\mathfrak{S}}$. Also (Van der Waerden,[11] p. 45) $((M_1M_2), \mathfrak{S}) = \mathfrak{O}$.

We shall now assume

AXIOM 5.[12] *For any modulus $\mathfrak{S}$ the multipliers of ϕ modulo $\mathfrak{S}$ form a multiplicative group in $\mathfrak{O}$* (Ward,[13] p. 162).

We denote this group by $\mathfrak{G}$.

THEOREM 9.11. *The restricted periods of ϕ modulo $\mathfrak{S}$ form a module.*

PROOF. With the notation of theorem 9.1, let N_1 be the inverse of M_1 in $\mathfrak{G}$, so that $N_1M_1 \equiv 1 \pmod{\mathfrak{S}}$. Then by (7.2)

$$\phi_{x+m_2-m_1} \equiv N_1M_1\phi_{x-m_1+m_2} \equiv N_1M_1M_2\phi_{x-m_1} \equiv N_1M_2\phi_x \pmod{\mathfrak{S}}.$$

By axiom 5, theorem 7.1 N_1M_2 is a multiplier so that $m_2 - m_1$ is a period.

THEOREM 9.2. *Let $\mathfrak{S}$ be a modulus, $\mathfrak{G}$ its group, $\mathfrak{s}$ its restricted period. Let $\mathfrak{T}$ be any divisor of $\mathfrak{S}$. Then $\mathfrak{T}$ also is a modulus. If $\mathfrak{K}$ is its group and $\mathfrak{t}$ its restricted period, $\mathfrak{G} \subseteq \mathfrak{K}$, $\mathfrak{t} \supseteq \mathfrak{s}$.*

PROOF. Clear.

THEOREM 9.3. *The set of all moduli of ϕ and the set of all moduli of restricted periods are identical.*

PROOF. If $\mathfrak{S}$ is an ordinary modulus, its group of multipliers consists of the single element 1 of $\mathfrak{O}$. On the other hand, if $\mathfrak{S}$ is a modulus of restricted periods, $\mathfrak{S}$ has the multiplier 1 by axiom 5 and hence is an ordinary modulus.

THEOREM 9.31.[13] *If $\tau(\mathfrak{S})$ and $\mu(\mathfrak{S})$ are respectively the module of restricted periods and the module of periods of the modulus $\mathfrak{S}$ of ϕ, then $\tau(\mathfrak{S}) \supseteq \mu(\mathfrak{S})$.*

PROOF. Clear from Theorem 9.3 and axiom 5.

10. In view of theorem 9.3, it is unnecessary to show that the moduli of the restricted periods of ϕ are closed under union, and theorem 9.2 makes it evident that τ is an arithmetical function on $\bar{\pi}$ to $\bar{\sigma}$. Even if we retain axiom 3 of section 7, we cannot prove the analogue of theorems 5.3 and 7.3 viz.:—"If $\mathfrak{A}$, $\mathfrak{B}$ are moduli of ϕ and if $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$, then $\tau(\mathfrak{M}) = [\tau(\mathfrak{A}), \tau(\mathfrak{B})]$." We must content ourselves with $\tau(\mathfrak{M}) \subseteq [\tau(\mathfrak{A}), \tau(\mathfrak{B})]$.

To see why this lack occurs, let us try to show that $[\tau(\mathfrak{A}), \tau(\mathfrak{B})] \subseteq \tau(\mathfrak{M})$. If m is any element of $[\tau(\mathfrak{A}), \tau(\mathfrak{B})]$, we infer from (4.2) that

$$\phi_{x+m} \equiv M\phi_x \pmod{\mathfrak{A}}, \qquad \phi_{x+m} \equiv N\phi_x \pmod{\mathfrak{B}}$$
$$((M), \mathfrak{A}) = \mathfrak{O}, \qquad ((N), \mathfrak{B}) = \mathfrak{O}.$$

To show that m lies in $\tau(\mathfrak{M})$, it is necessary and sufficient to show that there exists an element S of $\mathfrak{O}$ such that

$$\phi_{x+m} \equiv S\phi_x \pmod{\mathfrak{M}}, \qquad ((S), \mathfrak{M}) = \mathfrak{O}.$$

Since $\mathfrak{A} \supseteq \mathfrak{M}$, $\mathfrak{B} \supseteq \mathfrak{M}$, we must also have

$$S \equiv M \pmod{\mathfrak{A}}, \qquad S \equiv N \pmod{\mathfrak{B}}.$$

---

[12] This axiom always holds if $\mathfrak{O}$ is a ring of algebraic integers or more generally whenever the ring $\mathfrak{O}/\mathfrak{S}$ is finite.

[13] Generalizes Carmichael[2], p. 355.

Now such an element S need not exist. For example, take for $\mathfrak{O}$ the ring of rational integers, and let $\mathfrak{A} = (6)$, $\mathfrak{B} = (9)$, $M = 5$, $N = 4$. Then $\mathfrak{M} = (18)$, and no S exists.

On the other hand if $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{O}$, such an S does exist since the Chinese remainder theorem holds in a commutative ring with unit element (van der Waerden,[11] p. 85). Thus a "decomposition theorem" holds for the restricted period analogous to theorems 5.31 and 7.31.

DECOMPOSITION THEOREM 10.31. *If $\mathfrak{A}$, $\mathfrak{B}$ are moduli and $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{O}$, then $\tau(\mathfrak{AB}) = [\tau(\mathfrak{A}), \tau(\mathfrak{B})]$.*

Since theorem 7.3 fails, we cannot introduce maximal restricted period moduli, and the theorems of sections 6 and 8 have no analogues.

11. It remains to discuss the relationship between the rank of apparition and restricted period of any element of Σ. Let us suppose that ϕ is an arithmetic function on $\mathfrak{o}$ to $\mathfrak{O}$, and that axioms 1, 2, 3 and 5 hold.

Consider the elements ϕ_0 and ϕ_1. Since $x \mid 0$, $1 \mid x$ for every x of $\mathfrak{o}$, $\phi_x \supseteq \phi_0$ and $\phi_1 \supseteq \phi_x$ for every value of ϕ in $\mathfrak{O}$. The simplest way to satisfy these two conditions is for ϕ_0 to equal the zero element and ϕ_1 the unit element of the ring $\mathfrak{O}$. An arithmetic function with this property will be called *normal*. We assume

AXIOM 6. *ϕ is a normal arithmetic function on $\mathfrak{o}$ to $\mathfrak{O}$.*

THEOREM 11.1.[14] *Every modulus of ϕ is a divisor of ϕ, and the rank of apparition of any modulus divides its restricted period.*

PROOF. Let $\mathfrak{S}$ be any modulus, m a restricted period of $\mathfrak{S}$. Then since

$$\phi_{m+x} \equiv M\phi_x \pmod{\mathfrak{S}}, \qquad \phi_m \equiv M\phi_0 \equiv 0 \pmod{\mathfrak{S}}.$$

Hence $m \equiv 0 \bmod \rho(\mathfrak{S})$.

CALIFORNIA INSTITUTE OF TECHNOLOGY.

REFERENCES

[1] E. Lucas, *Amer. Jour. of Math.* vol. 1 (1878) pp. 184–239, 289–321.
[2] R. D. Carmichael, *Quarterly Journal* vol. 48 (1920) pp. 343–372.
[3] H. T. Engstrom, *Trans. Amer. Math. Soc.* vol. 33 (1931) pp. 210–218.
[4] M. Ward, *Trans. Amer. Math. Soc.* vol. 35 (1933) pp. 600–628.
[5] D. H. Lehmer, *Annals of Math.* (2), vol. 31 (1930) pp. 419–448.
[6] M. Hall, *Amer. Jour. of Math.* vol. 58 (1936) pp. 577–584.
[7] M. Ward, *Trans. Amer. Math. Soc.* (reference later).
[8] L. E. Dickson, *History*, vol. 1, chapter V.
[9] G. H. Halphen, *Traite des Fonctions Elliptiques*, Part I, chap. IV.
[10] O. Ore, *Annals of Math.* (2) vol. 36 (1935), pp. 406–437.
[11] Van der Waerden, *Modern Algebra Part* 2, Berlin (1931).
[12] M. Ward, *Bulletin Amer. Math. Soc.* (reference later).
[13] M. Ward, *Trans. Amer. Math. Soc.* vol. 33 (1931) pp. 153–165.

[14] This result generalizes a theorem of Hall[6] on linear divisibility sequences. For the Lucas function, the rank of apparition and restricted period are equal.