THE MAPPINGS OF THE POSITIVE INTEGERS INTO THEMSELVES WHICH PRESERVE DIVISION

MORGAN WARD

1. Introduction, First Theorem. Let L denote the lattice of the integers 0, 1, 2, $\cdots$ partially ordered by division. We study here mappings

$$\phi: \quad \phi_0, \phi_1, \phi_2, \cdots, \phi_n=\phi(n), \cdots$$

of L into itself which preserve division; that is,

(i) *If n divides m, then ϕ_n divides ϕ_m.*

Since ϕ_1 divides every ϕ_n and every ϕ_n divides ϕ_0, we lose little generality by assuming

(ii) $\phi_0=0, \quad \phi_1=1.$

Any mapping with properties (i) and (ii) will be called a divisibility sequence on L.

A mapping ϕ is said to be of "*positive character*" if

(iii) $\phi_n>0$ for $n>0$.

A divisibility sequence of positive character will be called a *normal sequence* or *normal mapping* of L.

In many instances, we are interested in the occurrence of multiples of some assigned modulus m among the terms of a normal sequence ϕ. If $\phi_r \equiv 0 \pmod{m}$ for some $r>0$, we call m a *divisor* of ϕ and r a "*place of apparition*" of m in ϕ. If in addition $\phi_s \not\equiv 0 \pmod{m}$ for every proper divisor s of r, r is called a "*rank of apparition*" of m in ϕ. If m is not a divisor of ϕ, we assign to it the rank of apparition zero, which is consistent with the definitions.

It follows that every modulus m has at least one rank of apparition in ϕ. If each modulus has exactly one rank of apparition, we say that ϕ "*admits a rank function*". Indeed if the rank of m in ϕ is denoted by $\rho(m)$ then ρ is a divisibility sequence. Furthermore

(iv) $\phi_n \equiv 0 \pmod{m}$ *if and only if* $n \equiv 0 \pmod{\rho_m}$.

Under this condition, multiples of any integer m if they appear at all in ϕ are regularly spaced as in the identity mapping $i(n)=n$.

Normal sequences are of common occurrence in number theory; the totient function and its various generalizations [3, chap. 5] is a

Received April 19, 1954.

familiar example. For other examples and generalizations see [3, chap. 17], [4], [6], [9], [10].

Normal sequences with property (iv) are of considerable arithmetical interest, and special instances, notably the Lucas sequences [6] have been intensively studied [1], [5].

We study here general properties of all divisibility sequences and in particular develop necessary and sufficient conditions that a normal sequence shall admit a rank function. Our first main result is as follows.

THEOREM 1. *A necessary and sufficient condition that a normal mapping ϕ admit a rank function is that it have the following property*:

$$\text{(v)} \qquad \phi(pn) \smile \phi(qn) = \phi(n) \qquad p, q \text{ any distinct primes.}$$

Here we are using the lattice notation explained in § 3; the left side of (v) is the greatest common divisor of $\phi(pn)$ and $\phi(qn)$.

2. Further Results, Second Theorem. Our other results are formulated in terms of the notion of the "generator" of a normal sequence. Let

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \tag{2.1}$$

be the prime factorization of any positive integer n of L. Define a new mapping ψ of L by $\psi(0)=0$, $\psi(1)=1$ and

$$\psi(n) = \phi(n) \div \bigcap_{1 \le i \le k} \phi\left(\frac{n}{p_i}\right), \qquad n > 1. \tag{2.2}$$

Then ψ is called the generator of ϕ. It has properties (ii) and (iii), but not in general property (i). It is shown in § 5 that formula (2.2) may be inverted to express ϕ in terms of ψ thus:

$$\phi(n) = \bigcap_{(c)} \prod_{1 \le i \le r} \psi(c_i). \tag{2.3}$$

Here (c): $1=c_1, c_2, \cdots, c_{r-1}, c_r=n$ is a complete chain of divisors of n in the lattice L, c_i covering c_{i+1} for $i=1, 2, \cdots, r-1$. The indicated least common multiple $\bigcap$ of the products $\prod \psi(c_i)$ is to be extended over all such chains (c) of divisors of n.

For example, if $n=12$, there are three complete chains: 1, 2, 4, 12; 1, 2, 6, 12 and 1, 3, 6, 12. Thus (2.3) becomes

$$\phi(12) = \psi(1)\psi(2)\psi(4)\psi(12) \cap \psi(1)\psi(2)\psi(6)\psi(12) \cap \psi(1)\psi(3)\psi(6)\psi(12).$$

Conversely, it turns out that if we start off with a mapping ψ of positive character with $\psi_0=0$, $\psi_1=1$ and define ϕ by (2.3), then ϕ is a

normal mapping, and ψ is its generator. The relationships between arithmetical properties of ϕ and ψ are developed in §§ 6 and 7.

If ϕ is of positive character, we may define a new numerical function ζ by the Dedekind-Möbius inversion formulas [2, p. 61]

$$\zeta(n)=\prod_{d\supseteq n}\phi\left(\frac{n}{d}\right)^{\mu(d)}; \qquad \phi(n)=\prod_{d\supseteq n}\zeta(d)\,. \tag{2.4}$$

Here μ as usual is the Möbius function.

ζ is uniquely determined by ϕ, but does not define a mapping of L because $\zeta(n)$ is not necessarily an integer. If $\zeta(n)$ is an integer for every n, ϕ is evidently a normal sequence; we call ζ in this case the "*Dedekind generator*" of ϕ.

THEOREM 2. *If ϕ is a normal sequence, then a necessary and sufficient condition that ϕ admit a rank function is that its Dedekind generator should exist, and be equal to its ordinary generator.*

The best known instance of this theorem is when ϕ is the Lucas sequence $\phi_n=(\alpha^n-\beta^n)/(\alpha-\beta)$ where $p=\alpha+\beta$, $q=\alpha\beta$ are co-prime integers chosen so that $|pq|>1$; $|p^2-4q|>0$. Then ψ is the Sylvester [7] cyclotomic sequence

$$\psi_n=\prod_{\substack{1\le r\le n\\ r\cup n=1}}\left(\alpha-e^{2\pi i\frac{r}{n}}\beta\right).$$

3. **Notations.** We use whenever convenient the standard notations of lattice algebra for arithmetical division and its associated operations over L considered as a distributive residuated lattice [8], [11]. We thus write $a\supseteq b$, $a\not\supseteq b$ and $a\supset b$ for "a divides b", "a does not divide b" and "a properly divides b". If neither $a\supseteq b$ nor $b\supseteq a$, we say a and b are "*non-comparable*". If $a\supseteq b$ and $a\supseteq x\supseteq b$ implies either $a=x$ or $b=x$ we say "*a covers b*".

$a\cup b$, $a\cap b$ and ab stand respectively for the greatest common divisor (g.c.d.), least common multiple (l.c.m.), and product of a and b. If $a_1, a_2, \cdots, a_k$ are k given integers of L, we write $\bigcup a_i$, $\bigcap a_i$ and $\prod a_i$ for their g.c.d., l.c.m. and product suppressing the range of i where no confusion can arise.

If $x*y$ denotes any one of the three operations $x\cup y$, $x\cap y$ or xy in L, and ϕ is any mapping of L, we say that ϕ is "$*$-factorable" if $\phi(x*y)=\phi(x)*\phi(y)$ whenever $x\cup y=1$ and "completely $*$-factorable" if $\phi(x*y)=\phi(x)*\phi(y)$ for every x, y. The star-product of two mappings ϕ and θ is defined as usual by $(\phi*\theta)_n=\phi_n*\theta_n$.

In proofs we use when convenient $\Longrightarrow$ and $\Longleftrightarrow$ for "implies", and "implies and is implied by". We use without specific mention the familiar formulas [12]

$$b\bigcup a_i=\bigcup ba_i\,,\qquad b\bigcap a_i=\bigcap ba_i\,,$$
$$b\bigcup 0=b\bigcap 1=b\,;\quad b\bigcup 1=1,\quad b\bigcap 0=0\,.$$

4. Divisibility Sequences, Binary Sequences. Let ϕ be any divisibility sequence; that is, a mapping of L with properties (i) and (ii) of the introduction. Define $\alpha_0=\beta_0=0$ and

$$\alpha_n=\phi_n\,,\qquad \beta_n=1\quad \text{if}\quad \phi_n\neq 0$$
$$\alpha_n=\bigcap_{\substack{x\supseteq n\\ \phi_x\neq 0}}\phi_x\,,\quad \beta_n=0\quad \text{if}\quad \phi_n=0.$$

Then α and β are divisibility sequences, and $\phi=\alpha\beta$. Furthermore α is a normal mapping of L, while β consists exclusively of zeros and ones. We call β a "*binary (divisibility) sequence*".

We may immediately obtain a binary sequence from any divisibility sequence by reducing each term modulo 2. More generally, if m is any modulus, we may obtain from the divisibility sequence ϕ a binary sequence θ which describes the distribution of multiples of m in ϕ by letting $\theta_n=0$ or 1 according as $\phi\equiv 0$ or $\phi\not\equiv 0 \pmod m$. The sequences obtained in this manner from linear divisibility [12] or elliptic divisibility sequences [13] are usually periodic.

Again, if E is any subset of L with the properties that 0 is not in E and if x is in E, so is every divisor of x, then the characteristic function of E is evidently a binary sequence. A simple example is the set of square-free integers; the characteristic function is μ^2.

Let β be any binary sequence. If $\beta_k=0$, k is called a zero of β. If in addition $\beta_d\neq 0$ for $d\supset k$, k is called a prime zero of β. The prime zeros of β evidently form a multiplicative basis for the set of all zeros of β. Perhaps the most interesting property of this basis is expressed by the following theorem whose proof is left to the reader.

THEOREM. *The zeros of a binary divisibility sequence have a finite basis if and only if the sequence is periodic. The period of the sequence is then the* l.c.m. *of the prime zeros of its basis.*

5. The Generator of A Normal Sequence. From now on, all mappings considered are of positive character. Let ψ be any such mapping with $\psi_0=0$, $\psi_1=1$ and define a new mapping ϕ by means of formula (2.3) and $\phi_0=0$, $\phi_1=1$. Then ϕ is evidently normal. Hold n fixed, and let (2.1) be its prime decomposition. Each complete chain

(c): $1=c_1, c_2, \cdots, c_{r-1}, c_r=n$; $\quad c_i$ covers c_{i+1}

in the sublattice of all divisors of n is of the same length $r=a_1+a_2+\cdots+a_k+1$, while c_{r-1} is one of the k elements n/p_i which cover n. We may accordingly group the chains into k mutually exclusive classes C_i by putting into class C_i all chains (c) with $c_{r-1}=n/p_i$. But any chain of class C_i consists of a complete chain of divisors of n/p_i plus the fixed element $c_r=n$. Hence formula (2.3) may be written

$$\phi_n=\bigcap_{C_i}\bigcap_{(c')}(\psi_{c'_1}\cdots\psi_{c'_{r-1}})\psi_n$$

where the inner l.c.m. is taken over all complete chains (c') of divisors of n/p_i. Thus by (2.3) again

$$\phi_n=\bigcap_i\phi(n/p_i)\psi(n)=\psi(n)[\phi_{n/p_1}\cap\cdots\cap\phi_{n/p_k}].$$

Therefore ψ is the generator of ϕ as defined in formula (2.2).

Conversely, if we define ψ by (2.2), we find by direct calculation that (2.3) holds for small n. We therefore proceed by induction and assume that (2.3) is true for all integers less than n, and hence in particular for the k integers n/p_i which cover n.

On transforming the right side of (2.3) as in the first part of this proof, we obtain by (2.2) and the hypothesis of the induction

$$\bigcap_{(c)}\prod_i\psi_{c_i}=\bigcap_{C_i}\prod_i\psi_{c'_i}\psi_n=\bigcap_i(\phi_{n/p_i}\psi_n)=\psi_n\bigcap_i\phi_{n/p_i}=\phi_n.$$

Thus the formulas (2.2) and (2.3) are equivalent.

6. Factorable sequences. Various factorability properties of normal sequences may be elegantly stated as properties of its generator. We postpone the consideration of g.c.d. factorability until the next section, since it is intimately connected with the existence of a rank function. We omit proofs of the results stated here, since we merely wish to show the importance of the notion of a generator.

Either of the following two conditions is necessary and sufficient for a normal sequence ϕ with generator ψ to be product-factorable:

$$\phi_n=\prod_{p^t\exists n}\psi_{p^t}. \tag{6.1}$$

Here the product is extended over all prime powers p^t dividing n.

$$\psi_{nm}=\psi_n\cup\psi_m \qquad n,\ m \text{ co-prime.} \tag{6.2}$$

A necessary and sufficient condition for ϕ to be l.c.m.-factorable is that

$$\psi_n=1, \qquad n \text{ not a power of a prime.} \tag{6.3}$$

Any one of the following three sets of conditions are necessary and sufficient for ϕ to be completely product factorable:

(6.4) $\psi(mn)=\psi(m\cap n)=\psi(m)\cup\psi(n)$, $n,\ m>1$.

(6.5) $\psi(mn)=\psi(m)\cup\psi(n)$ if $m,\ n$ are co-prime

and $\psi(p^a)=\psi(p)$ for every prime p.

(6.6) $\psi(n)=\psi(p_1,\cdots,p_k)=\phi(p_1)\phi(p_2),\cdots,\phi(p_k)$.

Here as in (2.1), $p_1,\ p_2,\cdots,p_k$ are the distinct prime factors of n.

7. G.C.D. factorable mappings. A mapping ϕ is said to be *completely* g.c.d. *factorable* if it has the property

(vi) $\phi(n\cup m)=\phi(n)\cup\phi(m)$.

Every such mapping evidently preserves division.

LEMMA 7.1. (Ward [14]): *Conditions* (iv) *and* (vi) *are equivalent for normal mappings of* L; *that is, a normal mapping admits a rank function if and only if it is completely* g.c.d. *factorable.*

Proof. Assume that ϕ is a normal mapping satisfying Condition (iv). Let $\rho=\rho(k)$ be the rank of $k=\phi_n\cup\phi_m$ in ϕ. Then ρ is positive. Also $k\supseteq\phi_n,\ \phi_m\Longrightarrow\rho\supseteq n,\ m\Longrightarrow\rho\supseteq n\cup m\Longrightarrow k\supseteq\phi(n\cup m)$. But by (i),

$$n\cup m\supseteq n,\ m\Longrightarrow\phi_{n\cup m}\supseteq\phi_n,\ \phi_m\Longrightarrow\phi_{n\cup m}\supseteq k.$$

Hence $\phi_{n\cup m}=\phi_n\cup\phi_m$ and (iv) implies (vi).

Conversely, let ϕ be a normal mapping with property (vi), and let k be any modulus. If k is not a divisor of ϕ, the rank of k is zero, and (iv) is satisfied. If k is a divisor of ϕ, let ϕ_r be the first term with positive index r which k divides. By (i),

$$n\equiv 0 \pmod r\Longrightarrow\phi_n\equiv 0 \pmod k.$$

Assume conversely that $\phi_n\equiv 0 \pmod k$. Then by (vi), $\phi_{n\cup r}\equiv 0 \pmod k$. But $0<n\cup r\leq r$. Hence $n\cup r=r$ or $n\equiv 0 \pmod r$. In other words,

$$\phi_n\equiv 0 \pmod k\Longrightarrow n\equiv 0 \pmod r.$$

Hence r is the rank of k in ϕ. Since k was arbitrary, (vi) implies (iv), which completes the proof.

The factorability condition on ϕ may be replaced by an equivalent condition on its generator ψ.

LEMMA 7.2 *A normal mapping* ϕ *admit a rank function if and*

only if its generator ψ satisfies the condition

(vii) $$\psi(n)\cup\psi(m)=1 \qquad n,\ m \text{ non-comparable.}$$

Proof. Assume that ϕ is normal, and admits a rank function, but that (vii) is false. Then there exist integers n, m and a prime q such that

(7.1) $$\psi(n)\equiv\psi(m)\equiv 0 \pmod{q}, \text{ but } n\not\supset m,\ m\not\supset n.$$

By formula (2.2),

$$(7.1)\Longrightarrow\phi(n)\equiv\phi(m)\equiv 0 \pmod{q}.$$

Suppose that q^a exactly divides $\phi(n)$ and q^b exactly divides $\phi(m)$. We may evidently assume that $b\geq a$. Let r be the rank of q^a in ϕ. Then since $n\equiv m\equiv 0 \pmod{r}$, we have $n\cup m\equiv 0 \pmod{r}$. But if (2.1) gives the factorization of n so that $p_1, p_2, \cdots, p_k$ are its distinct prime factors, then

(7.2) $$\phi(n/p_i)\not\equiv 0 \bmod q^a, \qquad 1\leq i\leq h.$$

For in the contrary case, $\psi(n)\equiv 0 \pmod{q}$ and (2.2) together imply

$$\phi(n)\equiv\psi(n)\bigcap_i\phi\left(\frac{n}{p_i}\right)\equiv 0 \pmod{q^{a+1}}$$

which is a contradiction.

Now

$$(7.2)\Longrightarrow n\,|\,p_i\not\equiv 0 \pmod{r} \qquad i=1, 2, \cdots, k.$$

But $n\equiv 0 \pmod{r}$. Hence $n=r$ and $n\supseteq n\cup m\supseteq m$ contradicting (7.1). Therefore (iv) implies (vii).

Assume conversely that ϕ is normal with generator ψ satisfying (vii). To show that ϕ then admits a rank function, it will suffice to prove that *every prime power q^a has a unique rank of apparition in ϕ.* If q^a is not a divisor of ϕ then it has the unique rank zero. If q^a is a divisor of ϕ then there exists a positive index r such that

(7.3) $$\phi_r\equiv 0 \pmod{q^a}, \quad \phi_n\not\equiv 0 \pmod{q^a}, \qquad 0<n<r.$$

To prove that r is the rank of q^a in ϕ, it will suffice to show that if $\phi_n\equiv 0 \bmod q^a$ then $n\equiv 0 \pmod{r}$. This we do by contradiction. For otherwise, there exists a least positive $n>r$ such that $\phi_n\equiv 0 \bmod q^a$, but n, r noncomparable. Evidently, $\psi_r\equiv 0 \pmod{q}$. Hence $\psi_n\not\equiv 0 \pmod{q}$ by Condition (vii). But then formula (2.2) implies that $\phi(n/p_i)\equiv 0 \pmod{q^a}$ for some prime divisor p_i of n. Therefore, by the minimal

choice of n, either $r \supseteq n/p_i$ or $n/p_i \supseteq r$. In the first case, $r \supset n$. In the second case $n/p_i \leq r$ so that by (7.3), $n/p_i = r$ and $r \supset n$. In either case $r \not\supset n$ is contradicted. Hence (vii) implies (iv), which completes the proof of the lemma.

8. Proof of Theorem 1. In view of Lemma 7.1, the proof of Theorem 1, requires only the demonstration that if ϕ is normal, Condition (v) implies Condition (vi); for $pn \cup qn = n$ so that the implication (vi) $\Longrightarrow$ (v) is trivial. Note also that (v) is essentially a weakening of (vi), since it amounts to asserting (vi) only in the special case when $n \cup m$ covers both n and m.

Let ϕ be normal, and s a fixed positive integer. Then the normal mapping θ defined by

$$\theta(n) = \phi(sn)/\phi(s), \qquad n = 0, 1, 2, \cdots \tag{8.1}$$

is called a subsequence of ϕ. The following lemma is an easy consequence of this definition.

LEMMA 8.1. *If ϕ is normal, and has the property* (v), *then so has every subsequence of ϕ.*

LEMMA 8.2. *If ϕ is normal, and has the property* (v), *then ϕ is* g.c.d. *factorable; that is*

$$\phi(n) \cup \phi(m) = 1 \quad \text{if} \quad n \cup m = 1. \tag{viii}$$

Note that by (ii), (viii) is a special case of (vi); the proof is by induction on the number of prime factors of n and m. First if n and m are distinct primes p and q, then (viii) follows from (v) on taking $n = 1$.

Suppose that $n = p$ and m is the product of $l \geq 2$ primes, $m = q_1, q_2, \cdots, q_l$ where the q_i are distinct from p but not necessarily distinct from one another. Assume that (viii) has been proved for $n = p$ and m a product of $l-1$ primes. Now take $p = p$, $q = q_l$ and $n = m/q_l$ in (v). Then

$$\phi(pm/q_l) \cup \phi(m) = \phi(m/q_l).$$

Now

$$q_l \not\supset p \Longrightarrow p \supseteq pm/q_l \Longrightarrow \phi(p) \supseteq \phi(pm/q_l).$$

Consequently,

$$\phi(p) \cup \phi(m) = \phi(p) \cup \phi(pm/q_l) \cup \phi(m) = \phi(p) \cup \phi(m/q_l) = 1$$

by the hypothesis of the induction. Hence (viii) is true if n is a prime number.

Next assume that $n=p_1p_2\cdots p_k$ is the product of $k\geq 2$ primes p_i distinct from all the primes q_j dividing m so that $n\cup m=1$, and also assume that (viii) has been proved for n a product of $k-1$ primes. Now apply (v) with $p=p_k$, $q=q_1$ and $n=nm/p_kq_1$. Thus

$$\phi(nm/q)\cup\phi(nm/p)=\phi(nm/pq)\,.$$

Now

$$n\supseteq nm/q\Rightarrow\phi(n)\supseteq\phi(nm/q)\Rightarrow\phi(n)\cup\phi(nm/p)=\phi(n)\cup\phi(nm/q)\cup\phi(nm/p)$$
$$=\phi(n)\cup\phi(nm/pq)=\phi(n)\cup\phi(nm/pq_1)\,.$$

Repeat this argument replacing m successively by

$$m/q_1,\ m/q_1q_2,\ \cdots,\ m/q_1q_2\cdots q_l=1$$

and leaving n and p unchanged; we find that

$$\phi(n)\cup\phi(nm/p)=\phi(n)\cup\phi(nm/pq_1)$$
$$=\phi(n)\cup\phi(nm/pq_1q_2)=\cdots=\phi(n)\cup\phi(n/p)=\phi(n/p).$$

But

$$m\supseteq nm/p\Rightarrow\phi(m)\supseteq\phi(nm/p)\Rightarrow\phi(n)\cup\phi(m)=\phi(n)\cup\phi(nm/p)\cup\phi(m)$$
$$=\phi(n/p)\cup\phi(m)=1$$

by the hypothesis of the induction. Hence (viii) is true for every n prime to m, completing the proof of Lemma 8.2.

Theorem 1 may now be proved as follows: Let ϕ be a normal mapping satisfying (v) and let both n and m be positive, since (vi) is trivially satisfied if n or m is zero. Let $s=n\cup m$. Then $n=n's$, $m=m's$ with $n'\cup m'=1$. Consider the subsequence θ of ϕ defined by (8.1). By Lemma 8.1, θ has property (v). Hence Lemma 8.2 implies

$$\theta(n')\cup\theta(m')=1\Rightarrow\phi(n)/\phi(s)\cup\phi(m)/\phi(s)=1$$
$$\Rightarrow\phi(n)\cup\phi(m)=\phi(s)=\phi(n\cup m)\,.$$

Hence (v) implies (vi), completing the proof of Theorem 1.

9. Proof of second theorem—necessity. Assume that ϕ is normal, and admits a rank function, and let ψ be its generator. We shall show that

(ix) $$\phi_n=\prod_{d\supseteq n}\psi_d$$

so that ψ is the Dedekind generator of ϕ. The proof is based on a consequence of Dedekind's cross-classification principle [2]; namely

LEMMA 9.1. *If a_1, a_2, $\cdots$, a_k are positive integers, then*

$$a_1 \cap a_2 \cap \cdots \cap a_k = \amalg a_1 \amalg (a_1 \cup a_2 \cup a_3) \cdots \dot{\div} \amalg (a_1 \cup a_2) \amalg (a_1 \cup a_2 \cup a_3 \cup a_4) \cdots .$$

This result is a generalization of the familiar formula $a_1 \cap a_2 = a_1 a_2 \dot{\div} a_1 \cup a_2$ and is perhaps easiest proved by showing that the highest powers of p dividing both sides of the formula are the same.

On applying the result to formula (2.2), we obtain

$$\begin{aligned}\psi(n) &= \phi(n) \dot{\div} \left[\phi\left(\frac{n}{p_1}\right) \cap \phi\left(\frac{n}{p_2}\right) \cap \cdots \cap \phi\left(\frac{n}{p_k}\right)\right] \\ &= \phi(n) \amalg \left(\phi\left(\frac{n}{p_1}\right) \cup \phi\left(\frac{n}{p_2}\right)\right) \amalg \left(\phi\left(\frac{n}{p_1}\right) \cup \phi\left(\frac{n}{p_2}\right) \cup \phi\left(\frac{n}{p_3}\right) \cup \phi\left(\frac{n}{p_4}\right)\right) \cdots \\ &\quad \dot{\div} \amalg \phi\left(\frac{n}{p_1}\right) \amalg \left(\phi\left(\frac{n}{p_1}\right) \cup \phi\left(\frac{n}{p_2}\right) \cup \phi\left(\frac{n}{p_3}\right)\right) \cdots .\end{aligned}$$

Now since ϕ admits a rank function, ϕ is completely g.c.d. factorable by Lemma 7.1. Therefore the formula above may be written

$$\begin{aligned}\psi(n) &= \phi(n) \amalg \phi\left(\frac{n}{p_1 p_2}\right) \amalg \phi\left(\frac{n}{p_1 p_2 p_3 p_4}\right) \cdots \\ &\quad \dot{\div} \amalg \phi\left(\frac{n}{p_1}\right) \amalg \phi\left(\frac{n}{p_1 p_2 p_3}\right) \cdots \\ &= \amalg_{d \supseteq n} \phi\left(\frac{n}{d}\right)^{\mu(d)}\end{aligned}$$

where μ is the Möbius function. Hence (ix) follows by the Dedekind inversion formula, completing the proof of the necessity.

10. Proof of second theorem—sufficiency. Now assume that ϕ is normal, and that its Dedekind generator exists and equals its ordinary generator; that is, Condition (ix) is satisfied. We shall show that

$$\text{(vi)} \qquad \psi(n) \cup \psi(m) = 1 . \qquad n, m \text{ non-comparable.}$$

Hence it will follow from Lemma 7.2 that (ix) is a sufficient condition for ϕ to admit a rank function.

Assume n, m non-comparable. Then if $l = n \cap m$, $n < l$ and $m < l$. Let q_1, q_2, $\cdots$, q_s be the distinct prime factors of l, and let p be any prime p^{a_n}, p^{b_n} the highest powers of p dividing $\phi(n)$ and $\psi(n)$ respectively.

Now by formula (2.2),

$$\phi_l = \psi_l [\phi_{l/q_1} \cap \cdots \cap \phi_{l/q_s}] .$$

Hence $a_l = b_l + a_{l/q}$, where $a_{l/q}$ is the largest of $a_{l/q_1}, \cdots, a_{l/q_s}$. But by (ix), $a_l = \sum_{d \supseteq l} b_d$. Hence $b_d = 0$ unless $d = l$ or $d \supseteq l/q$.

Not both b_n and b_m are positive. For since $n \supset l$ and $m \supset l$, in the contrary case $n \supseteq l/q$ and $m \supseteq l/q$ by the remark above. But then $l = n \cap m \supseteq l/q$ so that $q=1$, contrary to q a prime.

It follows that p does not divide both $\psi(n)$ and $\psi(m)$. Since p was an arbitrarily chosen prime, (v) follows, which completes the proof of Theorem 2.

In closing, note that it follows from Theorem 2 and Lemma 7.2 that if ϕ has the Dedekind generator ζ (that is,

$$\zeta(n) = \Pi\, \phi(n/a)^{\mu(d)}$$

is an integer for every n); then a necessary and sufficient condition that ϕ should admit a rank function is that its Dedekind generator satisfy the condition $\zeta(n) \cup \zeta(m) = 1$ if n, m are non-comparable.

REFERENCES

1. R.D. Carmichael, *On the numerical factors of the arithmetic forms*, Ann. Math. (2), **15** (1913–14), 30–70.
2. R. Dedekind, *Werke*, Vol. 1, Brunswick (1930).
3. L.E. Dickson, *History*, Vol. 1, Washington (1919).
4. M. Hall, *Divisibility sequences of the third order*, Amer. J. Math., **58** (1936), 577–84.
5. D.H. Lehmer, Thesis: *On an extended theory of Lucas functions*, Ann. Math. (2), **31** (1930), 419–48.
6. E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184–240; 289–321.
7. J.J. Sylvester, *On certain ternary cubic form equations*, Amer. J. Math., 2 (1879), 357–83.
8. Morgan Ward and R.P. Dilworth, *Residuated lattices*, Trans. Amer. Math. Soc., **45** (1939), 335–50.
9. Morgan Ward, *Arithmetical properties of sequences in rings*, Ann. Math. (2), **39** (1938), 210–19.
10. ———, *Arithmetical properties of polynomials associated with the lemniscate elliptic functions*, Proc. Nat. Acad. Sci., **36** (1950), 359–62.
11. ———, *Residuated distributive lattices*, Duke Math. J., **6** (1940), 641–51.
12. ———, *Linear divisibility sequences*, Trans. Amer. Math. Soc., **41** (1937), 276–86.
13. ———, *The law of repetition of primes in an elliptic divisibility sequence*, Duke Math. J., **15** (1948), 941–46.
14. ———, *Note on divisibility sequences*, Bull, Amer. Math. Soc., **42** (1936), 843–45.

CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA