Unitary functions (mod r), II.

By ECKFORD COHEN (Knoxville, Tenn.)

1. Introduction. This paper constitutes the second part of an investigation of the class of unitary functions of $n \pmod r$, n and r integers, $r>0$ [3]. The notation, terminology, and definitions of Part I will be assumed in this paper. Reference numbers marked with an asterisk refer to the bibliography of [3].

A basic aspect of I was the development of an arithmetical inversion theory of the class U_r of unitary functions (mod r), corresponding to that [3*] of the class E_r of even functions (mod r). It is noted that $U_r \subseteq E_r$. Another important subclass of E_r is the set P_r of primitive functions (mod r), which satisfy the property $f(n,r)= =f(\gamma(n,r),r)$; here $\gamma(r)$ is the maximal square-free divisor of r and $\gamma(n,r)\equiv\gamma((n,r))$. In [1, § 7] it was shown that the functions $f(n,r)$ of P_r are characterized by repersentations of the form,

$$f(n,r)=\sum_{\substack{d\mid\gamma(r)\\(n,d)=1}} g\left(d,\frac{r}{d}\right). \tag{1.1}$$

A complete inversion theory for such representations of functions of P_r was developed in [3*, § 2]. For a group-theoretical characterization of P_r, see section 7 of the present paper.

In this paper it will be shown that *all* functions of U_r are representable in a form (4. 7) analogous to that of (1. 1). The corresponding inversion theory is carried out in section 4. It is of interest to observe that the statement of the main result (Theorem 4. 1) is quite simple in comparison with the corresponding result in P_r [3*, Theorem 2. 3].

In section 5 the Inversion Theorem is applied to obtain asimple formula for the combinatorial function $\omega_s(n,r)$, defined as follows: Let S denote an arbitrary set of positive integers; then $\omega_s(n,r)$ denotes the set of all $a \pmod r$ such that $(a,r)_*=1$ and $(n-a,r)_*\in S$. In the special case $S\equiv 1$, we have the result,

$$\theta^*(n,r)\equiv\omega_1(n,r)=\sum_{\substack{d\| r\\(n,d)_*=1}} \mu^*(d)\varphi^*\left(\frac{r}{d}\right). \tag{1.2}$$

The function $\theta^*(n,r)$ is the unitary analogue of Nagell's totient function $\theta(n,r)$, and the representation (1. 2) of $\theta^*(n,r)$ is analogous to that deduced for $\theta(n,r)$ in [1, (7. 6)]. The formula obtained for $\omega_S(n,r)$ for an arbitrary set S will be found in Theorem 5. 1. This result is an analogue of a generalization [2, Theorem 13] of the result concerning $\theta(n, r)$ mentioned above (see Remark 5. 1.). The proof of the present paper is, however, quite different and somewhat more direct than that of [2]. The theorem of section 5 is applied in section 6 to two special cases of S, the k-free numbers and the k-th powers.

Sections 2 and 3 are devoted to the trigonometric aspects of the class U needed for the later discussion. In particular, section 3 contains a treatment of the trigonometric inversion theory of U, independent of that deveploed in [3, § 5]. It will be observed that the statement of the Fourier inversion principle in Theorem 3. 1 differs somewhat from that of Part I, the new formulation being more convenient for the present discussion.

For the properties of finite cyclic groups needed in this paper the reader is referred to Rédei [5, § 90].

2. Preparatory lemmas. In this section we prove some properties of the unitary analogues of Euler's totient and of Ramanujan's sum. We need first a lemma concerning semi-reduced residue systems (mod r), (cf. [4*, § 2]); an integer a is called *unitary* (mod r) if $(a, r)_* = 1$, and the set of unitary elements in a residue system (mod r) is said to form a *semi-reduced residue system* (mod r).

Lemma 2. 1. *Let* $d * \delta = r$; *any semi-reduced residue system* (mod r) *can be partitioned into* $\varphi^*(d)$ *semi-reduced residue systems* (mod) δ.

Proof. We use a group-theoretical argument (cf. [3, § 7]). Let C_r denote the additive group of the integers (mod r), or equivalently, any additive cyclic group of order r. A unitary element of C_r is therefore one whose components in the (direct) Sylow summands of C_r are all different from the identity. Evidently, there are $\varphi^*(r)$ unitary elements of C_r. Let C_δ denote the subgroup of order δ of C_r and Γ_d the factor group C_r/C_δ. The elements of Γ_d consist of the cosets $K_a = a + C_\delta$, where a ranges over the elements of C_d, $C_d \oplus C_\delta = C_r$. Under the isomorphism $\Gamma_d \cong C_d$, there are $\varphi^*(d)$ unitary elements of Γ_d, K_a being unitary when a is unitary in C_d. The unitary elements of C_r contained in a unitary coset K_a of Γ_d are precisely the elements, $a+x$, where x ranges over the $\varphi^*(\delta)$ unitary elements of C_δ. This proves the lemma, because a non-unitary coset K_a contains no unitary elements of C_r.

An immediate corollary is

Remark 2. 1. *If* $\delta \| r$, *then any semi-reduced residue system* (mod r) *contains such a system* (mod δ).

The following result is analogous to Hölder's formula for Ramanujan's sum [2 *, (5)].

Lemma 2. 2.

$$c^*(n, r) = \mu^*\left(\frac{r}{t}\right)\varphi^*(t), \quad t = (n, r)_*. \tag{2. 1}$$

Proof. By definition and the fact that $c^*(n, r)$ is unitary (mod r), we have

$$c^*(n, r) = c^*(t, r) = \sum_{(x,r)_* = 1} e(tx, r).$$

Hence application of Lemma 2. 1 yields

$$c^*(n, r) = \sum_{(x,r)_*=1} e\left(x, \frac{r}{t}\right) = \varphi^*(t) \sum_{\left(x, \frac{r}{t}\right)_*=1} e\left(x, \frac{r}{t}\right) = \varphi^*(t) c^*\left(1, \frac{r}{t}\right),$$

and (2. 1) results by [3, (2. 4)].

Lemma 2. 3. *If* $d_1 \| r$, $d_2 \| r$, *then*

$$c^*\left(\frac{r}{d_1}, d_2\right) = \frac{\varphi^*(d_2)}{\varphi^*(d_1)} c^*\left(\frac{r}{d_2}, d_1\right). \tag{2. 2}$$

Proof. By Lemma 2. 1, one obtains, with $d_1\delta_1 = d_2\delta_2 = r$,

$$c^*\left(\frac{r}{d_1}, d_2\right) = \sum_{(x,d_2)_*=1} e\left(\frac{xr}{d_1}, d_2\right) = \frac{1}{\varphi^*(\delta_2)} \sum_{(x,r)_*=1} e\left(\frac{xr}{d_2}, d_1\right)$$

$$= \frac{\varphi^*(\delta_1)}{\varphi^*(\delta_2)} \sum_{(x,d_1)_*=1} e\left(\frac{xr}{d_2}, d_1\right) = \frac{\varphi^*(\delta_1) c^*(\delta_2, d_1)}{\varphi^*(\delta_2)}.$$

The result follows by the multiplicativity and positivity of $\varphi^*(r)$.

The following orthogonality property of $c^*(n, r)$ is needed for the trigonometric inversion theory of § 3.

Lemma 2. 4 (cf. [2 $*$, (6)]). *If* $d_1 \| r$, $d_2 \| r$, *then*

$$\sum_{d \| r} c^*\left(\frac{r}{d}, d_1\right) c^*\left(\frac{r}{d_2}, d\right) = \begin{cases} r & (d_1 = d_2) \\ 0 & (d_1 \neq d_2). \end{cases} \tag{2. 3}$$

Proof. With $d_1\delta_1 = d_2\delta_2 = r$, $m = \delta_1$, $n = \delta_2$, the result contained in [3, (3. 7)] becomes

$$\sum_{d \| r} \frac{c^*(\delta_1, d) c^*(\delta_2, d)}{\varphi^*(d)} = \begin{cases} \dfrac{r}{\varphi^*(d_2)} & \text{if} \quad \delta_1 = \delta_2, \\ 0 & \text{otherwise.} \end{cases}$$

The relation (2. 3) follows on applying Lemma 2. 3 to $c^*(\delta_1, d)$.

3. Trigonometric inversion. The fact that $e(n, r)$ is contained in the class V_r of periodic functions (mod r) was implicitly used in the proofs of Lemmas 2. 2 and 2. 3. It will be remarked that $U_r \subseteqq E_r \subseteqq V_r$. The property $U_r \subseteqq E_r$ was used in developing the inversion theory of [3]; the alternative treatment of this section is based rather upon the property, $U_r \subseteqq V_r$.

Lemma 3. 1 [4 $*$, Lemma 2. 1]. *The integers of the form* dx, $d * \delta = r$, $x (\text{mod } \delta)$, $(x, \delta)_* = 1$, *constitute a complete residue system* (mod r).

Theorem 3. 1. *If* $f(n, r) \in U_r$ *then* $f(n, r)$ *can be represented in the form,*

$$f(n, r) = \sum_{d \| r} \alpha(d, r) c^*(n, d), \tag{3. 1}$$

where for each $d\|r$,

$$\alpha(d,r)=\frac{1}{r}\sum_{\delta\|r} f\left(\frac{r}{\delta},r\right)c^*\left(\frac{r}{d},\delta\right), \tag{3.2}$$

or equivalently,

$$\alpha\left(\frac{r}{(n,r)_*},r\right)=\frac{1}{r}\sum_{d\|r} f\left(\frac{r}{d},r\right)c^*(n,d). \tag{3.3}$$

Conversely, if $\alpha(n,r)$ is a unitary function (mod r), *then $\alpha(n,r)$ has a representation* (3. 3) *where $f(n,r)$ is defined by* (3. 1).

PROOF. Suppose that $f(n,r)\in U_r$; then $f(n,r)$ possesses a representation [1 $*$, § 2]

$$f(n,r)=\sum_{k\,(\mathrm{mod}\,r)} a_r(k)e(nk,r), \tag{3.4}$$

where

$$a_r(n)=\frac{1}{r}\sum_{u\,(\mathrm{mod}\,r)} f(u,r)e(-un,r). \tag{3.5}$$

We apply Lemma 3. 1, observing that in this lemma, x may be assumed semiprime to r, $(x,r)_*=1$, by virtue of Remark 2. 1. It follows then that

$$a_r(n)=\frac{1}{r}\sum_{d*\delta=r}\sum_{(x,\delta)_*=1} f(dx,r)e(-dxn,r)=\frac{1}{r}\sum_{d*\delta=r} f(d,r)\sum_{(x,\delta)_*=1} e(-xn,\delta)$$

and hence

$$a_r(n)=\frac{1}{r}\sum_{\delta\|r} f\left(\frac{r}{\delta},r\right)c^*(n,\delta). \tag{3.6}$$

Therefore, $a_r(n)\in U_r$, so that by a similar argument applied to (3. 4),

$$f(n,r)=\sum_{d\|r}\sum_{(x,d)_*=1} a_r\left(\frac{rx}{d}\right)e\left(\frac{nrx}{d},r\right)$$

$$=\sum_{d\|r} a_r\left(\frac{r}{d}\right)\sum_{(x,d)_*=1} e(nx,d)=\sum_{d\|r} a_r\left(\frac{r}{d}\right)c^*(n,d).$$

With $\alpha(n,r)$ defined by $\alpha(n,r)=a_r(r/(n,r)^*)$, it follows by (3. 6) that $f(n,r)$ has the representation (3. 1) with $\alpha(d,r)$ determined by either (3. 2) or (3. 3).

Conversely, let $\alpha(n,r)$ be a function of U_r and suppose that $f(n,r)$ is defined by (3. 1). It therefore follows, for a fixed unitary divisor D of r, that

$$\sum_{\delta\|r} f\left(\frac{r}{\delta},r\right)c^*\left(\frac{r}{D},\delta\right)=\sum_{d\|r}\alpha(d,r)\sum_{\delta\|r} c^*\left(\frac{r}{\delta},d\right)c^*\left(\frac{r}{D},\delta\right).$$

Application of Lemma 2. 4 yields (3. 2) with d replaced by D, and the theorem is proved.

We make an application of Theorem 3. 1. Let S denote an arbitrary set of positive integers, and let $\varrho_S(n)$ be the characteristic function of S: $\varrho_S(r)=1$ or 0 according as $r\in S$ or $r\notin S$.

Corollary 3. 1. 1.

$$\varrho_S((n, r)_*) = \frac{1}{r} \sum_{d \| r} c_S^* \left(\frac{r}{d}, r\right) c_*(n, d), \tag{3. 7}$$

where

$$c_S^*(n, r) = \sum_{d \| (n,r)_*} d \mu_S^* \left(\frac{r}{d}\right), \qquad \mu_S^*(r) = \sum_{\substack{d * \delta = r \\ \delta \in S}} \mu^*(d). \tag{3. 8}$$

Remark 3. 1. $c_S^*(1, r) = \mu_S^*(r)$.

PROOF. $\varrho_S((n, r)_*)$ is unitary (mod r); it has a representation,

$$\varrho_S((n, r)_*) = \sum_{d \| r} \alpha_S(d, r) c^*(n, d), \tag{3. 9}$$

where by (3. 3) and [3, (2. 4)]

$$r\alpha_S\left(\frac{r}{(n, r)_*}, r\right) = \sum_{d * \delta = r} \varrho_S(\delta) c^*(n, d) = \sum_{d * \delta = r} \varrho_S(\delta) \sum_{D \| (n,d)_*} D \mu^* \left(\frac{d}{D}\right)$$

$$= \sum_{D \| (n,r)_*} D \sum_{\substack{d * \delta = r \\ (d = D * E)}} \varrho_S(\delta) \mu^* \left(\frac{d}{D}\right) = \sum_{D \| (n,r)_*} D \sum_{\substack{E * \delta = r/D \\ \delta \in S}} \mu^*(E) = c_S^*(n, r).$$

Hence $\alpha_S(d, r) = c_S^*(r/d, r)/r$ for each unitary divisor d of r, and (3. 7) results from (3. 9).

In case S consists of 1 alone, $c_S^*(n, r)$ and $\mu_S^*(r)$ reduce to $c^*(n, r)$ and $\mu^*(r)$, respectively. In this case, (3. 7) yields a new proof of [3, (6. 4)]. Place $\varepsilon(r) = \varrho_1(r)$.

Corollary 3. 1. 2 ($S \equiv 1$).

$$\varepsilon((n, r)_*) = \frac{\varphi^*(r)}{r} \sum_{d \| r} \left(\frac{\mu^*(d)}{\varphi^*(d)}\right) c^*(n, d). \tag{3. 10}$$

PROOF. Apply Lemma 2. 2 to (3. 7) with $S \equiv 1$.

4. Arithmetical inversion of primitive type. We need some lemmas. We recall [3, (2. 3)] that

$$\sum_{d \| r} \mu^*(d) = \varepsilon(r) \equiv \begin{cases} 1 & (r = 1) \\ 0 & (r \neq 1). \end{cases} \tag{4. 1}$$

Remark 4. 1. *If* $d_1 \| r$, $d_2 \| r$, *then* $(d_1, d_2)_* = (d_1, d_2)$. (Vacuous sums will be assumed zero in the following.)

Lemma 4. 1. *If* $r = r_1 * r_2$ *and* $D \| r$, *then*

$$\sum_{\substack{\delta * e = D \\ (\delta, r_1) = 1}} \mu^*(e) = \begin{cases} \mu^*(D) & \text{if} \quad D \| r_1, \\ 0 & \text{if} \quad D \nparallel r_1. \end{cases} \tag{4. 2}$$

PROOF. By (4. 1)

$$\sum_{\substack{\delta * e=D \\ (\delta, r_1)=1}} \mu^*(e)=\sum_{\delta * e=D} \mu^*(e)\varepsilon((\delta, r_1))=\sum_{\delta * e=D} \mu^*(e) \sum_{d \| (\delta, r_1)} \mu^*(d) \tag{4. 3}$$

$$=\sum_{\substack{d \| r_1 \\ d \| D}} \mu^*(d) \sum_{\substack{\delta * e=D \\ \delta=d * \delta'}} \mu^*(e)=\sum_{e \|(r_1, D)} \mu^*(d) \sum_{\delta' * e=\frac{D}{d}} \mu^*(e),$$

and (4. 3) follows on a second application of (4. 1).

Next we note the case $n=0$ of [3, (2. 3)]:

$$\sum_{d \| r} \varphi^*(d)=r. \tag{4. 4}$$

Lemma 4. 2. *If $r=r_1 * r_2$, $D \| r$, then*

$$\sum_{\delta \| r_2} \varphi^*(d) c^*\left(\frac{r_2}{d}, D\right)=\begin{cases} r_2 \mu^*(D) & \text{if} \quad D \| r, \\ 0 & \text{otherwise.}\end{cases} \tag{4. 5}$$

PROOF. Denote the left of (4. 5) by Σ. Applying [3, (2. 4)] and rearranging, one obtains by (4. 4),

$$\sum=\sum_{\substack{\delta * e=D \\ \delta \| r_2}} \delta \mu^*(e) \sum_{d \| \frac{r_2}{\delta}} \varphi^*(d)=r_2 \sum_{\substack{\delta * e=D \\ \delta \| r_2}} \mu^*(e)=r_2 \sum_{\substack{\delta * e=D \\ (d, r_1)=1}} \mu^*(e),$$

and the lemma results by (4. 2).

The following lemma is crucial in passing from the trigonometric representations of functions of U_r to the arithmetical representations of the type under consideration.

Lemma 4. 3. *For all r,*

$$c^*(n, r)=\sum_{\substack{d \| r \\ (n, d)_*=1}} d \mu^*(d) \varphi^*\left(\frac{r}{d}\right). \tag{4. 6}$$

Remark 4. 2. *By* [3, (2. 5)], $(\mu^*(r))^2=1$ *for all r.*

PROOF. We apply the unitary analogue [3, Lemma 2. 1] of the Möbius inversion formula to (3. 10) to obtain

$$\frac{c^*(n, r) \mu^*(r)}{\varphi^*(r)}=\sum_{d \| r} \frac{d}{\varphi^*(d)} \varepsilon((n, d)_*) \mu^*\left(\frac{r}{d}\right).$$

The lemma follows by Remark 4. 2 and the multiplicative properties of $\varphi^*(r)$ and $\mu^*(r)$.

Remark 4. 3. The property (4. 6) of $c^*(n, r)$ contrasts sharply with the corresponding property [1, (7. 2)] of Ramanujan's sum $c(n, r)$, the latter being valid only for *square-free* values of r. It is the universality of the relation (4. 6) which leads to the following arithmetical inversion theorem for the functions of U_r.

Theorem 4. 1. *Every function $f(n, r)$ of U_r has a representation,*

$$f(n, r) = \sum_{\substack{d \| r \\ (n,d)_* = 1}} h\left(d, \frac{r}{d}\right). \tag{4.7}$$

where $h(r_1, r_2)$ is determined by

$$h(r_1, r_2) = \mu^*(r_1) \sum_{d \| r_1} f\left(\frac{r}{d}, r\right) \mu^*(d), \qquad r = r_1 * r_2. \tag{4.8}$$

Conversely, if $h(r_1, r_2)$ is an arbitrary function defined for relatively prime arguments r_1, r_2, then $h(r_1, r_2)$ has a representation (4. 8), *where $f(n, r)$ is a function of U_r defiined by* (4. 7).

PROOF. Let $f(n, r)$ be a function of U_r. Then $f(n, r)$ has a representation determined by (3. 1) and (3. 2). Applyimg Lemma 4. 3 to (3. 1) one obtains

$$f(n, r) = \sum_{d \| r} \alpha(d, r) \sum_{\substack{e \| d \\ (n,e)_* = 1 \\ (d = \delta * e)}} e\mu^*(e) \varphi^*\left(\frac{d}{e}\right) = \sum_{\substack{e \| r \\ (n,e)_* = 1}} e\mu^*(e) \sum_{\delta \| \frac{r}{e}} \alpha(\delta e, r) \varphi^*(\delta).$$

Thus $f(n, r)$ has a representation (4. 7) with

$$h(r_1, r_2) = r_1 \mu^*(r_1) \sum_{d \| r_2} \alpha(dr_1, r) \varphi^*(d), \; r = r_1 * r_2.$$

Substituting from (3. 2), it follows then that

$$h(r_1, r_2) = \frac{\mu^*(r_1)}{r_2} \sum_{\delta \| r} f\left(\frac{r}{\delta}, r\right) \sum_{d \| r_2} \varphi^*(d) c^*\left(\frac{r_2}{d}, \delta\right), \; r = r_1 * r_2.$$

Application of Lemma 4. 2 yields (4. 8) and the first half of the theorem is proved.

Let $h(r_1, r_2)$ be a function ot two positive, integral variables r_1, r_2 such that $(r_1, r_2) = 1$. Let $f(n, r)$ be a function of U_r defined by (4. 7). Denoting the right member of (4. 8) by T, we have for $r = r_1 * r_2$, by Remarks 4. 1 and 4. 2,

$$\mu^*(r_1) T = \sum_{d \| r_1} \mu^*(d) \sum_{\substack{D \| r \\ \left(\frac{r}{d}, D\right)_* = 1}} h\left(D, \frac{r}{D}\right) = \sum_{D \| r} h\left(D, \frac{r}{D}\right) \sum_{\substack{d \| r_1 \\ \left(\frac{r}{d}, D\right)_* = 1}} \mu^*(d).$$

The summation conditions imply that $(D, r_2) = 1$ so that

$$\mu^*(r_1) T = \sum_{D \| r_1} h\left(D, \frac{r}{D}\right) \sum_{\substack{d \| r_1 \\ \left(\frac{r_1}{d}, D\right) = 1}} \mu^*(d).$$

Lemma 4. 1 is applicable to the inner sum with D and r_1 interchanged; in particular, since $D \| r_1$, the sum vanishes unless $D = r_1$, in which case it has the value $\mu^*(r_1)$. That is, $\mu^*(r_1) T = \mu^*(r_1) h(r_1, r_2)$, and $T = h(r_1, r_2)$, completing the proof of the theorem.

5. A combinatorial problem. In this section, we evaluate the function $\omega_S(n, r)$ defined in the Introduction. First we prove two lemmas.

Lemma 5. 1. *If $r_1 * r_2 = r$ and S is an arbitrary set of integers, then*

$$\sum_{d*\delta=r_1} \mu^*(d) c_S(\delta, r) = r_1 \mu_S^*(r_2). \tag{5. 1}$$

PROOF. This result follows immediately on applying the inversion theorem of [3, § 4] to the function $c_S^*(n, r)$ as defined by (3. 8).

Lemma 5. 2. *If k and r_1 are unitary divisors of r, $r = r_1 * r_2$, then*

$$\sum_{d \| r_1} \mu^*(d) c^*\left(\frac{r}{d}, k\right) = \begin{cases} r_1 \varphi^*\left(\frac{k}{r_1}\right) & \text{if } r_1 \| k, \\ 0 & \text{if } r_1 \nparallel k. \end{cases} \tag{5. 2}$$

PROOF. Let the left of (5. 2) be denoted Σ. Using the representation (4. 6) of $c^*(n, r)$, one obtains by Remark 4. 1,

$$\Sigma = \sum_{d \| r_1} \mu^*(d) \sum_{\substack{D \| k \\ \left(\frac{r}{d}, D\right) = 1}} D\mu^*(D) \varphi^*\left(\frac{k}{D}\right) = \sum_{D \| k} D\mu^*(D)\varphi^*\left(\frac{k}{D}\right) \sum_{\substack{d \| r_1 \\ \left(\frac{r}{d}, D\right) = 1}} \mu^*(d)$$

and hence

$$\Sigma = \sum_{\substack{D \| k \\ (D, r_2) = 1}} D\mu^*(D)\varphi^*\left(\frac{k}{D}\right) \sum_{\substack{d \| r_1 \\ \left(\frac{r_1}{d}, D\right) = 1}} \mu^*(d).$$

Lemma 4. 1 is applicable to the inner sum, with the roles of r_1 and D interchanged; thus

$$\Sigma = \mu^*(r_1) \sum_{\substack{D \| k \\ (D, r_2) = 1 \\ r_1 \| D}} D\mu^*(D)\varphi^*\left(\frac{k}{D}\right), \tag{5. 3}$$

so that $\Sigma = 0$ if $r_1 \nparallel k$. If $r_1 \| k$, place $k = r_1 * R_2$, $R_2 \| r_2$; it is then evident that the summation variable D in (5. 3) must be restricted to the single value r_1. Hence, by Remark 4. 2, $\Sigma = r_1 \varphi^*(k/r_1)$ if $r_1 \| k$. The proof is complete.

The function $\omega_S(n, r)$ can be defined as the number of $x, y \pmod r$ such that

$$n \equiv x + y \pmod r, \ (x, r)_* = 1, \ (y, r)_* \in S. \tag{5. 4}$$

This additive formulation is useful in the proof of the main result which follows.

Theorem 5. 1. *For an arbitrary set S of positive integers, the function $\omega_s(n, r)$ is unitary* (mod r) *and has the following unique representation of the form* (4. 7):

$$\omega_S(n, r) = \sum_{\substack{d \| r \\ (n, d)_* = 1}} \mu_S^*(d) \varphi^*\left(\frac{r}{d}\right). \tag{5. 5}$$

PROOF. By (5. 4), the function $\omega_S(n, r)$ can be expressed in the form,

$$\omega_S(n, r) = \sum_{n \equiv a+b (\mathrm{mod}\, r)} \varepsilon((a, r)_*)\, \varrho_S((b, r)_*),$$

using the notation of I and the functions defined in § 3. By (3. 7) and (3. 10), we obtain then

$$\omega_S(n, r) = \frac{\varphi^*(r)}{r^2} \sum_{\substack{d_1 \| r \\ d_2 \| r}} \left(\frac{\mu^*(d_1)}{\varphi^*(d_1)}\right) c_S^*\left(\frac{r}{d_2}, r\right) \sum_{n \equiv a+b (\mathrm{mod}\, r)} c^*(a, d_1) c^*(b, d_2).$$

Application of the orthogonality property [3, (3. 6)] of $c^*(n, r)$ yields then

$$\omega_S(n, r) = \frac{\varphi^*(r)}{r} \sum_{d \| r} \left(\frac{\mu^*(d)}{\varphi^*(d)}\right) c_S^*\left(\frac{r}{d}, r\right) c^*(n, d). \tag{5. 6}$$

This representation makes it evident that $\omega_S(n, r) \in U_r$; moreover, (5. 6) furnishes the Fourier expansion of (3. 1) of $\omega_S(n, r)$.

By the inversion theorem of § 4, $\omega_S(n, r)$ has an arithmetical representation,

$$\omega_S(n, r) = \sum_{\substack{d \| r \\ (n, d)_* = 1}} h_S\left(d, \frac{r}{d}\right), \tag{5. 7}$$

where

$$h_S(r_1, r_2) = \mu^*(r_1) \sum_{D \| r_1} \omega_S\left(\frac{r}{D}, r\right) \mu^*(D), \quad r = r_1 * r_2. \tag{5. 8}$$

Substitution from (5. 6) in (5. 8) leads to

$$h_S(r_1, r_2) = \frac{\varphi^*(r) \mu^*(r_1)}{r} \sum_{d \| r} \left(\frac{\mu^*(d)}{\varphi^*(d)}\right) c_S^*\left(\frac{r}{d}, r\right) \sum_{D \| r_1} \mu^*(D) c^*\left(\frac{r}{D}, d\right).$$

By Lemma 5. 2, the inner sum $=0$ unless $r_1 \| d$, when it has the value $r_1 \varphi^*(d/r_1)$. Hence by the multiplicative properties of $\varphi^*(r)$,

$$h_S(r_1, r_2) = \frac{\varphi^*(r_2) \mu^*(r_1)}{r_2} \sum_{\substack{d \| r \\ (d = r_1 * \delta)}} \mu^*(d) c_S^*\left(\frac{r}{d}, r\right),$$

and by similar properties of $\mu^*(r)$,

$$h_S(r_1, r_2) = \frac{\varphi^*(r_2)}{r_2} \sum_{\delta \| r_2} \mu^*(\delta) c_S^*\left(\frac{r_2}{\delta}, r\right).$$

On the basis of Lemma 5. 1 (with r_1 and r_2 interchanged), the inner sum has the value $r_2 \mu_S^*(r_1)$, and hence

$$h_S(r_1, r_2) = \varphi^*(r_2) \mu_S^*(r_1), \quad r = r_1 * r_2. \tag{5. 9}$$

The formula (5. 5) is a consequence of (5. 7) and (5. 9). The uniqueness of the representation (5. 9) of $h_S(r_1, r_2)$ results from converse part of the Inversion Theorem.

Remark 5. 1. The function $\omega_S(n, r)$ is the unitary analogue of the function $\theta_S(n, r)$, defined to be the number of solutions of the congruence in (5. 4) with the side conditions, $(x, r)=1$, $(y, r)\in S$. This function was evaluated in [2, Theorem 13] with a result analogous to (5. 5). The following contrasts are to be noted. While the inversion theorem of § 3 for functions of U_r was applied to obtain (5. 5), the corresponding theorem in P_r does not in general lead to the evaluation of $\theta_S(n, r)$ obtained in [2]. In fact, the latter result is not even in the required form (1. 1). It should, however, be observed that for exceptional sets S, $\theta_S(n, r)$ admits of an analysis similar to that used in this section with respect to $\omega_S(n, r)$; in particular, we mention the treatment of Nagell's totient ($S\equiv 1$) in [4].

6. A combinatorial problem: special cases. In this section we specialize Theorem 5. 1 to special sets S, in particular, to the set L_k of k-th powers and the set Q_k of k-free integers (k a non-negative integer). In case $S=Q_k$, $\omega_S(n, r)$ and $\mu_S(r)$ will be denoted $Q_k(n, r)$ and $\mu_k^*(r)$, respectively. In case $S=L_k$, these functions will be denoted $L_k(n, r)$ and $\lambda_k^*(r)$, respectively. From (3. 8) it follows that

$$\mu_k^*(r)=\sum_{\substack{d*\delta=r\\ \delta\ k\text{-free}}}\mu^*(d),\quad \lambda_k^*(r)=\sum_{d*\delta^k=r}\mu^*(d). \tag{6. 1}$$

It is easily observed (cf. [3, Lemma 2. 2]) that $\mu_k^*(r)$ and $\lambda_k^*(r)$ are multiplicative. Hence it suffices to know their values when $r=p^m$, p prime, $m>0$. In particular, by (6. 1), $\mu_k^*(1)=\lambda_k^*(1)=1$,

$$\mu_k^*(p^m)=\begin{cases}-1 & (m\geqq k)\\ 0 & (m<k)\end{cases}\qquad (k\geqq 1), \tag{6. 2}$$

$$\lambda_k^*(p^m)=\begin{cases}-1 & (k\nmid m)\\ 0 & (k\mid m)\end{cases}\qquad (k\geqq 1). \tag{6. 3}$$

Note from (6. 1) that $\mu_1^*(r)=\lambda_0^*(r)=\mu^*(r)$. Also it will be observed that $L_0=Q_1\equiv 1$, $L_1=Q_0=Z$, the set of positive integers.

From Theorem 5. 1, we have

$$Q_k(n, r)=\sum_{\substack{d\mid r\\ (n,d)_*=1}}\mu_k^*(d)\varphi^*\left(\frac{r}{d}\right), \tag{6. 4}$$

$$L_k(n, r)=\sum_{\substack{d\mid r\\ (n,d)_*=1}}\lambda_k^*(d)\varphi^*\left(\frac{r}{d}\right). \tag{6. 5}$$

These results will now be applied to determine solvability criteria for (5. 4) in the cases $S=Q_k$, $S=L_k$.

Theorem 6. 1(a). *If $k\geqq 1$, then $Q_k(n, r)=0$ if and only if r is twice an odd integer, n is odd, and $k=1$.*

(b) *If $k\geqq 1$, then $L_k(n, r)=0$ if and only if r is twice an odd integer, n is odd, and $k>1$.*

PROOF. In view of the multiplicativity of $\mu_k^*(r)$, $\lambda_k^*(r)$, and $\varphi_k^*(r)$, it follows from (6. 4) and (6. 5) that $Q_k(n, r)$ and $L_k(n, r)$ are also multiplicative in r. We therefore have only to consider the cases arising when $r=p^m$, $n=p^l$, $m>0$, $l=0$ or m, p prime.

It is easily verfied that if $k\geqq 1$,

$$Q_k(p^l, p^m)=\begin{cases} p^m-2 & \text{if } \ l<m,\ k\leqq m. \\ p^m-1 & \text{otherwise.} \end{cases}$$

Hence $Q_k(p^l, p^m)=0 \rightleftarrows p=2$, $m=1$, $l=0$, $k=1$. This suffices to prove Part (a). Similarly, for $k\geqq 1$,

$$L_k(p^l, p^m)=\begin{cases} p^m-2 & \text{if } \ l<m,\ k\nmid m, \\ p^m-1 & \text{otherwise.} \end{cases}$$

and therefore $L_k(p^l, p^m)=0 \rightleftarrows p=2$, $m=1$, $l=0$, $k>1$. This proves part (b) and the proof is complete.

Theorem 6. 1 is the unitary analogue of a result relating to $\theta_S(n, r)$ which was proved in [2, Theorem 14]. These criteria can also be proved in a direct manner.

7. Group-theoretical remarks. In [3, § 7] it was pointed out that the class E_r could be described equivalently, in terms of group theory, as the set of those functions defined on the (additive) cyclic group C_r of order r, which are invariant under all automorphisms of C_r. An analogous interpretation of U_r was also given in [3].

To obtain a group-theoretical interpretation of P_r, we note first that the maximal subgroups of C_r are the subgroups of order r/p, where p ranges over the distinct prime divisors of r. The intersection of these subgroups is the subgroup $\Gamma_r=C_{r/\gamma(r)}$ of order $r/\gamma(r)$ contained in C_r, namely the Frattini subgroup of $C_r(\Gamma_1=C_1)$. We define now a function $f(\alpha)$ with definition domain C_r to be *primitive* if it is *invariant under the set T_r of all permutations of C_r which induce automorphisms in the factor group H_r of the group C_r modulo its Frattini subgroup Γ_r*.

We note that H_r is cyclic of order $\gamma(r)$. Moreover, if α_1 and α_2 are two elements of C_r of index n_1 and $_2$, respectively, such that $\alpha_1\equiv\alpha_2 \pmod{\Gamma_r}$, then $\gamma(n_1)=\gamma(n_2)$. Thus, to each coset K_i of H_r there is attached a number, $m_i=m(K_i)$, representing the maximal square-free divisor of the index of any element of K_i; m_i is the index of K_i in H_r. Two cosets K_1, K_2 are mapped onto each other by some automorphism of H_r if and only if $m_1=m_2$. It follows that *the concept of primitive function on C_r is merely a reformulation of the notion of of primitive function* (mod r).

It is evident that T_r forms a subgroup of the group of all permutations of C_r. Moreover, if A_r denotes the group of automorphisms of C_r, then $A_r\subseteqq T_r$, in view of the fact that Γ_r, like all other subgroups, is a characteristic subgroup of C_r.

Bibliography

[1] Eckford Cohen, Representations of even functions (mod r), I. Aritmetical identities, *Duke Math. J.* **25** (1958), 401 – 421.

[2] Eckford Cohen, A class of residue systems (mod r) and related arithmetical functions, I. A generalization of Mobius inversion, *Pacific J. of Math.* **9** (1959), 13 – 23.

[3] Eckford Cohen, Unitary functions (mod r), I, *Duke Math. J.*, **28** (1961), 475 – 486.

[4] Eckford Cohen, Nagell's totient function, *Math. Scandinavica,* **8** (1960), 55 – 58.

[5] Ladislaus Rédei, Algebra, *Leipzig*, 1959.

(Received December 16, 1961.)