THE MULTIPLICATIVE SEMIGROUP OF INTEGERS MODULO m

EDWIN HEWITT AND H. S. ZUCKERMAN

1. Introduction. Throughout this paper, m denotes a fixed integer >1. The set of all residue classes modulo m is denoted by S_m. For an integer x, $[x]$ denotes the residue class containing x. Under the usual multiplication $[x]\cdot[y] = [xy]$, S_m is a semigroup. The subgroup of S_m consisting of all residue classes $[x]$ such that $(x, m) = 1$ is denoted by G_m.

We write $m = \prod_{j=1}^{r} p_j^{\alpha_j}$, where the p_j are distinct primes and the α_j are positive integers. Following the usual conventions, we take void products to be 1 and void sums to be 0.

In 2.6–2.11 of [2], the structure of finite commutative semigroups is discussed. In § 2, we work out this structure for S_m. In § 3, we give a construction based on [2], 3.2 and 3.3, for all of the semicharacters of S_m. In § 4, we prove that if χ is a semicharacter of S_m assuming a value different from 0 and 1, then $\sum_{[x]\in S_m} \chi([x]) = 0$. In § 5, we compute $\chi([x])$ explicitly in terms of the integer x, for an arbitrary semicharacter χ of S_m. In § 6, we discuss the structure of the semigroup of all semicharacters of S_m.

Our interest in S_m arose from seeing the interesting paper [4] of Parízek and Schwarz. Some of their results appear in somewhat different form in § 2. Other writers ([1], [5], [6], [7]) have also dealt with S_m from various points of view. In particular, a number of the results of § 2 appear in [6] and in more detail in [7]. We have also benefitted from conversations with R. S. Pierce.

2. The structure of S_m. Let G be any finite commutative semigroup, and let a denote an idempotent of G. The sets $T_a = \{x : x \in G, x^m = a$ for some positive integer $m\}$ are pairwise disjoint subsemigroups of G whose union is G. The set $U_a = \{x : x \in T_a, x^l = x$ for some positive integer $l\}$ is a subgroup of G and is the largest subgroup of G that contains a. For a complete discussion, see [2], 2.6-2.11. In the present section, we identify the idempotents a of S_m and the sets T_a and U_a. We first prove a lemma.

2.1 LEMMA. *Let x be any non-zero integer, written in the form*

$$\prod_{j=1}^{r} p_j^{\beta_j}\cdot a, \qquad \beta_j \geqq 0\ , (a, m) = 1\ .$$

Received January 9, 1960. The authors gratefully acknowledge financial support from the National Science Foundation, under Grant NSF—G 5439.

Then there is an integer c prime to m such that

$$x \equiv \prod_{j=1}^{r} p_j^{\lambda_j} \cdot c \pmod{m},$$

where $\lambda_j = \min(\alpha_j, \beta_j)$ $(j = 1, \cdots, r)$. *If*

$$x \equiv \prod_{j=1}^{r} p_j^{\mu_j} \cdot d \pmod{m},$$

where $0 \leqq \mu_j \leqq \alpha_j$ $(j=1, \cdots, r)$ *and* $(d, m) = 1$, *then* $\mu_j = \lambda_j$ $(j=1, \cdots, r)$. *However, it may happen that* $d \not\equiv c \pmod{m}$.

Proof. Let $b = \prod_{\substack{j \\ \alpha_j = \beta_j}} p_j$. Then we have

$$\begin{aligned} x + bm &= p_1^{\beta_1} \cdots p_r^{\beta_r} a + p_1^{\alpha_1} \cdots p_r^{\alpha_r} b \\ &= \prod_{j=1}^{r} p_j^{\min(\alpha_j, \beta_j)} \cdot (Aa + B), \end{aligned}$$

where

$$A = \prod_{j=1}^{r} p_j^{\max(0, (\beta_j - \alpha_j))}$$

and

$$B = \prod_{j=1}^{r} p_j^{\max(0, (\alpha_j - \beta_j))} \cdot b .$$

Then it is easy to see that $(Aa + B, m) = 1$, so that

$$x \equiv \prod_{j=1}^{r} p_j^{\min(\alpha_j, \beta_j)} \cdot c \pmod{m},$$

where $c = Aa + B$ is prime to m. The last two statements of the lemma are also easily checked.

2.2 THEOREM. *Consider the* 2^r *sequences* $\{\delta_1, \cdots, \delta_r\}$, *where* $\delta_j = 0$ *or* α_j $(j = 1, \cdots, r)$. *Corresponding to each such sequence, there is exactly one idempotent of the semigroup* S_m, *and different sequences give different idempotents. The idempotent corresponding to* $\{\delta_1, \cdots, \delta_r\}$ *can be written as*

$$\left[\prod_{j=1}^{r} p_j^{\delta_j} \cdot d\right],$$

where d is any solution of the congruence

$$\prod_{j=1}^{r} p_j^{\delta_j} \cdot d \equiv 1 \left(\bmod \prod_{j=1}^{r} p_j^{\alpha_j - \delta_j}\right).$$

Proof. An element $[x]$ of S_m is idempotent if and only if $x^2 \equiv x \pmod{m}$. If x is written as in 2.1, this congruence becomes $\prod_{j=1}^r p_j^{2\lambda_j} \cdot c^2 \equiv \prod_{j=1}^r p_j^{\lambda_j} c \pmod{m}$, which is equivalent to

$$(1) \qquad \prod_{j=1}^r p_j^{\lambda_j} \cdot c \equiv 1 \left(\operatorname{mod} \prod_{j=1}^r p_j^{\alpha_j - \lambda_j}\right) .$$

The congruence (1) has a solution c if and only if $\prod_{j=1}^r p_j^{\lambda_j}$ is relatively prime to $\prod_{j=1}^r p_j^{\alpha_j - \lambda_j}$, that is, if and only if $\lambda_j = 0$ or α_j $(j = 1, \cdots, r)$. If c_0 is a solution of (1), then all solutions of (1) are given by

$$c = c_0 + y \prod_{j=1}^r p_j^{\alpha_j - \lambda_j} ,$$

where y is an integer. Plainly

$$\left[\prod_{j=1}^r p_j^{\lambda_j} c\right] = \left[\prod_{j=1}^r p_j^{\lambda_j} c_0\right]$$

for all such c.

We have thus proved the existence of a unique idempotent

$$\left[\prod_{j=1}^r p_j^{\delta_j} \cdot d\right]$$

corresponding to a sequence $\{\delta_1, \cdots, \delta_r\}$, where $\delta_j = 0$ or α_j $(j = 1, \cdots, r)$. If $\{\delta_1, \cdots, \delta_r\}$ and $\{\delta_1', \cdots, \delta_r'\}$ are distinct such sequences, the corresponding idempotents are distinct by 2.1.

2.21 COROLLARY. *Let*

$$\left[\prod_{j=1}^r p_j^{\delta_j} \cdot d\right]$$

and

$$\left[\prod_{j=1}^r p_j^{\delta_j'} \cdot d'\right]$$

be idempotents in S_m, *written as in* 2.2. *Then their product is the idempotent*

$$\left[\prod_{j=1}^r p_j^{\max(\delta_j, \delta_j')} \cdot d''\right] ,$$

as in Theorem 2.2.

This follows directly from 2.1 and the obvious fact that products of idempotents are idempotent.

We next determine the sets T_a and U_a defined above.

2.3 THEOREM. *Let*

$$[x] = \left[\prod_{j=1}^{r} p_j^{\lambda_j} c\right]$$

be any element of S_m, *where* $0 \leqq \lambda_j \leqq \alpha_j$ $(j = 1, \cdots, r)$ *and* $(c, m) = 1$. *Then* $[x] \in T_a$, *where the idempotent*

$$a = \left[\prod_{\substack{1 \leqq j \leqq r \\ \lambda_j > 0}} p_j^{\alpha_j} \cdot d\right],$$

and d *is as in* 2.2.

Proof. The idempotent a such that $[x] \in T_a$ has the property that $[x]^{nk} = a$ for some positive integer k and all integers $n \geqq$ some fixed positive integer n_0 (see [2], 2.6.2). For $n = n_0 \cdot \max(\alpha_1, \cdots, \alpha_r)$, 2.1 implies that

$$a = [x]^{nk} = [x^{nk}] = \left[\prod_{j=1}^{r} p_j^{nk\lambda_j} \cdot c^{nk}\right] = \left[\prod_{j=1}^{r} p_j^{\min(nk\lambda_j, \alpha_j)} \cdot d'\right] = \left[\prod_{j=1}^{r} p_j^{\delta_j} \cdot d\right],$$

where $\delta_j = 0$ if $\lambda_j = 0$ and $\delta_j = \alpha_j$ if $\lambda_j > 0$, and d' and d are relatively prime to m.

2.4 THEOREM. *Let*

$$a = \left[\prod_{j=1}^{r} p_j^{\delta_j} \cdot d\right]$$

be any idempotent of S_m, *written as in* 2.2. *The group* U_a *consists of all elements of* S_m *of the form*

$$\left[\prod_{j=1}^{r} p_j^{\delta_j} \cdot c\right]$$

where $(c, m) = 1$.

Proof. Let $[x] \in U_a$. Then for some integers $l > 1$ and $k \geqq 1$ and all integers $n \geqq n_0$, we have $[x]^l = [x]$ and $[x]^{nk} = a$. This implies that $[x] = [x]^{nk+l}$. Writing x as in 2.1 and using 2.1, we now have

$$\prod_{j=1}^{r} p_j^{\lambda_j} \cdot c \equiv \prod_{j=1}^{r} p_j^{\lambda_j(nk+l)} c^{nk+l} \equiv \prod_{\substack{1 \leqq j \leqq r \\ \lambda_j > 0}} p_j^{\alpha_j} \cdot h \pmod{m},$$

provided that n is sufficiently large; here $(h, m) = 1$. From 2.1 we infer that $\lambda_j = 0$ or α_j $(j = 1, \cdots, r)$. Since $[x] \in U_a \subset T_a$, 2.3 now implies that $\lambda_j = \delta_j$ $(j = 1, \cdots, r)$.

Now let $x = \prod_{j=1}^{r} p_j^{\delta_j} \cdot c$, where $(c, m) = 1$. Then 2.3 shows that $[x] \in T_a$. To prove that $[x] \in U_a$, we need to find an integer $l > 1$ such that $[x]^l = [x]$. This is equivalent to finding an l such that

$$\left(\prod_{j=1}^{r} p_j^{\delta_j}\cdot c\right)^l \equiv \prod_{j=1}^{r} p_j^{\delta_j}\cdot c \pmod{m} ,$$

and this congruence is equivalent to the congruence

$$\left(\prod_{j=1}^{r} p_j^{\delta_j}\cdot c\right)^{l-1} \equiv 1 \left(\bmod \prod_{j=1}^{r} p_j^{\alpha_j-\delta_j}\right) .$$

Since

$$\prod_{j=1}^{r} p_j^{\delta_j}\cdot c$$

is relatively prime to the modulus, such an l exists.

We now identify the groups U_a.

2.5 THEOREM. *Let*

$$a = \left[\prod_{j=1}^{r} p_j^{\delta_j}\cdot d\right]$$

be any idempotent of S_m, *written as in* 2.2. *Let*

$$A = \prod_{j=1}^{r} p_j^{\alpha_j-\delta_j} .$$

The group U_a *is isomorphic to the group* G_A.

Proof. For every integer x, let $[x]'$ be the residue class modulo A to which x belongs. For $[x]\in S_m$, let $\tau([x]) = [x]'$. Plainly τ is single-valued and is a homomorphism of S_m onto S_A. We need only show that τ is one-to-one on U_a. If $(c, m) = (c^*, m) = 1$ and

$$\tau\left(\left[\prod_{j=1}^{r} p_j^{\delta_j}\cdot c\right]\right) = \tau\left(\left[\prod_{j=1}^{r} p_j^{\delta_j}\cdot c^*\right]\right) ,$$

then

$$\prod_{j=1}^{r} p_j^{\delta_j}\cdot c \equiv \prod_{j=1}^{r} p_j^{\delta_j}\cdot c^* \pmod{A} ,$$

which implies that $c \equiv c^* \pmod{A}$, because $\left(\prod_{j=1}^{r} p_j^{\delta_j}, A\right) = 1$. Since $\prod_{j=1}^{r} p_j^{\delta_j}\cdot A = m$, we can multiply the last congruence by $\prod_{j=1}^{r} p_j^{\delta_j}$ to obtain

$$\prod_{j=1}^{r} p_j^{\delta_j}\cdot c \equiv \prod_{j=1}^{r} p_j^{\delta_j}\cdot c^* \pmod{m} .$$

3. **A construction of the semicharacters of** S_m. A semicharacter of S_m is a complex-valued multiplicative function defined on S_m that is not identically zero. The set X_m of all semicharacters of S_m forms a semigroup under pointwise multiplication, since [1] is the unit of S_m

and $\chi([1]) = 1$ for all $\chi \in X_m$. In this section, we apply the construction of [2], 3.2 and 3.3, to obtain the semicharacters of S_m. In § 5, we will give a second construction of the semicharacters of S_m, more explicit than the present one, and independent of [2]. This construction will enable us to identify X_m as a semigroup (§ 6).

Theorems 3.2 and 3.3 of [2] give a description of all semicharacters of S_m in terms of the groups U_a. Let χ_a be any character of the group U_a. We extend χ_a to a function on all of S_m in the following way:

$$(1)\quad \chi([x]) = \begin{cases} 0 \text{ if } ab \neq a \text{ for the idempotent } b \text{ such that } [x] \in T_b; \\ \chi_a([x]a) \text{ if } ab = a \text{ for the idempotent } b \text{ such that } [x] \in T_b. \end{cases}$$

The set of all such functions χ is the set X_m.

3.1 THEOREM. *The semigroup X_m has exactly*

$$\prod_{j=1}^{r} (1 + p_j^{\alpha_j} - p_j^{\alpha_j - 1})$$

elements.

Proof. For each idempotent $a = [p_1^{\delta_1} \cdots p_r^{\delta_r} c]$ as in 2.2, (1) yields as many distinct semicharacters of S_m as there are characters of the group U_a. The group U_a has just as many characters as elements. By 2.5, U_a consists of

$$\varphi\left(\prod_{j=1}^{r} p_j^{\alpha_j - \delta_j}\right) = \prod_{\substack{1 \leq j \leq r \\ \delta_j = 0}} \{p_j^{\alpha_j - 1}(p_j - 1)\}$$

elements. Also, distinct idempotents a and b of S_m yield distinct semicharacters of S_m under the definition (1). Therefore the number of elements in X_m is

$$(2)\qquad \sum_{\delta} \varphi\left(\prod_{j=1}^{r} p_j^{\alpha_j - \delta_j}\right) = \sum_{\delta} \varphi\left(\prod_{\substack{1 \leq j \leq r \\ \delta_j = 0}} p_j^{\alpha_j}\right) = \sum_{\delta} \left(\prod_{\substack{1 \leq j \leq r \\ \delta_j = 0}} \varphi(p_j^{\alpha_j})\right)$$
$$= \prod_{j=1}^{r} (1 + \varphi(p_j^{\alpha_j})) = \prod_{j=1}^{r} (1 + p_j^{\alpha_j} - p_j^{\alpha_j - 1}) .$$

The sums in (2) are taken over all sequences $\{\delta_1, \cdots, \delta_r\}$ where each δ_j is 0 or α_j.

3.2 THEOREM. *Let χ be a semicharacter of S_m as given in* (1) *with the idempotent $a = [p_1^{\delta_1} \cdots p_r^{\delta_r} d]$, and let χ' be a semicharacter with the idempotent $a = [p_1^{\delta_1'} \cdots p_r^{\delta_r'} d']$. Then the semicharacter $\chi\chi'$ is given by* (1) *with the idempotent $a'' = [p_1^{\min(\delta_1, \delta_1')} \cdots p_r^{\min(\delta_r, \delta_r')} d]$.*

This theorem follows at once from 2.21 and the definition (1).

We now prove two facts needed in § 4.

3.3 THEOREM. *Let χ be a semicharacter of S_m that assumes somewhere a value different from 0 and 1. Then χ assumes a value different from 1 somewhere on G_m.*

Proof. Definition (1) implies that the character χ_a of U_a assumes a value different from 1. It is also easy to see that $G_m = U_{[1]}$. For $[x] \in G_m$, definition (1) implies that $\chi([x]) = \chi_a(a[x])$. We need therefore only show that the mapping $[x] \to a[x]$ carries G_m onto U_a.

Write $a = [p_1^{\delta_1} \cdots p_r^{\delta_r} d]$. Every element of U_a can be written as $[p_1^{\delta_1} \cdots p_r^{\delta_r} c]$ where $(c, m) = 1$, by 2.4. We must produce an $[x] \in G_m$ such that $a[x] = [p_1^{\delta_1} \cdots p_r^{\delta_r} c]$. That is, we must produce an integer x such that

$$(3) \qquad \prod_{j=1}^{r} p_j^{\delta_j} \cdot dx \equiv \prod_{j=1}^{r} p_j^{\delta_j} \cdot c \pmod{m}$$

and $(x, m) = 1$. The congruence (3) is equivalent to

$$(4) \qquad dx \equiv c \left(\bmod \prod_{j=1}^{r} p_j^{\alpha_j - \delta_j} \right).$$

Since d is relatively prime to the modulus in (4), the congruence (4) has a solution x_0. We determine x as a number

$$x_0 + l \prod_{j=1}^{r} p_j^{\alpha_j - \delta_j},$$

where l is an integer for which

$$x_0 + l \prod_{j=1}^{r} p_j^{\alpha_j - \delta_j} \equiv 1 \left(\bmod \prod_{j=1}^{r} p_j^{\delta_j} \right).$$

Clearly

$$x = x_0 + l \prod_{j=1}^{r} p_j^{\alpha_j - \delta_j}$$

satisfies (3) and the condition $(x, m) = 1$.

3.4. Let $\{\lambda_1, \cdots, \lambda_r\}$ be a sequence of integers such that $0 \leqq \lambda_j \leqq \alpha_j$ $(j = 1, \cdots, r)$, and consider the set $V(\lambda_1, \cdots, \lambda_r)$ of all $[p_1^{\lambda_1} \cdots p_r^{\lambda_r} x] \in S_m$ with $(x, m) = 1$. It is easy to see that this set is contained in T_a, where a is the idempotent

$$\left[\prod_{\substack{1 \leqq j \leqq r \\ \lambda_j > 0}} p_j^{\alpha_j} \cdot d \right].$$

3.5 THEOREM. *Given $\lambda_1, \cdots, \lambda_r$, there is a positive integer k such that the mapping $[x] \to [p_1^{\lambda_1} \cdots p_r^{\lambda_r} x]$ of G_m onto $V(\lambda_1, \cdots, \lambda_r)$ is exactly k to one.*

Proof. Let u be any integer such that $(u, m) = 1$, and let $[x_1]$, $\cdots$, $[x_{k_u}]$ be the distinct elements of G_m such that $[p_1^{\lambda_1} \cdots p_r^{\lambda_r} x_j] = [p_1^{\lambda_1} \cdots p_r^{\lambda_r} u]$. That is,

$$p_1^{\lambda_1} \cdots p_r^{\lambda_r} x_j \equiv p_1^{\lambda_1} \cdots p_r^{\lambda_r} u \pmod{m} \quad (j = 1, \cdots, k_u) .$$

Let u^* be any solution of $uu^* \equiv 1 \pmod{m}$. If $(v, m) = 1$, then we have

$$p_1^{\lambda_1} \cdots p_r^{\lambda_r} u^* v x_j \equiv p_1^{\lambda_1} \cdots p_r^{\lambda_r} v \pmod{m} .$$

Since $(u^* v x_j, m) = 1$ $(j = 1, \cdots, k_u)$ and the elements $[u^* v x_1], \cdots, [u^* v x_{k_u}]$ are distinct in G_m, it follows that $k_u \leqq k_v$. Similarly, we have $k_v \leqq k_u$.

4. A property of semicharacters of S_m. It is well known and obvious that if H is a finite group and χ is a character of H, then $\sum_{x \in H} \chi(x) = 0$ or $o(H)$ according as $\chi \neq 1$ or $\chi = 1$. This result does not hold in general for finite commutative semigroups. As a simple example, consider the cyclic finite semigroup $T = \{x, x^2, \cdots, x^l, \cdots, x^{l+k-1}\}$, where $x^{l+k} = x^l$, and l and $l + k$ are the first pair of positive integers $m, n, m < n$, for which $x^m = x^n$. The following facts are easy to show, and follow from the general theory in [2]. The subset $\{x^l, x^{l+1}, \cdots, x^{l+k-1}\}$ is the largest subgroup of T. Its unit is the element x^{uk}, where the integer u is defined by $l \leqq uk < l + k$. The general semicharacter of T is the function χ whose value at x^h is $\exp(2\pi i h j/k)$, where $j = 0, 1, \cdots, k - 1$. For $j = 1, 2, \cdots, k - 1$, the sum $\sum_{h=1}^{k+l-1} \chi(x^h)$ is equal to

$$\frac{1 - \exp\left(\dfrac{2\pi i(k + l)j}{k}\right)}{1 - \exp\left(\dfrac{2\pi i j}{k}\right)} ,$$

which is 0 if and only if $k/(k, l)$ divides j. Hence the sum of a semicharacter assuming values different from 0 and 1 need not be 0.

Curiously enough, the above-mentioned property of groups holds for the semigroup S_m.

4.1 THEOREM. *Let χ be a semicharacter of S_m that assumes somewhere a value different from* 0 *and* 1. *Then* $\sum_{[x] \in S_m} \chi([x]) = 0$.

Proof. It is obvious from 2.1 that the sets $V(\lambda_1, \cdots, \lambda_r)$ of 3.4 are pairwise disjoint and that their union is S_m. We therefore need only show that $\sum_{[x] \in V(\lambda_1, \cdots, \lambda_r)} \chi([x]) = 0$ for all $\{\lambda_1, \cdots, \lambda_r\}$. By 3.3, χ assumes a value different from 1 somewhere on the group G_m, so that $\sum_{[x] \in G_m} \chi([x]) = 0$. (Note that χ on G_m is a character of the group G_m.) Thus we have $0 = \sum_{[x] \in G_m} \chi([p_1^{\lambda_1} \cdots p_r^{\lambda_r}])\chi([x]) = \sum_{[x] \in G_m} \chi([p_1^{\lambda_1} \cdots p_r^{\lambda_r} x]) = k \sum \chi([y])$, where $[y]$ runs through $V(\lambda_1, \cdots, \lambda_r)$.

5. A second construction of semicharacters of S_m. In this section, we compute explicitly all of the semicharacters of S_m. The case m even is a little different from the case m odd. When m is even, we will take $p_1 = 2$. To compute the semicharacters of S_m, we need to examine the structure of S_m in more detail than was done in § 3. For this purpose, we fix once and for all the following numbers.

5.1 DEFINITION. *For $j = 1, \cdots, r$, let*
$g_j =$ *a primitive root modulo* $p_j^{\alpha_j}$ *if* p_j *is odd;*
$g_1 = 5$ *if* $p_1 = 2$;
$h_j = g_j + y_j p_j^{\alpha_j}$ *where* y_j *is such that* $h_j \equiv 1 \pmod{m/p_j^{\alpha_j}}$;
$h_0 = -1 + y_0 p_1^{\alpha_1}$ *where* y_0 *is such that* $h_0 \equiv 1 \pmod{m/p_1^{\alpha_1}}$;
$q_j = p_j + z_j p_j^{\alpha_j}$ *where* z_j *is such that* $q_j \equiv 1 \pmod{m/p_j^{\alpha_j}}$;
For $j = 1, \cdots, r$, $l = 1, \cdots, r$, $j \neq l$, and p_l odd, let k_{jl} be a positive integer such that $p_j \equiv g_l^{k_{jl}} \pmod{p_l^{\alpha_l}}$.
For $j = 2, \cdots, r$ and $p_1 = 2$ let
k_{j1} *be a positive integer such that* $p_j \equiv (-1)^{(p_j-1)/2} g_1^{k_{j1}} \pmod{p_1^{\alpha_1}}$.

Plainly $y_0, y_1, \cdots, y_r$ and $z_1, \cdots, z_r$ exist. For p_l odd, the integers k_{jl} exist because g_l is a primitive root modulo $p_l^{\alpha_l}$. For $p_1 = 2$, the integers k_{j1} exist for $\alpha_1 \geqq 3$ by [3], p. 82, Satz 126. For $\alpha_1 = 1$ or 2, k_{j1} can be any positive integer.

5.2. Let x be any integer $\neq 0$. Then $x = \prod_{j=1}^r p_j^{\beta_j(x)} \cdot a(x)$, where $\beta_j(x) \geqq 0$ and $(a(x), m) = 1$. Plainly the numbers $\beta_j = \beta_j(x)$ and $a = a(x)$ are uniquely determined by x. For $j = 1, \cdots, r$ and p_j odd, let $e_j = e_j(x)$ be any positive integer such that

$$a(x) \equiv g_j^{e_j(x)} \pmod{p_j^{\alpha_j}} .$$

The number $e_j(x)$ is uniquely determined modulo $\varphi(p_j^{\alpha_j})$. For $p_1 = 2$, let

$e_1 = e_1(x)$ be any positive integer such that

$$a(x) \equiv (-1)^{(a(x)-1)/2} g_1^{e_1(x)} \pmod{p_1^{\alpha_1}} .$$

For $\alpha_1 \geqq 3$, $e_1(x)$ exists and is uniquely determined modulo $p_1^{\alpha_1-2}$ (see [3], p. 82, Satz 126). For $\alpha_1 = 1$ or 2, $e_1(x)$ can be any positive integer.

If m is even, let

$$(1_e) \qquad A(x) = \left(\prod_{j=2}^r h_0^{(p_j-1)\beta_j/2}\right)\left(\prod_{l=1}^r \prod_{\substack{j=1\\ j\neq 1}}^r h_l^{\beta_j k_{jl}}\right)\left(\prod_{j=1}^r q_j^{\beta_j}\right) h_0^{(a-1)/2}\left(\prod_{j=1}^r h_j^{e_j}\right) .$$

If m is odd, let

$$(1_0) \qquad A(x) = \left(\prod_{l=1}^r \prod_{\substack{j=1\\ j\neq 1}}^r h_l^{\beta_j k_{jl}}\right)\left(\prod_{j=1}^r q_j^{\beta_j}\right)\left(\prod_{j=1}^r h_j^{e_j}\right) .$$

If m is even, it is easy to see from 5.1 that

$$(2)\qquad A(x) \equiv \left(\prod_{j=2}^{r}(-1)^{(p_j-1)\beta_j/2}\right)\left(\prod_{j=2}^{r} g_1^{\beta_j k_{j1}}\right)p_1^{\beta_1}(-1)^{(a-1)/2}g_1^{e_1} \pmod{p_1^{\alpha_1}}$$
$$\equiv \left(\prod_{j=2}^{r}(-1)^{(p_j-1)/2}g_1^{k_{j1}}\right)^{\beta_j} p_1^{\beta_1}(-1)^{(a-1)/2}g_1^{e_1}$$
$$\equiv \prod_{j=2}^{r} p_j^{\beta_j}\cdot p_1^{\beta_1}a \equiv x \pmod{p_1^{\alpha_1}},$$

and, if $n = 2, \cdots, r$,

$$A(x) \equiv \prod_{\substack{j=1\\ j\neq n}}^{r} g_n^{\beta_j k_{jn}}\cdot p_n^{\beta_n} g_n^{e_n} \equiv \prod_{\substack{j=1\\ j\neq n}}^{r} p_j^{\beta_j}\cdot p_n^{\beta_n}a \equiv x \pmod{p_n^{\alpha_n}}.$$

Therefore $A(x) \equiv x \pmod{m}$ if m is even.

If m is odd, then for $n = 1, \cdots, r$, we have

$$A(x) \equiv \prod_{\substack{j=1\\ j\neq n}}^{r} g_n^{\beta_j k_{jn}}\cdot p_n^{\beta_n} g_n^{e_n} \equiv \prod_{\substack{j=1\\ j\neq n}}^{r} p_j^{\beta_j}\cdot p_n^{\beta_n}a \equiv x \pmod{p_n^{\alpha_n}}.$$

Therefore $A(x) \equiv x \pmod{m}$ if m is even or odd.

5.3. Suppose that χ is any semicharacter of S_m. Let ψ be the function defined for all integers x by the relation $\psi(x) = \chi([x])$. Then ψ is obviously a semicharacter of the integers under multiplication, and $\psi(x) = \psi(y)$ if $x \equiv y \pmod{m}$. We will construct the semicharacters of S_m by finding all of the functions ψ with these properties. As 5.2 shows, ψ is determined by its values on $h_0, h_1, \cdots, h_r$ and $q_1, \cdots, q_r$. We now set down relations involving the h's and q's which restrict the values that ψ can assume on these integers.

5.4. If p_j is odd, then

$$h_j^{\varphi(p_j^{\alpha_j})} \equiv 1 \pmod{p_j^{\alpha_j}}, \quad h_j^{\varphi(p_j^{\alpha_j})} \equiv 1 \left(\mathrm{mod}\ \frac{m}{p_j^{\alpha_j}}\right);$$

hence

$$h_j^{\varphi(p_j^{\alpha_j})} \equiv 1 \pmod{m}.$$

Also,

$$h_0^2 \equiv 1 \pmod{p_1^{\alpha_1}}, \qquad h_0^2 \equiv 1 \left(\mathrm{mod}\ \frac{m}{p_1^{\alpha_1}}\right);$$

hence $h_0^2 \equiv 1 \pmod{m}$.

If $p_1 = 2$ and $\alpha_1 = 1$, then $h_0 \equiv 1 \pmod 2$, $h_0 \equiv 1 \pmod{m/2}$; hence $h_0 \equiv 1 \pmod{m}$.

If $p_1 = 2$ and $\alpha_1 = 1$ or 2, then
$h_1 \equiv 5 \equiv 1 \pmod{p_1^{\alpha_1}}$, $h_1 \equiv 1 \pmod{m/p_1^{\alpha_1}}$; hence $h_1 \equiv 1 \pmod{m}$.
If $p_1 = 2$ and $\alpha_1 \geqq 3$, then
$h_1^{2^{\alpha_1-2}} \equiv 1 \pmod{p_1^{\alpha_1}}$, $h_1^{2^{\alpha_1-2}} \equiv 1 \pmod{m/p_1^{\alpha_1}}$; hence $h_1^{2^{\alpha_1-2}} \equiv 1 \pmod{m}$.
(The first congruence on the line above is proved in [3], p. 81, Satz 125.)

For $j = 1, \cdots, r$, we have

$$q_j^{\alpha_j} \equiv 0\ , \qquad q_j^{\alpha_j}h_j \equiv 0\ , \qquad q_j^{\alpha_j+1} \equiv 0 \pmod{p_j^{\alpha_j}}\ ,$$

$$q_j^{\alpha_j} \equiv 1\ , \qquad q_j^{\alpha_j}h_j \equiv 1\ , \qquad q_j^{\alpha_j+1} \equiv 1 \left(\bmod\ \frac{m}{p_j^{\alpha_j}}\right) .$$

Therefore we have

$$q_j^{\alpha_j} \equiv q_j^{\alpha_j}h_j \equiv q_j^{\alpha_j+1} \pmod{m}\ .$$

Also, if $p_1 = 2$, we have

$$q_1^{\alpha_1} \equiv 0\ , \qquad q_1^{\alpha_1}h_0 \equiv 0 \pmod{p_1^{\alpha_1}}\ ,$$

$$q_1^{\alpha_1} \equiv 1\ , \qquad q_1^{\alpha_1}h_0 \equiv 1 \left(\bmod\ \frac{m}{p_1^{\alpha_1}}\right) .$$

Therefore we have

$$q_1^{\alpha_1} \equiv q_1^{\alpha_1}h_0 \pmod{m}\ .$$

5.5 If ψ is to be a function on the integers such that $\psi(x) = \chi([x])$ for some semicharacter χ of S_m, then the choices of the values of ψ at the h's and q's are restricted by the congruences modulo m derived in 5.4. Thus, since $\chi([1]) = 1$, we have

$$\psi(h_j)^{\varphi(p_j^{\alpha_j})} = 1 \text{ if } p_j \text{ is odd;}$$
$$\psi(h_0) = \pm 1, \text{ and } \psi(h_0) = 1 \text{ if } \alpha_1 = 1 \text{ and } p_1 = 2;$$
$$\psi(h_1) = 1 \text{ if } p_1 = 2 \text{ and } \alpha_1 = 1 \text{ or } 2;$$
$$\psi(h_1)^{2^{\alpha_1-2}} = 1 \text{ if } p_1 = 2 \text{ and } \alpha_1 \geqq 3.$$

Also we have

$$\psi(q_j)^{\alpha_j} = \psi(q_j)^{\alpha_j}\psi(h_j) = \psi(q_j)^{\alpha_j+1} \text{ for } j = 1, \cdots, r\ .$$

If $p_1 = 2$, we have

$$\psi(q_1)^{\alpha_1} = \psi(q_1)^{\alpha_1}\psi(h_0)\ .$$

The last two equalities give us:

$$\psi(q_j) \neq 0 \text{ implies } \psi(h_j) = \psi(q_j) = 1;$$

and

$$\psi(q_1) \neq 0 \text{ implies } \psi(h_0) = 1 \text{ if } p_1 = 2.$$

5.6. To construct our functions ψ, we now choose numbers ω_0, $\omega_1, \cdots, \omega_r$ and $\mu_1, \cdots, \mu_r$ which are to be $\psi(h_0)$, $\psi(h_1), \cdots, \psi(h_r)$ and $\psi(q_1), \cdots, \psi(q_r)$. The relations in 5.5 show that we must take these numbers such that:

$$\omega_j^{\varphi(p_j^{\alpha_j})} = 1 \text{ if } j = 1, \cdots, r \text{ and } p_j \text{ is odd;}$$
$$\omega_0 = \pm 1;\ \omega_0 = 1 \text{ if } p_1 = 2 \text{ and } \alpha_1 = 1, \text{ or if } m \text{ is odd}^1;$$
$$\omega_1 = 1 \text{ if } p_1 = 2 \text{ and } \alpha_1 = 1 \text{ or } 2;$$
$$\omega_1^{2^{\alpha_1-2}} = 1 \text{ if } p_1 = 2 \text{ and } \alpha_1 \geqq 3;$$
$$\mu_j = 0 \text{ or } 1 \text{ if } j = 1, \cdots, r;$$
$$\omega_j = 1 \text{ if } \mu_j = 1, j = 1, \cdots, r;$$
$$\omega_0 = 1 \text{ if } p_1 = 2 \text{ and } \mu_1 = 1.$$

Formulas (1_e) and (1_0) of 5.2 now require us to define $\psi(x)$ for non-zero integers x as follows:

$$(3_e)\quad \psi(x) = \Big(\prod_{j=2}^{r} \omega_0^{(p_j-1)\beta_j(x)/2}\Big)\Big(\prod_{l=1}^{r}\prod_{\substack{j=1\\ j\neq l}}^{r} \omega_l^{\beta_j(x)k_{jl}}\Big)\Big(\prod_{j=1}^{r} \mu_j^{\beta_j(x)}\Big) \cdot \omega_0^{(a(x)-1)/2}\Big(\prod_{j=1}^{r} \omega_j^{e_j(x)}\Big) \text{ if } m \text{ is even}^2;$$

$$(3_0)\quad \psi(x) = \Big(\prod_{l=1}^{r}\prod_{\substack{j=1\\ j\neq l}}^{r} \omega_l^{\beta_j(x)k_{jl}}\Big)\Big(\prod_{j=1}^{r} \mu_j^{\beta_j(x)}\Big)\Big(\prod_{j=1}^{r} \omega_j^{e_j(x)}\Big) \text{ if } m \text{ is odd.}$$

Finally, we define $\psi(0) = \psi(m)$.

The q's, h's, and k's appearing in (1) and (3) were fixed once and for all in terms of m. The ω's and μ's are at our disposal and serve to define ψ. The β's are determined uniquely from x; but the e's are not. As noted in 5.2, e_j is determined modulo $\varphi(p_j^{\alpha_j})$ if p_j is odd, and e_1 is determined modulo $p_1^{\alpha_1-2}$ if $p_1 = 2$ and $\alpha_1 \geqq 3$. Since $\omega_j^{\varphi(p_j^{\alpha_j})} = 1$ if p_j is odd, $\omega_1^{2^{\alpha_1-2}} = 1$ if $p_1 = 2$ and $\alpha_1 \geqq 3$, and $\omega_1 = 1$ if $p_1 = 2$ and $\alpha_1 \leqq 2$, we see that ψ is uniquely defined by the formulas (3_e) and (3_0).

5.7. We now prove that $\psi(xy) = \psi(x)\psi(y)$. Since ψ is obviously bounded and not identically zero, this will show that ψ is a semicharacter.

Suppose first that $x \neq 0, y \neq 0$. Then we have

$$x = \prod_{j=1}^{r} p_j^{\beta_j(x)} \cdot a(x)\ ,\quad y = \prod_{j=1}^{r} p_j^{\beta_j(y)} \cdot a(y)\ ,\quad xy = \prod_{j=1}^{r} p_j^{\beta_j(x)+\beta_j(y)} \cdot a(x)a(y)\ .$$

[1] We take $\omega_0 = 1$ when m is odd merely as a matter of convenience. Actually, as will shortly be apparent, ω_0 does not appear in the definition of ψ if m is odd.

[2] We take $0^0 = 1$.

Therefore $a(xy) = a(x)a(y)$ and $\beta_j(xy) = \beta_j(x) + \beta_j(y)$ for $j = 1, \cdots, r$. Also we have

$$g_j^{e_j(xy)} \equiv a(xy) \equiv a(x)a(y) \equiv g_j^{e_j(x)}g_j^{e_j(y)} \equiv g_j^{e_j(x)+e_j(y)} \pmod{p_j^{\alpha_j}}$$

if p_j is odd. Since g_j is a primitive root modulo $p_j^{\alpha_j}$ and $\omega_j^{\varphi(p_j^{\alpha_j})} = 1$, it follows that $e_j(xy) \equiv e_j(x) + e_j(y) \pmod{\varphi(p_j^{\alpha_j})}$ and $\omega_j^{e_j(xy)} = \omega_j^{e_j(x)}\omega_j^{e_j(y)}$ if p_j is odd ($j = 1, \cdots, r$). If $p_1 = 2$, then $a(x)$ and $a(y)$ are odd, and plainly

$$\frac{a(xy)-1}{2} \equiv \frac{a(x)-1}{2} + \frac{a(y)-1}{2} \pmod{2} .$$

Therefore we have

$$\omega_0^{(a(xy)-1)/2} = \omega_0^{(a(x)-1)/2}\omega_0^{(a(y)-1)/2}$$

for both admissible values of ω_0. Furthermore,

$$\begin{aligned}(-1)^{(a(xy)-1)/2}g_1^{e_1(xy)} &\equiv a(x)a(y) \\ &\equiv (-1)^{(a(x)-1)/2}g_1^{e_1(x)}(-1)^{(a(y)-1)/2}g_1^{e_1(y)} \pmod{p_1^{\alpha_1}} ,\end{aligned}$$

if $p_1 = 2$. Therefore we have

$$g_1^{e_1(xy)} \equiv g_1^{e_1(x)+e_1(y)} \pmod{p_1^{\alpha_1}} ,$$

if $p_1 = 2$.
Hence, if $\alpha_1 \geqq 3$ and $p_1 = 2$, we have $e_1(xy) \equiv e_1(x) + e_1(y) \pmod{p_1^{\alpha_1-2}}$, as follows from [3], p. 82, Satz 126 (recall that $g_1 = 5, p_1 = 2$). Hence

$$\omega_1^{e_1(xy)} = \omega_1^{e_1(x)}\omega_1^{e_1(y)} \qquad \text{if } \alpha_1 \geqq 3, p_1 = 2 .$$

The last equality also holds if $\alpha_1 \leqq 2$ and $p_1 = 2$, since $\omega_1 = 1$ in this case.

The foregoing computations, together with (3), now show that $\psi(xy) = \psi(x)\psi(y)$ if $xy \neq 0$.

We next show that $\psi(xy) = \psi(x)\psi(y)$ if $xy = 0$. We compute $\psi(m)$. Since $\beta_j(m) = \alpha_j > 0$ for $j = 1, \cdots, r$, we have

$$\prod_{j=1}^{r} \mu_j^{\beta_j(m)} = \begin{cases}1 \text{ if } \mu_1 = \cdots = \mu_r = 1 , \\ 0 \text{ otherwise.}\end{cases}$$

If $\mu_1 = \cdots = \mu_r = 1$, then by 5.6, we have $\omega_0 = \omega_1 = \cdots = \omega_r = 1$, so that $\psi(x) = 1$ for all x. In this case, we have $\psi(xy) = \psi(x)\psi(y)$ for all x and y. If some $\mu_j = 0$, then $\psi(m) = 0$, and hence $\psi(0) = 0$. In this case, $\psi(xy) = \psi(x)\psi(y)$ if $xy = 0$.

5.8. We now prove that $\psi(x) = \psi(y)$ if $x \equiv y \pmod{m}$. Suppose first that $xy \neq 0$ and $x \equiv y \pmod{m}$. Then

$$\prod_{j=1}^{r} p_j^{\beta_j(x)} \cdot a(x) \equiv \prod_{j=1}^{r} p_j^{\beta_j(y)} \cdot a(y) \pmod{m} .$$

From this, we see that $\beta_j(x) > 0$ if and only if $\beta_j(y) > 0$. If, for some j, we have $\beta_j(x) > 0$ and $\mu_j = 0$, then $\beta_j(y) > 0$ and $\psi(x) = 0 = \psi(y)$.

Now we can suppose that $\mu_j = 1$ for all j such that $\beta_j(x) > 0$. Then $\omega_j = 1$ if $\beta_j(x) > 0$ $(j = 1, \cdots, r)$ and $\omega_0 = 1$ if $\beta_1(x) > 0$. If m is odd, or if m is even and $\beta_1(x) > 0$, we have

$$(4) \qquad \psi(x) = \Big(\prod_{\substack{l=1 \\ \beta_l(x)=0}}^{r} \prod_{\substack{j=1 \\ j\neq l}}^{r} \omega_l^{\beta_j(x)k_{jl}} \Big) \Big(\prod_{\substack{j=1 \\ \beta_j(x)=0}}^{r} \omega_j^{e_j(x)} \Big) ,$$

$$(5) \qquad \psi(y) = \Big(\prod_{\substack{l=1 \\ \beta_l(x)=0}}^{r} \prod_{\substack{j=1 \\ j\neq l}}^{r} \omega_l^{\beta_j(y)k_{jl}} \Big) \Big(\prod_{\substack{j=1 \\ \beta_j(x)=0}}^{r} \omega_j^{e_j(y)} \Big) .$$

If m is even and $\beta_1(x) = 0$, we have

$$(6) \qquad \psi(x) = \Big(\prod_{j=2}^{r} \omega_0{}^{(p_j-1)\beta_j(x)/2} \Big) \Big(\prod_{\substack{l=1 \\ \beta_l(x)=0}}^{r} \prod_{\substack{j=1 \\ \beta_j(x)>0}}^{r} \omega_l^{\beta_j(x)k_{jl}} \Big) \omega_0{}^{(a(x)-1)/2} \Big(\prod_{\substack{j=1 \\ \beta_j(x)=0}}^{r} \omega_j^{e_j(x)} \Big) ,$$

$$(7) \qquad \psi(y) = \Big(\prod_{j=2}^{r} \omega_0{}^{(p_j-1)\beta_j(y)/2} \Big) \Big(\prod_{\substack{l=1 \\ \beta_l(x)=0}}^{r} \prod_{\substack{j=1 \\ \beta_j(x)>0}}^{r} \omega_l^{\beta_j(y)k_{jl}} \Big) \omega_0{}^{(a(y)-1)/2} \Big(\prod_{\substack{j=1 \\ \beta_j(x)=0}}^{r} \omega_j^{e_j(y)} \Big) .$$

Since $x \equiv y \pmod{m}$, we see from 5.2 that $A(x) \equiv A(y) \pmod{m}$ and hence

$$(8) \qquad A(x) \equiv A(y) \pmod{p_n^{\alpha_n}} \text{ for } n = 1, \cdots, r .$$

The congruence

$$(9) \qquad A(x) \equiv \prod_{\substack{j=1 \\ j\neq n}}^{r} h_n^{\beta_j(x)k_{jn}} \cdot q_n^{\beta_n(x)} h_n^{e_n(x)} \pmod{p_n^{\alpha_n}}$$

holds if p_n is odd. To verify this, use (1_e) and (1_0) together with 5.1. Notice that for $n = 1$, we use only (1_0).

The congruences (8) and (9), together with the fact that $\beta_n(x) = 0$ if and only if $\beta_n(y) = 0$, now show that

$$\prod_{\substack{j=1 \\ j\neq n}}^{r} h_n^{\beta_j(x)k_{jl}} \cdot h_n^{e_n(x)} \equiv \prod_{\substack{j=1 \\ j\neq n}}^{r} h_n^{\beta_j(y)k_{jn}} \cdot h_n^{e_n(y)} \pmod{p_n^{\alpha_n}}$$

if p_n is odd and $\beta_n(x) = 0$. This implies that

$$\sum_{\substack{j=1 \\ j\neq n}}^{r} \beta_j(x)k_{jn} + e_n(x) \equiv \sum_{\substack{j=1 \\ j\neq n}}^{r} \beta_j(y)k_{jn} + e_n(y) \pmod{\varphi(p_n^{\alpha_n})} ,$$

and

$$(10) \qquad \prod_{\substack{j=1 \\ j\neq n}}^{r} \omega_n^{\beta_j(x)k_{jn}} \cdot \omega_n^{e_n(y)} = \prod_{\substack{j=1 \\ j\neq n}}^{r} \omega_n^{\beta_j(y)k_{jn}} \cdot \omega_n^{e_n(y)} ,$$

if p_n is odd and $\beta_n(x) = 0$.

Similarly, if $p_1 = 2$ and $\beta_1(x) = 0$, in which case $g_1 = 5$, (2) implies that

$$(11)\qquad A(x) \equiv \left(\prod_{j=2}^{r} (-1)^{(p_j-1)\beta_j(x)/2}\right)\left(\prod_{j=2}^{r} 5^{\beta_j(x)k_{j1}}\right)(-1)^{(a(x)-1)/2}5^{e_1(x)} \pmod{2^{\alpha_1}} .$$

The congruences (8) and (11), together with the fact that $\beta_1(y) = 0$, now show that

$$(-1)^{\sum_{j=2}^{r}\frac{1}{2}(p_j-1)\beta_j(x)+\frac{1}{2}(a(x)-1)}5^{\sum_{j=2}^{r}\beta_j(x)k_{j1}+e_1(x)} \equiv$$

$$\equiv (-1)^{\sum_{j=2}^{r}\frac{1}{2}(p_j-1)\beta_j(y)+\frac{1}{2}(a(y)-1)}5^{\sum_{j=2}^{r}\beta_j(y)+e_1(y)} \pmod{2^{\alpha_1}}$$

From this congruence, we find that

$$\sum_{j=2}^{r}\frac{1}{2}(p_j-1)\beta_j(x)+\frac{1}{2}(a(x)-1) \equiv$$

$$\sum_{j=2}^{r}\frac{1}{2}(p_j-1)\beta_j(y)+\frac{1}{2}(a(y)-1) \pmod 2$$

if $\alpha_1 \geqq 2$, and

$$\sum_{j=2}^{r}\beta_j(x)k_{j1}+e_1(x) \equiv \sum_{j=2}^{r}\beta_j(y)k_{j1}+e_1(y) \pmod{2^{\alpha_1-2}}$$

if $\alpha_1 \geqq 3$. Since $\omega_0 = 1$ if $\alpha_1 = 1$ and $\omega_1 = 1$ if $\alpha_1 = 1$ or 2, we now have

$$(12)\qquad \prod_{j=2}^{r}\omega_0{}^{(p_j-1)\beta_j(x)/2}\cdot\omega_0{}^{(a(x)-1)/2} = \prod_{j=2}^{r}\omega_0{}^{(p_j-1)\beta_j(y)/2}\cdot\omega_0{}^{(a(y)-1)/2}$$

if $\alpha_1 \geqq 1$, and

$$(13)\qquad \prod_{j=2}^{r}\omega_1^{\beta_j(x)k_{j1}}\cdot\omega_1^{e_1(x)} = \prod_{j=2}^{r}\omega_1^{\beta_j(y)k_{j1}}\cdot\omega_1^{e_1(y)}$$

if $\alpha_1 \geqq 1$. Multiplying (10) over the relevant values of n, we have

$$(14)\qquad \left(\prod_{\substack{n=1\\ \beta_n(x)=0\\ p_n>2}}^{r}\ \prod_{\substack{j=1\\ j\neq n}}^{r}\omega_n^{\beta_j(x)k_{jn}}\right)\left(\prod_{\substack{n=1\\ \beta_n(x)=0\\ p_n>2}}^{r}\omega_n^{e_n(x)}\right) = \left(\prod_{\substack{n=1\\ \beta_n(x)=0\\ p_n>2}}^{r}\ \prod_{\substack{j=1\\ j\neq n}}^{r}\omega_n^{\beta_j(y)k_{jn}}\right)\left(\prod_{\substack{n=1\\ \beta_n(x)=0\\ p_n>2}}^{r}\omega_n^{e_n(y)}\right) .$$

If m is odd, or if m is even and $\beta_1(x) > 0$, (14), (4), and (5) show that $\psi(x) = \psi(y)$. If m is even and $\beta_1(x) = 0$, we multiply (12), (13), and (14) together. Comparing the result with (6) and (7), we find that $\psi(x) = \psi(y)$ in this case also.

We have therefore proved that $\psi(x) = \psi(y)$ if $x \equiv y \pmod m$ and $xy \neq 0$. If $x \equiv 0 \pmod m$ and $x \neq 0$, then $\psi(x) = \psi(m)$. Since $\psi(0) = \psi(m)$ by definition, the proof is complete.

5.9. The foregoing construction of the functions ψ, and from these the semicharacters χ of S_m, $\chi([x]) = \psi(x)$, clearly gives us all of the semicharacters of S_m. As the ω's and μ's of 5.6 run through all admissible values, each semicharacter χ appears exactly once. We could show this by exhibiting, for each pair ψ and ψ', a number x such that $\psi(x) \neq \psi'(x)$. Rather than do this, we prefer to count the ψ's and compare their number with the number obtained in 3.1.

For p_j odd, the number of possible values of ω_j is $\varphi(p_j^{\alpha_j})$ if $\mu_j = 0$ and 1 if $\mu_j = 1$. Hence this number is $\varphi(p_j^{\alpha_j(1-\mu_j)})$. For $p_1 = 2$, there are several cases to consider ($\mu_1 = 0$ or 1, $\alpha_1 = 1$, $\alpha_1 = 2$, $\alpha_1 \geqq 3$). In each case, it is easy to see that the number of admissible pairs $\{\omega_0, \omega_1\}$ is $\varphi(2^{\alpha_1(1-\mu_1)})$. Thus, for each sequence $\{\mu_1, \cdots, \mu_r\}$, the total number of sequences $\{\omega_0, \omega_1, \cdots, \omega_r\}$ is equal to

$$\prod_{j=1}^{r} \varphi(p_j^{\alpha_j(1-\mu_j)}) \, .$$

Summing this number over all possible $\{\mu_1, \cdots, \mu_r\}$, we obtain $\prod_{j=1}^{r} (1 + p_j^{\alpha_j} - p_j^{\alpha_j - 1})$, as in Theorem 3.1.

6. The structure of X_m.

6.1. Let χ and χ' be any semicharacters of S_m, and let $(\mu_1, \cdots, \mu_r; \omega_0, \omega_1, \cdots, \omega_r)$ and $(\mu_1', \cdots, \mu_r'; \omega_0', \omega_1', \cdots, \omega_r')$ be the parameters as in 5.6 that determine χ and χ', respectively. The product $\chi\chi'$ then has as its parameters

$$(1) \qquad (\mu_1\mu_1', \cdots, \mu_r\mu_r'; \omega_0\omega_0', \omega_1\omega_1', \cdots, \omega_r\omega_r') \, .$$

Thus, all of the χ's in X_m for which the μ's are a fixed sequence of 0's and 1's form a group, plainly the direct product of cyclic groups, one corresponding to each zero value of μ. These are maximal subgroups of X_m, and X_m is the union of these subgroups. The multiplication rule (1) shows clearly how elements of different subgroups are multiplied. The rule (1) shows also that X_m resembles a direct product of groups and $\{0, 1\}$ semigroups. It fails to be one because of the condition in 5.6 that $\mu_j = 1$ implies $\omega_j = 1$.

6.2. The characters modulo m of number theory (see [3], p. 83) are of course among the semicharacters that we have computed. They are exactly those for which $\mu_1 = \mu_2 = \cdots = \mu_r = 0$. In the description of § 3, they are the semicharacters that are characters on the group G_m and are 0 elsewhere on S_m.

6.3. We can also map X_m into S_m, and represent X_m as a subset of S_m with a new definition of multiplication. Let χ be in X_m and let

χ have parameters $(\mu_1, \cdots, \mu_r; \omega_0, \omega_1, \cdots, \omega_r)$. For m odd and $j = 0, 1, \cdots, r$ or m even and $j = 0, 2, 3, \cdots, r$, let w_j be any integer such that $\omega_j = \exp(2\pi i w_j/\varphi(p_j^{\alpha_j}))$. For m even and $\alpha_1 = 1$ or 2, let $w_1 = 0$; for m even and $\alpha_1 \geqq 3$, let w_1 be any integer such that $\omega_1 = \exp(2\pi i w_1/2^{\alpha_1 - 2})$.

We now define the mapping

$$\chi \to \tau(\chi) = \left[h_0^{w_0(1-\mu_1)} \prod_{j=1}^{r} (h_j^{w_j(1-\mu_j)} q_j^{\alpha_j \mu_j})\right], \tag{2}$$

which carries X_m into S_m. Evidently τ is single-valued.

6.4 THEOREM. *The mapping τ is one-to-one.*

Proof. Suppose that χ and χ' are semicharacters of S_m with parameters as in 6.1. Suppose that $\tau(\chi) = \tau(\chi')$, that is,

$$h_0^{w_0(1-\mu_1)} \prod_{j=1}^{r} (h_j^{w_j(1-\mu_j)} q_j^{\alpha_j \mu_j}) \equiv h_0^{w_0'(1-\mu_1')} \prod_{j=1}^{r} (h_j^{w_j'(1-\mu_j')} q_j^{\alpha_j \mu_j'}) \pmod{m} . \tag{3}$$

This congruence, along with 5.1, implies that

$$h_l^{w_l(1-\mu_l)} p_l^{\alpha_l \mu_l} \equiv h_l^{w_l'(1-\mu_l')} p_l^{\alpha_l \mu_l'} \pmod{p_l^{\alpha_l}}$$

for $l = 1, \cdots, r$ and p_l odd. Since $(h_l, p_l) = 1$, and μ_l and μ_l' are 0 or 1, it is obvious that $\mu_l = \mu_l'$. If $\mu_l = \mu_l' = 1$, then from 5.6, we have $\omega_l = \omega_l' = 1$. If $\mu_l = \mu_l' = 0$, then $h_l^{w_l} \equiv h_l^{w_l'} \pmod{p_l^{\alpha_l}}$, so that $w_l \equiv w_l' \pmod{\varphi(p_l^{\alpha_l})}$ and hence $\omega_l = \omega_l'$.

If $p_1 = 2$, (2) implies that

$$h_0^{w_0(1-\mu_1)} h_1^{w_1(1-\mu_1)} p_1^{\alpha_1 \mu_1} \equiv h_0^{w_0'(1-\mu_1')} h_1^{w_1'(1-\mu_1')} p_1^{\alpha_1 \mu_1'} \pmod{p_1^{\alpha_1}} . \tag{4}$$

Again, we have $\mu_1 = \mu_1'$. If $\mu_1 = \mu_1' = 1$, then 5.6 states that $\omega_0 = \omega_0' = \omega_1 = \omega_1' = 1$. If $\alpha_1 = 1$, then $\omega_0 = \omega_0' = 1$, also by 5.6. If $\alpha_1 = 2$ and $\mu_1 = \mu_1' = 0$, then (3), along with 5.1, shows that $(-1)^{w_0} \equiv (-1)^{w_0'} \pmod{4}$, and hence $\omega_0 = \omega_0'$. If $\alpha_1 \geqq 3$ and $\mu_1 = \mu_1' = 0$, then we have $(-1)^{w_0} 5^{w_1} \equiv (-1)^{w_0'} 5^{w_1'} \pmod{2^{\alpha_1}}$. Once again, [3], p. 82, Satz 126 shows that $(-1)^{w_0} = (-1)^{w_0'}$ and that $w_1 \equiv w_1' \pmod{2^{\alpha_1 - 2}}$. Hence $\omega_0 = \omega_0'$ and $\omega_1 = \omega_1'$. Therefore τ is one-to-one.

6.5. The set $\tau(X_m)$ consists of all the elements $[p_1^{\delta_1} \cdots p_r^{\delta_r} a]$ of S_m for which $\delta_j = 0$ or α_j, and $(a, m) = 1$. It is evident from (2) that $\tau(X_m)$ is contained in the set $\{[p_1^{\delta_1} \cdots p_r^{\delta_r} a]\}$. The reverse inclusion is established by a routine examination of cases, which we omit.

6.6. The mapping τ plainly defines a new multiplication in $\tau(X_m)$: $\tau(\chi)^* \tau(\chi') = \tau(\chi')$. Every residue class $\tau(\chi)$ contains a number

$$x = h_0^{w_0(1-\mu_1)} \prod_{j=1}^{r} (h_j^{w_j(1-\mu_j)} q_j^{\alpha_j \mu_j}) .$$

If x' is another number of this form, then it can be shown that $[x]^*[x']$ is equal to $[xx'/\prod q_j^{\alpha_j}]$, where the product $\prod q_j^{\alpha_j}$ is taken over all j, $j = 1, \cdots, r$, for which $p_j \mid xx'$. We omit the details.

LITERATURE

1. Eckford Cohen, *A finite analogue of the Goldbach problem*, Proc. Amer. Math. Soc. **5** (1954), 478–483.
2. Edwin Hewitt and H. S. Zuckerman, *Finite dimensional convolution algebras*, Acta Math. **93** (1955), 67–119.
3. Edmund Landau, *Vorlesungen über Zahlentheorie*, Band I. S. Hirzel Verlag, Leipzig, 1927.
4. B. Parízek, and Š. Schwarz, *O multiplikatívnej pologrupe zvyškových tried* (mod m), Mat.-Fyz. Časopis Slov. Akad. Ved **8** (1958), 136–150.
5. E. T. Parker, *On multiplicative semigroups of residue classes*, Proc. Amer. Math. Soc. **5** (1954) 612–616.
6. H. S. Vandiver and Milo W. Weaver, *Introduction to arithmetic factorization and congruences from the standpoint of abstract algebra*, Herbert Ellsworth Slaught Memorial Papers, no. 7, 1958. Math. Assoc. of America.
7. Milo W. Weaver, *Cosets in a semi-group*, Math. Mag. **25** (1952), 125–136.

THE UNIVERSITY OF WASHINGTON