THE MULTIPLICATIVE SEMIGROUP OF INTEGERS MODULO $m$

Edwin Hewitt and Herbert 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 \( \alpha_j \) 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 \( \chi \) is a semicharacter of \( S_m \) assuming a value different from 0 and 1, then \( \Sigma_{[x]\in S_m} \chi([x]) = 0 \). In § 5, we compute \( \chi([x]) \) explicitly in terms of the integer \( x \), for an arbitrary semicharacter \( \chi \) 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 \( T_a = \{x : x \in G, x^m = a \} \) 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

\[
\prod_{j=1}^r p_j^{\beta_j} \cdot a, \quad \beta_j \geq 0, \ (a, m) = 1 .
\]

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

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

where $\lambda_{j} = \min (\alpha_{j}, \beta_{j})$ ($j = 1, \ldots, r$). If

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

where $0 \leq \mu_{j} \leq \alpha_{j}$ ($j = 1, \ldots, r$) and $(d, m) = 1$, then $\mu_{j} = \lambda_{j}$ ($j = 1, \ldots, r$). However, it may happen that $d \neq c \pmod{m}$.

**Proof.** Let $b = \prod_{\alpha_{j} = \beta_{j}} p_{j}^{\alpha_{j}}$. Then we have

$$x + bm = p_{1}^{\delta_{1}} \cdots p_{r}^{\delta_{r}}a + p_{1}^{\alpha_{1}} \cdots p_{r}^{\alpha_{r}}b$$

$$= \prod_{j=1}^{r} p_{j}^{\min(\alpha_{j}, \beta_{j})} \cdot (Aa + B),$$

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 $\alpha_{j}$ ($j = 1, \cdots, r$). 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

$$\prod_{j=1}^{r} p_{j}^{\delta_{j}} \cdot d \equiv 1 \pmod{\prod_{j=1}^{r} p_{j}^{\alpha_{j} - \beta_{j}}}. $$
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
\[ \prod_{j=1}^{r} p_{j}^{\delta_j} \cdot c^2 \equiv \prod_{j=1}^{r} p_{j}^{\delta_j} \cdot c \pmod{m}, \]
which is equivalent to
\[
(1) \quad \prod_{j=1}^{r} p_{j}^{\delta_j} \cdot c \equiv 1 \pmod{\prod_{j=1}^{r} p_{j}^{\lambda_j}}.
\]
The congruence (1) has a solution \(c\) if and only if \(\prod_{j=1}^{r} p_{j}^{\delta_j}\) is relatively
prime to \(\prod_{j=1}^{r} p_{j}^{\lambda_j}\), that is, if and only if \(\lambda_j = 0\) or \(\alpha_j (j = 1, \ldots, r)\).
If \(c_0\) is a solution of (1), then all solutions of (1) are given by
\[ c = c_0 + y \prod_{j=1}^{r} p_{j}^{\delta_j - \lambda_j}, \]
where \(y\) is an integer. Plainly
\[
\left[ \prod_{j=1}^{r} p_{j}^{\delta_j} \cdot c \right] = \left[ \prod_{j=1}^{r} p_{j}^{\delta_j} \cdot c_0 \right]
\]
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 \(\{\delta_1, \ldots, \delta_r\}\), where \(\delta_j = 0\) or \(\alpha_j (j = 1, \ldots, r)\).
If \(\{\delta_1, \ldots, \delta_r\}\) and \(\{\delta'_1, \ldots, \delta'_r\}\) are distinct such sequences, the corre-
sponding 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
be any element of $S_m$, where $0 \leq \lambda_j \leq \alpha_j$ $(j = 1, \ldots, r)$ and $(c, m) = 1$. Then $[x] \in T_a$, where the idempotent

$$a = \left[ \prod_{1 \leq j \leq r \atop \lambda_j > 0} p_j^{\delta_j} \cdot d \right],$$

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 $n \geq n_0$ (see [2], 2.6.2). For $n = n_0 \cdot \max (\alpha_1, \ldots, \alpha_r)$, 2.1 implies that

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

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 $k \geq 1$ and all integers $n \geq n_0$, 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

$$\prod_{j=1}^{r} p_j^{\delta_j} \cdot c = \prod_{j=1}^{r} p_j^{\lambda_j (nk+1) \cdot c^{nk+1}} \equiv \prod_{1 \leq j \leq r \atop \lambda_j > 0} p_j^{\delta_j} \cdot h \pmod{m},$$

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

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
\[
\left(\prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c\right)^{l} \equiv \prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c \pmod{m},
\]
and this congruence is equivalent to the congruence
\[
\left(\prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c\right)^{l-1} \equiv 1 \pmod{\prod_{j=1}^{r} p_{j}^{a_j - b_j}}.
\]
Since
\[
\prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c
\]
is relatively prime to the modulus, such an \(l\) exists.

We now identify the groups \(U_a\).

2.5 Theorem. Let
\[
a = \left[\prod_{j=1}^{r} p_{j}^{a_j} d\right]
\]
be any idempotent of \(S_m\), written as in 2.2. Let
\[
A = \prod_{j=1}^{r} p_{j}^{a_j - b_j}.
\]
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 \(\tau\) is single-valued and is a homomorphism of \(S_m\) onto \(S_A\). We need only show that \(\tau\) is one-to-one on \(U_a\). If \((c, m) = (c^*, m) = 1\) and
\[
\tau\left(\left[\prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c\right]\right) = \tau\left(\left[\prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c^*\right]\right),
\]
then
\[
\prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c \equiv \prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c^* \pmod{A},
\]
which implies that \(c \equiv c^* \pmod{A}\), because \((\prod_{j=1}^{r} p_{j}^{b_{j}}, A) = 1\). Since \(\prod_{j=1}^{r} p_{j}^{b_{j}} \cdot A = m\), we can multiply the last congruence by \(\prod_{j=1}^{r} p_{j}^{b_{j}}\) to obtain
\[
\prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c \equiv \prod_{j=1}^{r} p_{j}^{b_{j}} \cdot c^* \pmod{m}.
\]

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 $\chi_a$ be any character of the group $U_a$. We extend $\chi_a$ to a function on all of $S_m$ in the following way:

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

The set of all such functions $\chi$ is the set $X_m$.

3.1 Theorem. The semigroup $X_m$ has exactly

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

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

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

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

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

$$
= \prod_{j=1}^r (1 + \varphi(p_j^{s_j})) = \prod_{j=1}^r (1 + p_j^{s_j} - p_j^{s_j-1}).
$$

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

3.2 Theorem. Let $\chi$ 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 $\chi'$ 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 $X$ be a semicharacter of $S_m$ that assumes somewhere a value different from 0 and 1. Then $X$ assumes a value different from 1 somewhere on $G_m$.

Proof. Definition (1) implies that the character $\chi_a$ 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 $[x] \rightarrow a[x]$ carries $G_m$ onto $U_a$.

Write $a = [p_1^{\lambda_1} \cdots p_r^{\lambda_r}]$. Every element of $U_a$ can be written as $[p_1^{\lambda_1} \cdots p_r^{\lambda_r} c]$ where $(c, m) = 1$, by 2.4. We must produce an $[x] \in G_m$ such that $a[x] = [p_1^{\lambda_1} \cdots p_r^{\lambda_r} c]$. That is, we must produce an integer $x$ such that

\begin{equation}
\prod_{j=1}^{r} p_j^{\lambda_j} \cdot x \equiv \prod_{j=1}^{r} p_j^{\lambda_j} \cdot c \pmod{m}
\end{equation}

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

\begin{equation}
dx \equiv c \left( \mod \prod_{j=1}^{r} p_j^{\lambda_j - \delta_j} \right).
\end{equation}

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

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

where $l$ is an integer for which

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

Clearly

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

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

3.4. Let $\{\lambda_1, \cdots, \lambda_r\}$ be a sequence of integers such that $0 \leq \lambda_j \leq \alpha_j$ ($j = 1, \cdots, r$), 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

$$\left[ \prod_{\lambda_j \in \lambda, \lambda_j > 0} \prod_{1 \leq j \leq r} p_j^{\lambda_j} \cdot d \right].$$

3.5 Theorem. Given $\lambda_1, \cdots, \lambda_r$, there is a positive integer $k$ such that the mapping $[x] \rightarrow [p_1^{\lambda_1} \cdots p_r^{\lambda_r} x]$ 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 \([x_1, \ldots, x_k]\) be the distinct elements of \( G_m \) such that \([p_1^{x_1} \cdots p_r^{x_r}] = [p_1^{x_1} \cdots p_r^{x_r} u] \). That is,
\[
p_1^{x_1} \cdots p_r^{x_r} u \equiv p_1^{x_1} \cdots p_r^{x_r} \pmod{m} (j = 1, \ldots, k_u).
\]
Let \( u^* \) be any solution of \( uu^* \equiv 1 \pmod{m} \). If \((v, m) = 1\), then we have
\[
p_1^{x_1} \cdots p_r^{x_r} u^* v x_j \equiv p_1^{x_1} \cdots p_r^{x_r} v \pmod{m}.
\]
Since \((u^* v x_j, m) = 1\) and the elements \([u^* v x_j], \ldots, [u^* v x_{k_u}]\) are distinct in \( G_m \), it follows that \( k_v = k_u \). Similarly, we have \( k_v = k_u \).

4. A property of semicharacters of \( S_m \). It is well known and obvious that if \( H \) is a finite group and \( \chi \) 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 \( T = \{x, x^2, \ldots, x^l, \ldots, x^{l+k-1}\} \), 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 \( \{x^l, x^{l+1}, \ldots, x^{l+k-1}\} \) is the largest subgroup of \( T \). Its unit is the element \( x^{uk} \), where the integer \( u \) is defined by \( l \leq uk < l + k \). The general semicharacter of \( T \) is the function \( \chi \) whose value at \( x^h \) is \( \exp(2\pi i h j/k) \), where \( j = 0, 1, \ldots, k-1 \). For \( j = 1, 2, \ldots, k-1 \), the sum \( \sum_{h=1}^{k-1} \chi(x^h) \) is equal to
\[
\frac{1 - \exp\left(\frac{2\pi i (l + k) j}{k}\right)}{1 - \exp\left(\frac{2\pi i j}{k}\right)},
\]
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 \( \chi \) 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 \( V(\lambda_1, \ldots, \lambda_r) \) of 3.4 are pairwise disjoint and that their union is \( S_m \). We therefore need only show that \( \sum_{[x] \in V(\lambda_1, \ldots, \lambda_r)} \chi([x]) = 0 \) for all \( \{\lambda_1, \ldots, \lambda_r\} \). By 3.3, \( \chi \) assumes a value different from 1 somewhere on the group \( G_m \), so that \( \sum_{[x] \in G_m} \chi([x]) = 0 \). (Note that \( \chi \) on \( G_m \) is a character of the group \( G_m \).) Thus we have \( 0 = \sum_{[x] \in G_m} \chi([p_1^{x_1} \cdots p_r^{x_r}]) \chi([x]) = \sum_{[x] \in G_m} \chi([p_1^{x_1} \cdots p_r^{x_r}]) \chi([x]) = k \sum \chi([y]) \), where \([y] \) runs through \( V(\lambda_1, \ldots, \lambda_r) \).
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 $p_i = 2$. 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 $j = 1, \ldots, r$, let

\[ g_j = \text{a primitive root modulo } p_j^{p_j}, \text{ if } p_j \text{ is odd}; \]
\[ g_1 = 5 \text{ if } p_1 = 2; \]
\[ h_j = g_j + y_j p_j^{p_j} \text{ where } y_j \text{ is such that } h_j \equiv 1 \pmod{m/p_j^{p_j}}; \]
\[ h_0 = -1 + y_0 p_1^{p_1} \text{ where } y_0 \text{ is such that } h_0 \equiv 1 \pmod{m/p_1^{p_1}}; \]
\[ q_j = p_j + z_j p_j^{p_j} \text{ where } z_j \text{ is such that } q_j \equiv 1 \pmod{m/p_j^{p_j}}; \]

For $j = 1, \ldots, r, l = 1, \ldots, r, j \neq l$, and $p_l$ odd, let $k_{jl}$ be a positive integer such that $p_j \equiv g_j^{k_{jl}} \pmod{p_l^{p_l}}$.

For $j = 2, \ldots, r$ and $p_j = 2$ let

\[ k_{jl} \text{ be a positive integer such that } p_j \equiv (-1)^{p_j-1/2} g_j^{k_{jl}} \pmod{p_l^{p_l}}. \]

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

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

\[ a(x) \equiv g_j^{e_j(x)} \pmod{p_j^{p_j}}. \]

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

\[ e_1 = e_1(x) \text{ be any positive integer such that } \]
\[ a(x) \equiv (-1)^{e_1(x)\alpha_1 - 1/2} g_1^{e_1(x)} \pmod{p_1^{p_1}}. \]

For $\alpha_1 \geq 3$, $e_1(x)$ 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

\[ A(x) = \left( \prod_{j=2}^r h_0^{(p_j - 1/2)\beta_j} \right) \left( \prod_{l=1}^r \prod_{j \neq l} h_j^{p_j \beta_j} \right) \left( \prod_{j=1}^r q_j^{e_j} \right) h_0^{(\alpha - 1)/2} \left( \prod_{j=1}^r h_j^{e_j} \right). \]

If $m$ is odd, let

\[ A(x) = \left( \prod_{l=1}^r \prod_{j \neq l} h_j^{p_j \beta_j} \right) \left( \prod_{j=1}^r q_j^{e_j} \right) \left( \prod_{j=1}^r h_j^{e_j} \right). \]
If \( m \) is even, it is easy to see from 5.1 that

\[
(2) \quad A(x) \equiv \left( \prod_{j=2}^{r} (-1)^{(a-1)/2} g_{j}^{\beta_{j}} \right) \left( \prod_{j=2}^{r} g_{j}^{\beta_{j}k_{j}} \right) p_{1}^{\beta_{1}} (-1)^{(a-1)/2} g_{1}^{\xi_{1}} \pmod{p_{i}^{\xi_{i}}} \\
\equiv \left( \prod_{j=2}^{r} (-1)^{(a-1)/2} g_{j}^{\beta_{j}} \right) p_{1}^{\beta_{1}} (-1)^{(a-1)/2} g_{1}^{\xi_{1}} \\
\equiv \prod_{j=2}^{r} p_{j}^{\beta_{j}} a \equiv x \pmod{p_{i}^{\xi_{i}}},
\]

and, if \( n = 2, \ldots, r \),

\[
A(x) \equiv \prod_{j=2}^{r} g_{n}^{\beta_{j}k_{j}} \cdot p_{n}^{\beta_{n}} g_{n}^{\xi_{n}} \equiv \prod_{j=2}^{r} p_{j}^{\beta_{j}} \cdot p_{n}^{\beta_{n}} a \equiv x \pmod{p_{n}^{\xi_{n}}},
\]

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

If \( m \) is odd, then for \( n = 1, \ldots, r \), we have

\[
A(x) \equiv \prod_{j=1}^{r} g_{n}^{\beta_{j}k_{j}} \cdot p_{n}^{\beta_{n}} g_{n}^{\xi_{n}} \equiv \prod_{j=1}^{r} p_{j}^{\beta_{j}} \cdot p_{n}^{\beta_{n}} a \equiv x \pmod{p_{n}^{\xi_{n}}},
\]

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

5.3. Suppose that \( \chi \) is any semicharacter of \( S_{m} \). Let \( \psi \) be the function defined for all integers \( x \) by the relation \( \psi(x) = \chi([x]) \). Then \( \psi \) 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 \( \psi \) with these properties. As 5.2 shows, \( \psi \) is determined by its values on \( h_{0}, h_{1}, \ldots, h_{r} \) and \( q_{1}, \ldots, q_{r} \).

We now set down relations involving the \( h \)'s and \( q \)'s which restrict the values that \( \psi \) can assume on these integers.

5.4. If \( p_{j} \) is odd, then

\[
h_{j}^{\psi(p_{j}^{\alpha_{j}})} \equiv 1 \pmod{p_{j}^{\alpha_{j}}} , \quad h_{j}^{\psi(p_{j}^{\alpha_{j}})} \equiv 1 \pmod{m/p_{j}^{\alpha_{j}}};
\]

hence

\[
h_{j}^{\psi(p_{j}^{\alpha_{j}})} \equiv 1 \pmod{m}.
\]

Also,

\[
h_{0}^{2} \equiv 1 \pmod{p_{1}^{\alpha_{1}}} , \quad h_{0}^{2} \equiv 1 \pmod{m/p_{1}^{\alpha_{1}}};
\]

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 $p_i = 2$ and $\alpha_i = 1$ or 2, then

$$h_i = 5 \equiv 1 \pmod{p_i^{\alpha_i}}, \quad h_i = 1 \pmod{m/p_i^{\alpha_i}}; \text{ hence } h_i \equiv 1 \pmod{m}.$$ 

If $p_i = 2$ and $\alpha_i \geq 3$, then

$$h_i^{\alpha_i-2} \equiv 1 \pmod{p_i^{\alpha_i}}, \quad h_i^{\alpha_i-1} \equiv 1 \pmod{m/p_i^{\alpha_i}}; \text{ hence } h_i^{\alpha_i-2} \equiv 1 \pmod{m}.$$ 

(The first congruence on the line above is proved in [3], p. 81, Satz 125.)

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

$$q_j^{a_j} = 0, \quad q_j^{a_j}h_j = 0, \quad q_j^{a_j+1} \equiv 0 \pmod{p_j^{a_j}},$$

$$q_j^{a_j} = 1, \quad q_j^{a_j}h_j = 1, \quad q_j^{a_j+1} \equiv 1 \pmod{m/p_j^{a_j}}.$$ 

Therefore we have

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

Also, if $p_i = 2$, we have

$$q_i^{a_i} = 0, \quad q_i^{a_i}h_0 \equiv 0 \pmod{p_i^{a_i}},$$

$$q_i^{a_i} = 1, \quad q_i^{a_i}h_0 \equiv 1 \pmod{m/p_i^{a_i}}.$$ 

Therefore we have

$$q_i^{a_i}h_0 \equiv q_i^{a_i} \pmod{m}.$$ 

5.5 If $\psi$ is to be a function on the integers such that $\psi(x) = \chi([x])$ for some semicharacter $\chi$ of $S_m$, then the choices of the values of $\psi$ 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

$$\psi(h_j)^{\alpha_j(p_j^{a_j})} = 1 \text{ if } p_j \text{ is odd};$$

$$\psi(h_0) = \pm 1, \text{ and } \psi(h_0) = 1 \text{ if } \alpha_i = 1 \text{ and } p_i = 2;$$

$$\psi(h_i) = 1 \text{ if } p_i = 2 \text{ and } \alpha_i = 1 \text{ or } 2;$$

$$\psi(h_i)^{\alpha_i-2} = 1 \text{ if } p_i = 2 \text{ and } \alpha_i \geq 3.$$ 

Also we have

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

If $p_i = 2$, we have

$$\psi(q_i)^{a_i} = \psi(q_i)^{a_i}\psi(h_0).$$

The last two equalities give us:

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

and
ψ(q_i) \neq 0 \text{ implies } ψ(h_0) = 1 \text{ if } p_1 = 2.

5.6. To construct our functions ψ, we now choose numbers ω_o, ω_1, ⋯, ω_r and μ_1, ⋯, μ_r which are to be ψ(h_0), ψ(h_1), ⋯, ψ(h_r) and ψ(q_1), ⋯, ψ(q_r). The relations in 5.5 show that we must take these numbers such that:

- ω_j (when j = 1, ⋯, r and p_j is odd);
- ω_o = ± 1; ω_o = 1 if p_i = 2 and α_i = 1, or if m is odd;
- ω_1 = 1 if p_i = 2 and α_i = 1 or 2;
- ω_i^{2α_i-2} = 1 if p_i = 2 and α_i ≥ 3;
- μ_j = 0 or 1 if j = 1, ⋯, r;
- ω_j = 1 if μ_j = 1, j = 1, ⋯, r;
- ω_o = 1 if p_i = 2 and μ_i = 1.

Formulas (1_e) and (1_o) of 5.2 now require us to define ψ(x) for non-zero integers x as follows:

\begin{equation}
ψ(x) = \left( \prod_{j=2}^{r} \omega_o^{(p_j-1)\beta_j(x)/2} \right) \left( \prod_{l=1}^{r} \prod_{j=1}^{r} \omega_l^{\alpha_l \beta_j(x)} k_{jl} \right) \left( \prod_{j=1}^{r} \mu_j^{\gamma_j(x)} \right)
\end{equation}

- \omega_o^{α(x)-1/2} \left( \prod_{j=1}^{r} \omega_j^{\gamma_j(x)} \right) \text{ if } m \text{ is even};

\begin{equation}
ψ(x) = \left( \prod_{l=1}^{r} \prod_{j=1}^{r} \omega_l^{\beta_j(x) k_{jl}} \right) \left( \prod_{j=1}^{r} \mu_j^{\gamma_j(x)} \right) \left( \prod_{j=1}^{r} \omega_j^{\gamma_j(x)} \right) \text{ if } m \text{ is odd}.
\end{equation}

Finally, we define ψ(0) = ψ(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 ϕ(p_j) if p_j is odd, and e_1 is determined modulo p_1 x_1-2 if p_1 = 2 and α_1 ≥ 3. Since ω_j^{α_j x_1-2} = 1 if p_j is odd, ω_1^{α_1-1} = 1 if p_1 = 2 and α_1 ≥ 3, and ω_1 = 1 if p_1 = 2 and α_1 ≤ 2, we see that ψ is uniquely defined by the formulas (3_e) and (3_o).

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

Suppose first that x ≠ 0, y ≠ 0. Then we have

\begin{align*}
x &= \prod_{j=1}^{r} p_j^{β_j(x)} \cdot a(x), \quad y = \prod_{j=1}^{r} p_j^{β_j(y)} \cdot a(y), \quad xy = \prod_{j=1}^{r} p_j^{β_j(x)+β_j(y)} \cdot a(x)a(y).
\end{align*}

1 We take ω_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^φ = 1.
Therefore $a(xy) = a(x)a(y)$ and $\beta_j(xy) = \beta_j(x) + \beta_j(y)$ for $j = 1, \ldots, r$. Also we have
\[
g_{j}^{\beta_j(xy)} = a(xy) \equiv a(x)a(y) \equiv g_{j}^{\beta_j(x)}g_{j}^{\beta_j(y)} \equiv g_{j}^{\beta_j(x) + \epsilon_j(y)} \quad (\text{mod } p_i^{\alpha_i})
\]
if $p_i$ is odd. Since $g_j$ is a primitive root modulo $p_i^{\alpha_i}$ and $\omega_i^{\beta_j(p_i^{\alpha_i})} = 1$, it follows that $e_j(xy) \equiv e_j(x) + e_j(y) \pmod{\varphi(p_i^{\alpha_i})}$ and $\omega_i^{\beta_j(xy)} = \omega_i^{\beta_j(x)}\omega_i^{\beta_j(y)}$ if $p_i$ is odd ($j = 1, \ldots, r$). If $p_i = 2$, then $a(x)$ and $a(y)$ are odd, and
\[
a(xy) - 1 \equiv a(x) - 1 + a(y) - 1 \pmod{2}.
\]
Therefore we have
\[
\omega_i^{(a(xy)-1)/2} = \omega_i^{(a(x)-1)/2}\omega_i^{(a(y)-1)/2}
\]
for both admissible values of $\omega_i$. Furthermore,
\[
(-1)^{(a(xy)-1)/2}g_i^{\beta_1(xy)} = a(x)a(y)
\]
\[
\equiv (-1)^{(a(x)-1)/2}g_i^{\beta_1(x)}(-1)^{(a(y)-1)/2}g_i^{\beta_1(y)} \pmod{p_i^{\alpha_i}},
\]
if $p_i = 2$. Therefore we have
\[
g_i^{\beta_1(xy)} \equiv g_i^{\beta_1(x) + \epsilon_1(y)} \pmod{p_i^{\alpha_i}},
\]
if $p_i = 2$.

Hence, if $\alpha_i \geq 3$ and $p_i = 2$, we have $e_i(xy) \equiv e_i(x) + e_i(y) \pmod{p_i^{\alpha_i-2}}$, as follows from [3], p. 82, Satz 126 (recall that $g_i = 5$, $p_i = 2$). Hence
\[
\omega_i^{\beta_1(xy)} = \omega_i^{\beta_1(x)}\omega_i^{\beta_1(y)} \quad \text{if } \alpha_i \geq 3, p_i = 2.
\]
The last equality also holds if $\alpha_i \leq 2$ and $p_i = 2$, since $\omega_i = 1$ 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 $j = 1, \ldots, r$, 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
\[ \prod_{j=1}^{r} p_{j}^{\beta_{j}(x)} \cdot a(x) = \prod_{j=1}^{r} p_{j}^{\beta_{j}(y)} \cdot a(y) \pmod{m}. \]

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 \( \beta_{j}(x) > 0 \) \( (j = 1, \ldots, r) \) 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

\[ \psi(x) = \left( \prod_{l=1}^{r} \prod_{j=1}^{r} \omega_{l}^{\beta_{j}(x)^{k_{jl}}} \right) \left( \prod_{j=1}^{r} \omega_{0}^{\beta_{j}(x)} \right), \]

(4)

\[ \psi(y) = \left( \prod_{l=1}^{r} \prod_{j=1}^{r} \omega_{l}^{\beta_{j}(y)^{k_{jl}}} \right) \left( \prod_{j=1}^{r} \omega_{0}^{\beta_{j}(y)} \right). \]

(5)

If \( m \) is even and \( \beta_{1}(x) = 0 \), we have

\[ \psi(x) = \left( \prod_{j=1}^{r} \omega_{0}^{(\alpha_{j})/2} \beta_{j}(x)/2 \right) \left( \prod_{j=1}^{r} \omega_{0}^{\beta_{j}(x)^{k_{jl}}} \right) \omega_{0}^{(a(x) - 1)/2} \left( \prod_{j=1}^{r} \omega_{0}^{\beta_{j}(x)} \right), \]

(6)

\[ \psi(y) = \left( \prod_{j=1}^{r} \omega_{0}^{(\alpha_{j})/2} \beta_{j}(y)/2 \right) \left( \prod_{j=1}^{r} \omega_{0}^{\beta_{j}(y)^{k_{jl}}} \right) \omega_{0}^{(a(y) - 1)/2} \left( \prod_{j=1}^{r} \omega_{0}^{\beta_{j}(y)} \right). \]

(7)

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

\[ A(x) = A(y) \pmod{p_{n}^{\alpha_{n}}} \] for \( n = 1, \ldots, r \).

The congruence

\[ A(x) = \prod_{j=1}^{r} h_{n}^{\beta_{j}(x)^{k_{jn}}} \cdot q_{n}^{\alpha_{n}(x)} h_{n}^{e_{n}(x)} \pmod{p_{n}^{\alpha_{n}}} \]

holds if \( p_{n} \) is odd. To verify this, use (1c) and (1a) together with 5.1. Notice that for \( n = 1 \), we use only \((1a)\).

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

\[ \prod_{j=1}^{r} h_{n}^{\beta_{j}(x)^{k_{jn}}} \cdot h_{n}^{e_{n}(x)} = \prod_{j=1}^{r} h_{n}^{\beta_{j}(y)^{k_{jn}}} \cdot h_{n}^{e_{n}(y)} \pmod{p_{n}^{\alpha_{n}}} \]

if \( p_{n} \) is odd and \( \beta_{n}(x) = 0 \). This implies that

\[ \sum_{j=1}^{r} \beta_{j}(x)k_{jn} + e_{n}(x) \equiv \sum_{j=1}^{r} \beta_{j}(y)k_{jn} + e_{n}(y) \pmod{\varphi(p_{n}^{\alpha_{n}})}, \]

and

\[ \prod_{j=1}^{r} \omega_{n}^{\beta_{j}(x)^{k_{jn}}} \cdot \omega_{n}^{e_{n}(x)} = \prod_{j=1}^{r} \omega_{n}^{\beta_{j}(y)^{k_{jn}}} \cdot \omega_{n}^{e_{n}(y)}, \]

(10)
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

$$A(x) \equiv \left( \prod_{j=2}^{r} (\frac{1}{5} (\prod_{j=2}^{r} 5^{\beta_j(x)k_j}(-1)^{(\alpha(x)-1)/5}e_1'(x)}) \right) \mod 2^{\alpha_1}.$$\(\tag{11}\)

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

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

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

From this congruence, we find that

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

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

if $\alpha_1 \geq 2$, and

$$\sum_{j=2}^{r} \beta_j(x)k_j + e_1(x) \equiv \sum_{j=2}^{r} \beta_j(y)k_j + e_1(y) \mod 2^{\alpha_1 - 1}$$

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

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

if $\alpha_1 \geq 1$, and

$$\prod_{j=2}^{r} \omega_1^{(\beta_j(x)k_j)1} \cdot \omega_1^{(e_1(x))} = \prod_{j=2}^{r} \omega_1^{(\beta_j(y)k_j)1} \cdot \omega_1^{(e_1(y))}$$\(\tag{13}\)

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

$$\left( \prod_{n=1}^{r} \sum_{j=1}^{r} \omega_0^{(\beta_j(x)k_j)1} \right) \left( \prod_{n=1}^{r} \sum_{j=1}^{r} \omega_0^{(e_1(x))} \right) = \left( \prod_{n=1}^{r} \sum_{j=1}^{r} \omega_0^{(\beta_j(y)k_j)1} \right) \left( \prod_{n=1}^{r} \sum_{j=1}^{r} \omega_0^{(e_1(y))} \right).$$\(\tag{14}\)

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

For $p_j$ odd, the number of possible values of $\omega_j$ is $\varphi(p_j^{\mu_j})$ if $\mu_j = 0$ and 1 if $\mu_j = 1$. Hence this number is $\varphi(p_j^{\mu_j(1-\mu_j)})$. For $p_j = 2$, there are several cases to consider ($\mu_j = 0$ or 1, $\alpha_j = 1$, $\alpha_j = 2$, $\alpha_j \geq 3$). In each case, it is easy to see that the number of admissible pairs $(\omega_1, \omega_r)$ is $\varphi(2^{\mu_1(1-\mu_1)})$. Thus, for each sequence $(\mu_1, \cdots, \mu_r)$, the total number of sequences $(\omega_1, \omega_2, \cdots, \omega_r)$ is equal to

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

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

6. The structure of $X_m$.

6.1. Let $\chi$ and $\chi'$ 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 $\chi$ and $\chi'$, respectively. The product $\chi \chi'$ then has as its parameters

$$(1) \quad (\mu_1 \mu'_1, \cdots, \mu_r \mu'_r; \omega_0 \omega'_0, \omega_1 \omega'_1, \cdots, \omega_r \omega'_r).$$

Thus, all of the $\chi$'s in $X_m$ for which the $\mu$'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 $\mu$. 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 $\chi$ be in $X_m$ and let
χ have parameters (μ₁, ⋯, μᵦ; ω₀, ω₁, ⋯, ωᵦ). For m odd and j = 0, 1, ⋯, r or m even and j = 0, 2, 3, ⋯, r, let wᵢ be any integer such that \( \omega_j = \exp(2\pi i w_j/\varphi(p^r_{(j)})). \) For m even and \( \alpha_i = 1 \) or 2, let \( w_i = 0; \) for m even and \( \alpha_i \geq 3, \) let \( w_i \) be any integer such that \( \omega_i = \exp(2\pi i w_i/2^{a_i-2}). \)

We now define the mapping

\[
(2) \quad \chi \to \tau(\chi) = \left[ h_0^{\omega_0(1-\mu_1)} \prod_{j=1}^{r} (h_j \omega_j^{(1-\mu_j)} q_j^{\mu_j}) \right],
\]

which carries \( X_m \) into \( S_m. \) Evidently \( \tau \) is single-valued.

6.4 Theorem. The mapping \( \tau \) is one-to-one.

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

\[
(3) \quad h_0^{w_0(1-\mu_1)} \prod_{j=1}^{r} (h_j \omega_j^{(1-\mu_j)} q_j^{\omega_j \mu_j}) \equiv h_0^{w'_0(1-\mu_1')} \prod_{j=1}^{r} (h_j \omega'_j^{(1-\mu'_j)} q_j^{\omega'_j \mu'_j}) \pmod{m}.
\]

This congruence, along with 5.1, implies that

\[
h_0^{w_0(1-\mu_1)} h_1^{\omega_1(1-\mu_1)} p_1^{\omega_1 \mu_1} \equiv h_0^{w'_0(1-\mu_1')} h_1^{\omega'_1(1-\mu_1')} p_1^{\omega'_1 \mu_1'} \pmod{p_1^{n_1}}
\]

for \( l = 1, \ldots, r \) and \( p_i \) odd. Since \( (h_1, p_i) = 1, \) and \( \mu_1 \) and \( \mu_1' \) are 0 or 1, it is obvious that \( \mu_1 = \mu_1'. \) If \( \mu_1 = \mu_1' = 1, \) then from 5.6, we have \( \omega_1 = \omega_1' = 1. \) If \( \mu_1 = \mu_1' = 0, \) then \( h_0^{w_0} \equiv h_0^{w'_0} \pmod{p_1^{n_1}}, \) so that \( w_1 \equiv w'_1 \pmod{\varphi(p_1^{n_1})} \) and hence \( \omega_1 = \omega_1'. \)

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

\[
(4) \quad h_0^{w_0(1-\mu_1)} h_1^{w_1(1-\mu_1)} p_1^{\omega_1 \mu_1} \equiv h_0^{w'_0(1-\mu_1')} h_1^{w'_1(1-\mu_1')} p_1^{\omega'_1 \mu_1'} \pmod{p_1^{n_1}}.
\]

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 \( \alpha_i = 1, \) then \( \omega_0 = \omega'_0 = 1, \) also by 5.6. If \( \alpha_i = 2 \) 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 \( \alpha_i \geq 3 \) and \( \mu_1 = \mu_1' = 0, \) then we have \( (-1)^{w_0} 2^{w_1} = (-1)^{w'_0} 2^{w'_1} \pmod{2^{a_i-2}}. \) Hence \( \omega_0 = \omega'_0 \) and \( \omega_1 = \omega_1'. \) Therefore \( \tau \) is one-to-one.

6.5. The set \( \tau(X_m) \) consists of all the elements \( [p_1^{n_1} \cdots p_r^{n_r} a] \) of \( S_m \) for which \( \delta_j = 0 \) or \( \alpha_j, \) and \( (a, m) = 1. \) It is evident from (2) that \( \tau(X_m) \) is contained in the set \( \{[p_1^{n_1} \cdots p_r^{n_r} a]\}. \) The reverse inclusion is established by a routine examination of cases, which we omit.

6.6. The mapping \( \tau \) plainly defines a new multiplication in \( \tau(X_m): \)

\[
\tau(\chi) \ast \tau(\chi') = \tau(\chi').
\]

Every residue class \( \tau(\chi) \) contains a number

\[
x = h_0^{\omega_0(1-\mu_1)} \prod_{j=1}^{r} (h_j \omega_j^{(1-\mu_j)} q_j^{\omega_j \mu_j}).
\]
If \( x' \) is another number of this form, then it can be shown that \([x]*[x']\) is equal to \([xx' / \prod q_j^{r_j}]\), where the product \( \prod q_j^{r_j} \) is taken over all \( j, j = 1, \ldots, r \), for which \( p_j | xx' \). We omit the details.

**LITERATURE**


THE UNIVERSITY OF WASHINGTON
Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 2120 Oxford Street, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.
M. Altman, **An optimum cubically convergent iterative method of inverting a linear bounded operator in Hilbert space** ........................................... 1107

Nesmith Cornett Ankeny, **Criterion for rth power residuacity** .................................................. 1115

Julius Rubin Blum and David Lee Hanson, **On invariant probability measures I** .......................... 1125

Frank Featherstone Bonsall, **Positive operators compact in an auxiliary topology** .................. 1131

Billy Joe Boyer, **Summability of derived conjugate series** ...................................................... 1139

Delmar L. Boyer, **A note on a problem of Fuchs** ................................................................. 1147

Hans-Joachim Bremermann, **The envelopes of holomorphy of tube domains in infinite dimensional Banach spaces** .......................................................... 1149

Andrew Michael Bruckner, **Minimal superadditive extensions of superadditive functions** ................................................................. 1155

Billy Finney Bryant, **On expansive homeomorphisms** ............................................................... 1163

Jean W. Butler, **On complete and independent sets of operations in finite algebras** ............... 1169

Lucien Le Cam, **An approximation theorem for the Poisson binomial distribution** ............. 1181

Paul Civin, **Involutions on locally compact rings** ................................................................. 1199

Earl A. Coddington, **Normal extensions of formally normal operators** ................................. 1203

Jacob Feldman, **Some classes of equivalent Gaussian processes on an interval** ................. 1211

Shaul Foguel, **Weak and strong convergence for Markov processes** .................................. 1221

Martin Fox, **Some zero sum two-person games with moves in the unit interval** ................. 1235

Robert Pertsch Gilbert, **Singularities of three-dimensional harmonic functions** ............... 1243

Branko Grünbaum, **Partitions of mass-distributions and of convex bodies by hyperplanes** .... 1257

Sidney Morris Harmon, **Regular covering surfaces of Riemann surfaces** ............................ 1263

Edwin Hewitt and Herbert S. Zuckerman, **The multiplicative semigroup of integers modulo m** ................................................................................................................ 1291

Paul Daniel Hill, **Relation of a direct limit group to associated vector groups** .................. 1309

Calvin Virgil Holmes, **Commutator groups of monomial groups** ........................................ 1313

James Fredrik Jakobsen and W. R. Utz, **The non-existence of expansive homeomorphisms on a closed 2-cell** ........................................................................................................ 1319

John William Jewett, **Multiplication on classes of pseudo-analytic functions** .................. 1323

Helmut Klingen, **Analytic automorphisms of bounded symmetric complex domains** ........ 1327

Robert Jacob Koch, **Ordered semigroups in partially ordered semigroups** ......................... 1333

Marvin David Marcus and N. A. Khan, **On a commutator result of Taussky and Zassenhaus** .... 1337

John Glen Marica and Steve Jerome Bryant, **Unary algebras** ................................................. 1347

Edward Peter Merkes and W. T. Scott, **On univalence of a continued fraction** ................. 1361

Shu-Teh Chen Moy, **Asymptotic properties of derivatives of stationary measures** .......... 1371

John William Neuberger, **Concerning boundary value problems** ....................................... 1385

Edward C. Posner, **Integral closure of differential rings** ..................................................... 1393

Marian Reichaw-Reichbach, **Some theorems on mappings onto** ........................................ 1397

Marvin Rosenblum and Harold Widom, **Two extremal problems** ........................................ 1409

Morton Lincoln Slater and Herbert S. Wilf, **A class of linear differential-difference equations** ............................................................................................................. 1419

Charles Robson Storey, Jr., **The structure of threads** ............................................................ 1429

J. François Treves, **An estimate for differential polynomials in \( \frac{\partial}{\partial z}, \ldots, \frac{\partial}{\partial z_n} \)** 1447

J. D. Weston, **On the representation of operators by convolutions integrals** ....................... 1453

James Victor Whittaker, **Normal subgroups of some homeomorphism groups** .................. 1469