SEMICHARACTERS OF THE MULTIPLICATIVE SEMIGROUP OF INTEGERS MODULO m

By BOHUMÍR PARÍZEK and ŠTEFAN SCHWARZ, Bratislava

Let S be a commutative semigroup. A semicharacter of S is a complex-valued multiplicative function defined on S that is not identically zero.

Let $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $\alpha_j \geqq 1$, be the decomposition of the integer $m > 1$ into distinct primes. 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 $[x][y] = [xy]$, $S(m)$ is a semigroup. The subgroup of $S(m)$ containing all residue classes $[x]$ such that $(x, m) = 1$ is denoted by $G(m)$.

The purpose of this paper is to find all semicharacters χ of $S(m)$, especially also to compute $\chi([x])$ explicitly in terms of the integer x for an arbitraty semicharacter χ of $S(m)$.

The general theory of semicharacters of a finite (and some types of infinite) commutative semigroups has been given independently by Hewitt and Zuckerman ([1]) and by one of us ([5]). The present paper is independent of the general theory contained in [1] and [5].

Semicharacters of $S(m)$ are treated in a forthcomming paper of Hewitt and Zuckerman ([2]), which the authors kindly gave to our disposal. Our presentation is based on the results of [4], where an explicit decomposition of $S(m)$ into a direct product of subsemigroups of prime power order is given. For convenience of the reader these results are shortly reproduced below.

1.

It is easy to see that $S(m)$ contains 2^r idempotents (including [0] and [1]). An idempotent $[e] \neq [1]$ is called maximal if the relation $[e][f] = [e]$, in which $[f] \neq [1]$ and $[f]$ is an idempotent, implies $[e] = [f]$.

In [3] we proved that $S(m)$ contains exactly r maximal idempotents. Each of them is of the form $[e_j] = [p_j^{\alpha_j} a_j]$, where $[a_j]$ is an element $\in G(m)$.*

The following is the main result of [4]:

* $[a_j] \in G(m)$ is, in general, not uniquely determined by $[e_j]$ and under suitable conditions there may exist also an $[b_j] \in S(m) - G(m)$ with the property $[e_j] = [p_j^{\alpha_j} b_j]$.

Theorem 1. *Let $[e_j]$ be a maximal idempotent of $S(m)$. Denote $T_j = \{[x] \mid [x] \in S(m), [x][e_j] = [e_j]\}$. Then $S(m)$ can be written in the form of a direct product*

$$S(m) = T_1 \, . \, T_2 \, \dots \, T_r. \tag{1}$$

Denote further $G_j = \{[x] \mid [x] \in G(m), [x]\,[e_j] = [e_j]\}$. Then $G(m)$ can be written as a direct product of the r subgroups

$$G(m) = G_1 \, . \, G_2 \, . \, \dots \, . \, G_r.$$

The semigroup T_j contains exactly $p_j^{\alpha_j}$ different elements: $T_j = \left\{\left[e_j + k\frac{m}{p_j^{\alpha_j}}\right] \middle| \, 0 \leqq k \leqq p_j^{\alpha_j} - 1\right\}$. The group G_j contains $\varphi(p_j^{\alpha_j}) = p_j^{\alpha_j} - p_j^{\alpha_j - 1}$ different elements: $G_j = \left\{\left[e_j + k\frac{m}{p_j^{\alpha_j}}\right] \middle| \, 0 \leqq k \leqq p_j^{\alpha_j} - 1, \, (k, p_j) = 1\right\}$.

It follows directly from the definition of T_j that $[e_j]$ is the zero element of the semigroup T_j. (But of course if $r > 1$ it is not a zero element of the whole semigroup $S(m)$.)

Further, since $[1]\,[e_j] = [e_j]$, T_j (and G_j) contains the element $[1]$, which is the unity element of $S(m)$, T_j and G_j.

Clearly $G_j \subset T_j$ and $G_j \neq T_j$. G_j is the largest group contained in T_j and having $[1]$ as the unity element. This follows from the following considerations. Let be $[b] \in T_j - G_j$. We then can write $[b] = \left[e_j + k\frac{m}{p_j^{\alpha_j}}\right]$ with $(k, p_j) > 1$.

Now, since any product containing $[e_j]$ and $\left[\frac{m}{p_j^{\alpha_j}}\right]$ is $[0]$, we have

$$[b]^\rho = \left[e_j + k\frac{m}{p_j^{\alpha_j}}\right]^\rho = \left[e_j + k^\rho\left(\frac{m}{p_j^{\alpha_j}}\right)^\rho\right] \quad \text{for every integer } \rho \geqq 1. \tag{2}$$

If especially $\rho = \alpha_j$, we have $[b]^\rho = [e_j]$. By other words: Every element $[b] \in T_j - G_j$ considered as an element of the semigroup T_j is nilpotent and cannot be contained in a group containing [1] as the unity element.

This argument shows at the same time that T_j cannot contain idempotents different from [1] and $[e_j]$.

Remark 1. The semigroup T_j is isomorphic to the semigroup $S(p_j^{\alpha_j})$. To prove this denote the residue class (mod $p_j^{\alpha_j}$) containing x by $\langle x \rangle$ and consider the mapping

$$\left[e_j + k\frac{m}{p_j^{\alpha_j}}\right] \in T_j \to \left\langle k\frac{m}{p_j^{\alpha_j}}\right\rangle \in S(p_j^{\alpha_j}).$$

It is easily verified that this is an isomorphism of T_j to $S(p_j^{\alpha_j})$, which carries $G_j \subset T_j$ to the group $G(p_j^{\alpha_j}) \subset S(p_j^{\alpha_j})$. (See [4].) We shall use this isomorphism to establish the structure of T_j and G_j.

Remark 2. We should like to note the following remark of a computational character. To find in concrete cases the maximal idempotents $[e_j]$ we proceed in the following manner: Since $[e_j] = [p_j^{\alpha_j} a_j]$, we have

$$p_j^{\alpha_j} a_j \equiv p_j^{2\alpha_j} a_j^2 \qquad (\text{mod } p_1^{\alpha_1} \dots p_j^{\alpha_j} \dots p_r^{\alpha_r})$$

and – since $(a_j, m) = 1$ –

$$p_j^{\alpha_j} a_j \equiv 1 \qquad \left(\text{mod } \frac{m}{p_j^{\alpha_j}}\right).$$

This congruence defines $a_j \left(\text{mod } \frac{m}{p_j^{\alpha_j}}\right)$ uniquely. Hence e_j is uniquely determined modulo m.

To find the components of any element $[x] \in S(m)$ in the decomposition (1) we proceed as follows: Every $[x] \in S(m)$ can be uniquely written in the form

$$[x] = \prod_{j=1}^{r}\left[e_j + k_j(x)\frac{m}{p_j^{\alpha_j}}\right], \tag{3}$$

where $k_j(x)$ is an integer satisfying $0 \leqq k_j(x) \leqq p_j^{\alpha_j} - 1$. Since $[e_1 e_2 \cdots e_r] = [0]$, $\left[e_j\frac{m}{p_j^{\alpha_j}}\right] = [0]$ and $\left[\frac{m}{p_j^{\alpha_j}} \cdot \frac{m}{p_i^{\alpha_i}}\right] = [0]$ for $i \neq j$, we obtain by multiplying the brackets on the right:

$$[x] = \left[k_1(x)\frac{m}{p_1^{\alpha_1}} e_2 e_3 \dots e_r + k_2(x)\frac{m}{p_2^{\alpha_2}} e_1 e_3 \dots e_r + \dots + k_r(x)\frac{m}{p_r^{\alpha_r}} e_1 e_2 \dots e_{r-1}\right].$$

Taking the last relation (mod $p_j^{\alpha_j}$) we get

$$x \equiv k_j(x)\frac{m}{p_j^{\alpha_j}} e_1 \dots e_{j-1} e_{j+1} \dots e_r \qquad (\text{mod } p_j^{\alpha_j}).$$

This linear congruence defines $k_j(x)$ (mod $p_j^{\alpha_j}$) uniquely.

2.

For further purposes we mention the following known fact: If a semigroup S with a unity element can be written as a direct product of subsemigroups $S = S_1 \, . \, S_2$ (S_1, S_2 containing unity elements) and χ is a semicharacter of S, then χ induces on S_1 and S_2 semicharacters χ_1, χ_2 of S_1, S_2 respectively and if $x = x_1 \, . \, x_2$ ($x_1 \in S_1$, $x_2 \in S_2$), $\chi(x) = \chi_1(x_1)\,\chi_2(x_2)$ holds. Conversely, if ψ_1, ψ_2 are semicharacters of S_1 and S_2 and $x = x_1 \, . \, x_2$ ($x_i \in S_i$), then $\psi(x) = \psi_1(x_1)\,\psi_2(x_2)$ is a semicharacter of S. (An explicit proof of this statement is given in a slightly other form in [6], Theorem 5,1.)

To describe the semicharacters of $S(m)$ it is sufficient to find the semicharacters of each of the subsemigroups T_j.

We recall that by the unity semicharacter of a semigroup S we denote the function which is identically 1 on S. The unity semicharacter of T_j will be denoted by $\chi_0^{(j)}$.

Lemma 1. *Let χ be any semicharacter of T_j, which is not the unity semicharacter $\chi_0^{(j)}$ of T_j. Then for every $[b] \in T_j - G_j$ we have $\chi([b]) = 0$.*

Proof. We have necessarily $\chi([e_j]) = 0$. For otherwise $[x][e_j] = [e_j]$ for every $[x] \in T_j$ would imply $\chi([x]) \cdot \chi([e_j]) = \chi([e_j])$, hence $\chi([x]) = 1$ for every $[x] \in T_j$, contrary to the assumption.

If $[b] \in T_j - G_j$, we have as above $[b]^{\alpha_j} = [e_j]$, hence $\{\chi([b])\}^{\alpha_j} = \chi([e_j]) = 0$, therefore $\chi([b]) = 0$, q. e. d.

If χ is any semicharacter of T_j, χ induces a semicharacter on the group G_j. We have $\chi([1]) = 1$. For $\chi([1]) = \chi([1]^2) = \chi([1]) \cdot \chi([1])$ implies $\chi([1])\{\chi([1]) - 1\} = 0$, hence either $\chi([1]) = 0$ or $\chi([1]) = 1$. The first possibility cannot occur since $\chi([1]) = 0$ would imply $\chi([x]) = \chi([x])\,\chi([1]) = 0$ for every $[x] \in T_j$, contrary to the definition of a semicharacter. By other words: χ induces on G_j a character of G_j in the usual sense (used in the theory of groups).

With respect to Lemma 1 we can say that if χ is not the unity semicharacter of T_j, it is of the form:

$$\chi([x_j]) = \begin{cases} 0 & \text{for } [x_j] \in T_j - G_j, \\ \psi([x_j]) & \text{for } [x_j] \in G_j, \end{cases}$$

where ψ is a character of the group G_j.

Conversely, let ψ be a character of the group G_j and define the function χ by the statement:

$$\chi([x_j]) = \begin{cases} 0 & \text{for } [x_j] \in T_j - G_j, \\ \psi([x_j]) & \text{for } [x_j] \in G_j. \end{cases}$$

We show that χ is a semicharacter of T_j, i. e.

$$\chi([x_j y_j]) = \chi([x_j]) \cdot \chi([y_j]) \tag{4}$$

for every couple $[x_j]$, $[y_j] \in T_j$. If both $[x_j]$, $[y_j]$ belong to G_j the relation (4) holds with respect to the multiplicative property of the function ψ on G_j. To prove our statement it is sufficient to show that if at least one of the elements $[x_j]$, $[y_j]$ belongs to $T_j - G_j$ so does the product $[x_j y_j]$. (For then we have zeros on both sides of the relation (4).) Let be $[x_j] \in T_j - G_j$, $[y_j] \in T_j$. It follows from the relation (2) proved above that there is an integer $\rho([x_j]) \geqq 1$ such that $[x_j]^{\rho([x_j])} = [e_j]$. But then

$$\{[x_j y_j]\}^{\rho([x_j])} = [x_j]^{\rho([x_j])} \cdot [y_j]^{\rho([x_j])} = [e_j]\,[y_j]^{\rho([x_j])} = [e_j].$$

(The last relation is a consequence of the fact that $[e_j]$ is the zero element of T_j.) The relation $\{[x_j y_j]\}^{\rho([x_j])} = [e_j]$ implies $[x_j y_j] \in T_j - G_j$.

Summarily we proved:

Lemma 2. *Every semicharacter χ of the semigroup T_j different from the unity semicharacter of T_j is of the form*

$$\chi([x_j]) = \begin{cases} 0 & \text{for } [x_j] \in T_j - G_j, \\ \psi([x_j]) & \text{for } [x_j] \in G_j, \end{cases}$$

and conversely. Hereby ψ is a character of the group G_j.

Since the group G_j has $p_j^{\alpha_j} - p_j^{\alpha_j - 1}$ distinct characters, we conclude that T_j has $p_j^{\alpha_j} - p_j^{\alpha_j - 1} + 1$ distinct semicharacters (including the unity semicharacter $\chi_0^{(j)}$). With respect to the fact mentioned at the beginning of this section we get the result:

Theorem 2. *The semigroup $S(m)$ has exactly $\prod_{j=1}^{r} (1 + p_j^{\alpha_j} - p_j^{\alpha_j - 1})$ distinct semicharacters.*

3.

In the case m even we will take in the following always $p_1 = 2$.

To find all semicharacters of T_j we have to distinguish two cases.

A. Suppose first that either $p_j > 2$ is an odd prime, or $p_j^{\alpha_j} = 2$, or $p_j^{\alpha_j} = 4$.

The group $G_j = \left\{\left[e_j + k\dfrac{m}{p_j^{\alpha_j}}\right] \middle| 0 \leqq k < p_j^{\alpha_j}, (k, p_j) = 1\right\}$, being isomorphic to $G(p_j^{\alpha_j})$, is a cyclic group of order $\varphi(p_j^{\alpha_j})$. There exists therefore an element $k = y_j$ such that $[g_j] = \left[e_j + y_j \dfrac{m}{p_j^{\alpha_j}}\right]$ is a generating element of G_j. Hence to every $[x_j] \in G_j$ there is an uniquely determined integer $\rho_j([x_j])$, $0 < \rho_j([x_j]) \leqq \varphi(p_j^{\alpha_j})$ such that $[x_j] = [g_j]^{\rho_j([x_j])}$.

Any character ψ of G_j is completely described by knowing the value $\psi([g_j])$. Denote $\omega_j = \exp \dfrac{2\pi i}{\varphi(p_j^{\alpha_j})}$. The semicharacters of T_j different from the unity semicharacter $\chi_0^{(j)}$ are determined by

$$\chi_b^{(j)}([g_j^{\rho_j([x_j])}]) = \begin{cases} 0 & \text{for } [x_j] \in T_j - G_j \\ \omega_j^{b\rho_j([x_j])} & \text{for } [x_j] \in G_j \end{cases}$$

$$(b = 1, 2, \ldots, \varphi(p_j^{\alpha_j})).$$

To be able to distinguish between the characters $\chi_b^{(j)}$ and $\chi_0^{(j)}$ we have to consider the value of $\chi^{(j)}$ not only on $[g_j]$ but also on $[e_j]$. By Lemma 1 if $\chi^{(j)}([e_j]) = 1$, then $\chi^{(j)}([g_j]) = 1$. Hence:

Lemma 3a. *If the order of T_j is $p_j^{\alpha_j}$ and either p_j is odd, or $p_j^{\alpha_j} = 2$, or $p_j^{\alpha_j} = 4$, a semicharacter $\chi^{(j)}$ is completely given by prescribing $\chi^{(j)}([e_j])$ and $\chi^{(j)}([g_j])$ with the restriction that $\chi^{(j)}([e_j]) = 1$ implies $\chi^{(j)}([g_j]) = 1$. The admissible values of $\chi^{(j)}([g_j])$ are the numbers $1, \omega_j, \omega_j^2, \ldots, \omega^{\varphi(p_j^{\alpha_j}) - 1}$.*

All characters of T_j are schematically given by the table:

	$[e_j]$	$[g_j]$
$\chi_0^{(j)}$	1	1
$\chi_1^{(j)}$	0	ω_j
$\chi_2^{(j)}$	0	ω_j^2
$\vdots$	$\vdots$	$\vdots$
$\chi_{\varphi(p_j^{\alpha_j})}^{(j)}$	0	1

B. Suppose next that $p_1 = 2$ and $\alpha_1 \geqq 3$, i. e. $p_1^{\alpha_1} = 2^{\alpha_1} \geqq 8$. Consider the isomorphic image of G_1, i. e. $G(2^{\alpha_1})$. It is well known that the group $G(2^{\alpha_1})$ is not cyclic, but to every element $\langle a \rangle \in G(2^{\alpha_1})$ there is an integer τ such that $\langle a \rangle = \left\langle (-1)^{\frac{a-1}{2}} 5^{\tau} \right\rangle$ with $0 \leqq \tau < 2^{\alpha_1 - 2}$. Denote $\omega_1 = \exp \frac{2\pi i}{2^{\alpha_1 - 2}}$. The characters ψ_t of $G(2^{\alpha_1})$ are determined by the values of ψ_t on $\langle -1 \rangle$ and $\langle 5 \rangle$:

	$\langle -1 \rangle$	$\langle 5 \rangle$
ψ_1	-1	ω_1
ψ_2	1	ω_1
ψ_3	-1	ω_1^2
ψ_4	1	ω_1^2
$\vdots$		
$\psi_{2^{\alpha_1-1}-1}$	-1	1
$\psi_{2^{\alpha_1}-1}$	1	1

Consider now the isomorphism

$$\left[e_1 + k\frac{m}{2^{\alpha_1}}\right] \in G_1 \leftrightarrow \left\langle k\frac{m}{2^{\alpha_1}} \right\rangle \in G(2^{\alpha_1})$$

($k = 1, 3, 5, \ldots, 2^{\alpha_1} - 1$). Find integers z_1 and z_2, $1 \leqq z_1 \leqq 2^{\alpha_1} - 1$, $1 \leqq z_2 \leqq$ $\leqq 2^{\alpha_1} - 1$ such that $z_1 \frac{m}{2^{\alpha_1}} \equiv -1 \pmod{2^{\alpha_1}}$ and $z_2 \frac{m}{2^{\alpha_1}} \equiv 5 \pmod{2^{\alpha_1}}$ and denote

$$[\tilde{g}_0] = \left[e_1 + z_1\frac{m}{2^{\alpha_1}}\right], \quad [\tilde{g}_1] = \left[e_1 + z_2\frac{m}{2^{\alpha_1}}\right].$$

Then $[\tilde{g}_0]$, $[\tilde{g}_1]$ are $\in T_1$ and they are the images of $\langle -1 \rangle$ and $\langle 5 \rangle$ in T_1. We have the following

Lemma 3b. *If $p_1 = 2$ and $p_1^{\alpha_1} \geqq 8$, then a semicharacter $\chi^{(1)}$ of T_1 is uniquely determined by the values of $\chi^{(1)}$ on the elements $[e_1]$, $[\tilde{g}_0]$, $[\tilde{g}_1]$. Hereby $\chi^{(1)}([e_1])$ takes the values 0 or 1, $\chi^{(1)}([\tilde{g}_0])$ takes the values ± 1 and $\chi^{(1)}([\tilde{g}_1])$ takes the values $1, \omega_1, \omega_1^2, \ldots, \omega_1^{2^{\alpha_1-2}-1}$, where $\omega_1 = \exp\frac{2\pi i}{2^{\alpha_1-2}}$, with the restriction that $\chi^{(1)}([e_1]) = 1$ implies $\chi^{(1)}([\tilde{g}_0]) = \chi^{(1)}([\tilde{g}_1]) = 1$.*

The following table indicates a complete set of characters of T_1:

	$[e_1]$	$[\tilde{g}_0]$	$[\tilde{g}_1]$
$\chi_0^{(1)}$	1	1	1
$\chi_1^{(1)}$	0	-1	ω
$\chi_2^{(1)}$	0	1	ω
$\chi_3^{(1)}$	0	-1	ω^2
$\chi_4^{(1)}$	0	1	ω^2
$\vdots$			
$\chi_{2^{\alpha_1-1}-1}^{(1)}$	0	-1	1
$\chi_{2^{\alpha_1}-1}^{(1)}$	0	1	1

4.

Let now be m as above and decompose $S(m)$ into the direct product $S(m) = T_1 . T_2 . \ldots . T_r$. If $\chi^{(j)}$ is any character of T_j, then $\chi = \chi^{(1)} . \chi^{(2)} \ldots . \chi^{(r)}$ is a character of $S(m)$. If the $\chi^{(j)}$ -s (for $j = 1, 2, \ldots, r$) run independently through all characters $\chi_0^{(j)}, \chi_1^{(j)}, \ldots, \chi_{\varphi(p_j^{\alpha_j})}^{(j)}$, we get all characters of $S(m)$.

Suppose first that either

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \tag{5}$$

or

$$m = 2p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \tag{6}$$

or

$$m = 4p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \tag{7}$$

and $p_1, p_2, \ldots, p_r$ are odd primes and $\alpha_1 \alpha_2 \ldots \alpha_r > 0$.

In this case every $\chi^{(j)}$ depends on two „parameters" and with respect to the foregoing considerations we can state the following

Theorem 3a. *If m is an integer of the form (5), or (6), or (7), we get every semicharacter of $S(m)$ by prescribing its values on*

$$[e_1], [g_1], [e_2], [g_2], \dots, [e_r], [g_r].$$

Hereby $\chi([e_j])$ takes the values 0 or 1, $\chi([g_j])$ takes any of the values $1, \omega_j, \omega_j^2, \dots, \omega_j^{\varphi(p_j^{\alpha_j})-1}$, where $\omega_j = \exp \frac{2\pi i}{\varphi(p_j^{\alpha_j})}$, with the restriction that if for a fixed j we have $\chi([e_j]) = 1$, we must prescribe also $\chi([g_j]) = 1$.

Remark. In the case (6) $\chi([g_1]) = 1$ (since $\omega_1 = 1$). In the case (7) $\chi([g_1])$ is either 1, or -1 (since $\omega_1 = -1$).

In the case $p_1 = 2$ and $\alpha_1 \geqq 3$ the semicharacters of T_1 depend on three „parameters" and we have:

Theorem 3b. *Let be $m = 2^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $\alpha_1 \geqq 3$, $\alpha_2 \alpha_3 \dots \alpha_r > 0$, and $p_2, p_3, \dots, p_r$ are odd primes. Any semicharacter of $S(m)$ is determined by prescribing its values on*

$$[e_1], [g_0], [\tilde{g}_1], [e_2], [g_2], \dots, [e_r], [g_r].$$

Hereby $\chi([e_j])$ $(j = 1, 2, \dots, r)$ is either 0 or 1; $\chi([g_0])$ is either -1 or 1; $\chi([\tilde{g}_1])$ is one of the numbers $1, \omega_1, \dots, \omega_1^{2^{\alpha_1-2}-1}$, where $\omega_1 = \exp \frac{2\pi i}{2^{\alpha_1 - 2}}$; for $j \geqq 2$ $\chi([g_j])$ is one of the numbers $1, \omega_j, \omega_j^2, \dots, \omega_j^{\varphi(p_j^{\alpha_j})-1}$, $\omega_j = \exp \frac{2\pi i}{\varphi(p_j^{\alpha_j})}$, and the choice of the values of χ is restricted by the requirement that if $\chi([e_1]) = 1$, we have also $\chi([g_0]) = \chi([\tilde{g}_1]) = 1$ and if for $j \geqq 2$ $\chi([e_j]) = 1$, we have also $\chi([g_j]) = 1$.

5.

It is also possible to compute the values of $\chi([x])$ – in some sense – explicitly in terms of the integer x.

A. Suppose first that $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $p_1^{\alpha_1}$ is either odd, or $p_1^{\alpha_1} = 2$, or $p_1^{\alpha_1} = 4$.

Let χ be a fixed chosen semicharacter of $S(m)$. For $j = 1, 2, \dots, r$ denote $\chi([e_j]) = \mu_j$, $\chi([g_j]) = \omega_j^{l_j}$, where μ_j, $\omega_j^{l_j}$ are determined by χ in accordance with Theorem 3a; hence $\mu_j = 0$ or 1, and if $\mu_j = 1$, we have $\chi([g_j]) = 1$. The semicharacter χ induces on T_j a semicharacter of T_j, which we shall denote by $\chi^{(j)}$.

By Theorem 1 every $[x] \in S(m)$ can be written in the form

$$[x] = \left[e_1 + k_1(x) \frac{m}{p_1^{\alpha_1}}\right]\left[e_2 + k_2(x) \frac{m}{p_2^{\alpha_2}}\right] \dots \left[e_r + k_r(x) \frac{m}{p_r^{\alpha_r}}\right]. \tag{8}$$

The numbers $k_1(x), k_2(x), \dots, k_r(x)$ are uniquely determined by $[x]$ and the requirement $0 \leqq k_j(x) \leqq p_j^{\alpha_j} - 1$.

If $(k_j(x), p_j) = 1$, we have $[x_j] = \left[e_j + k_j(x) \frac{m}{p_j^{\alpha_j}}\right] \in G_j$ and $[x_j] = [g_j]^{\rho_j(x)}$ with $0 < \rho_j(x) \leqq \varphi(p_j^{\alpha_j})$.

If $(k_j(x), p_j) = p_j$, we have $[x_j] = \left[e_j + k_j(x) \frac{m}{p_j^{\alpha_j}}\right] \in T_j - G_j$.

For $j = 1, 2, \dots, r$ define the following function:

$$\Phi_j(x) = \begin{cases} \mu_j & \text{if } (k_j(x), p_j) > 1, \\ \mu_j + (1 - \mu_j) \cdot \omega_j^{b_j \rho_j(x)} & \text{if } (k_j(x), p_j) = 1. \end{cases}$$

If $\mu_1 = 1$, we have $\Phi_j(x) = 1$ independently whether $(k_j(x), p_j) = 1$, or $(k_j(x), p_j) > 1$. If $\mu_j = 0$, we have

$$\Phi_j(x) = \begin{cases} 0 & \text{if } (k_j(x), p_j) > 1, \\ \omega_j^{b_j \rho_j(x)} & \text{if } (k_j(x), p_j) = 1. \end{cases}$$

Hence Φ_j takes on x the same value as $\chi^{(j)}([x_j])$ for $[x_j] = \left[e_j + k_j(x) \frac{m}{p_j^{\alpha_j}}\right]$. Therefore

$$\chi([x]) = \Phi_1(x) \cdot \Phi_2(x) \cdot \dots \cdot \Phi_r(x). \tag{9}$$

Since x defines $k_j(x)$ and $\rho_j(x)$ uniquely, the function (9) can be considered as the desired expression of $\chi([x])$ in terms of x.

B. Suppose now that $m = 2^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $\alpha_1 \geqq 3$ and $p_2, \dots, p_r$ are odd primes. Any $[x] \in S(m)$ can be again written in the form (8). If $(k_1(x), 2) = 1$, we have $[x_1] = \left[e_1 + k_1(x) \frac{m}{2^{\alpha_1}}\right] \in G_1$ and $[x_1]$ can be written in the form $[\tilde{g}_0]^{\sigma(x)} \cdot [g_1]^{\rho_1(x)}$ with $0 \leqq \sigma(x) \leqq 1$ and $0 \leqq \rho_1(x) < 2^{\alpha_1 - 2}$. If on the other hand $(k_1(x), 2) = 2$, we have $[x_1] \in T_1 - G_1$.

Let χ be a fixed semicharacter of $S(m)$. Denote

$$\chi([e_1]) = \mu_1,$$
$$\chi([\tilde{g}_0]) = (-1)^{b_0}, \quad 0 \leqq b_0 \leqq 1,$$
$$\chi([\tilde{g}_1]) = \omega_1^{b_1}, \quad \omega_1 = \exp \frac{2\pi i}{2^{\alpha_1 - 2}}, \quad 0 \leqq b_1 < 2^{\alpha_1 - 2}.$$

Define the following function

$$\psi_1(x) = \begin{cases} \mu_1 & \text{if } (k_1(x), 2) = 2, \\ \mu_1 + (1 - \mu_1)(-1)^{b_0 \sigma(x)} \omega_1^{b_1 \rho_1(x)} & \text{if } (k_1(x), 2) = 1. \end{cases}$$

Then ψ_1 takes on x the same value as $\chi^{(1)}([x_1])$ on $[x_1] = \left[e_1 + k_1(x)\frac{m}{2_1^{\alpha_1}}\right]$. Therefore

$$\chi([x]) = \psi_1(x) \cdot \Phi_2(x) \cdot \ldots \cdot \Phi_r(x)$$

is the required explicit formula for $\chi([x])$ in terms of x.

6.

We illustrate the foregoing considerations on an example. We have to find all semicharacters of the semigroup $S(360)$.

Since $m = 2^3 \cdot 3^2 \cdot 5$, there exist exactly $[\varphi(8) + 1]\,[\varphi(9) + 1]\,[\varphi(5) + 1] = 175$ distinct semicharacters.

The maximal idempotents of $S(360)$ are of the form $[e_1] = [8a_1]$, $[e_2] = [9a_2]$, $[e_3] = [5a_3]$, $0 < a_i < 360$, $(a_i, 360) = 1$. The relation $[8a_1] = [64a_1^2]$. i. e. $8a_1 \equiv \equiv 64a_1^2 \pmod{360}$ implies $a_1 = 17$, hence $[e_1] = [136]$. Analogously $[e_2] = [81]$, $[e_3] = [145]$.

We have further:

$$T_1 = \{[136 + k_1 45] \mid 0 \leqq k_1 \leqq 7\} =$$
$$= \{[136], [181], [226], [271], [316], [1], [46], [91]\},$$
$$G_1 = \{[181], [271], [1], [91]\},$$
$$T_2 = \{[81], [121], [161], [201], [241], [281], [321], [1], [41]\},$$
$$G_2 = \{[121], [161], [241], [281], [1], [41]\},$$
$$T_3 = \{[145], [217], [289], [1], [73]\},$$
$$G_3 = \{[217], [289], [1], [73]\}.$$

The group G_1 is isomorphic to $G(8)$. This isomorphism is realized by the mapping $[136 + k_1 \cdot 45] \in T_1 \leftrightarrow \langle 45k_1 \rangle = \langle 5k_1 \rangle \in G(8)$, $k_1 = 1, 3, 5, 7$. The images of [181], [271], [1], [91] $\in G_1$ are successively $\langle 5 \rangle$, $\langle 7 \rangle$, $\langle 1 \rangle$, $\langle 3 \rangle \in G(8)$. Since $[271] \leftrightarrow \langle -1 \rangle$ $[181] \leftrightarrow \langle 5 \rangle$, we may choose $[g_0] = [271]$, $[\tilde{g}_1] = [181]$ and all elements $\in G_1$ are of the form $[271^{b_0} \cdot 181^{b_1}]$, $0 \leqq b_0 \leqq 1$, $0 \leqq b_1 \leqq 1$.

Consider now the group G_2 and the isomorphism $[81 + 40k_2] \in G_2 \leftrightarrow \langle 4k_2 \rangle \in G(9)$. Since $\langle 5 \rangle = \langle 4 \cdot 8 \rangle$ is a generating element of the group $G(9)$, we may choose $[g_2] = [81 + 8 \cdot 40] = [41]$ as a generating element of the group G_2.

Finally the isomorphism $G_3 \leftrightarrow G(5)$ realized by $[145 + k_3 \cdot 72] \in G_3 \leftrightarrow \langle 2k_3 \rangle \in \in G(5)$ and the fact that $\langle 2 \rangle$ is a generating element of $G(5)$ imply that [217] is a generating element of G_3.

Hence any semicharacter χ of $S(360)$ is completely given by prescribing its (admissible) values on the following elements:

[136], [271], [181]; [81], [41]; [145], [217].

Taking account to the restrictions mentioned in Theorems 3a and 3b, we get the following table of all semicharacters of $S(360)$. Hereby the integers b and c run independently over all integers satisfying the inequalities $0 \leqq b < 6$, $0 \leqq c < 4$.

[136]	[271]	[181]	[81]	[41]	[145]	[217]	The number of semicharacters
0	±1	±1	0	$\exp\frac{2\pi ib}{6}$	0	$\exp\frac{2\pi ic}{4}$	96
1	1	1	0	$\exp\frac{2\pi ib}{6}$	0	$\exp\frac{2\pi ic}{4}$	24
0	±1	±1	1	1	0	$\exp\frac{2\pi ic}{4}$	16
0	±1	±1	0	$\exp\frac{2\pi ib}{6}$	1	1	24
1	1	1	1	1	0	$\exp\frac{2\pi ic}{4}$	4
1	1	1	0	$\exp\frac{2\pi ib}{6}$	1	1	6
0	±1	±1	1	1	1	1	4
1	1	1	1	1	1	1	1
							175

Let now be, for instance, χ the semicharacter of $S(360)$ defined by the following values of χ:

	[136]	[271]	[181]	[81]	[41]	[145]	[217]
χ	1	−1	1	1	1	0	$\exp\frac{3}{4} \cdot 2\pi i$

We have to find $\chi(100)$.

We use Remark 2 to establish the integres k_1, k_2, k_3 in the decompostion $[100] = = [136 + 45k_1] \cdot [81 + 40k_2] \cdot [145 + 72k_3]$. We have $100 \equiv k_1 \cdot 45 \cdot 81 \cdot 145 \pmod 8$, hence $k_1 = 4$. Analogously $k_2 = 7$, $k_3 = 0$. Hence $[100] = [316] \cdot [1] \cdot [145]$.

Since $(k_1, 2) = 2$, we have $\psi_1(100) = \chi([136]) = 1$. Further since $(k_2, 9) = 1$, we have $\Phi_2(100) = 1$ and since $(k_3, 5) = 5$, we have $\Phi_3(100) = 0$. Hence $\chi([100]) = = \psi_1(100) \cdot \Phi_2(100) \cdot \Phi_3(100) = 0$.

REFERENCES

[1] Hewitt E. and Zuckerman H. S., *Finite dimensional convolution algebras*, Acta Math. 93 (1955), 67—119.

[2] Hewitt E. and Zuckerman H. S., *The multiplicative semigroup of integers* modulo *m* (To appear).

[3] Parízek B. and Schwarz Š., *O multiplikatívnej pologrupe zvyškových tried* (mod *m*), Mat. fyz. časopis SAV 8 (1958), 136—150.

[4] Parízek B., *O rozklade pologrupy zvyškových tried* (mod *m*) *na direktný súčin*, Mat. fyz. časopis SAV 10 (1960), 18—29.

[5] Schwarz Š., Теория характеров комутативных полугрупп, Чех. мат. журнал 4 (79) (1954), 219—247.

[6] Schwarz Š., *The theory of characters of commutative Hausdorff bicompact semigroups*, Czechoslovak Math. J. 6 (81) (1956), 330—364.

Received April 30, 1960.

Katedra matematiky
Slovenskej vysokej školy technickej
v Bratislave

ПОЛУХАРАКТЕРЫ МУЛТИПЛИКАТИВНОЙ ПОЛУГРУППЫ КЛАССОВ ВЫЧЕТОВ (mod *m*)

Богумир Паризек и Штефан Шварц

Резюме

Полухарактером полугруппы S называется комплексная мултипликативная функция определенная на S и не равна тождественно нулю.

Пусть $m > 1$ — натуральное число и $S(m)$ — мултипликативная полугруппа классов вычетов (mod m). Целью настоящей статьи является нахождение всех полухарактеров полугруппы $S(m)$. Метод получения всех полухарактеров изложен в приведенных выше теоремах 3а и 3б.