Mathematica Slovaca

Štefan Schwarz

The role of semigroups in the elementary theory of numbers

Mathematica Slovaca, Vol. 31 (1981), No. 4, 369--395

Persistent URL: `http://dml.cz/dmlcz/128855`

Math. Slovaca 31, 1981, No. 4, 369—395

THE ROLE OF SEMIGROUPS IN THE ELEMENTARY THEORY OF NUMBERS

ŠTEFAN SCHWARZ

One of the motives to write this paper has been the observation that from time to time various generalizations of the classical Euler—Fermat theorem are published.

The aim of this paper is to show that one of the methods how to really understand various results obtained in this connection is via the description of the multiplicative semigroup of residue classes (mod m) as it is done in section 2 below. This description is visualized in Fig. 1.

We emphasize that we are not seeking the shortest proofs of some special problems. We rather develop a general point of view from which many special results concerning congruences (mod m) often become almost obvious.

In section 1 we recall some simple facts concerning finite commutative semigroups. The goal is to introduce the necessary notations and to present some results for those who are not working directly in semigroups. In sections 2 and 3 we give a description of the multiplicative semigroup S_m of residue classes (mod m). [This has been done (in a partly different way) also in [2], [8], [9].] Section 4 has to a certain extent an auxiliary character. It contains information concerning the orders of the elements in the so-called maximal subgroups of S_m. In section 5 we give various generalizations of the Euler—Fermat theorem. In section 6 some further simple questions are solved. Here the choice has been made taking into account problems which appeared (mainly in the Amer. Math. Monthly) in the past few years. In section 7 an (internal) direct product decomposition of S_m is given. Several consequences are deduced. In section 8 formulas for the product of all elements contained in the maximal subgroups and maximal one idempotent subsemigroups of S_m are given.

Though the material discussed here has been treated in hundreds of papers and monographs, the point of view taken in the present paper leads in a natural way to some observations which as far as I am able to decide have never been explicitly stated in the vast amount of literature. (See in particular Theorems 5,2 and 5,3, Theorems 7,1 and 7,3 and Theorems 8,1 and 8,2.)

From the methodical point of view it should be underlined that we are primarily interested in the multiplicative structure of the ring of residue classes (mod m).

But, of course, we freely use also the additive properties of this ring, which give a special feature to the semigroup S_m.

1. Preliminaries

In all of this section S is a finite commutative semigroup. If $x \in S$, then the sequence

$$(1,1) \qquad x, x^3, x^3, \ldots$$

contains only a finite number of different elements. Denote by x^k, $k = k(x)$, the least power of x which appears in (1,1) more than once. Denote further by $k + d$, $d = d(x) \geqq 1$, the least exponent for which $x^k = x^{k+d}$ holds. Then (1,1) is of the form

$$(1,2) \qquad x, x^2, \ldots, x^{k-1} | x^k, \ldots, x^{k+d-1} | \; x^k, \ldots$$

It is well known and easy to prove that $\{x^k, \ldots, x^{k+d-1}\}$ is a cyclic group of order d. Hence (1,1) contains a (unique) idempotent $e = x^r$ and the least number $r = r(x)$ having this property is uniquely determined by the inequalities $k \leqq r \leqq k + d - 1$ and the fact that d/r. It is easy to see that x^{r+1} is one of the generators of the group $\{x^k, \ldots, x^{k+d-1}\}$. Hence $\{x^k, \ldots, x^{k+d-1}\} = \{xe, x^2e, \ldots, x^de = e\}$.

If e is the idempotent contained in the sequence (1,1), we shall say that x *belongs to* e. Denote by E the set of all idempotents $\in S$ Denote further by $P(e)$ the set of all elements $\in S$ belonging to the idempotent e. Then $S = \bigcup_{e \in E} P(e)$ is a union of disjoint subsemigroups of S. We call $P(e)$ *the maximal subsemigroup* of S belonging to the idempotent e. It is the largest subsemigroup of S containing e and no other idempotent.

To every $e \in E$ there is a unique largest group $G(e)$ (subgroup of S) containing e as its identity element. We call $G(e)$ the *maximal group* belonging to the idempotent e. Clearly $G(e) \subset P(e)$.

The group $G(e)$ can be characterized as the set of all $x \in P(e)$ satisfying $xe = x$. We have $G(e) = P(e) \cdot e$. The mapping ψ_e: $P(e) \to G(e)$ defined by $\psi_e(x) = xe$ is a homomorphism of the semigroup $P(e)$ onto the group $G(e)$ leaving all elements $\in G(e)$ invariant.

Note explicitly: If S contains an identity element, say 1, then $P(1) = G(1)$.

With any $x \in S$ we have associated three integers $k(x)$, $d(x)$, $r(x)$, where $k(x) \leqq r(x) \leqq k(x) + d(x) - 1$ and $d(x)/r(x)$. Denote

$$K = \max\{k(x) \mid x \in S\} \quad \text{and} \quad D = \text{l.c.m}\{d(x) \mid x \in S\}$$

and define R as the unique integer satisfying $K \leqq R < K + D$ and D/R. Clearly, K, D, R are characteristics of S. We have:

Proposition 1,1. *For any $x \in S$ we have $x^K = x^{K+D}$. The numbers $K = K(S)$ and $D = D(S)$ (as defined above) are the least positive integers having this property.*

Proposition 1,2. *For any $x \in S$ the element x^R is an idempotent and $R = R(S)$ is the least positive integer having this property.*

Proposition 1,1 may be called the *Euler—Fermat theorem for the finite semigroup S.* The numerical values for K and D in the case of the multiplicative semigroup of residue classes (mod m) go back to Lucas (1890) and Carmichael (1910). Incredible though it may sound the observation concerning the value of R seems to appear for the first time in the present paper.

Remark. The majority of the results stated above is true also for non-commutative semigroups. But in this case $P(e)$ need not be a semigroup. There is a rather limited number of classes of semigroups for which the exact values of K and D are known. In this paper we restrict our attention to the semigroup S_m to be introduced below.

2. The description of S_m

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $\alpha_i \geqq 1$ be the factorization of a given integer $m > 1$ into the product of different primes. By S_m we denote the multiplicative semigroup of all residue classes (mod m). The class containing the number x will be denoted by $[x]$. $G(1)$ denotes the maximal group belonging to the idempotent $[1]$, i.e. the set of all $[x]$ for which $(x, m) = 1$. [$G(1)$ is usually called the group of units of S_m.]

Any element $x \in S_m$ can be written in the form

$$(2.1) \qquad x = [p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \cdot a],$$

where $[a] \in G(1)$ and $k_i \geqq 0$.

Lemma 2,1. *To any element x of the form (2,1) there is a $[b] \in G(1)$ such that*

$$x = [p_1^{\min(k_1, \alpha_1)} \cdot p_2^{\min(k_2, \alpha_2)} \dots p_r^{\min(k_r, \alpha_r)} \cdot b].$$

Proof. Since $x = [p_1^{k_1}] \dots [p_r^{k_r}][a]$, it is sufficient to prove it for one factor, say $y = [p_1^{k_1}]$, where we may suppose that $k_1 > \alpha_1$. We have $y = [p_1^{\alpha_1}][p_1^{k_1-\alpha_1} + p_2^{\alpha_2} \dots p_r^{\alpha_r}]$. The second factor is in $G(1)$ since it is not divisible by $p_1, p_2, \dots, p_r$. Hence $y = [p_1^{\alpha_1} \cdot a_1]$, $[a_1] \in G(1)$. Treating in the same way all factors in which $k_i > \alpha_i$, we obtain Lemma 2,1.

Remark: It should be noted that given x the element $[b] \in G(1)$ is not uniquely determined.

Lemma 2,2. *Let be $0 \leqq k_i \leqq \alpha_i$, $0 \leqq l_i \leqq \alpha_i$ $(i = 1, 2, \dots, r)$.If $[p_1^{k_1} \dots p_r^{k_r}]G(1) \cap [p_1^{l_1} \dots p_r^{l_r}]G(1) \neq \emptyset$, then $k_i = l_i$ $(i = 1, \dots, r)$.*

Proof. If $[p_1^{k_1} \dots p_r^{k_r}a] = [p_1^{l_1} \dots p_r^{l_r}b]$, $[a], [b] \in G(1)$ and, say $k_1 > l_1$, we may write $[p_1^{l_1}]\,[p_1^{k_1-l_1} p_2^{k_2} \dots p_r^{k_r} \cdot a - p_2^{l_2} \dots p_r^{l_r} \cdot b] = [0]$. But this is impossible since the left-hand side is not divisible by $p_1^{\alpha_1}$.

Corollary 2.1. *The semigroup S_m admits a decomposition into $(\alpha_1+1)(\alpha_2+1) \dots (\alpha_r+1)$ mutually disjoint sets in the form $S = \bigcup_{k_1,\dots,k_r}[p_1^{k_1} \dots p_r^{k_r}]\, G(1)$, where $0 \leqq k_i \leqq \alpha_i$ $(i=1, \dots, r)$.*

We now proceed to the description of *all idempotents* $\in S_m$. But first we make (for simplicity and typographical reasons) the following convention. In what follows we shall deal with products of the form (2,1). It will be often important that some of the p_i do not appear and only $s(<r)$ different prime powers have an exponent $\neq 0$. In such cases to avoid unnecessary subscripts we shall consider instead of expressions as $[p_{i_1}^{k_{i_1}} p_{i_2}^{k_{i_2}} \dots p_{i_s}^{k_{i_s}}a]$, $k_{i_v} \geqq 1$ the expression $[p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}a]$, $k_i \geqq 1$, having in mind that this is only a typical representative of products of s different prime powers.

Suppose that $e = [p_1^{k_1} \dots p_s^{k_s}a]$, $[a] \in G(1)$, $1 \leqq k_i \leqq \alpha_i$, $1 \leqq s \leqq r$, is an idempotent $\in S_m$. Denote $v(m) = \max(\alpha_1, \dots, \alpha_r)$. Then $e = e^2 = \dots = e^v$ implies $e = [p_1^{vk_1} \dots p_s^{vk_s}a^v]$. By Lemma 2,1 $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s}c]$ with a suitably chosen $[c] \in G(1)$. If $s = r$, we have $e = [0]$, suppose therefore in the following $s < r$. If an element $[p_1^{\alpha_1} \dots p_s^{\alpha_s}c]$, $[c] \in G(1)$ is an idempotent, then $[p_1^{2\alpha_1} \dots p_s^{2\alpha_s}c^2] = [p_1^{\alpha_1} \dots p_s^{\alpha_s}c]$, i.e.

$$(2,2) \qquad p_1^{\alpha_1} \dots p_s^{\alpha_s}c \equiv 1 \pmod{p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}}.$$

The congruence (2,2) determines c uniquely $(\bmod\ p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r})$. If c is a solution, then all solutions are $c + t \cdot p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}$ with an integer t. Since $[p_1^{\alpha_1} \dots p_s^{\alpha_s}(c + tp_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r})] = [p_1^{\alpha_1} \dots p_s^{\alpha_s}c]$, the element $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s}c]$ is independent of the choice of the solution of (2.2). We have proved: If e is an idempotent, then e is necessarily of the form $e = [p_1^{\alpha_1} \cdot \dots p_s^{\alpha_s}c]$, where c is any solution of (2,2).

Let conversely c_0 be a fixed chosen solution of (2,2) and $p_1^{\alpha_1} \dots p_s^{\alpha_s}c_0 = 1 + t_0 p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}$. Clearly c_0 is not divisible by $p_{s+1}, \dots, p_r$. Choose now an integer t_1 such that $c_0 + t_1 p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}$ is not divisible by $p_1, \dots, p_s$. Then $[a_0] = [c_0 + t_1 p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}] \in G(1)$.

The choice of t_1 is always possible. If c_0 is divisible by none of the $p_1, \dots, p_s$, put $t_1 = 0$. If c_0 is divisible by $p_1, \dots, p_v$ and not divisible by $p_{v+1}, \dots, p_s$, put $t_1 = p_{v+1} \dots p_s$.

The element $\varepsilon = [p_1^{\alpha_1} \dots p_s^{\alpha_s}a_0]$ is an idempotent $\in \mathrm{S_m}$ since

$$\varepsilon^2 = [p_1^{\alpha_1} \dots p_s^{\alpha_s}a_0]\,[p_1^{\alpha_1} \dots p_s^{\alpha_s}c_0] =$$

$$= [p_1^{\alpha_1} \dots p_s^{\alpha_s}a_0]\,[1 + t_0 p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}] = [p_1^{\alpha_1} \dots p_s^{\alpha_s}a_0] = \varepsilon\,.$$

We have:

Theorem 2,1. *Let there be $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $\alpha_i \geqq 1$. The semigroup S_m contains* *exactly* 2^r *idempotents (including* $[0]$ *and* $[1]$*). Any idempotent* $\in S_m$ *can be written in the form* $e=[p_1^{l_1} \dots p_r^{l_r}a]$, *where* l_i *is either* 0 *or* α_i *and* $[a]$ *is a suitably chosen element* $\in G(1)$.

In the set E we introduce two operations: $\wedge$ and $\vee$. Let e', $e'' \in E$ and

$$e'=[p_1^{l_1} \dots p_r^{l_r}a'], \text{ where } l_i \text{ is either 0 or } \alpha_i,$$

$$e''=[p_1^{j_1} \dots p_r^{j_r}a''], \text{ where } j_i \text{ is either 0 or } \alpha_i.$$

We define

$$e' \wedge e'' = e'e'' = [p_1^{\max(l_1,j_1)} \dots p_r^{\max(l_r,j_r)} \cdot c],$$

$$e' \vee e'' = [p^{\min(l_1,j_1)} \dots p^{\min(l_r,j_r)} \cdot d],$$

where $[c]$, $[d]$ are determined by the requirement that $e' \wedge e''$, $e' \vee e''$ are idempotents $\in S_m$. It is easy to see that E with respect to these operations becomes a *Boolean algebra.*

Two kinds of idempotents play a special role:

The *primitive idempotents* are the idempotents of the form

$$f_i=\left[\frac{m}{p_i^{\alpha_i}}a_i\right], \quad [a_i] \in G(1) \quad (i=1, \dots, r).$$

The *maximal idempotents* $\in E$ are the idempotents of the form

$$\bar{f}_i=[p_i^{\alpha_i} \cdot b_i], \quad [b_i] \in G(1) \quad (i=1, \dots, r).$$

In this terminology: If $m=p^\alpha$, then $f_1=[1]$ is a primitive idempotent, while $\bar{f}_1=[0]$ is a maximal idempotent.

If $e=[p_1^{\alpha_1} \dots p_s^{\alpha_s}a] \in E$, $s \geqq 1$, then $e=\bar{f}_1 \cdot \bar{f}_2 \dots \bar{f}_s$.

Lemma 2,3. *Any idempotent* $\in S_m$ *which is* $\neq 1$ *is a product of maximal idempotents.*

The following multiplicative properties of idempotents follow directly from the definition:

(i) $$f_i \bar{f}_j = \begin{cases} f_i & \text{for } i \neq j, \\ [0] & \text{for } i=j. \end{cases}$$

(ii) $$f_i f_j = [0] \text{ for } i \neq j.$$

The additive properties which we shall use are the following:

i) $$f_i+\bar{f}_i=[1].$$

ii) $$f_1+\dots+f_r=[1].$$

The first follows from the fact that $f_i+\bar{f}_i$ is an idempotent and in the above notation $\left[\frac{m}{p_i^{\alpha_i}}a_i+p_i^{\alpha_i}b_i\right]$ is clearly contained in $G(1)$. Analogously for the second property.

If $e=\bar{f}_1 \dots \bar{f}_s$, then $e=(1-f_1) \dots (1-f_s) = 1-(f_1+\dots+f_s) = f_{s+1}+\dots+f_r$. Hence, any idemptotent $e \neq 0$ can be written as a sum of primitive idempotents. (This is of course well known and holds for large classes of commutative rings.) Note explicitly that the product of any idempotents is an idempotent, while the sum of two (non-primitive) idempotents need not be an idempotent. This makes clear the advantage of the multiplicative representation of idempotents in general considerations. (In contradistinction to this, for numerical computations the additive representation is more advantageous.)

We now identify the *maximal subsemigroups* belonging to a given idempotent e. Let there be

$$e=[p_1^{\alpha_1} \dots p_s^{\alpha_s} a], \quad 1 \leqq s \leqq r, \quad [a] \in G(1). \tag{2,3}$$

An element $x=[p_1^{k_1} \dots p_r^{k_r} y]$, $k_i \geqq 0$, $[y] \in G(1)$ belongs to e if and only if we have $[p_1^{tk_1} \dots p_r^{tk_r} y^t] = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$ for some integer $t \geqq 1$.

By Lemma 2,1 we may write (with a suitably chosen $[b] \in G(1)$) $[p_1^{\min(tk_1, \alpha_1)} \dots p_r^{\min(tk_r, \alpha_r)} \cdot b] = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$, whence by Lemma 2,2 $k_{s+1} = \dots = k_r = 0$.

Conversely: Let $x=[p_1^{k_1} \dots p_s^{k_s} b]$, where $1 \leqq k_i \leqq \alpha_i$ and $[b]$ any element $\in G(1)$. Denote $\sigma = \max(\alpha_1, \dots, \alpha_s)$. Then $x^\sigma = [p_1^{\sigma k_1} \dots p_s^{\sigma k_s} b^\sigma]$ and by Lemma 2,1 there is a $[c] \in G(1)$ such that

$$x^\sigma = [p_1^{\alpha_1} \dots p_s^{\alpha_s} c] = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]\,[ca^{-1}] = e[ca^{-1}].$$

If v is the order of $[ca^{-1}]$ in $G(1)$, we have $x^{\sigma v} = e$. This implies:

Theorem 2,2. *If $e=[p_1^{\alpha_1} \dots p_s^{\alpha_s} a] \in E$, then the maximal semigroup belonging to e is the union of $\alpha_1 \alpha_2 \dots \alpha_s$ disjoint subsets $P(e) = \bigcup_{k_1, \dots, k_s} [p_1^{k_1} \dots p_s^{k_s}]G(1)$, where $1 \leqq k_i \leqq \alpha_i$ $(i=1, \dots, s)$.*

To identify the *maximal group* belonging to e, recall that for any semigroup $G(e) = P(e) \cdot e$. If e is of the form (2,3) we have by Theorem 2,2

$$G(e) = \bigcup_{k_1, \dots, k_s} [p_1^{k_1} \dots p_s^{k_s}]\,[p_1^{\alpha_1} \dots p_s^{\alpha_s} a]G(1). \tag{2,4}$$

Now (for fixed $k_1, \dots, k_s$) by Lemma 2,1 $[p_1^{k_1} \dots p_s^{k_s}]\,[p_1^{\alpha_1} \dots p_s^{\alpha_s}] = [p_1^{\alpha_1} \dots p_s^{\alpha_s} c]$ with $[c] \in G(1)$ and each of the summands in (2.4) is of the form $[p_1^{\alpha_1} \dots p_s^{\alpha_s}\, ca]G(1) = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]\,[c]G(1) = e \cdot G(1)$.

We have proved:

Theorem 2,3. *If $e \in E$, the maximal group $G(e)$ belonging to e is given by the formula $G(e) = eG(1)$.*

Remark 1. The mapping $\Phi_e \colon G(1) \to G(e)$ defined by $\Phi_e(x) = x \cdot e$ is a homomorphism of $G(1)$ onto $G(e)$. The kernel of this homomorphism will be described later (see Lemma 4,2).

Remark 2. Note explicitly: If an element $x \in S_m$ is given in the (usual) form $x=[p_1^{k_1} \dots p_s^{k_s}a]$, $[a] \in G(1)$, $k_i \geqq 1$, we can immediately say that $x \in P(\bar{f}_1 \dots \bar{f}_s)$ and $x \in G(\bar{f}_1 \dots \bar{f}_s)$ iff $k_i \geqslant \alpha_i$ for all $i=1, 2, \dots, s$.

The results obtained are schematically described (for $r=3$) in Figure 1. Here the circles denote maximal groups, the rectangles denote maximal subsemigroups belonging to the corresponding idempotents. If $e=[p_1^{\alpha_1} \dots p_s^{\alpha_s}a] \in E$, it will be shown that card $G(e) = |G(e)| = \varphi(m/p_1^{\alpha_1} \dots p_s^{\alpha_s})$ and $|P(e)| = p_1^{\alpha_1-1} \dots p_s^{\alpha_s-1}|G(e)|$. Hence if $e' < e''$ (in the sense of the ordering in the Boolean algebra E), then $|P(e')| \leqq |P(e'')|$ and $|G(e')| \leqq |G(e'')|$. This has been incorporated in Figure 1.

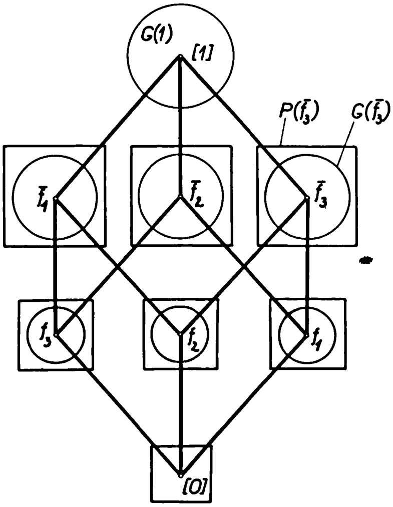

Fig. 1

Remark. If S is a commutative semigroup, the principal ideal generated by x is the set $I_x = \{x, Sx\}$. By the H-class containing x we mean the set of all y generating the same ideal I_x of S, i.e. $H(x) = \{y \mid (x, Sx) = (y, Sy)\}$. The semigroup S is a union of disjoint H-classes. An H-class is a group iff it contains an idempotent. In the set of H-classes we may introduce a partial ordering by writing $H(x) \leqq H(z)$ if $I_x \subset I_z$.

If $S=S_m$, it is easy to see that each of the sets $[p_1^{k_1} \dots p_r^{k_r}]G(1)$ mentioned in Corollary 2,2 is exactly one H-class. Hence there are exactly $(\alpha_1+1) \dots (\alpha_r+1)$ different H-classes.

Let $e=[p_1^{\alpha_1} \dots p_s^{\alpha_s}a]$, $[a] \in G(1)$. Then it follows from Theorem 2,2 that $P(e)$ is the union of exactly $\alpha_1 \alpha_2 \dots \alpha_s$ H-classes of S_m. The H-classes contained in $P(e)$ (in the ordering just mentioned) form a lattice with the least element $G(e) = [p_1^{\alpha_1}$

$\dots p_s^{\alpha_s}]G(1)$ and the greatest element $[p_1 \dots p_s]G(1)$. From this point of view it is more appropriate to describe "the position" of $G(e)$ in $P(e)$ in the way given in Figure 2 (i.e. to emphasize that $G(e)$ is "at the bottom" of $P(e)$).

To have the figure as simple as possible the ordering of the H-classes is not incorporated in Figure 1.

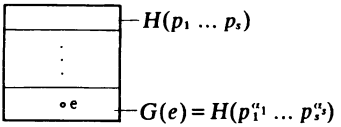

Fig. 2

3. How to find $k(x)$ and $d(x)$?

In this section the element

$$(3,1) \qquad x = [p_1^{k_1} \dots p_s^{k_s}a], \quad 1 \leqq s \leqq r, \quad k_i \geqq 1, \quad [a] \in G(1)$$

is given.

We have to find a (possibly reasonable) method how to compute the numbers $k(x)$ and $d(x)$.

If $x \in G(1)$, then $k(x) = 1$ and $d(x)$ is the least positive integer for which $x^d = [1]$. In the following suppose that $x \notin G(1)$.

Denote by $\mu = \mu(x)$ the least integer such that $\mu \cdot k_i \geqq \alpha_i$ for all $i = 1, 2, \dots, s$. Call $\mu(x)$ the *indicator* of x. Clearly $1 \leqq \mu(x) \leqq \max(\alpha_1, \dots, \alpha_s)$. Whith respect to Lemma 2,1 the number $\mu(x)$ is independent of the form in which the class $[x]$ is presented. It follows (see Theorem 2,3) that $\mu(x)$ is the least integer such that x^μ is contained in a group, namely the group $[p_1^{\alpha_1} \dots p_s^{\alpha_s}]G(1)$ containing the idempotent $e = \bar{f}_1 \dots \bar{f}_s$. Hence $k(x) = \mu(x)$.

Now the group $\{x^\mu, x^{\mu+1}, \dots, x^{\mu+d-1}\}$ is identical with the group $\{xe, x^2e, \dots, x^{d(x)}e\}$. Hence $d(x)$ is the least integer $d \geqq 1$ such that $x^d e = e$. This can be written in the form $(x^d - 1)e \equiv 0 (\mathrm{mod}\ m)$, which implies $x^d - 1 \equiv 0 (\mathrm{mod}\ m/p_1^{\alpha_1} \dots p_s^{\alpha_s})$ if $s < r$. If $s = r$, then $d(x) = 1$.

In view of the preceding considerations we may summarize as follows:

Theorem 3,1. *Let x be of the form (3,1). Then $x^l = x^{l+h}$ holds if and only if*

i) *$l \geqq \mu(x)$, where $\mu(x)$ is the indicator of x;*

ii) *h is a positive multiple of $d(x)$, where $d(x)$ is the least integer such that $x^d \equiv 1 (\mathrm{mod}\ m/p_1^{\alpha_1} \dots p_s^{\alpha_s})$ if $s < r$, and $d(x) = 1$ if $s = r$.*

This Theorem has been proved in [5]. It may be called the "individual" Euler—Fermat theorem for the given element $x \in S_m$. (Compare with Theorem 5,1 and Theorem 5,2 below.)

Remark. From the computational point of view it can be shown that the number $d(x)$ for x given in (3,1) can be found as follows. For $i = s+1, \ldots, r$ find the least d_i such that $x^{d_i} \equiv 1 (\bmod p_i^{\alpha_i})$. Then $d(x) = \text{l.c.m.}[d_{s+1}, \ldots, d_r]$. (This follows immediately from Lemma 4,3 to be proved below. We omit the explicit proof.)

4. An internal direct decomposition of $G(e)$

The aim of this section is to find the value of the highest order of an element $\in G(e)$. [For $G(1)$ this is well known. See, e.g., [12] or [14].] We need this only to show that some of our results proved below are the best possible.

By the way we obtain an internal direct decomposition of $G(1)$ and $G(e)$ which does not seem to be generally known (and which will be used in section 7).

Consider the maximal group belonging to a primitive idempotent $f_i = \left[\frac{m}{p_i^{\alpha_i}} a\right] \in E$ $(1 \leqq i \leqq r)$. By Theorem 2,3 we have $G(f_i) = G(1)f_i$. If $[x], [y] \in G(1)$, we have $[x]f_i = [y]f_i$ (in S_m) if and only if $x \equiv y (\bmod p_i^{\alpha_i})$. This implies

$$G(f_i) = \{[h]f_i \mid 1 \leqq h < p_i^{\alpha_i}, (h, p_i) = 1\}.$$

The fact that the structure of this group is known will not be used before the end of the section.

Each of the groups $G(f_i)$ is "at the bottom" in Figure 1 "far away from $G(1)$".

Consider now the set $G_i = \{\bar{f}_i + g \mid g \in G(f_i)\}$. Each of the elements $\bar{f}_i + [h]f_i$ is in $G(1)$ (since it is divisible by none of the primes $p_1, \ldots, p_r$). The set G_i is a semigroup since $(\bar{f}_i + [h_1]f_i)(\bar{f}_i + [h_2]f_i) = \bar{f}_i + [h_1 h_2]f_i$. It is a group since a subsemigroup of a finite group is a group. G_i is clearly isomorphic with $G(f_i)$.

Lemma 4,1. *The group $G(1)$ is the direct product of its r subgroups: $G(1) = G_1 \cdot G_2 \ldots G_r$.*

Proof. i) Let there be $x \in G(1)$. Since $xf_i \in G(1)f_i = G(f_i)$, the element $x_i = \bar{f}_i + xf_i$ is contained in G_i. Now $x_1 x_2 \ldots x_r = (\bar{f}_1 + xf_1) \ldots (\bar{f}_r + xf_r) = x(f_1 + \ldots + f_r) = x$. Hence $G(1) \subset G_1 \ldots G_r$ and since trivially $G_1 \ldots G_r \subset G(1)$, we have $G(1) = G_1 \cdot G_2 \ldots G_r$.

ii) To prove that the product is direct we have to show that $G_i \cap G_j = [1]$ for $i \neq j$. Let $u = \bar{f}_i + g'$, $v = \bar{f}_j + g''$, $g' \in G(f_i)$, $g'' \in G(f_j)$. If $u = v$, we have $uf_i = vf_i$, i.e. $(\bar{f}_i + g') f_i = (\bar{f}_j + g'')f_i$, $g'f_i = f_i$ (since $g''f_i \in G(f_j)f_i = [0]$). Hence $g' = f_i$ and $u = \bar{f}_i + g' = \bar{f}_i + f_i = [1]$. Analogously $uf_j = vf_j$ implies $v = [1]$. This proves Lemma 4,1.

Remark. The explicit description of the groups G_i as subsets of $G(1)$ is sometimes important in number-theoretical questions. It enables also to find the groups $G(e)$ as subsets of S_m (and not merely their structural properties up to an isomorphism).

Lemma 4,2. *Let there be* $e=\bar{f}_1 \ldots \bar{f}_s \in E$ and $s<r$.

i) *If* $1 \leqq i \leqq s$, *then* $G_i e = e$.
ii) *If* $s+1 \leqq i \leqq r$, *then* $G_i e$ *is a subgroup of* $G(\iota)$ *which is isomoprhic with* G_i.

Proof. i) Since $(\bar{f}_i+[h]f_i)\bar{f}_i=\bar{f}_i$ for any h, we have in the first case $G_i e = G_i \bar{f}_1 \ldots \bar{f}_i \ldots \bar{f}_s = (G_i \bar{f}_i)e = \bar{f}_i e = e$.
ii) In the second case [since for $i \geqq s+1$ we have $f_i e = f_i$] $(\bar{f}_i + [h]f_i)e = \bar{f}_i e + {}+[h]f_i$ and $G_i e = \{\bar{f}_i e + g \mid g \in G(f_i)\}$.

The mapping F: $G_i \to G_i e$ defined by $\bar{f}_i + [h]f_i \mapsto \bar{f}_i e + [h]f_i$ is a $1-1$ mapping from G_i onto $G_i e$ since $\bar{f}_i e + [h_1]f_i = \bar{f}_i e + [h_2]f_i$ implies $[h_1]f_i = [h_2]f_i$, hence $\bar{f}_i+[h_1]f_i = \bar{f}_i + [h_2]f_i$. It is a homomorphism since

$$(\bar{f}_i+[h_1]f_i)\,(\bar{f}_i+[h_2]f_i)=\bar{f}_i+[h_1h_2]f_i \mapsto \bar{f}_i e+[h_1h_2]f_i= \\ =(\bar{f}_i e+[h_1]f_i)\,(\bar{f}_i e+[h_2]f_i).$$

Hence F is an isomorphism. This proves Lemma 4,2.

Remark. Lemma 4,2 describes explicitly the kernel of the homomorphism Φ_e: $G(1) \to G(e)$ defined by $\Phi_e(x)=xe$. If $e=\bar{f}_1 \ldots \bar{f}_s$, then the kernel of Φ_e is the subgroup $G_1 \ldots G_s$ of $G(1)$. Also since G_i is the kernel of the homomorphism $G(1) \to G(\bar{f}_i)$ defined by $x \mapsto x\bar{f}_i$, we have $G_i=\{x \in G(1) \mid x\bar{f}_i=\bar{f}_i\}$. (This shows that it is possible to define G_i multiplicatively as $\{x \in G(1) \mid x\bar{f}_i=\bar{f}_i\}$. We prefer the definition given above in order to have an explicit description of G_i.)

Lemma 4,3. *Let* $e=\bar{f}_1 \ldots \bar{f}_s \in E$, $1 \leqq s \leqq r$. *Then the maximal group* $G(e)$ *is the direct product of its subgroups*:

$$G(e)=(G_{s+1}e)\,(G_{s+2}e)\ldots(G_r e). \tag{4,1}$$

Proof. By Theorem 2,3 $G(e) = G(1) \cdot e = G_1 \ldots G_r \cdot e$ and $G_i e \subset G(e)$. By Lemma 4,2 for $i=1, \ldots, s$ we have $G_i e = e$. Hence $G(e) = G_{s+1} \ldots G_r e = (G_{s+1}e) \ldots (G_r e)$ so that the product decomposition (4,1) holds.

To prove that the product is direct it is sufficient to show that for $i, j \in \{s+1, \ldots, r\}$, $i \neq j$ we have $G_i e \cap G_j e = e$. This is done by the same argument as in Lemma 4,1. Let $u=\bar{f}_i e+g'$, $v=\bar{f}_j e+g''$, $g' \in G(f_i)$, $g'' \in G(f_j)$. If $u=v$, then $uf_i=vf_i$, $(\bar{f}_i e+g')f_i = (\bar{f}_j e+g'')f_i$, $g'=f_i e$. Hence $u=\bar{f}_i e+g' = \bar{f}_i e+f_i e=e$. This proves our statement.

Since G_i is isomorphic with $G(f_i)$, G_i is a group of order $\varphi(p_i^{\alpha_i})$, the structure of which is known. If p_i is odd or $p_i^{\alpha_i}=2$ or $p_i^{\alpha_i}=4$, then G_i is cyclic of order $\varphi(p_i^{\alpha_i})$. If $p_i^{\alpha_i}=2^{\alpha_i}$ and $\alpha_i>2$, G_i is not cyclic, the order of each element $\in G_i$ is a power of 2 and G_i contains an element of order 2^{α_i-2}.

Define (the Carmichael function):

$$\lambda(m)=\begin{cases} 1 & \text{if } m=1, \\ 2^{\alpha-2} & \text{if } m=2^\alpha,\ \alpha>2, \end{cases}$$

$$\lambda(m)=\begin{cases}\varphi(m) \text{ if } m=2, 4, p^{\alpha} \text{ with } p \text{ an odd prime,}\\ \text{l.c.m. } [\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_r^{\alpha_r})]\\ \text{if } m=p_1^{\alpha_1} \ldots p_r^{\alpha_r}.\end{cases}$$

Then we can state that each of the groups G_i contains an element, say g_i, of order $\lambda(p_i^{\alpha_i})$. The element $g=g_1 g_2 \ldots g_r \in G(1)$ is exactly of order $\lambda(m)$. Finally any element $\in G(1)$ has an order dividing $\lambda(m)$. Hence for any $x \in G(1)$ we have $x^{\lambda(m)}=[1]$.

An analogous result holds for the group $G(e)$. If $e=\bar{f}_1 \ldots \bar{f}_s \in E$, $1 \leqq s \leqq r$, consider the decomposition of $G(e)$ given in Lemma 4,3. Each of the groups $G_i e$ $(s+1 \leqq i \leqq r)$ is isomorphic with the corresponding group G_i and it contains the element $g_i e \in G(e)$ of order $\lambda(p_i^{\alpha_i})$. The element $ge = (g_{s+1}e) \ldots (g_r e)$ is exactly of order $\lambda(m/p_1^{\alpha_1} \ldots p_s^{\alpha_s})$ and the order of any element $\in G(e)$ is a divisor of this number.

Summarily (including the case $s=r$, i.e. $e=[0]$):

Theorem 4,1. *For any $x \in G(1)$ we have $x^{\lambda(m)}=[1]$. If $e=\bar{f}_1 \ldots \bar{f}_s$, $1 \leqq s \leqq r$, then for any $x \in G(e)$ we have $x^{\lambda(m/p_1^{\alpha_1} \ldots p_s^{\alpha_s})}=e$. Hereby the exponents cannot be replaced by a smaller number.*

From Lemma 4,3 we also obtain:

***Corollary* 4,1.** *If $e=\bar{f}_1 \ldots \bar{f}_s$, then $|G(e)| = \varphi(m/p_1^{\alpha_1} \ldots p_s^{\alpha_s})$.*

Remark 1. Suppose that $m=2p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Then it can be immediately verified that $f_1=[p_2^{\alpha_2} \ldots p_r^{\alpha_r}]$ is a primitive idempotent $\in S_m$. Hence $\bar{f}_1=[1-p_2^{\alpha_2} \ldots p_r^{\alpha_r}]$ is a maximal idempotent $\in S_m$. The maximal group $G(f_1)$ is the one point group $\{f_1\}$ and $G_1=\{[1]\}$. In this (but in no other case) the product decomposition in Lemma 4,1 contains only $r-1$ non-trivial factors. This implies for Lemma 4,3: If e as a product of maximal idempotents does not contain the factor $[1-p_2^{\alpha_2} \ldots p_r^{\alpha_r}]$, then one of the groups $G_{s+1}e, \ldots, G_r e$ reduces to $\{e\}$.

Other pecularities which take place in this (but no other) case are: $G(\bar{f}_1)$ is isomorphic to $G(1)$ and $P(f_1)$ is isomorphic to $P(0)$.

Remark 2. Motivated by further purposes and emphasizing the multiplicative structure of S_m we described $G(e)$ as a direct product. From the point of view of numerical computations there is a simpler additive description which is a consequence of the ring structure of S_m and follows also from Lemma 4,3. If $e=\bar{f}_1 \ldots \bar{f}_s$, then $G(e)$ consists of all elements of the form

$$(\bar{f}_{s+1}+[h_{s+1}]f_{s+1}) \ldots (\bar{f}_r+[h_r]f_r)\bar{f}_1 \ldots \bar{f}_s = [h_{s+1}]f_{s+1}+\ldots+[h_r]f_r,$$

where

$$1 \leqq h_i < p_i^{\alpha_i},\ (h_i, p_i)=1\ (i=s+1, \ldots, r).$$

Hence we may write symbolically $G(e)=G(f_{s+1}) \oplus \ldots \oplus G(f_r)$. We say "symbolically" since $G(f_i)$ is a multiplicative (but not an additive) subgroup of S_m. The sign $\oplus$ means that every $x \in G(e)$ can be written uniquely as $x = x_{s+1} + \dots + x_r$, $x_i \in G(f_i)$ and (in order to get $G(e)$) none of the summands can be omitted.

5. Generalizations of the Euler—Fermat theorem

We suppose again $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ and consider the semigroup S_m.

Lemma 5,1. *Denote $v(m) = \max(\alpha_1, \dots, \alpha_r)$. Then for any $x \in S_m$ the element $x^{v(m)}$ is contained in a maximal group of S_m.*

Proof. If $x \in G(1) = P(1)$, the statement is trivially true. Suppose therefore $x \in P(e)$ and $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a] \in E$, $1 \leqq s \leqq r$. By Theorem 2,2 we may write $x = [p_1^{k_1} \dots p_s^{k_s} b]$, $[b] \in G(1)$, $1 \leqq k_i \leqq \alpha_i$. We have $x^{v(m)} = [p_1^{vk_1} \dots p_s^{vk_s} b^2]$. Here $vk_i \geqq \alpha_i$. By Lemma 2,1 there is a $[c] \in G(1)$ such that $x^v = [p_1^{\alpha_1} \dots p_s^{\alpha_s} c]$. By Theorem 2,3 $x^v \in G(e)$. This proves our statement

Corollary 5,1. *For any $x \in S_m$* we have $k(x) \leqq v(m)$.

As a matter of fact we have proved more:

Corollary 5,1a. *If $x \in P(e)$ and $e = \bar{f}_1 \dots \bar{f}_s \in E$, then $k(x) \leqq \max(\alpha_1, \alpha_2, \dots, \alpha_s)$.*

The estimation is sharp. Denote-for a while — $\sigma = \max(\alpha_1, \dots, \alpha_s)$. Then for $x = [p_1 \dots p_s] \in P(e)$ we have $x^\sigma \in G(e)$, while $x^{\sigma-1} \notin G(e)$.

Lemma 5,2. *For any $x \in S_m$ the number $d(x)$ is a divisor of $\lambda(m)$.*

Proof. If $x \in G(1)$, this is true by Theorem 4,1. Suppose that $x \in P(e)$, $e = \bar{f}_1 \dots \bar{f}_s$. The group $\{x^{k(x)}, \dots, x^{k(x)+d(x)-1}\} = \{xe, x^2e, \dots, x^de\}$ is a subgroup of $G(e)$ and $d(x)$ is the least integer for which $(xe)^d = e$. Now the order of any element $\in G(e)$ is a divisor of $\lambda(m/p_1^{\alpha_1} \dots p_s^{\alpha_s})$, hence $d(x)/\lambda(m/p_1^{\alpha_1} \dots p_s^{\alpha_s})$, and therefore $d(x)/\lambda(m)$ for any $x \in P(e)$.

Note that $\lambda(m)$ cannot be replaced by a smaller number since $G(1)$ contains an element of order $\lambda(m)$.

Again we have proved somewhat more:

Corollary 5,2. *If $e = \bar{f}_1 \dots \bar{f}_s$ and $x \in P(e)$, then $d(x)/\lambda(m/p_1^{\alpha_1} \dots p_s^{\alpha_s})$.*

Theorem 5,1. *(The global Euler—Fermat theorem.) For any $x \in S_m$ we have $x^{v(m)} = x^{v(m)+\lambda(m)}$.*

Proof. Since x^v is contained in a subgroup of S_m, the set $\{x^{k(x)}, \dots, x^{k(x)+d(x)-1}\}$ is identical with $\{x^v, x^{v+1}, \dots, x^{v+d(x)-1}\}$. Hence $x^v = x^{v+d(x)}$, which implies $x^v = x^{v+d} = x^{v+2d} = \dots$ and since $d(x)/\lambda(m)$, we have $x^v = x^{v+\lambda(m)}$.

A slightly stronger form of Theorem 5,1 will be given in Proposition 7,1.

Remark. If we insist on the natural requirement to make the exponents independent of the special choice of the element x, neither v nor $v + \lambda$ can be replaced by a smaller number. It is the best possible generalization of the classical

Euler—Fermat theorem (which deals only with $x \in G(1)$). The observation concerning $\nu(m)$ seems to go back to Lucas (1890). A historical survey, including the history of various confusions, is contained in paper [10].

A few words should be added to the term "best possible generalization". Theorem 5,1 is a statement concerning polynomials of the form $x^M - x^L$ $(M > L \geqq 1)$ which vanish identically in S_m. If we consider monic polynomials $f(x)$ of any form which are identically zero in S_m, the degree of $f(x)$ may be essentially smaller than $\nu(m) + \lambda(m)$. Let there be, e.g., $m = p^\alpha$, $p > 2$, $\alpha \geqq 1$. Then $x^p - x$ is divisible by p (for any $x \in S_m$), hence $(x^p - x)^\alpha$ is a polynomial of degree αp which vanishes for all $x \in S_m$. Hereby $p\alpha < \nu(m) + \lambda(m) = \alpha + p^{\alpha-1}(p-1)$ if $\alpha \geqq 2$. (Even $p\alpha$ is "in general" not the lowest possible degree. This question is treated in detail in [15].)

If we specify "the position" of x in S_m, we may obtain a result analogous to Theorem 5,1. The following result is simply the Euler—Fermat theorem for the semigroup $P(e)$ in the sense of Section 1.

Theorem 5,2. *(The local Euler—Fermat theorem.) Let $e = \bar{f}_1 \dots \bar{f}_s \in E$, $1 \leqq s \leqq r$. For any $x \in P(e)$ we have*

$$x^{\max(\alpha_1 \dots, \alpha_s)} = x^{\max(\alpha_1, \dots, \alpha_s) + \lambda(m/p_1^{\alpha 1} \dots p_s^{\alpha s})} \tag{5,1}$$

and none of the exponents can be replaced by a smaller number.

Proof. Denote — for a while — $\sigma = \max(\alpha_1, \dots, \alpha_s)$. By Corollary 5,1a $x^\sigma \in G(e)$ and σ cannot be replaced by a smaller number. Next the group $\{x^{k(x)}, \dots, x^{k(x)+d(x)-1}\} = \{xe, \dots, x^{d(x)}e\}$ is a subgroup of $G(e)$ and $d(x)$ is the least integer for which $(xe)^d = e$. By Corollary 5,2 $d(x)$ divides $\lambda(m/p_1^{\alpha_1} \dots p_s^{\alpha_s})$ and this number cannot be replaced by a smaller one since $G(e)$ contains an element of order $\lambda(m/p_1^{\alpha_1} \dots p_s^{\alpha_s})$. Finally the group $\{x^{k(x)}, \dots, x^{k(x)+d(x)-1}\}$ is identical with the group $\{x^\sigma, x^{\sigma+1}, \dots, x^{\sigma+d(x)-1}\}$, hence $x^\sigma = x^{\sigma+d(x)}$. This implies $x^\sigma = x^{\sigma+d} = x^{\sigma+2d} = \dots$ and since $\lambda(m/p_1^{\alpha_1} \dots p_s^{\alpha_s})$ is a positive multiple of $d(x)$, we have (5,1). This proves Theorem 5,2.

In the following we shall need

Lemma 5,3. *If $m \neq 8$ and $m \neq 24$, then $\nu(m) \leqq \lambda(m)$.*

Proof. Let $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ and suppose $p_1 < p_2 < \dots < p_r$. If p is odd, $\alpha < \lambda(p^\alpha) = p^{\alpha-1}(p-1)$. Further $\nu(2) = 1 = \lambda(2)$, $\nu(2^2) = 2 = \lambda(2^2)$ and for $\alpha \geqq 4$ we have $\nu(2^\alpha) = \alpha \leqq 2^{\alpha-2} = \lambda(2^\alpha)$. Hence, if m is not of the form $m = 2^3 p_2^{\alpha_2} \dots p_r^{\alpha_r}$, we have $\nu(m) \leqq \lambda(m)$.

i) Let $m = 2^3$. Then $\nu(2^3) = 3 > \lambda(2^3) = 2$. This is the first exceptional case.

ii) Suppose $m = 2^3 p_2^{\alpha_2} \dots p_r^{\alpha_r}$ and $r \geqq 2$. If $\max(\alpha_2, \dots, \alpha_r) = \alpha_j \geqq 3$, we have $\alpha_j = \nu(m) < \lambda(p_j^{\alpha_j}) \leqq \lambda(m)$. Suppose therefore moreover $\alpha_i \leqq 2$ for all $i = 2, \dots, r$. If $r \geqq 3$ (hence $p_3 \geqq 5$), we have

$$\lambda(m) = \text{l.c.m}\,[2, \dots, p_3^{\alpha_3-1}(p_3 - 1), \dots] \geqq 4 > \nu(m) = 3.$$

iii) There remains the case of $m=2^3\cdot p_2^{\alpha_2}$ and $\alpha_2\leqq 2$. If $\alpha_2=2$, $\lambda(m) = [2, p_2(p_2-1)] = p_2(p_2-1) > \nu(m) = 3$. If $\alpha_2=1$ and $p_2\geqq 5$, $\lambda(m) = [2, p_2-1] \geqq 4>\nu(m) = 3$. If $\alpha_2=1$ and $p_2=3$, i.e. $m=24$, we have $\lambda(24) = 2<\nu(24)=3$, the second exceptional case. This proves Lemma 5,3.

We now prove a theorem which is a kind of generalization of the Euler—Fermat theorem and has an algebraic (rather than number-theoretical) flavour.

Theorem 5,3. *Let $m>1$, and $m\neq 8$ and $m\neq 24$. Then for any $x\in S_m$ the element $x^{\lambda(m)}$ is an idempotent $\in S_m$. Hereby the number $\lambda(m)$ is the least integer having this property.*

Proof. By Theorem 5,1 we have $x^\nu=x^{\nu+\lambda}$ for all $x\in S_m$. If $\lambda(m)-\nu(m)>0$, multiply the last relation by $x^{\lambda-\nu}$. We obtain $x^\lambda=x^{2\lambda}$, i.e. x^λ is an idempotent. If $\lambda(m)=\nu(m)$, we have directly $x^\lambda=x^{2\lambda}$.

Remark. If $m=8$, or $m=24$, we have $\nu(m)=3$ and $\lambda(m)=2$. In S_8 and S_{24} the element x^4 is an idempotent for all $x\in S_8$ and $x\in S_{24}$, respectively, and the exponent 4 cannot be replaced by a smaller number.

Corollary 5,3. *Let $m>1$, and $m\neq 8$ and $m\neq 24$. Then for any $x\in S_m$ we have $x^{2\lambda(m)}-x^{\lambda(m)}=[0]$.*

6. Some further applications.

We now give some examples to show how useful the description of S_m may be as given in section 2.

Example 6,1. Let $m>1$ be given. We have to find all $x\in S_m$ for which $x^{\varphi(m)+1}=x$. $(*)$

If x satisfies $(*)$, then $\{x, x^2, \ldots, x^{\varphi(m)}\}$ is cyclic group with $x^{\varphi(m)}=e$ as the identity element. Hence x is contained in the maximal group $G(e)$. Conversely, if an element is contained in a maximal group, say $x\in G(e_1)$, we have $x^{d(x)}=e_1$ and since $d(x)/\lambda(m)/\varphi(m)$, we have $x^{\varphi(m)}=e_1$, whence $x^{\varphi(m)+1} = x$.

We have proved:

Proposition 6,1. *The relation $x^{\varphi(m)+1}=x$ holds if and only if x is contained in a subgroup of S_m.*

This has been proved in [6].

Example 6,2. Under what conditions (concerning m) does there exist an integer $L>1$ such that $x^L=x$ holds for all $x\in S_m$.

If $x=x^L$, $L>1$ holds for all x, we have necessarily $\nu(m)=1$, i.e. $m=p_1\ldots p_r$ is squarefree. In this case S_m is a union of disjoint groups $S_m=\bigcup_{e\in E} G(e)$. By Theorem 5,1 we then have $x=x^{\lambda(m)+1}$ for all $x\in S_m$. Hereby $L=\lambda(m)+1$ is the least integer for which $x=x^L$ for all $x\in S_m$.

It is immediately seen that any L satisfying $x^L=x$ (for all $x\in S_m$) is of the form

$L = l \cdot \lambda(m) + 1$, where $l > 0$ is an integer. Note also that in this case $\lambda(m) = = \text{l.c.m}\,[p_1 - 1, p_2 - 1, \ldots, p_r - 1]$.

We have proved:

Proposition 6,2. *The relation $x^L = x$ with some $L > 1$ holds for all $x \in S_m$ if and only if m is squarefree. The least L having this property is $L = \lambda(m) + 1$.*

This has been proved in [3].

Example 6,3. Let $\pi_L : S_m \to S_m$ be the mapping defined by $x \mapsto x^L$. Under what conditions (concerning m and L) π_L is a permutation of the elements $\in S_m$.

This has been solved in [1]. The problem is the same as to ask under what conditions any element $x \in S_m$ is an L-th power (See [11].) An analogous somewhat more general question has been solved in [13].

Proposition 6,3. *The mapping π_L is a permutation of the elements $\in S_m$ if and only if the following two conditions hold:* i) *m is squarefree,* ii) $(L, \lambda(m)) = 1$.

Proof. If S_m contains a non-zero nilpotent element, π_L cannot be a permutation. For, if π_L is a permutation, so are π_L^2, π_L^3, ... But for any nilpotent element $x \in S_m$ we have $\pi_L^v(x) = x^{vL} = [0]$. Hence if π_L is a permutation, $m = p_1 \ldots p_r$ must be squarefree and $S_m = \bigcup_{e \in E} G(e)$ is a union of disjoint groups.

1. Let π_L be a permutation. Then each of the groups $G(e)$ as a whole is invariant under this mapping. [For, $x \in G(e)$ implies $x^L \in G(e)$.] Now π_L restricted to $G(f_i)$ (a cyclic group of order $p_i - 1$) is a permutation if and only if $(L, p_i - 1) = 1$. Hence a necessary condition in order that π_L should be a permutation is also the fulfilment of the conditions $(L, p_i - 1) = 1$ $(i = 1, \ldots, r)$, which is equivalent to $(L, \lambda(m)) = 1$.

2. Let m be squarefree and $(L, \lambda(m)) = 1$. We first prove that $x \mapsto x^L$ restricted to $G(1)$ is a permutation on $G(1)$. To show this it is sufficient to show that for a_1, $a_2 \in G(1)$ the relation $a_1^L = a_2^L$ implies $a_1 = a_2$. Since $(L, \lambda(m)) = 1$, there exist two integers u, v such that $uL + v\lambda(m) = 1$. Then $a_1^L = a_2^L$ implies $a_1^{uL} = a_2^{uL}$ and (since $a_1^{\lambda(m)} = a_2^{\lambda(m)} = [1]) a_1^{uL+v\lambda} = a_2^{uL+v\lambda}$, hence $a_1 = a_2$.

To end the proof let $x \in S_m$ and $x \in G(e)$ for some $e \in E$. By Theorem 2,3 x can be written in the form $x = [a]e$, $[a] \in G(1)$. Since $[a] = [b]^L$ with some $[b] \in G(1)$, we have $x = [a]e = [b^L e] = [be]^L$ and $[be] \in G(e)$. Hence any element $\in G(e)$ is an L-th power and therefore π_L is a permutation on S_m. This proves Proposition 6,3.

The smallest L satisfying $(L, \lambda(m)) = 1$ is the smallest prime which does not divide $\lambda(m)$.

Example 6,4. The foregoing two examples lead to the following pertinent question. Consider the set Q_m of all mappings π_L: $S_m \to S_m$ defined by $x \mapsto x^L$ (not necessarily a permutation of S_m). Under the usual composition $\pi_L \pi_M(x) = x^{ML}$ the set Q_m is a finite abelian semigroup. Denote by $\bar{Q}_m$ the subgroup of all permutations of the type considered. What can be said about Q_m and $\bar{Q}_m$?

We restrict ourselves to the case when m is squarefree. By means of Theorem 5,1 this can be easily extended to the general case.

Proposition 6,4. *Suppose that m is squarefree. Then*

i) *Q_m is isomorphic with the semigroup $S_{\lambda(m)}$;*
ii) *$\bar{Q}_m$ is isomorphic with the group of units of $S_{\lambda(m)}$.*

Proof. Since for any $x \in S_m$ $x = x^{\lambda(m)+1}$, we also have $\pi_{\lambda+1} = \pi_1$ and $\pi_{\lambda+j} = \pi_j$ for any integer $j > 0$. The mappings $\{\pi_1, \pi_2, \dots, \pi_\lambda\}$ are all different one from the other. Indeed, $\pi_i = \pi_j$, $1 \leqq i \leqq j \leqq \lambda$ would imply $x^i = x^j$ (in particular) for all $x \in G(1)$. Hence $x = x^{j-i+1}$ for all $x \in G(1)$. Now $l = j - i + 1 \leqq \lambda$ and $x = x^l$ with $l < \lambda + 1$ (for all $x \in G(1)$) contradicts Theorem 4,1 (or Proposition 6,2).

Note that π_λ is the zero element $\in Q_m$. It sends each element of a maximal group into the corresponding idempotent. [I.e. $\pi_\lambda(S_m) = E$.]

The mapping $F\colon Q_m \to S_{\lambda(m)}$ defined by $F(\pi_L) = [L]$ has the property that $F(\pi_L \pi_M) \equiv [L]\,[M] \pmod{\lambda}$. It is onto. Hence Q_m is isomorphic with $S_{\lambda(m)}$.

By Proposition 6,3 π_L is a permutation of S_m if and only if $(L, \lambda) = 1$ and $1 \leqq L < \lambda$. Hence $\bar{Q}_m$ is a group consisting of all $\pi_L \in Q_m$ for which $(L, \lambda) = 1$. This proves Proposition 6,4.

Remark. Problems analogous to that treated in Example 6,4 for wider classes of semigroups are treated in [4].

7. An internal direct decomposition of S_m

It is immediately clear that S_m is isomorphic to the (external) direct product $S_{p_1^{\alpha_1}} \times S_{p_2^{\alpha_2}} \times \dots \times S_{p_r^{\alpha_r}}$. To see this it is sufficient to assign to any $x \in S_m$ an r-tuple $(x_1, x_2, \dots, x_r)$, where $x_i \equiv x \pmod{p_i^{\alpha_i}}$. This is a $1-1$ correspondence which preserves the obvious multiplication.

What is not obvious is the question how to embed isomorphically $S_{p_i^{\alpha_i}}$ into the semigroup S_m.

Denote $V_i = \{[0], f_i, [2]\,f_i, \dots, [p_i^{\alpha_i} - 1]f_i\}$. An element $[h]f_i \in V_i$ is equal to $[0]$ (in S_m) iff h is divisible by $p_i^{\alpha_i}$, hence iff $h = 0$. Also any two elements $[h']f_i$, $[h'']f_i$ with $h' \neq h''$ are different since $[h' - h'']f_i = [0]$ would imply that $h' - h''$ is divisible by $p_i^{\alpha_i}$, which is impossible since $|h' - h''| < p_i^{\alpha_i}$.

To prove that V_i is a semigroup consider the product of $x = [h']f_i \in V_i$ and $y = [h'']f_i \in V_i$. We have $xy = [h'h'']f_i$. Write $h'h''$ in the form $h'h'' = h + up_i^{\alpha_i}$, where $h \in \{0, 1, 2, \dots, p_i^{\alpha_i} - 1\}$ and $u \geqq 0$ is an integer. Then $xy = [h + up_i^{\alpha_i}]f_i = [h]f_i$, hence $xy \in V_i$. Summarily:

Lemma 7,1. *The set V_i is a subsemigroup of S_m containing exactly $p_i^{\alpha_i}$ different elements $\in S_m$.*

V_i contains $G(f_i)$ and it can be written as a union of two disjoint sets in the form $V_i = G(f_i) \cup I(f_i)$, where $I(f_i) = \{[h]f_i \mid (h, p_i) > 1,\ 0 \leqq h < p_i^{\alpha_i}\}$. The set $I(f_i)$ is contained in $P(0)$, hence it is a nilpotent subsemigroup of S_m.[As a matter of fact $I(f_i)$ is even a nilpotent ideal of S_m since it follows from the foregoing considerations that $V_i = S_m f_i$.]

Consider now the sets

$$T_i = \{\bar{f}_i + v \mid v \in V_i\}, \qquad i = 1, 2, \dots, r.$$

T_i is a subsemigroup of S_m since $(\bar{f}_i + [h_1]f_i)(\bar{f}_i + [h_2]f_i) = \bar{f}_i + [h_1 h_2]f_i$ and $[h_1 h_2]f_i \in V_i$. Next $T_i \cap T_j = [1]$ if $i \neq j$. For, suppose $\bar{f}_i + [h_1]f_i = \bar{f}_j + [h_2]f_j$, $0 \leqq h_1 < p_i^{\alpha_i}$, $0 \leqq h_2 < p_j^{\alpha_j}$. Multiplying by f_i and f_j we obtain $[h_1]f_i = f_i$ and $f_j = [h_2]f_j$, whence (by Lemma 7,1) $[h_1] = [h_2] = [1]$. But then $\bar{f}_i + [h_1]f_i = \bar{f}_j + [h_2]f_j = [1]$.

The semigroup T_i contains $[1]$ as its unit element and $\bar{f}_i$ as its zero element. T_i contains G_i and it can be written in the form $T_i = G_i \cup I_i$, where $I_i = \{\bar{f}_i + [h]f_i \mid (h, p_i) > 1,\ 0 \leqq h < p_i^{\alpha_i}\}$. Clearly I_i is a semigroup and it is contained in $P(\bar{f}_i) \cdot |I_i| = p_i^{\alpha_i - 1}$. Moreover I_i is a nilpotent ideal of the semigroup T_i (but not of the semigroup S_m if $r > 1$).

The situation is visualized in Figure 3. Note that the whole semigroup T_i is "above" $G(\bar{f}_i)$.

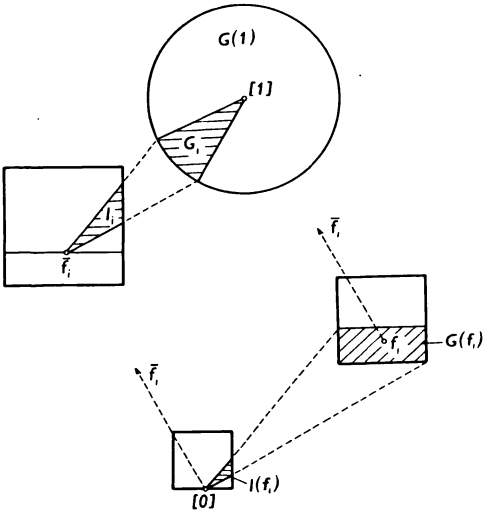

Fig. 3

We now easily prove:

Theorem 7,1. *The semigroup S_m admits the following decomposition into a direct product of its subsemigroups:*

$$S_m = T_1 \cdot T_2 \dots T_r.$$

Hereby $T_i = \{\bar{f}_i + [h]f_i \mid h = 0, 1, \dots, p_i^{\alpha_i} - 1\}$.

Proof. We have proved that $T_i \cap T_j = [1]$. The set $T_1\ T_2 \dots T_r$ contains formally $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ products. To prove our statement it is sufficient to show that two products

$$x = (\bar{f}_1 + v_1) \dots (\bar{f}_r + v_r), \quad v_i \in V_i,$$
$$y = (\bar{f}_1 + u_1) \dots (\bar{f}_r + u_r), \quad u_i \in V_i,$$

are different unless $u_i = v_i$ for all $i = 1, 2, \dots, r$. Suppose that $x = y$. Multiply by f_i. Taking account of the fact that for $j \neq i$ we have $v_j f_i = [0]$ and $\bar{f}_j f_i = f_i$, we obtain $x f_i = v_i f_i = v_i$ and $y f_i = u_i f_i = u_i$, hence $u_i = v_i$ for all $i \in \{1, 2, \dots, r\}$. This proves Theorem 7,1.

Remark. The set T_i can be defined multiplicatively as $T_i = \{x \in S_m \mid x\bar{f}_i = \bar{f}_i\}$. We prefer to define T_i by its explicit description. (See the Remark after Lemma 4,1 concerning the definition of G_i.)

We are now able to give product decompositions of the maximal subsemigroups $P(e)$. Consider the product

$$S_m = T_1\ T_2 \dots T_r = (G_1 \cup I_1)\ (G_2 \cup I_2) \dots (G_r \cup I_r).$$

S_m is a union of the product $G_1\ G_2 \dots G_r$ and $2^r - 1$ products of the form $I_1 \dots I_t\ G_{t+1} \dots G_r\ (1 \leqq t \leqq r)$.

Let $U = I_1 \dots I_t\ G_{t+1} \dots G_r$. Any element $a \in U$ belongs to the idempotent $\bar{f}_1 \dots \bar{f}_t \cdot 1 \dots 1$. If $U \neq U'$ and $a' \in U'$, then a and a' belong to two different idempotents. Hence if $e = \bar{f}_1 \dots \bar{f}_s$, then the set of all elements $\in S_m$ belonging to e is exactly the set $I_1 \dots I_s\ G_{s+1} \dots G_r$ so that $P(e) = I_1 \dots I_s\ G_{s+1} \dots G_r$.

Note that for $i \neq j$ $I_i \cap I_j = \emptyset$ and $G_i \cap G_j = [1]$. We have proved:

Theorem 7,2. *If $e = \bar{f}_1 \dots \bar{f}_s$ $(1 \leqq s \leqq r)$, then $P(e)$ is the direct product of r subsemigroups of S_m:*

$$P(e) = I_1 \dots I_s \cdot G_{s+1} \dots G_r.$$

Corollary 7,1. *If $e = \bar{f}_1 \dots \bar{f}_s$, then*

$$|P(e)| = p_1^{\alpha_1 - 1} \dots p_s^{\alpha_s - 1} \cdot \varphi(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}) =$$

$$= p_1^{\alpha_1 - 1} \dots p_s^{\alpha_s - 1}\ |G(e)| = \frac{m}{p_1 \dots p_r}\ (p_{s+1} - 1) \dots (p_r - 1).$$

Corollary 7,2. *The set of all nilpotent elements $P(0)$ is the direct product $P(0) = I_1\ I_2 \dots I_r$ and $|P(0)| = p_1^{\alpha_1 - 1} \dots p_r^{\alpha_r - 1}$.*

Note that if $r > 1$, then $P(0) \cap I_i = \emptyset$.

For the following Corollary recall the ordering in the Boolean algebra E (see Section 2).

Corollary 7,3. *If $e' > e''$, then $|P(e')| \geqq |P(e'')|$ and $|G(e')| \geqq |G(e'')|$.*

Proof. If $e' = \bar{f}_1 \dots \bar{f}_s$ and $e'' < e'$, then $e'' = \bar{f}_1 \dots \bar{f}_s \cdot \bar{f}_{s+1} \dots \bar{f}_{s+t}$, $1 \leqq t \leqq r-s$. It follows from Corollary 7,1 and Corollary 4,1 $|P(e')| = (p_{s+1}-1) \dots (p_{s+t}-1)\,|P(e'')|$ and $|G(e')| = \varphi(p_{s+1}^{\alpha_{s+1}} \dots p_{s+t}^{\alpha_{s+t}}) \cdot |G(e'')|$. Hence $|P(e')| \geqq |P(e'')|$ and the equality holds iff $t=1$ and $p_{s+1}=2$. Further $|G(e')| \geqq |G(e'')|$ and the sign of equality holds iff $t=1$ and $p_{s+1}^{\alpha_{s+1}}=2$.

Returning to Theorem 7,2 it is worth to note that the product $I_1 \dots I_s = I(e)$ is contained in $P(e)$ while for $s>1$ none of the I_i itself is contained in $P(e)$. Further $I(e)$ is a subsemigroup of $P(e)$ containing e. The set $I(e)$ can be characterized as the set $\{x \in P(e) \mid xe = e\}$. The semigroup $P(e)$ is a direct product of $I(e)$ and the group $G_{s+1} \dots G_r$ which is outside $P(e)$ (namely in $G(1)$). Of course since $G_{s+1} \dots G_r$ is isomorphic with $G(e)$, the semigroup $P(e)$ is isomorphic with the (external) direct product $I(e) \times G(e)$.

We are finally able to describe more precisely the homomorphism ψ_e: $P(e) \to G(e)$ defined by $\psi_e(x) = x \cdot e$ for $x \in P(e)$.

Let $e = \bar{f}_1 \dots \bar{f}_s \neq [0]$ and $x \in P(e) = I_1 \dots I_s\, G_{s+1} \dots G_r$. Then $x = (\bar{f}_1 + [h_1]f_1) \dots (\bar{f}_s + [h_s]f_s) \cdot a$, where $[h_1], \dots, [h_s]$ and a are uniquely determined by x. Next, since (for $1 \leqq i \leqq s$) we have $(\bar{f}_i + [h_i]f_i)e = e$, we obtain $xe = ae \in (G_{s+1} \dots G_r)e = G(e)$. Hence the homomorphism ψ_e sends the whole set $I_1 \dots I_s a \subset P(e)$ into the element $ae \in G(e)$. In particular it sends the whole semigroup $I(e) = I_1 \dots I_s$ into e. Thus $p_1^{\alpha_1-1} \dots p_s^{\alpha_s-1}$ elements $\in P(e)$ are always mapped onto one element $\in G(e)$. (This will be used in Lemma 8,1.)

Theorem 7,1 can be used to solve the following general question. Given two integers L, M, $1 \leqq L < M$ we have to find the number of solutions of $x^L = x^M$ in S_m.

Clearly the set of all solutions forms a subsemigroup $Z = Z(L, M, m)$ of S_m containing [0] and [1]. We first prove a formula for $|Z|$ and next we show on a numerical example how to describe explicitly all the elements $\in Z$.

By Theorem 7,1 any $x \in S_m$ can be written in the form $x = x_1 x_2 \dots x_r$, $x_i \in T_i$, and $x^L = x^M$ holds iff $x_i^L = x_i^M$ for every $i = 1, 2, \dots, r$.

Write again $T_i = G_i \cup I_i$.

i) We first find the number of solutions of $x_i^L = x_i^M$ supposing that $x_i \in I_i$.

If $x_i \in I_i$, then $x_i^L = x_i^M$ implies $x_i^L = x_i^M = x_i^{M+(M-L)} = \dots = x_i^{M+l(M-L)}$ for any integer $l \geqq 0$. But if $M + l(M-L) > \alpha_i$, then $x_i^{M+l(M-L)} = \bar{f}_i$. Hence we have necessarily $x_i^L = \bar{f}_i$. If conversely x_i satisfies $x_i^L = \bar{f}_i$, then for any $M > L$ we have $x_i^M = \bar{f}_i$.

Hence we have to find the number of solutions of $x_i^L = \bar{f}_i$.

An element $x = [p_i^\gamma]g_i \in I_i$ ($\gamma \geqq 1$, $g_i \in G_i$) is a solution of $x_i^L = \bar{f}_i$ iff $\gamma L \geqq \alpha_i$. If $\gamma = \gamma_i$ is the least such integer, then the number of solutions contained in I_i is clearly $p_i^{\alpha_i - \gamma_i}$. Since γ_i is an integer, we have

$$\gamma_i = \begin{cases} \dfrac{\alpha_i}{L} & \text{if } L/\alpha_i, \\ \left[\dfrac{\alpha_i}{L}\right]+1 & \text{if } L\nmid\alpha_i. \end{cases} \tag{7,1}$$

In particular, $\gamma_i = 1$ iff $L \geqq \alpha_i$.

ii) If $x_i \in G_i$, then $x_i^L = x_i^M$ is equivalent to $x_i^{M-L} = [1]$. If p_i is odd, then G_i is a cyclic group of order $\varphi(p_i^{\alpha_i})$ and there are $d_i = (M-L,\ \varphi(p_i^{\alpha_i}))$ elements $\in G_i$ satisfying $x_i^L = x_i^M$. If $p_i^{\alpha_i} = 2$, then the number of solutions in G_i is $d_i = 1$. If $p_i^{\alpha_i} = 4$, the number of solutions is $d_i = (M-L, 2)$. If $p_i^{\alpha_i} = 2^\alpha$, $\alpha \geqq 3$, then the number of solutions of $x_i^{M-L} = [1]$ is $(M-L, 2)\cdot(M-L, 2^{\alpha-2})$.

The foregoing considerations imply:

Theorem 7.3. *Let $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ and $1 \leqq L < M$. Then the number of solutions of $x^L = x^M$ in S_m is given by the formula*

$$|Z(L, M, m)| = \prod_{i=1}^{r} (p_i^{\alpha_i - \gamma_i} + d_i).$$

Here γ_i is defined by (7,1) *and*

$$d_i = \begin{cases} (M-L,\ \varphi(p_i^{\alpha_i})) & \text{if } \textit{if } p_i \textit{ is odd, or } p_i^{\alpha_i} = 2 \textit{ or } p_i^{\alpha_i} = 4; \\ (M-L, 2)\cdot(M-L, 2^{\alpha-2}) & \textit{if } p_i^{\alpha_i} = 2^\alpha, \alpha \geqq 3. \end{cases}$$

As a numerical ilustration consider the equation $x^2 = x^6$ in S_m, where $m = 3^2\, 5^3 = 1125$.

Here $p_1^{\alpha_1} = 3^2$, $\gamma_1 = \frac{2}{2} = 1$, $d_1 = (4, \varphi(1)) = 2$ and $p_2^{\alpha_2} = 5^3$, $\gamma_2 = \left[\frac{3}{2}\right] + 1 = 2$, $d_2 = (4, \varphi(125)) = 4$. Hence $|Z| = (3^{2-1} + 2)\,(5^{3-2} + 4) = 45$. There are exactly 45 solutions of $x^2 = x^6$ in S_m.

We next describe Z. A simple calculation shows that in S_m we have $f_1 = [5^3 \cdot 8] = [1000]$, hence $\bar f_1 = [126] = [3^2 \cdot 14]$. Further (since here primitive and maximal idempotents coincide) $f_2 = [3^2 \cdot 14]$ and $\bar f_2 = [5^3 \cdot 8]$. Therefore

$$T_1 = \{\bar f_1 + [h]f_1 \mid 0 \leqq h < 9\}, \quad T_2 = \{\bar f_2 + [h]f_2 \mid 0 \leqq h < 125\}.$$

The solutions of $x_1^2 = x_1^6$ in I_1 are $\{\bar f_1 + [h]f_1 \mid h = 0, 3, 6\}$. The solutions of $x_1^4 = [1]$ in G_1 are (as it can be easily verified) $\{\bar f_1 + [h]f_1 \mid h = 1,8\}$. Hence all solutions of $x_1^2 = x_1^6$ in T_1 constitute the following subsemigroup of T_1:

$$Z_1 = \{\bar f_1 + [h']f_1 \mid h' \in H'\}, \quad \text{where} \quad H' = \{0, 3, 6, 1, 8\}.$$

The solutions of $x_2^2 = x_2^6$ in I_2 are $\{\bar f_2 + [h]f_2 \mid h = 0{,}25, 50, 75, 100\}$. The four solutions of $x_2^4 = [1]$ in G_2 are $\{\bar f_2 + [h]f_2 \mid h = 1, 57, 68, 124\}$.

[Note that to find $x_2 \in G_2$ it is necessary in essential to solve $x^4 \equiv 1 \pmod{125}$. In numerical calculations we cannot avoid to find first a primitive root g (mod 5), next a primitive root (mod 5^2), which is either g or $g+5$, and to use then the known fact that a primitive root (mod p^2) is a primitive root (mod p^α) for any $\alpha>2$.]

All solutions of $x_2^2=x_2^6$ in T_2 form the semigroup $Z_2 = \{\bar{f}_2 + [h'']f_2 \mid h'' \in H''\}$, where $H'' = \{0, 25, 50, 75, 100, 1, 57, 68, 124\}$.

All 45 solutions in S_m are exactly the elements of the (direct) product of two subsemigroups $Z = Z_1 \cdot Z_2$.

For numerical calculations (see Remark 2 in Section 4) it is of course more convenient to use $(\bar{f}_1 + [h']f_1)(\bar{f}_2 + [h'']f_2) = [h']f_1 + [h'']f_2$. Hence all 45 solutions are $[h' \cdot 1000] + [h'' \cdot 126]$, where h', h'' run indenpendently over the sets H' and H'', respectively.

Remark. An interresting simple result is obtained for the solutions of $x=x^3$. By Theorem 7,3 we get

$$|Z(1,3,m)| = \begin{cases} 3^r & \text{for } m \text{ odd, or } m = 4p_2^{\alpha_2} \dots p_r^{\alpha_r}, \\ 2\cdot 3^{r-1} & \text{for } m = 2\cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}, \\ 5\cdot 3^{r-1} & \text{for } m = 2^\alpha p_2^{\alpha_2} \dots p_r^{\alpha_r},\ \alpha \geqq 3. \end{cases}$$

Suppose that m is odd. Put $Z_i = \{\bar{f}_i, \bar{f}_i - f_i, [1]\}$. Then the set of all solutions is given by $Z = Z_1 \cdot Z_2 \dots Z_r$. In the additive form these are the 3^r elements

$$[h_1]f_1 + [h_2]f_2 + \dots + [h_r]f_r.$$

where h_i run independently through the set $\{0, 1, -1\}$. The modifications necessary in the case of m being even are evident.

By the same method as we have proved Theorem 7,3 we may solve the question concerning the number of solutions of $x^L = x^M$ in a given maximal subsemigroup $P(e)$.

By considering the decomposition $P(e) = I_1 \dots I_s G_{s+1} \dots G_r$ we obtain:

Theorem 7,4. *Let* $e = \bar{f}_1 \dots \bar{f}_s$; *then the number of solutions of* $x^L = x^M$ $(1 \leqq L < M)$ *in* $P(e)$ *is given by the formula*

$$|Z(L,M,m,e)| = p_1^{\alpha_1-\gamma_1} \dots p_s^{\alpha_s-\gamma_s} d_{s+1} \dots d_r,$$

where γ_i *and* d_i *have the same meaning as in Theorem* 7,3.

Theorem 7,3 enables us to prove again some of the results of sections 5 and 6 in a somewhat stronger formulation.

Example 7,1. Let us ask under what conditions $x^L = x^M$ holds identically in S_m (i.e. for all $x \in S_m$).

This is the case iff

$$|Z(L,M,m)| = p_1^{\alpha_1} \dots p_r^{\alpha_r}. \tag{7,2}$$

If p_i is odd, or $p_i^{\alpha_i}=2$ or $p_i^{\alpha_i} \approx 4$, we have $p_i^{\alpha_i-\gamma_i} + d_i = p_i^{\alpha_i-\gamma_i} + (M-L, \varphi(p_i^{\alpha_i})) \leqq p_i^{\alpha_i} - (p_i^{\alpha_i-1} - p_i^{\alpha_i-\gamma_i})$. If $\gamma_i \gtreqless 2$, this term is $< p_i^{\alpha_i}$. If $p_i^{\alpha_i} = 2^{\alpha_i}$, $\alpha_i \geqq 3$, $p_i^{\alpha_i-\gamma_i} + d_i \leqq 2^{\alpha_i-\gamma_i} + (M-L, 2)2^{\alpha_i-2} \leqq 2^{\alpha_i-1} + 2^{\alpha_i-\gamma_i}$ and this is less than 2^{α_i} if $\gamma_i \geqq 2$.

If for at least one i the number γ_i were $\geqq 2$, then the product $\prod_{i=1}^{r}(p_i^{\alpha_i-\gamma_i}+d_i)$ would be less than m. Therefore we necessarily have $\gamma_i=1$ for all $i=1, 2, \dots$, r, i.e. $L \geqq \alpha_i$ for all $i=1, \dots, r$, hence $l \geqq \max(\alpha_1, \dots, \alpha_r) = v(m)$.

Write now (7,2) with $\gamma_i=1$ in the form

$$1=\prod_{i=1}^{r}\frac{p_i^{\alpha_i-1}+d_i}{p_i^{\alpha_i}}.$$

Since each factor to the right is $\leqq 1$, we have necessarily $p_i^{\alpha_i-1} + d_i = p_i^{\alpha_i}$, $d_i = p_i^{\alpha_i} - p_i^{\alpha_i-1} = \varphi(p_i^{\alpha_i})$. Hence $(M-L, \varphi(p_i^{\alpha_i})) = \varphi(p_i^{\alpha_i})$), i.e. $\lambda(p_i^{\alpha_i}) | M-L$, except the case $p_i^{\alpha_i}=2^\alpha$, $\alpha \geqq 3$. In this last case we have $\varphi(2^\alpha) = 2^{\alpha-1} = (M-L, 2)(M-L, 2^{\alpha-2})$, hence $2^{\alpha-2} | M-L$, i.e. again $\lambda(2^\alpha) | M-L$. We have obtained: For $i=1, \dots, r$ we have necessarily $\lambda(p_i^{\alpha_i}) | M-L$. Hence l.c.m $[\lambda(p_1^{\alpha_1}), \dots, \lambda(p_r^{\alpha_r})]$ divides $M-L$.

If conversely $\gamma_i=1$ for all i (i.e. $L \geqq v(m)$) and $M-L$ is divisible by $\lambda(m)$, it is immediately obvious that $|Z(L, M, m)|=m$. We have

Proposition 7,1. *The relation $x^L=x^M$ holds in S_m identically iff $L \geqq v(m)$ and $\lambda(m) | M-L$.*

This is a stronger edition of Theorem 5,1.

In particular we may ask under what conditions x^L is an idempotent $\in S_m$, i.e. the relation $x^L=x^{2L}$ holds identically in S_m. Proposition 7,1 implies that this is the case iff $L \geqq v(m)$ and $\lambda(m) | L$. Taking account of Lemma 5,3 we have:

Proposition 7,2. *If $m \neq 8$, $m \neq 24$, then x^L is an idempotent for any $x \in S_m$ iff $\lambda(m) | L$. If $m=8$ or $m=24$, then x^L is an idempotent (for any x) iff $L \geqq 4$ and L is even.*

Example 7,2. Let us ask under what conditions $x^L=x^M$ holds identically in $P(e)$.

This is the case iff $|Z(L, M, N, e)| = |P(e)|$, i.e.

$$(7,3) \qquad p_1^{\alpha_1-\gamma_1}\dots p_s^{\alpha_s-\gamma_s}d_{s+1}\dots d_r = p_1^{\alpha_i-1}\dots p_s^{\alpha_s-1}\varphi(p_{s+1}^{\alpha_{s+1}}\dots p_r^{\alpha_r}).$$

This implies $\gamma_1=\dots=\gamma_s=1$, hence $L \geqq \max(\alpha_1, \dots, \alpha_s)$ and (for $i=s+1, \dots, r$) $d_i=\varphi(p_i^{\alpha_i})$. The relation $d_i=\varphi(p_i^{\alpha_i})$ implies analogously as above $\lambda(p_i^{\alpha_i}) | M-L$ for $i=s+1, \dots, r$, and since l.c.m $[\lambda(p_{s+1}^{\alpha_{s+1}}), \dots, \lambda(p_r^{\alpha_r})] = \lambda(m/p_1^{\alpha_1}\dots p_s^{\alpha_s})$, we have necessarily $\lambda(m/p_1^{\alpha_1}\dots p_s^{\alpha_s})/M-L$.

Conversely if $\gamma_1=\dots=\gamma_s=1$ and $\lambda(m/p_1^{\alpha_1}\dots p_s^{\alpha_s})/M-L$, then (7,3) holds. We have:

Proposition 7,3. *Let be $e=\bar{f}_1\dots\bar{f}_s$. Then $x^L=x^M$ $(1 \leqq L < M)$ holds for all $x \in P(e)$ iff $L \geqq \max(\alpha_1, \dots, \alpha_s)$ and $\lambda(m/p_1^{\alpha_1}\dots p_s^{\alpha_s})$ divides $M-L$.*

Theorem 5,2 is a relation of this form with the smallest possible exponents.

8. New extensions of a classical result

There is an old result of Gauss stating that

$$\prod_{u\in G(1)} u = \begin{cases} [-1] & \text{if } m=4, \text{ or } m=p^{\alpha}, \text{ or } m=2p^{\alpha}, \\ & (p \text{ odd}, \alpha\geqq 1) \\ [1] & \text{in all other cases.} \end{cases}$$

We extend this result by considering the products $\Pi_e=\prod_{u\in G(e)} u$ and $\Pi'_e=\Pi_{u\in P(e)} u$ for a given idempotent $e\in S_m$. We may exclude the case $e=[0]$, since then $\Pi_e=\Pi'_e=[0]$ and the case $e=[1]$ given by Gauss (though this last one will follow from our considerations).

We suppose in the following again $m=p_1^{\alpha_1}\dots p_r^{\alpha_r}$.

The relation between Π_e and Π'_e is given by the following.

Lemma 8,1. *If* $e=\bar f_1\dots\bar f_s=[p_1^{\alpha_1}\dots p_s^{\alpha_s}a]$, $[a]\in G(1)$, $0<s<r$, *then* $\Pi'_e= =(\Pi_e)^v$, *where* $v=p_1^{\alpha_1-1}\dots p_s^{\alpha_s-1}$.

Proof. Since $e\in P(e)$, we may write $\Pi'_e=(\prod_{u\in P(e)} u)e=\prod_{u\in P(e)}(ue)$. We have seen (see Section 7) that the homomorphism $\psi_e\colon P(e)\to G(e)$ defined by $u\mapsto ue$ sends always $p_1^{\alpha_1-1}\dots p_s^{\alpha_s-1}$ different elements $\in P(e)$ into the same element $ue\in G(e)$. Hence $\Pi'_e=(\Pi_e)^{p_1^{\alpha_1-1}\dots p_s^{\alpha_s-1}}$, which proves Lemma 8,1.

If $e=\bar f_1\dots\bar f_s$, then by Lemma 4,3 we have $G(e)=G_{s+1}\dots G_r\cdot e$ and for $x\in G_i$ $(i=s+1,\dots,r)$ the mapping $x\mapsto xe_i$ is an isomorphism of G_i onto G_ie. Hence for $s+1\leqq i\leqq r\prod_{u\in G_ie} u=(\prod_{u\in G_i} u)\cdot e$. Denote $\beta_i=\dfrac{|G(e)|}{\varphi(p_i^{\alpha_i})}=\dfrac{\varphi(p_{s+1}^{\alpha_{s+1}}\dots p_r^{\alpha_r})}{\varphi(p_i^{\alpha_i})}$. We then have

$$(8,1)\qquad \Pi_e=\prod_{u\in G(e)} u=[\prod_{u\in G_{s+1}\dots G_r} u]e=[\prod_{u\in G_{s+1}} u]^{\beta_{s+1}}\dots[\prod_{u\in G_r} u]^{\beta_r}\cdot e.$$

It follows that the problem reduces (in essential) to find the values of $\prod_{u\in G_i} u$.

Lemma 8,2. *For* $i=1, 2, \dots, r$ *we have*

$$\prod_{u\in G_i} u=\begin{cases}\bar f_i-f_i & \textit{if } p_i>2,\ \alpha_i\geqq 1,\ \textit{or } p_i^{\alpha_i}=4, \\ [1] & \textit{if } p_i^{\alpha_i}=2,\ \textit{or } p_i^{\alpha_i}=2^{\alpha_i},\ \alpha_i\geqq 3.\end{cases}$$

Proof. By the definition

$$G_i=\{\bar f_i+[h]f_i\mid 0\leqq h<p_i^{\alpha_i}, (h, p_i)=1\},$$

$$\prod_{u\in G_i} u=\prod_h(\bar{f}_i+[h]f_i)=\bar{f}_i+[\varepsilon]f_i,$$

where ε is the product of $\varphi(p_i^{\alpha_i})$ positive integers less than and prime to $p_i^{\alpha_i}$. Denote this set by $U(p_i^{\alpha_i})$.

1. Suppose $p_i>2$; then $U(p_i^{\alpha_i})$ is a cyclic group of order $v=\varphi(p_i^{\alpha_i})$ with a generating element, say g_i, so that $\varepsilon\equiv g_i g_i^2 \dots g_i^v \equiv g_i^{v/2(v+1)}$ ((mod $p_i^{\alpha_i}$). Since $g_i^{v/2}\equiv -1 \pmod{p_i^{\alpha_i}}$ and $v+1$ is odd, we have $\varepsilon\equiv -1 \pmod{p_i^{\alpha_i}}$. Hence $\prod_{u\in G_i} u = \bar{f}_i - f_i$.

2. If $p_i^{\alpha_i}=2$, G_i is a one point group and $\prod_{u\in G_i} u=[1]$.

3. If $p_i^{\alpha_i}=4$, then $\prod_{u\in G_i} u = (\bar{f}_i + f_i)(\bar{f}_i + [3]f_i) = \bar{f}_i - f_i$.

4. If $p_i^{\alpha_i}=2^\alpha$, $\alpha\geqq 3$, we use the known fact that $\{\pm 5, \pm 5^2, \dots \pm 5^v\}$, where $v=2^{\alpha-2}$ constitutes the set of all odd residue classes (mod 2^α). Hence

$$\varepsilon\equiv(-1)^v(5\cdot 5^2 \dots 5^v)^2\equiv(5^{2^{\alpha-1}}\cdot 5^{-1})^2\equiv 1 \pmod{2^\alpha}.$$

Therefore $\prod_{u\in G_i} u=\bar{f}_i+f_i=[1]$. This proves Lemma 8,2.

Remark. If $r=1$, i.e. $m=p^\alpha$, $G(1)=G_1$, we may write $f_1=[1]$, $\bar{f}_1=[0]$ and Lemma 8,2 implies

$$\prod_{u\in G(1)} u=\begin{cases}[-1] & \text{if } m \text{ is odd or } m=4,\\ [1] & \text{if } m=2 \text{ or } m=2^\alpha,\ \alpha\geqq 3.\end{cases}$$

(This constitutes a part of the statement of Gauss.)

Henceforth we may suppose $r\geqq 2$.

We prove:

Theorem 8,1. *Let $m=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ and $r\geqq 2$. Let $e\neq[1]$ be an idempotent $\in S_m$ and $\Pi_e=\prod_{u\in G(e)} u$. We have:*

1. $\Pi_e=-e$ for any primitive idempotent, with the exception that $m=2^\alpha p_2^{\alpha_2}\dots p_r^{\alpha_r}$, $\alpha\neq 2$, $\alpha>0$ and e is the (primitive) idempotent $e=\left[\frac{m}{2^\alpha}a\right]$, $[a]\in G(1)$. In this exceptional case $\Pi_e=e$.

2. $\Pi_e=e$ for any non-primitive idempotent $\in S_m$, with the exception of the case when $m=2p_2^{\alpha_2}\dots p_r^{\alpha_r}$ and e is any of the $r-1$ (non-primitive) idempotents of the form $e=\left[\frac{m}{2p_i^{\alpha_i}}a_i\right]$, $[a_i]\in G(1)$. In these exceptional cases we have $\Pi_e=-e$.

Proof. Let $e=\bar{f}_1\dots\bar{f}_s$, $1\leqq s<r$, $r\geqq 2$. We shall use Lemma 8,2 and the formula (8,1). We have to consider several cases.

A. Suppose first that $r-s\geqq 2$ (i.e. e is a non-primitive idempotent $\in S_m$).

If all primes $p_{s+1}, \ldots, p_r$ are odd, or $r-s \geqq 3$, then all $\beta_{s+1}, \ldots, \beta_r$ are even. Since $(\bar{f}_i - f_i)^2 = [1]$, formula (8,1) implies $\Pi_e = e$.

There remains the case of $r-s=2$, i.e. $e = \bar{f}_1 \ldots \bar{f}_{r-2}$, hence $p_{s+1} = p_{r-1}$, $p_{s+2} = p_r$, where one of the primes, say p_{r-1}, is even and p_r is odd. In this case $G(e) = G_{r-1} \cdot G_r e$ and by (8,1)

$$\Pi_e = [\prod_{u \in G_{r-1}} u]^{\beta_{r-1}} [\prod_{u \in G_r} u]^{\beta_r} \cdot e$$

Here $\beta_{r-1} = \varphi(p_r^{\alpha_r})$ is even, while $\beta_r = \varphi(2^{\alpha_{r-1}})$ is equal to 1 for $\alpha_{r-1} = 1$ and even for $a_{r-1} \geqq 2$.

We shall now distinguish three cases, namely that $p_{r-1}^{\alpha_{r-1}} \cdot p_r^{\alpha_r}$ is either $2p_r^{\alpha_r}$ or $4p_r^{\alpha_r}$ or $2^{\alpha_{r-1}} \cdot p_r^{\alpha_r}$, $\alpha_{r-1} \geqq 3$.

a) If $p_{r-1}^{\alpha_{r-1}} = 2$, then (by Lemma 8,2)

$$\Pi_e = [1]^{\beta_{r-1}} \cdot (\bar{f}_r - f_r) \cdot e\,.$$

We shall show that this product is $-e$. By definition of e and $\bar{f}_r$ there are elements $[a']$, $[a|] \in G(1)$ such that $e = [a' \cdot m/2p_r^{\alpha_r}]$, $\bar{f}_r = [a| \cdot p_r^{\alpha_r}]$. Hence

$$(\bar{f}_r - f_r)e = ([2]\bar{f}_r - [1])e = [2]\,[p_r^{\alpha_r} \cdot a|]\,[a'm/2p_r^{\alpha_r}] - e = -e\,.$$

Thus $\Pi_e = -e$.

b) If $p_{r-1}^{\alpha_{r-1}} = 4$, we have

$$\Pi_e = [\prod_{u \in G_{r-1}} u]^{\beta_{r-1}} [\prod_{u \in G_r} u]^2 \cdot e = (\bar{f}_{r-1} - f_{r-1})^{\beta_{r-1}} (\bar{f}_r - f_r)^2 e = e\,.$$

c) If $p_{r-1}^{\alpha_{r-1}} = 2^{\alpha_{r-1}}$, $\alpha_{r-1} \geqq 3$, then $\prod_e = [1]^{\beta_{r-1}} (\bar{f}_r \sim f_r)^{\beta_r} \cdot e = e$.

B. Suppose next that $r-s=1$, i.e. $e = \bar{f}_1 \ldots \bar{f}_{r-1} \neq f_r$, where f_r is a primitive idempotent $\in S_m$. In this case we have $\Pi_e = [\prod_{u \in G_r} u]e = [\prod_{u \in G_r} u]f_r$.

a) If $p_r > 2$, then (by Lemma 8,2) $\Pi_e = (\bar{f}_r - f_r) \cdot f_r = -f_r = -e$.
b) If $p_r^{\alpha_r} = 2$, then $\Pi_e = [1]f_r = e$.
c) If $p_r^{\alpha_r} = 4$, then $\Pi_e = (\bar{f}_r - f_r) f_r = -e$.
d) If $p_r^{\alpha_r} = 2^{\alpha_r}$, $\alpha_r \geqq 3$, then $\Pi_e = [1]f_r = e$.

The proof of Theorem 8,1 is complete.

Remark. The formula (8,1) can be extended also to the case $e=[1]$, $r\geqq 2$. It has then the form

$$\prod_{u\in G(1)} u=[\prod_{u\in G_1} u]^{\beta_1}\dots[\prod_{u\in G_r} u]^{\beta_r}$$

and the same calculations show that the product is [1] with the exception of the case $m=2p^\alpha$, in which case it has the value $[-1]$. (This is the remaining part of the statement of Gauss.)

To find the value of Π'_e we use Lemma 8,1.

If $\Pi_e=e$, then $\Pi'_e=e$, so that we have to consider only the cases in which $\Pi_e=-e$.

A. Suppose that e is a primitive idempotent.

a) If all p_i $(i=1, \dots, r)$ are odd, then $\Pi'_e=(-e)^v$, where $v=p_1^{\alpha_1-1}\dots p_s^{\alpha_s-1}$, $s=r-1$, hence $\Pi'_e=-e$.

b) If $m=4p_2^{\alpha_2}\dots p_r^{\alpha_r}$ and e is the primitive idempotent $e=\left[\frac{m}{4}a\right]$, $[a]\in G(1)$, then $\Pi'_e=(-e)^v$, where $v=p_2^{\alpha_2-1}\dots p_r^{\alpha_r-1}$, hence $\Pi'_e=-e$.

B. If $m=2p_2^{\alpha_2}\dots p_r^{\alpha_r}$ and e is a (non-primitive) idempotent of the form, say, $e=[a\cdot m/2p_2^{\alpha_2}]$, $[a]\in G(1)$, then $\Pi'_e=(-e)^v$, where $v=p_3^{\alpha_3-1}\dots p_r^{\alpha_r-1}$, hence $\Pi'_e=-e$.

Combining these results with Theorem 8,1 we obtain finally (including $e=[1]$ and $e=[0]$):

Theorem 8,2. *For any idempotent $e\in S_m$ we have $\prod_{u\in P(e)} u=\prod_{u\in G(e)} u$. The common value of these products is specified in Theorem* 8,1.

REFERENCES

[1] CORDES, C. M.: Permutations mod m in the form x^n. Amer. Math. Monthly 83, 1976, 32—33.

[2] HEWITT, E.—ZUCKERMAN, H. S.: The multiplicative semigroup of integers (mod m). Pacific J. Math. 10, 1960, 1291—1308.

[3] HEWITT, E.: Certain congruences that hold identically. Amer. Math. Monthly 83, 1976, 270—271.

[4] KOWOL, G.—MITSCH, H.: Polynomial functions over commutative semigroups. Semigroup Forum 12, 1976, 109—118.

[5] LIVINGSTON, A. E.—LIVINGSTON, M. L.: The congruence $a^{r+s}=a^s$ (mod m). Amer. Math. Monthly 85, 1978, 97—100.

[6] MORGADO, J.: A property of the Euler φ-function concerning the integers which are regular (mod m). Portugal. Math. 33, 1974, 185—191.

[7] OSBORN, R.: A "good" generalization of the Euler—Fermat theorem. Math. Mag. 47, 1974, 28—31.

[8] PARÍZEK, B.—SCHWARZ, Š.: O multiplikatívnej pologrupe zvyškových tried (mod m). Mat.-Fyz. Časop. 8, 1958, 136—150.

[9] PARÍZEK, B.: O rozklade pologrupy zvyškov (mod m) na direktný súčin. Mat.-Fyz. Časop. 10, 1960, 18—29.

[10] SINGMASTER, D.: A maximal generalization of Fermat's theorem. Math. Mag. 39, 1966, 103—107.

[11] SMALL, CH.: Powers mod m. Math. Mag. 50, 1977, 84—86.

[12] VANDIVER, H. S.—WEAVER, H. W.: Introduction to arithmetic factorization and congruences from the standpoint of abstract algebra. H. E. Slaught Memorial Papers, no. 7, 1958, Math. Assoc. of America.

[13] ZANE, B.: Uniform distribution (mod m) of monomials. Amer. Math. Monthly 71, 1964, 162—164.

[14] BUCHŠTAB, A. A.: Teorija čisel. Gos. uč.-ped. izd., Moskva, 1960.

[15] DICKSON, L. E.—BODEWIG, E.: Introduction to the Theory of Numbers. (German edition.) Teubner, Leipzig, 1931.

Received October 12, 1979

Matematický ústav SAV
Obrancov mieru 49
886 25 Bratislava

РОЛЬ ПОЛУГРУПП В ЭЛЕМЕНТАРНОЙ ТЕОРИИ ЧИСЕЛ

Штефан Шварц

Резюме

Пусть S_m-мултипликативная полугруппа классов вычетов по составному модулю m. Изучается структура S_m, в частности описиватся множество идемпотентов, строение максимальных групп и максималшных полугрупп, принадлежащих к данному идемпотенту.

Цель этой работы показать, что многие различные теоремы, касающиеся сравнений по модулю m, легче понять, применяя методы известные из теории конечных коммутативных полугрупп (в том числе получаются и некоторые результаты, которые нельзя назвать общеизвестными). Эта точка зрения ведёт даже к результатам, которые (по всей вероятности) никогда небылы опубликованы. (См., например, Теоремы 5,2 и 5,3 или 8,1 и 8,2.)