Štefan Schwarz

An unconventional problem in the elementary theory of numbers

Czechoslovak Mathematical Journal, Vol. 31 (1981), No. 1, 159–169

Persistent URL: http://dml.cz/dmlcz/101733

Czechoslovak Mathematical Journal, 31 (106) 1981, Praha

AN UNCONVENTIONAL PROBLEM IN THE ELEMENTARY THEORY OF NUMBERS

ŠTEFAN SCHWARZ, Bratislava

(Received December 27, 1979)

Let $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $\alpha_i \geqq 1$, be the factorization of an integer $m > 1$ into different primes and $S(m)$ the multiplicative semigroup of residue classes (mod m). The class containing the number a will be denoted by $[a]$. We shall freely use the fact that $S(m)$ admits also an addition. We deal with residue classes as with elements of the finite semigroup $S(m)$. However, in some places, where various modules appear, it will be more convenient to deal with congruences.

In studying the structure of $S(m)$ I has been led to the following question. Let $[a] \in S(m)$. What can be said about the value of the sum

$$[A] = [A(a, m)] = [a + a^2 + \dots + a^{\varphi(m)}],$$

where $\varphi(m)$ is the Euler function?

It turns out that $[A]$ (and analogous sums to be considered below) can be easily computed by means of the idempotents contained in $S(m)$. The question is non-trivial only in the case $(a - 1, m) > 1$. The result given, e. g., in Theorem 1 seems to be of a considerable interest since there are few results in which the idempotents $\in S(m)$ (different from $[1]$) play an essential role.

I have not been able to find problems of this kind in Dickson's History of the Theory of Numbers nor elsewhere. This explains the title of the paper.

1. PRELIMINARIES

In the following we shall need some facts concerning $S(m)$ which have been proved in extenso in the paper [1]. Some of them are by far not commonly known.

Denote by $G(m)$ the group of units of $S(m)$, i.e. $G(m) = \{[a] \in S(m) \mid (a, m) = 1\}$. Then $S(m)$ can be written as a union of two disjoint sets $S(m) = G(m) \cup N(m)$, where $N(m) = \{[a] \in S(m) \mid (a, m) > 1\}$. The group $G(m)$ is order $\varphi(m)$. The order of any element $[a] \in G(m)$ is a divisor of $\lambda(m)$ (the Carmichael function). Here $\lambda(m)$ is defined as follows:

a)

$$\lambda(p^\alpha) = \begin{cases} \varphi(p^\alpha) \text{ if } p \text{ is odd, or } p^\alpha = 2, \text{ or } p^\alpha = 4\,, \\ 2^{\alpha-2} \text{ if } p^\alpha = 2^\alpha \text{ and } \alpha \geqq 3\,. \end{cases}$$

b) If $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$,

$$\lambda(m) = \text{l.c.m.}\ [\lambda(p_1^{\alpha_1}), \dots, \lambda(p_r^{\alpha_r})]\,.$$

Consider now any element $[a] \in S(m)$ and the sequence

$$(1) \qquad [a], [a]^2, [a]^3, \dots .$$

If $[a] \in G(m)$, then since $[a]^{\lambda(m)} = [1]$ there is a least integer $d(a)$ such that $[a]^{d(a)} = [1]$ and $d[a]/\lambda(m)$. The sequence (1) is of the form

$$[a], [a]^2, \dots, [a]^{d(a)} = [1], \mid [a], [a]^2, \dots,$$

hence periodic with the period $d(a)$.

If $[a] \in N(m)$, this need not be true. But it can be proved that for any $[a] \in S(m)$ we have $[a]^{\nu(m)} = [a]^{\nu/m) + \lambda(m)}$, where $\nu(m) = \max(\alpha_1, \alpha_2, \dots, \alpha_r)$. Hence to any $[a] \in S(m)$ there is a least integer $k(a) \geqq 1$ and a least integer $d(a)$ such that $[a]^{k(a)} = [a]^{k(a)+d(a)}$. Here $k(a) \leqq \nu(m)$ and $d(a) \mid \lambda(m)$. The sequence (1) is of the form

$$[a], [a]^2, \dots, [a]^{k(a)-1}, \mid [a]^{k(a)}, \dots, [a]^{k(a)+d(a)-1}, \mid [a]^{k(a)}, [a]^{k(a)+1}, \dots$$

hence ultimately periodic with the period $d(a)$. (It may happen that $k(a) = 1$ even for $[a] \in N(m)$ so that (1) is periodic.)

The sequence (1) contains one and only one idempotent $[e] = [e_a] \in S(m)$. If $[a] \in G(m)$, this idempotent is $[1]$. If $[a] \in N(m)$, then the least exponent $r = r(a)$ for which $[a]^r$ is an idempotent is uniquely determined by the conditions $k(a) \leqq r(a) \leqq k(a) + d(a) - 1$ and $d(a) \mid r(a)$.

If $[e]$ is the (unique) idempotent contained in the sequence (1), we shall say that $[a]$ *belongs to the idempotent* $[e]$.

In particular, for any $[a] \in S(m)$, $[a]^{\varphi(m)}$ is an idempotent, namely the idempotent to which $[a]$ belongs. (If $m \neq 8$ and $m \neq 24$ it can be shown that even $[a]^{\lambda(m)}$ is an idempotent.)

We now describe the set E of all idempotents contained in $S(m)$. The semigroup $S(m)$ contains exactly 2^r idempotents (including $[0]$ and $[1]$). Any idempotent $\in S(m)$ can be written in the form $[e] = [p_1^{l_1} \dots p_r^{l_r} . u]$, where l_i is either 0 or α_i and $[u]$ is a suitably chosen element $\in G(m)$. The element $[u]$ is not necessarily uniquely determined.

The set E is a Boolean algebra if the operations $\vee$ and $\wedge$ are defined as follows. Let $[e'], [e''] \in E$,

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

$$[e''] = [p_1^{j_1} \dots p_r^{j_r} v]\,, \quad \text{where } j_i \text{ is either 0 ot } \alpha_i\,,$$

and $[u], [v] \in G(m)$. Define

$$[e'] \wedge [e''] = [p_1^{\max(l_1, j_1)} \dots p_r^{\max(l_r, j_r)} u_1]\,,$$

$$[e'] \vee [e''] = [p_1^{\min(l_1, j_1)} \dots p_r^{\min(l_r, j_r)} v_1]\,,$$

where $[u_1], [v_1] \in G(m)$ are determined by the requirement that $[e'] \wedge [e'']$, $[e'] \vee \vee [e'']$ are idempotents $\in S(m)$. It is easy to show that with these operations E becomes a Boolean algebra. (Here $[e'] \wedge [e'']$ may be simply replaced by $[e' \,.\, e'']$.)

We give a computational procedure how to find the idempotent $[e_a]$ to which a given element $[a] \in S(m)$ belongs. Suppose that $[a] = [u p_{i_1}^{\beta_1} \dots p_{i_s}^{\beta_s}]$, $[u] \in G(m)$, $\{i_1, \dots, i_s\} \subset \{1, 2, \dots, r\}$ and $\beta_i \geqq 1$. Then $[e_a] = [v p_{i_1}^{\alpha_{i_1}} \dots p_{i_s}^{\alpha_{i_s}}]$ and $v \in G(m)$ can be computed from the condition $[v \,.\, p_{i_1}^{\alpha_{i_1}} \dots]^2 = [v p_{i_1}^{\alpha_{i_1}} \dots]$, i.e., by solving the congruence

$$v \,.\, p_{i_1}^{\alpha_{i_1}} \dots p_{i_s}^{\alpha_{i_s}} \equiv 1 \pmod{m \mid p_{i_1}^{\alpha_{i_1}} \dots p_{i_s}^{\alpha_{i_s}}}\,.$$

The idempotents $\in S(m)$ of the form

$$[\bar{f}_i] = [u_i p_i^{\alpha_i}]\,, \quad [u_i] \in G(m)\,,$$

$(i = 1, \dots, r)$ are called the *maximal idempotents* $\in S(m)$. Any idempotent which is $\neq [1]$ can be written as a product of maximal idempotents. Let a be an integer which is divisible by $p_{i_1}^{\beta_1} \dots p_{i_s}^{\beta_s}$, $\{i_1, \dots, i_s\} \subset \{1, 2, \dots, r\}$, i.e. $[a] = [u p_{i_1}^{\beta_1} \dots p_{i_s}^{\beta_s}]$, where $[u] \in G(m)$. Then it can be proved that $[a]$ belongs to the idempotent $[\bar{f}_{i_1} \cdot \bar{f}_{i_2} \cdots \bar{f}_{i_s}]$.

The *primitive idempotents* $\in S(m)$ are idempotents of the form $[f_i] = [u_i(m/p_i^{\alpha_i})]$, $[u_i] \in G(m)$. They posses the orthogonality property, i.e. $[f_i] \,.\, [f_j] = 0$ if $i \neq j$. Also $[f_i] + [\bar{f}_i] = [1]$. Any idempotent $\neq [0]$ can be written as a sum of primitive idempotents.

A numerical illustration of a part of the results just described is given at the end of the paper.

Finally, we recall the Chinese remainder theorem, which in our terminology has the following form:

If $[x] \in S(m)$ and $x \equiv a_1 \pmod{p_1^{\alpha_1}}, \dots, x \equiv a_{p_r} \pmod{p_r^{\alpha_r}}$, then $[x] = [a_1 f_1 + \dots \dots + a_r f_r]$.

2. THE CASE $[a] \in G(m)$

Suppose that $[a] \in G(m)$ and consider the element

$$[A] = [A(a, m)] = [a] + [a]^2 + \ldots + [a]^{\varphi(m)}.$$

If d is the order of $[a]$ in $G(m)$, we have

$$[A] = \left[(a + \ldots + a^d) \cdot \frac{\varphi(m)}{d}\right].$$

Since $\{[a], [a]^2, \ldots, [a]^d\}$ is a group, we have $[A][a] = [A]$, i.e. $[A][a-1] = [0]$. If $[a - 1] \in G(m)$, this implies $[A] = [0]$. So the difficulties are restricted to the case $(a - 1, m) > 1$, i.e., $[a - 1] \in N(m)$.

We begin with the case $m = p^\alpha$ and prove:

Lemma 1. *Let p be a prime, $\alpha \geqq 1$, a an integer with $(a, p) = 1$ and $A = a + a^2 + \ldots + a^{\varphi(p^\alpha)}$.*

a) *For p odd, we have*

$$A \equiv \begin{cases} 0 & (\text{mod } p^\alpha) \quad \textit{if} \quad (a-1, p) = 1\,. \\ \varphi(p^\alpha) & (\text{mod } p^\alpha) \quad \textit{if} \quad (a-1, p) = p\,, \end{cases}$$

b) *For $p = 2$, we have*

$$A \equiv \begin{cases} \varphi(2^\alpha)\,(\text{mod } 2^\alpha) & \textit{if } \alpha = 1, \textit{ or } \alpha \geqq 2 \textit{ and } a \textit{ is of the form } 4l + 1\,, \\ 0 \quad (\text{mod } 2^\alpha) & \textit{if } \alpha \geqq 2 \textit{ and } a \textit{ is of the form } 4l + 3\,. \end{cases}$$

Proof. With respect to the remark at the beginning of this section it is sufficient to consider only the case $(a - 1, p) = p$, i.e., a of the form $a = 1 + lp$ (l an integer). Further, if $\alpha = 1$ and p is odd we have $A \equiv (1 + lp) + \ldots + (1 + lp)^{p-1} \equiv p - 1 = \varphi(p) \pmod p$. If $\alpha = 1$ and $p = 2$, then $A \equiv 1 = \varphi(2) \pmod 2$.

Henceforth we may suppose $\alpha \geqq 2$.

We first have the following arithmetical identity:

$$A = (a + a^2 + \ldots + a^{\varphi(p^{\alpha-1})})(1 + a^{\varphi(p^{\alpha-1})} + a^{2\varphi(p^{\alpha-1})} + \ldots + a^{(p-1)\varphi(p^{\alpha-1})}).$$

The first factor can be decomposed in the same manner and repeating this procedure we obtain A as a product of α factors

$$A = U_0 U_1 \ldots U_{\alpha-1},$$

where

$$U_0 = a + a^2 + \ldots a^{p-1},$$

$$U_i = 1 + a^{\varphi(p^i)} + a^{2\varphi(p^i)} + \ldots + a^{(p-1)\varphi(p^i)} \quad \text{for} \quad 1 \leqq i \leqq \alpha - 1\,.$$

a) Suppose $p > 2$ and $a = 1 + lp$. Then

$$U_0 = (1 + lp) + \ldots + (1 + lp)^{p-1} \equiv p - 1 \pmod{p},$$

hence $U_0 = p - 1 + l_0 p$ with an integer l_0. For $1 \leqq i \leqq \alpha - 1$,

$$U_i = 1 + (1 + lp)^{\varphi(p^i)} + \ldots + (1 + lp)^{(p-1)\varphi(p^i)} \equiv$$

$$\equiv p + lp\,\varphi(p^i)\,[1 + 2 + \ldots + (p - 1)] \equiv$$

$$\equiv p + \tfrac{1}{2}l\,\varphi(p^i)\,p^2(p - 1) \equiv p \pmod{p^2}.$$

Hence $U_i = p + l_i p^2$ with an integer l_i. Therefore

$$A = [(p - 1) + l_0 p]\,[p + l_1 p^2] \ldots [p + l_{\alpha-1} p^2],$$

which immediately implies $A \equiv (p - 1)\,p^{\alpha-1} \pmod{p^\alpha}$. This proves Lemma 1 for $p > 2$.

b) If $p = 2$, our identity has the form

$$A = a(1 + a)(1 + a^2)(1 + a^4)\ldots(1 + a^{2^{\alpha-2}}).$$

α) If a is of the form $1 + 4l$, then (for $0 \leqq i \leqq \alpha - 2$) we have $1 + (1 + 4l)^{2^i} = 2(1 + 2l_i)$ (l_i an integer) so that

$$A = (1 + 4l)\,.\,2^{\alpha-1}\prod_{i=0}^{\alpha-2}(1 + 2l_i) \equiv 2^{\alpha-1} = \varphi(2^\alpha) \pmod{2^\alpha}.$$

β) If a is of the form $3 + 4l$, then $1 + a = 4(l + 1)$ while for $i \geqq 1$ we have $1 + (3 + 4l)^{2^i} = 2(1 + 2l_i)$ (l_i an integer). Hence

$$A = (3 + 4l)\,.\,2^2(l + 1)\,.\,2^{\alpha-2}\prod_{i=1}^{\alpha-2}(1 + 2l_i) \equiv 0 \pmod{2^\alpha}.$$

This completes the proof of Lemma 1.

We now turn to the case $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, $r > 1$, and consider the sum

$$A = A(a, m) = a + a^2 + \ldots + a^{\varphi(m)}, \quad (a, m) = 1.$$

Since $\varphi(p_i^{\alpha_i}) \mid \varphi(m)$ and $a^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$, we have

$$A \equiv (a + a^2 + \ldots + a^{\varphi(p_i^{\alpha_i})})\,\frac{\varphi(m)}{\varphi(p_i^{\alpha_i})} \pmod{p_i^{\alpha_i}}.$$

Hence (by Lemma 1):

a) For $p_i > 2$

$$A \equiv \begin{cases} 0 \pmod{p_i^{\alpha_i}} & \text{if } (a - 1, p_i) = 1, \\ \varphi(m) \pmod{p_i^{\alpha_i}} & \text{if } (a - 1, p_i) = p_i. \end{cases}$$

b) For $p_i = 2$

(2) $A \equiv \varphi(m) \pmod{2^\alpha}$ if $\alpha = 1$, or if $\alpha \geqq 2$ and a is of the form $4l + 1$,

(3) $A \equiv 0 \pmod{2^\alpha}$ if $\alpha \geqq 2$ and a is of the form $4l + 3$.

Knowing the values of $A \pmod{p_i^{\alpha_i}}$ we use the Chinese remainder theorem to find $A \pmod{m}$.

a) Suppose first that $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ is odd and $P = \{p_{i_1}, \dots, p_{i_s}\}$, $1 \leqq s \leqq r$, is the subset of those primes $\in \{p_1, \dots, p_r\}$ which divide $a - 1$, i.e., $a - 1 = up_{i_1}^{\beta_1} \dots p_{i_s}^{\beta_s}$, $\beta_i \geqq 1$, $(u, m) = 1$. For $i \in \{i_1, \dots, i_s\}$ we have $A \equiv \varphi(m) \pmod{p_i^{\alpha_i}}$, while for $i \notin \{i_1, \dots, i_s\}$ we have $A \equiv 0 \pmod{p_i^{\alpha_i}}$. Hence $A \equiv \varphi(m)(f_{i_1} + \dots + f_{i_s})$ $\pmod{m}$.

The element $[a - 1] \in S(m)$ belongs to the idempotent $[e] = [\bar{f}_{i_1}\bar{f}_{i_2} \dots \bar{f}_{i_s}] = [(1 - f_{i_1}) \dots (1 - f_{i_s})] = [1 - (f_{i_1} + \dots + f_{i_s})]$. Hence $[f_{i_1} + \dots + f_{i_s}] = [1 - e]$ and $A \equiv (1 - e)\,\varphi(m) \pmod{m}$. This formula holds also if $(a - 1, m) = 1$, (i.e. P is empty) for then $[a - 1]$ belongs to the idempotent $[e] = [1]$ and we know (see the introduction to this section) that in this case $A \equiv 0 \pmod{m}$.

b) Now let $m = 2^{\alpha_1}p_2^{\alpha_2} \dots p_r^{\alpha_r}$ and $P = \{p_{i_2}, \dots, p_{i_s}\}$, $1 \leqq s \leqq r - 1$, be those (odd) primes $\in \{p_2, \dots, p_r\}$ which divide $(a - 1)$. Since $(a, m) = 1$, $a - 1$ is even and we have $a - 1 = 2^{\beta_1}p_{i_2}^{\beta_2} \dots p_{i_s}^{\beta_s}u$, $\beta_i \geqq 1$, $(u, m) = 1$. Further (by the Chinese remainder theorem),

$$A \equiv a_1 f_1 + \varphi(m)(f_{i_2} + \dots + f_{i_s}) \pmod{m},$$

where a_1 is to be chosen in accordance with the formulas (2) and (3). [If P is empty, the second term on the right vanishes.]

α) If $\alpha_1 = 1$ or $\alpha_1 \geqq 2$ and a is of the form $4l + 1$, we have to insert $a_1 = \varphi(m)$ so that $A \equiv \varphi(m)(f_1 + f_{i_2} + \dots + f_{i_s}) \pmod{m}$ and by the same argument as above $A \equiv (1 - e)\,\varphi(m) \pmod{m}$, where $[e]$ is the idempotent to which $[a - 1] \in S(m)$ belongs. (This also holds if P is empty.)

Remark. If a is of the form $4l + 1$ and $\alpha_1 \geqq 2$, then $a - 1 = 2^{\beta_1}p_{i_2}^{\beta_2} \dots p_{i_s}^{\beta_s}$, where $\beta_1 \geqq 2$ and the element $[(a - 1)/2]$ belongs to the same idempotent as $[a - 1]$ (namely, $[e] = [\bar{f}_1\bar{f}_{i_2} \dots \bar{f}_{i_s}]$).

β) If $\alpha_1 \geqq 2$ and a is of the form $4l + 3$, we have $a_1 \equiv 0 \pmod{2^{\alpha_1}}$ and therefore $A \equiv \varphi(m)(f_{i_2} + \dots + f_{i_s})$. In this case $a - 1$ is divisible by 2 but not by 4 so that we have $a - 1 = 2p_{i_2}^{\beta_2} \dots p_{i_s}^{\beta_s}u$, $\beta_i \geqq 1$, $(u, m) = 1$. Now the element $[(a - 1)/2]$ belongs to the idempotent $[e] = [\bar{f}_{i_2} \dots \bar{f}_{i_s}] = [1 - (f_{i_2} + \dots + f_{i_s})]$, hence $[f_{i_2} + \dots + f_{i_s}] = [1 - e]$ and $A \equiv \varphi(m)(1 - e) \pmod{m}$. This formula also holds if $\{p_{i_2}, \dots, p_{i_s}\}$ is empty, for then $[e] = [1]$.

We have proved:

Theorem 1. *Let* $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ *and* $(a, m) = 1$.

a) *If all* p_i *are odd and* $[a - 1]$ *belongs to the idempotent* $[e]$, *then*

$$[a] + [a]^2 + \dots + [a]^{\varphi(m)} = [(1 - e)\,\varphi(m)]\,. \tag{4}$$

b) *The same result holds if* $m = 2 \,.\, p_2^{\alpha_2} \dots p_r^{\alpha_r}$.

c) *If* $m = 2^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ *and* $\alpha_1 \geqq 2$, *the relation* (4) *holds if* $[e]$ *is the idempotent to which* $[(a - 1)/2]$ *belongs.*

Remark. If $[a]$ runs through all the $\varphi(m)$ elements $\in G(m)$, the sum $A(a, m)$ attains at most 2^r different values. If $[e]$ is given, the value $[(1 - e)\, \varphi(m)]$ is attained since to any $[e]$ there is an $[a] \in S(m)$ such that $[a - 1]$ belongs to $[e]$. It is sufficient to put $[a] = [1 - e]$. Then $[a - 1] = [-e]$ and this element belongs to the idempotent $[e]$. Since $[1 - e]$ is an idempotent we immediately have that $[1 - e] + \dots + [1 - e]^{\varphi(m)} = [1 - e]\,[\varphi(m)]$.

Of course the classes $[(1 - e)\, \varphi(m)]$ (if $[e]$ runs through E) need not be all different and simple examples show that some of them may coincide. (See the numerical example at the end of the paper.) It can be proved that the number of different values is 2^s, where $1 \leqq s \leqq r$.

We can slightly modify the result of Theorem 1:

Theorem 2. *Suppose that the conditions of Theorem* 1 *are satisfied and m is not divisible by* 2^α, $\alpha \geqq 3$.

We then have

$$[a] + [a]^2 + \dots + [a]^{\lambda(m)} = [1 - e]\,[\lambda(m)]\,,$$

where e has the same meaning as in Theorem 1.

Proof. Denote $B = a + a^2 + \dots + a^{\lambda(m)}$.

The number $\lambda(m)$ is divisible by $\varphi(p_i^{\alpha_i})$ if p_i is odd or $p_i^{\alpha_i} = 2$ or $p_i^{\alpha_i} = 4$. Hence we may write analogously as above

$$B \equiv \left(a + a^2 + \dots + a^{\varphi(p_i^{\alpha_i})}\right) . \frac{\lambda(m)}{\varphi(p_i^{\alpha_i})} \pmod{p_i^{\alpha_i}}\,,$$

whence by Lemma 1:

$$B \equiv \begin{cases} 0 \pmod{p_i^{\alpha_i}} & \text{if} \quad p_i \text{ is odd and } \quad (a - 1, p_i) = 1\,, \\ \lambda(m) \pmod{p_i^{\alpha_i}} & \text{if} \quad p_i \text{ is odd and } \quad (a - 1, p_i) = p_i\,. \end{cases}$$

$$B \equiv \begin{cases} \lambda(m) \pmod{2}\,, & \\ \lambda(m) \pmod{2^2} & \text{if} \quad a \text{ is if the form } \quad 4l + 1\,, \\ 0 \pmod{2^2} & \text{if} \quad a \text{ is of the form } \quad 4l + 3\,. \end{cases}$$

The end of the proof follows by the same argument as in Theorem 1.

Remark. The fact that for $m = 2^\alpha$, $\alpha \geqq 3$, Theorem 2 does not hold can be proved directly. In this case we have

$$B = a + a^2 + \dots + a^{2^{\alpha - 2}} = a(1 + a)(1 + a^2) \dots (1 + a^{2^{\alpha - 3}})\,.$$

If $a = 1 + 4l$, then $1 + a = 2(1 + 2l)$. For $i \geqq 1$ we have $1 + a^{2^i} = 1 + (1 + 4l)^{2^i} = 2(1 + 4l_i)$, l_i an integer, hence

$$B = (1 + 4l)(1 + 2l)\, 2^{\alpha-2} \prod_{i=1}^{\alpha-3} (1 + 4l_i) \equiv$$
$$\equiv (1 + 2l)\, 2^{\alpha-2} \equiv 2^{\alpha-2} + (a - 1)\, 2^{\alpha-3} \pmod{2^\alpha}.$$

Now $2^{\alpha-2} + (a - 1)\, 2^{\alpha-3}$ depends on a and need not be equal to $\lambda(2^\alpha) = 2^{\alpha-2} \pmod{2^\alpha}$. (It is equal to $2^{\alpha-2}$ iff a is of the form $a = 1 + 8l$.)

3. THE CASE $[a] \in N(m)$

Lemma 1 and Theorem 1 need not hold if $(a, m) > 1$.

Consider, e.g., the semigroup $S(p^\alpha)$, $\alpha > 1$, p odd. The element $[a] = [p]$ belongs to the idempotent $[e] = [0]$. Since $\varphi(p^\alpha) > \alpha$, we have $A = a + \ldots + a^{\varphi(p^\alpha)} \equiv \equiv p + \ldots + p^{\alpha-1} \pmod{p^\alpha}$ and

$$A - (1 - e)\, \varphi(p^\alpha) \equiv p + \ldots + p^{\alpha-2} + 2p^{\alpha-1} \pmod{p^\alpha}.$$

The term on the right hand side is $\equiv 0 \pmod{p}$ but $\not\equiv 0 \pmod{p^2}$, hence $\not\equiv 0 \pmod{p^\alpha}$.

The modifications necessary in order to obtain a statement analogous to Theorem 1 in the case $(a, m) > 1$ are suggested by the fact that for any $[a] \in S(m)$ we have $[a]^{\nu(m)} = [a]^{\nu(m)+\lambda(m)} = [a]^{\nu(m)+\varphi(m)}$, where $\nu(m) = \max(\alpha_1, \ldots, \alpha_r)$. Hence instead of A we shall consider the sum $\bar{A} = a^\nu + a^{\nu+1} + \ldots + a^{\nu+\varphi(m)-1}$.

First we prove:

Lemma 2. *Let p be a prime, $\alpha \geqq 1$ and $\gamma \geqq \alpha$. Denote $A_\gamma = A_\gamma(a, p^\alpha) = a^\gamma + a^{\gamma+1} + \ldots + a^{\gamma+\varphi(p^\alpha)-1}$. We then have*:

a) *For p odd*:

$$\begin{array}{l}(5)\\(6)\end{array} \qquad A_\gamma \equiv \begin{cases} 0 \pmod{p^\alpha} & \text{if } (a - 1, p) = 1, \\ \varphi(p^\alpha) \pmod{p^\alpha} & \text{if } (a - 1, p) = p. \end{cases}$$

b) *For $p = 2$*:

$$\begin{array}{l}(7)\\(8)\\(9)\\ \end{array} \qquad A_\gamma \equiv \begin{cases} 0 \pmod{2^\alpha} & \textit{if } a \textit{ is even}, \\ 0 \pmod{2^\alpha} & \textit{if } \alpha \geqq 2 \textit{ and } a \textit{ is of the form } 4l + 3, \\ \varphi(2^\alpha) \pmod{2^\alpha} & \textit{if either } \alpha = 1 \textit{ and } a \textit{ is odd}, \\ & \textit{or } \alpha \geqq 2 \textit{ and } a \textit{ is of the form } 4l + 1. \end{cases}$$

Proof. If $(a, p) = 1$, then the set $\{[a]^\gamma, [a]^{\gamma+1}, \ldots, [a]^{\gamma+\varphi(m)-1}\}$ is the same as the set $\{[a], [a]^2, \ldots, [a]^{\varphi(m)}\}$. We may use Lemma 1 which leads to the results (5), (6), (8), (9).

If p/a, then $a^\gamma \equiv a^{\gamma+1} \equiv \ldots \equiv 0 \pmod{p^\alpha}$ and we have directly $A_\gamma \equiv 0 \pmod{p^\alpha}$. Since p/a implies $(a - 1, p) = 1$, this result falls under the result (5) for $p > 2$ and under the result (7) for $p = 2$. (Note that for p/a none of the cases (6), (8), (9) can occur.)

Theorem 3. a) *Suppose that* $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, *where either all* p_i *are odd or* $m = 2p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. *Then for any* $[a] \in S(m)$ *we have*

$$(10) \qquad [\bar{A}] = [a]^\nu + [a]^{\nu+1} + \ldots + [a]^{\nu+\varphi(m)-1} = [(1 - e)\,\varphi(m)]\,,$$

where $[e]$ *is the idempotent to which* $[a - 1]$ *belongs.*

b) *Suppose that* $m = 2^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, $\alpha_1 \geqq 2$.

α) *If* a *is even, then* (10) *holds,* $[e]$ *being again the idempotent to which* $[a - 1]$ *belongs.*

β) *If* a *is odd,* (10) *holds if* $[e]$ *is the idempotent to which* $[(a - 1)/2]$ *belongs.*

Proof. The elements of the set $\{a^\nu, a^{\nu+1}, \ldots, a^{\nu+\varphi(m)-1}\}$ taken $\pmod{p_i^{\alpha_i}}$ are $\varphi(m/p_i^{\alpha_i})$ times written elements $\{a^\nu, a^{\nu+1}, \ldots, a^{\nu+\varphi(p_i^{\alpha_i})-1}\}$. Hence

$$\bar{A} \equiv [a^\nu + \ldots + a^{\nu+\varphi(p_i^{\alpha_i})-1}] \cdot \frac{\varphi(m)}{\varphi(p_i^{\alpha_i})} \pmod{p_i^{\alpha_i}}\,.$$

We use Lemma 2:

a) For $p_i > 2$,

$$\bar{A} \equiv \begin{cases} 0 \pmod{p_i^{\alpha_i}} & \text{if} \quad (a - 1, p_i) = 1\,, \\ \varphi(m) \pmod{p_i^{\alpha_i}} & \text{if} \quad (a - 1, p_i) = p_i\,. \end{cases}$$

b) For $p_1 = 2$ we have

$$\bar{A} \equiv \begin{cases} 0 \pmod{2^{\alpha_1}} & \text{if} \quad a \text{ is even}\,, \\ 0 \pmod{2^{\alpha_1}} & \text{if} \quad \alpha_1 \geqq 2 \quad \text{and } a \text{ is of the form} \quad a = 4l + 3\,, \\ \varphi(2^{\alpha_1}) \pmod{2^{\alpha_1}} & \text{if} \quad \text{either} \quad \alpha_1 = 1 \quad \text{and } a \text{ is odd}\,, \\ & \text{or} \quad \alpha_1 \geqq 2 \quad \text{and } a \text{ is of the form} \quad a = 4l + 1\,. \end{cases}$$

The proof follows now the same lines as in Theorem 1 but we have to consider an additional case, namely $m = 2^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ and a is even.

If a is even, $a - 1$ is odd. Let $P = \{p_{i_2}, \ldots, p_{i_s}\}$ be the set of all those primes $\in \{p_2, \ldots, p_r\}$ which divide $a - 1$. We have $a - 1 = p_{i_2}^{\beta_2} \ldots p_{i_s}^{\beta_s} u$, $(u, m) = 1$. By the Chinese remainder theorem, $\bar{A} \equiv 0 . f_1 + \varphi(m)(f_{i_2} + \ldots + f_{i_s}) \pmod{m}$. Hence $[a - 1]$ belongs to the idempotent $[e] = [\bar{f}_{i_2} \ldots \bar{f}_{i_s}]$, whence $[1 - e] = [f_{i_2} + \ldots + f_{i_s}]$ and $[A] = [(1 - e)\,\varphi(m)]$. This completes the proof of Theorem 3.

We may use Theorem 3 to find the value of $[C] = [a] + [a]^2 + \ldots + [a]^{\varphi(m)}$ if $(a, m) > 1$ and $\nu > 1$. Write $[C] = [a] + \ldots + [a]^{\nu-1} + [\bar{A}] - ([a]^{\varphi(m)+1} + \ldots$

$\ldots + [a]^{\varphi(m)+\nu-1})$. If $[a]$ belongs to the idempotent $[e_1]$, we have $[a]^{\varphi(m)} = [e_1]$, hence $[a]^{\varphi(m)+j} = [a]^j [e_1]$ so that

$$[C] = [\bar{A}] + [a - ae_1] + [a^2 - a^2e_1] + \ldots + [a^{\nu-1} - a^{\nu-1}e_1] =$$
$$= [(1 - e)\,\varphi(m)] + [1 - e_1]\,[a + a^2 + \ldots + a^{\nu-1}]\,.$$

Corollary. *Let $[a]$ be any element $\in S(m)$ and suppose that $[a]$ belongs to the idempotent $[e_1]$. Then if $\nu > 1$,*

$$[a] + [a]^2 + \ldots + [a]^{\varphi(m)} =$$
$$= [1 - e_1]\,[a + a^2 + \ldots + a^{\nu-1}] + [(1 - e)\,\varphi(m)]\,.$$

Here if $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ (p_i = odd) or $m = 2p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, then $[e]$ denotes the idempotent to which $[a - 1]$ belongs. If $m = 2^{\alpha_1}p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, $\alpha_1 \geqq 2$ and a is even, then $[e]$ denotes again the idempotent to which $[a - 1]$ belongs. If in this last case a is odd, $[e]$ denotes the idempotent to which $[(a - 1)/2]$ belongs.

Finally, by the method used above we may prove the following statement analogous to Theorem 2.

Theorem 4. *If m is not divisible by 2^α, $\alpha \geqq 3$, then Theorem 3 remains valid if $\varphi(m)$ is replaced by $\lambda(m)$, while $[e]$ has the same meaning as in Theorem 3.*

4. A NUMERICAL ILLUSTRATION

We conclude our considerations by illustrating the foregoing results on a numerical example.

Let $m = 1575 = 3^2 \,.\, 5^2 \,.\, 7$, hence $\varphi(m) = 720$ and $\lambda(m) = 60$.

The semigroup $S(m)$ contains $2^3 = 8$ idempotents. The Boolean algebra E is described in Figure 1.

The maximal idempotents are:

$$[\bar{f}_1] = [351] = [3^2 \,.\, 214]\,, \quad [\bar{f}_2] = [1450] = [5^2 \,.\, 58]\,,$$
$$[\bar{f}_3] = [1351] = [7 \,.\, 193]\,.$$

The primitive idempotents are:

$$[f_1] = [1225] = [5^2 \,.\, 7 \,.\, 16]\,, \quad [f_2] = [126] = [3^2 \,.\, 7 \,.\, 2]\,,$$
$$[f_3] = [225] = [3^2 \,.\, 5^2]\,.$$

The products $\{[e]\,[\varphi(m)]\}$, $e \in E$, are: $[0]$, $[720]$ and

$$\{[\bar{f}_1], [\bar{f}_2], [\bar{f}_3]\} \,.\, [720] = \{[720], [1350], [945]\}\,,$$
$$\{[f_1], [f_2], [f_3]\} \,.\, [720] = \{[0], [945], [1350]\}\,.$$

Hence there are only 4 different products $[e\,\varphi(m)]$, $e \in E$.

α) Take, e.g., $a = 22$. Since $(22, m) = 1$ we may use Theorem 1. Since $a - 1 = 3 \,.\, 7$, $[a - 1]$ belongs to the idempotent $[126]$. Since $[(1 - 126) \,.\, 720] = [1350]$, we have the following equality in $S(1575)$:

$$[22] + [22]^2 + \ldots + [22]^{720} = [1350]\,.$$

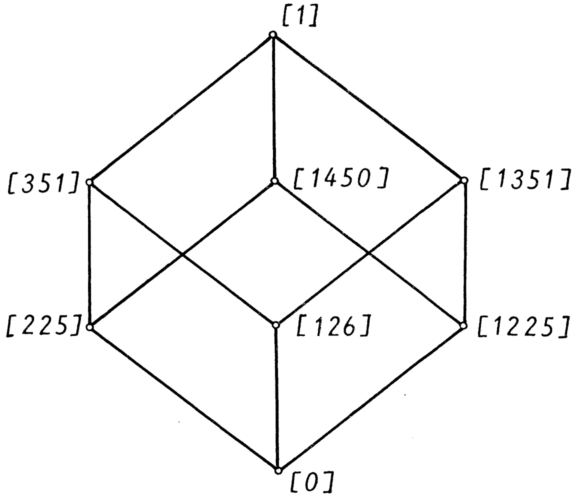

Fig. 1

By Theorem 2 we also have $[22] + [22]^2 + \ldots + [22]^{60} = [(1-126) \,.\, 60] = [375]$.

β) Take $[a] = [21]$. Here $(a, m) = (21, 1575) = 21 > 1$ and $[a - 1] = [2^2 \,.\, 5]$. Hence $[a - 1]$ belongs to the idempotent $[1450]$. By Theorem 3 we have (since $v = 2$)

$$[\bar{A}] = [21]^2 + [21]^3 + \ldots + [21]^{721} = [(1-1450) \,.\, 720] = [945]\,.$$

γ) To find the value of $[B] = [21] + \ldots + [21]^{720}$, write $[B] = [\bar{A}] + [21] - [21]^{721} = [\bar{A}] + [21]([1] - [21]^{720})$. The element $[21]^{720}$ is necessarily an idempotent and since $[21] = [3 \,.\, 7]$. we have $[21]^{720} = [126]$, so that $[B] = [\bar{A}] + [(1-126) \,.\, 21] = [1470]$.

References

[1] *Št. Schwarz:* The role of semigroups in the elementary theory of numbers. (To appear in Mathematica Slovaca.)

Author's address: 880 31 Bratislava, Gottwaldovo nám. 19, ČSSR (Slovenská vysoká škola technická).