Mathematica Slovaca

Štefan Schwarz
Extensions of Bauer's identical congruences

Mathematica Slovaca, Vol. 33 (1983), No. 2, 209--224

Persistent URL: http://dml.cz/dmlcz/130140

Math. Slovaca 33, 1983, No. 2, 209—224

EXTENSIONS OF BAUER'S IDENTICAL CONGRUENCES

ŠTEFAN SCHWARZ

In the present paper we shall use a part of the results obtained in [4] to prove some identical congruences which can be considered as extensions and modifications of the famous Bauer's congruences. (See Hardy—Wright, [2].)

For the convenience of the reader we recall some facts proved in [4] needed in the following.

Let $m=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ be the factorization of an integer $m>1$ into the product of different prime powers. Let S_m be the multiplicative semigroup of the ring of integers (mod m). The class containing the number a is denoted by $[a]$. We shall freely use the fact that S_m admits also an addition.

S_m contains 2^r different idempotents (including [0] and [1]). Any idempotent $e\in S_m$ can be written in the form $e=[p_1^{l_1}\dots p_r^{l_r}a]$, where l_i is either zero or α_i and a is an integer with $(a, m)=1$.

The idempotents of the form $[p_i^{\alpha_i}a]$ will be denoted as $\bar{f}_i$ and called the maximal idempotents of S_m. Any idempotent $e\in S_m$ which is different from [1] is a product of maximal idempotents $\in S$. Under the partial ordering $e'\leqq e''\Leftrightarrow e'e''=$ $=e'$ the set E of all idempotents forms a Boolean algebra. The r idempotents of the form $f_i=[a\cdot m/p_i^{\alpha_i}]$, $(a, m)=1$, are called the primitive idempotents $\in S_m$. We have $f_i+\bar{f}_i=[1]$, also $f_1+\dots+f_r=[1]$ and $\bar{f}_1\dots\bar{f}_r=[0]$.

To any idempotent $e\in E$ there exist a maximal group $G(e)$ containing e as its unit element and a maximal subsemigroup $P(e)$ of S containing e as the unique idempotent. Hence $P(e)=\{x\mid x\in S_m, x^l=e \text{ for some } l>0\}$. Clearly $S_m=\bigcup_{e\in E}P(e)$ and $G(e)\subset P(e)$. In particular $G(1)=G([1])$ is the group of order $\varphi(m)$ (Euler function) containing all $[a]$ with $(a, m)=1$. Note that $P([1])=G(1)$.

The following (internal) direct decomposition of $G(1)$ plays an important role. Denote

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

Then all G_i are subgroups of $G(1)$ and we have

$$G(1)=G_1\cdot G_2\dots G_r.$$

Analogously if $T_i=\{\bar{f}_i+[h]f_i \mid 0 \leqq h < p_i^{\alpha_i}\}$, then S_m admits the following (internal) direct decomposition:

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

Hereby $T_i \cap T_j = [0]$ for $i \neq j$.

Let $e \in E$, $e \neq [1]$, and $e=\bar{f}_1 \dots \bar{f}_s$ $(1 \leqq s < r)$. Then the group $G(e)$ has the following (internal) direct decomposition

$$G(e)=(G_{s+1}e) \dots (G_r e).$$

(*If* $s=r$, then $e=[0]$ and $G(e)=\{[0]\}$.)

Note for the following. The correspondence $p_i \leftrightarrow \bar{f}_i$ is one to one. There are of course $\binom{r}{s}$ different products of s maximal idempotents. For simplicity we write $e=\bar{f}_1 \dots \bar{f}_s$ having in mind that this is a typical representative of the product of s maximal idempotents.

Denote $T_i=G_i \cup I_i$, $G_i \cap I_i = \emptyset$ $(1 \leqq i \leqq r)$. Then the semigroup $P(e)$ admits the following decomposition

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

Here I_i are subsemigroups of S_m and $I_i \cap I_j = \emptyset$ if $i \neq j$. (If $e=[0]$, $P([0])=I_1 \dots I_r$.)

Finally if $e=\bar{f}_1 \dots \bar{f}_s$, we have (with card $A=|A|$)

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

In order to find a generalization of the Lagrange decomposition

$$(x-1)(x-2) \dots (x-p+1) \equiv x^{p-1}-1 \pmod p,$$

Bauer (1902) considered the product

$F(x)=\prod_{v \in G(1)}(x-v)$ and proved: For $p_i>2$ we have

$$F(x) \equiv (x^{p_i-1}-1)^{\varphi(m)/(p_i-1)} \pmod{p_i^{\alpha_i}},$$

and a similar result if $p_i=2$. Later Vandiver (1917) extended this result giving formulas for the value of $F(x)$ in S_m (i. e. not mod $p_i^{\alpha_i}$ but mod m). He also gave a formula for the product $\prod_{v \in S_m}(x-v)$. (See Theorem 2 and Theorem 7 below.)

The purpose of this paper is to give explicit formulae for the products $\prod_{v \in G(e)}(x-v)$ and $\prod_{v \in P(e)}(x-v)$, where e is any idempotent $\in S_m$. These formulae are certainly new since a rather thorough investigation of the existing literature shows that there is a very limited number of papers dealing explicitly with the groups $G(e)$ and semigroups $P(e)$ for $e \neq [1]$.

In the following we shall use only a special case of Bauer's identity, namely the case $m = p^\alpha$ ($\alpha \geqq 1$), the proof of which is given in [2].

Denote $V = \{0, 1, \ldots, p^\alpha - 1\}$, $V^{(1)} = \{a \in V \mid (a, p) = 1\}$, then the following holds:

Lemma 1.(Bauer). a) *If* $p > 2$, *then*

$$\prod_{v \in V^{(1)}} (x - v) \equiv (x^{p-1} - 1)^{p^{\alpha-1}} (\mathrm{mod}\, p^\alpha). \tag{1}$$

b) *If* $p = 2$ *and* $\alpha > 1$,

$$\prod_{v \in V^{(1)}} (x - v) \equiv (x^2 - 1)^{2^{\alpha-2}} (\mathrm{mod}\, 2^\alpha).$$

Remark. When dealing with residue classes as elements $\in S_{p^\alpha}$ we may write (1) in the form $\prod_{v \in G(1)} (x - v) = (x^{p-1} - [1])^{p^{\alpha-1}}$ (with the sign of equality). In the following we reserve the sign of the equality for all calculations to be carried out in S_m.

Notation. Throughout the paper we use the following notation. If A is a nonempty subset of S_m, then $U[x; A]$ denotes the product $\prod_{v \in A} (x - v)$ (with coefficients $\in S_m$).

As it does not lead to any misunderstanding we shall write $x + a$, $a \in S_m$ instead of $[1]\, x + a$ and replace $ax - a$ by $(x - 1)a$ having in mind that all coefficients of the polynomials considered are elements $\in S_m$.

If $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, we denote $V_i = \{0, 1, \ldots, p^{\alpha_i} - 1\}$, $V_i^{(1)} = \{a \in V_i \mid (a, p_i) = 1\}$, $V_i^{(0)} = \{a \in V_i \mid (a, p_i) > 1\}$, so that $V_i = V_i^{(1)} \cup V_i^{(0)}$.

1. The product $U[x; G_i]$

As remarked above the groups G_i play an important role, so that we have to deal first with the product

$$U[x; G_i] = \prod_{v \in G_i} (x - v).$$

We suppose $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. The case $r = 1$ is not interesting since it leads to Lemma 1. Hence we suppose $r \geqq 2$.

In the following Theorem 1 $|G_i|$ is the cardinality of G_i, hence $|G_i| = p_i^{\alpha_i - 1}(p_i - 1)$ for $p_i \geqq 2$.

Theorem 1. *With the notations introduced above we have*

$$U[x\,;\,G_i]=\begin{cases}[(x-\bar{f}_i)^{p_i\quad 1}-f_i]^{|G_i|\;(p_i\quad 1)} & \text{for } p_i>2,\\ [(x-\bar{f}_i)^2-f_i]^{|G_i|\;2} & \text{for } p_i=2,\ \alpha_i\geqq 2,\\ x-[1] & \text{for } p_i^{\alpha_i}=2.\end{cases}$$

Proof. Any element $v\in G_i$ can be written in the form $v=\bar{f}_i+hf_i$, $h\in V_i^{(1)}$. Hence

$$x-v=x-[\bar{f}_i+hf_i]=x(f_i+\bar{f}_i)-(\bar{f}_i+hf_i)=(x-1)\bar{f}_i+(x-h)f_i$$

and

$$U[x\,;\,G_i]=\prod_{h\in V_i^{(1)}}[(x-1)\bar{f}_i+(x-h)f_i]=(x-1)^{\gamma_i}\cdot\bar{f}_i+f_i\prod_{h\in V_i^{(1)}}(x-h),$$

where $\gamma_i=\varphi(p_i^{\alpha_i})$.

a) For $p_i>2$, we have by Lemma 1, (with $\beta_i=p_i^{\alpha_i-1}$).

$$\prod_{h\in V_i^{(1)}}(x-h)\equiv(x^{p_i-1}-1)^{\beta_i}(\mathrm{mod}\ p_i^{\alpha_i})$$

and, since $f_i[p_i^{\alpha_i}]=[0]$,

$$U[x\,;\,G_i]=(x-1)^{(p_i-1)\beta_i}\cdot\bar{f}_i+(x^{p_i-1}-1)^{\beta_i}\cdot f_i=$$
$$=[(x-1)^{p_i-1}\bar{f}_i+(x^{p_i-1}-1)f_i]^{\beta_i}=[\{(x-1)\bar{f}_i+xf_i\}^{p_i\quad 1}-f_i]^{\beta_i},$$

whence the first formula immediately follows.

b) For $p_i=2$, $\alpha_i\geqq 2$, we have by Lemma 1,

$$\prod_{h\in V_i^{(1)}}(x-h)\equiv(x^2-1)^{\beta_i}\ (\mathrm{mod}\ 2^{\alpha_i}),$$

where $\beta_i=2^{\alpha_i-2}$.

Hence

$$U[x\,;\,G_i]=(x-1)^{2\beta_i}\cdot\bar{f}_i+(x^2-1)^{\beta_i}\cdot f_i=[(x-1)^2\bar{f}_i+(x^2-1)f_i]^{\beta_i}=$$
$$=[(x-\bar{f}_i)^2-f_i]^{\beta_i}.$$

c) If $p_i^{\alpha_i}=2$ (i. e. m is divisible by 2, but not by 4), we have $V_i^{(1)}=\{1\}$, the group G_i reduces to the element $\bar{f}_i+1\cdot f_i=[1]$, so that $U[x\,;\,G_i]=x-[1]$.

This proves Theorem 1.

Suppose in the following again $m=p_1^{\alpha_1}\ldots p_r^{\alpha_r}$, where $r\geqq 2$. We use Theorem 1 to find $U[x\,;\,G(1)]\ =\ U[x\,;\,G_1G_2\ldots G_r]$.

$U[x\,;\,G(1)]=\prod_{v\in G_1\ldots G_r}(x-v)=\prod(x-v_1\ldots v_r)$, where $v_1,\ldots,v_r$ run independently over $G_1,\ldots,G_r$. Since $[1]=f_1+\ldots+f_r$, we may write $u[x\,;\,G(1)]=\sum_{i=1}^{r}U[x\,;\,G_1\ldots G_r]\cdot f_i$ and compute each of these summands separately.

Write v in the form

$$v = v_1 \dots v_r = (\bar{f}_1 + h_1 f_1) \dots (\bar{f}_r + h_r f_r)$$

with $h_i \in V_i^{(1)}$. For any i $(1 \leqq i \leqq r)$ we have $v \cdot f_i = v_1 v_2 \dots v_r f_i = v_i f_i$ independently of the $\varphi(m)/|G_i|$ possible values of $v_1 \dots v_{i-1} v_{i+1} \dots v_r$.

Hence

$$U[x\,;\,G(1)]f_i = \prod_{v \in G_i} (x f_i - v f_i)^{\varphi(m)/|G_i|} =$$

$$= \left[\prod_{v \in G_i} (x - v)\right]^{\varphi(m)/|G_i|} \cdot f_i = U[x\,;\,G_i]^{\varphi(m)/|G_i|} \cdot f_i.$$

a) If p_i is odd, then by Theorem 1

$$U[x\,;\,G_i] \cdot f_i = \{[(x - \bar{f}_i)^{p_i - 1} - f_i] f_i\}^{|G_i|/(p_i - 1)} =$$

$$= [x^{p_i - 1} \cdot f_i - f_i]^{|G_i|/(p_i - 1)} = (x^{p_i - 1} - 1)^{|G_i|/(p_i - 1)} \cdot f_i$$

and

$$U[x\,;\,G(1)] \cdot f_i = (x^{p_i - 1} - 1)^{\varphi(m)/(p_i - 1)} \cdot f_i.$$

b) If $m = 2 \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $r \geqq 2$, then since $|G_1| = 1$,

$$U[x\,;\,G(1)] \cdot f_1 = U[x\,;\,G_1]^{\varphi(m)} \cdot f_1 = (x - 1)^{\varphi(m)} \cdot f_1.$$

c) If $m = 2^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $\alpha_1 \geqq 2$, then

$$U[x\,;\,G(1)] \cdot f_1 = U[x\,;\,G_1]^{|G_2 \dots G_r|} f_1 =$$

$$= [(x - \bar{f}_1)^2 - f_1]^{\varphi(m)/2} \cdot f_1 = (x^2 f_1 - f_1)^{\varphi(m)/2} = (x^2 - 1)^{\varphi(m)/2} \cdot f_1.$$

This can be modified (due to the fact that $r \geqq 2$). First

$$\frac{1}{2}\,\varphi(m) = \frac{1}{2} \cdot 2^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \dots = 2^{\alpha_1 - 1} \cdot u,$$

where u is an integer. Next (with $\gamma = 2^{\alpha_1 - 1} u$)

$$(x^2 - 1)^{\gamma} \cdot f_1 = [(x - 1)^2 + 2(x - 1)]^{\gamma} \cdot f_1 = (x - 1)^{\varphi(m)} f_1 +$$

$$+ \sum_{k \geqq 1} \binom{2^{\alpha_1 - 1} \cdot u}{k} 2^k (x - 1)^{\varphi(m) - k} \cdot f_1.$$

It is easy to see that $\binom{2^{\alpha^1 - 1} \cdot u}{k} 2^k$ is divisible by 2^{α_1} and since $[2^{\alpha_1}] f_1 = 0$, we finally have $U[x\,;\,G(1)] f_1 = (x - 1)^{\varphi(m)} f_1$.
This implies:

Theorem 2. *Let $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $r \geqq 2$. Then*

$$U[x; G(1)] = \sum_{i=1}^{r} f_i (x^{p_i - 1} - 1)^{\varphi(m)\,(p_i - 1)}.$$

This formula has been (in essential) found by Vandiver (1917). Of course, since he does not use explicitly the idempotents, his formulations are rather complicated. (See Dickson [1], p. 89.)

2. The product $U[x; G(e)]$

Let now be e any idempotent $\in E$, $e \neq [1]$ and $e = \bar{f}_1 \bar{f}_2 \dots \bar{f}_s$, where $s \leqq 1 \leqq r$. We again suppose $r \geqq 2$.

We shall find explicit formulas for the product $\prod_{v \in G(e)} (x - v)$, $G(e)$ being (as above) the maximal subgroup of S_m belonging to the idempotent e.

In the following we suppose $s < r$, since for $s = r$ we have $e = [0]$ and $U[x; G(0)] = x$.

The group $G(e)$ is a direct product of its subgroups

$$G(e) = (G_{s+1} e) \cdot (G_{s+2} e) \dots (G_r e).$$

Any element $v \in G(e)$ is of the form $v = v_{s+1} \dots v_r$, where $v_j \in G_j e$, and $v_j = (\bar{f}_j + h_j f_j) \cdot \bar{f}_1 \dots \bar{f}_s$, $h_j \in V_j^{(1)}$, $j \geqq s+1$. Hence

$$U[x; G(e)] = \Pi(x - v_{s+1} \dots v_r), \text{ where } v_{s+1}, \dots, v_r,$$

run independently through $G_{s+1} \cdot e, \dots, G_r \cdot e$.

Write again

$$U[x; G(e)] = \sum_{i=1}^{r} U[x; G(e)] \cdot f_i.$$

If $i \in \{1, 2, \dots, s\}$, then $v_{s+1} \dots Ifr \cdot f_i = [0]$, so that

$$U[x; G(e)] \cdot f_i = x^{|G(e)|} \cdot f_i.$$

If $i \in \{s+1, \dots, r\}$, then $v_{s+1} \dots v_r \cdot f_i = v_{s+1} f_i \cdot v_{s+2} f_i \dots v_r f_i$. Since for $j \neq i$ $v_j f_i = (\bar{f}_j + h_j f_j) \bar{f}_1 \dots \bar{f}_s \cdot f_i = \bar{f}_j \bar{f}_1 \dots \bar{f}_s \cdot f_i = f_i$, we have independently of the $\dfrac{|G(e)|}{|G_i|}$ choices of $v_{s+1}, \dots, v_{i-1} \cdot v_{i+1} \dots v_r$, that $(v_{s+1} \dots v_r) f_i = v_i f_i$. Hence

$$U[x; G(e)] f_i = \prod_{v \in G_i} (x f_i - v f_i)^{|G(e)|\,|G_i|} = [U(x; G_i)]^{|G(e)\,|G_i|} \cdot f_i$$

and

$$U[x; G(e)] = (f_1 + \dots + f_s) x^{|G(e)|} + \sum_{i=s+1}^{r} [U(x; G_i)]^{|G(e)|\,|G_i|} \cdot f_i. \tag{2}$$

By Theorem 1 we have again $U[x;G_i]f_i=(x^{p_i-1}-1)^{|G_i|/p_i-1}\cdot f_i$ if p_i is odd and the same results hold if $p_i^{\alpha_i}=2$. If $p_i^{\alpha_i}=2^{\alpha_i}$, $\alpha_i\geqq 2$, we have $U[x;G_i]f_i = (x^2-1)^{|G_i|/2}\cdot f_i$.

If all $p_{s+1},\dots,p_r$ are odd, or one of them, say p_r, is even and $p_r^{\alpha_r}=2$, we immediately obtain

$$U[x;G(e)]=(f_1+\dots+f_s)x^{|G(e)|}+\sum\nolimits_{i=s+1}^{r}(x^{p_i-1}-1)^{|G(e)|/p_i-1}\cdot f_i.$$

There remains the case in which one of the $p_{s+1},\dots,p_r$, say p_r, is even and $p_r^{\alpha_r}=2^{\alpha_r}$, $\alpha_r\geqq 2$. In this case the last term in (2) is
Recall that $|G(e)|=\varphi(p_{s+1}^{\alpha_{s+1}}\dots p_r^{\alpha_r}) = |G_{s+1}|\dots|G_r|$. If $r-s\geqq 2$, then (analogously to the proof of Theorem 1) the right-hand side of (3) can be rewritten as $(x-1)^{|G(e)|}\cdot f_r$. If $s=r-1$, i. e. $e=\bar f_1\dots\bar f_{r-1}$ and $|G(e)|=2^{\alpha_r-1}$ this modification cannot be carried out but in this case we have

$$\begin{aligned}U[x;G(e)]&=(f_1+\dots+f_{r-1})x^{|G(e)|}+(x^2-1)^{|G(e)|/2}f_r=\\&=\bar f_r x^{|G(e)|}+f_r(x^2-1)^{|G(e)|/2}=[\bar f_r\cdot x^2+f_r(x^2-1)]^{|G(e)|/2}=\\&=(x^2-f_r)^{\beta_r},\end{aligned}$$

where $\beta_r=2^{\alpha_r-2}$.
We have proved:

Theorem 3. *Let $m=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ and $e=\bar f_1\dots\bar f_s$, $s<r$. Then*

$$U[x;G(e)]=(f_1+\dots+f_s)x^{|G(e)|}+\sum_{i=s+1}^{r}f_i(x^{p_i-1}-1)^{|G(e)|/(p_i-1)}$$

with the exception of the case $e=\bar f_1\dots\bar f_{r-1}$ and $p_r^{\alpha_r}=2^{\alpha_r}$, $\alpha_r\geqq 2$, in which case $U[x;G(e)] = (x^2-f_r)^{\beta_r}$, where $\beta_r=2^{\alpha_r-2}$.

Remark 1. In this exceptional case e is the primitive idempotent f_r with the corresponding maximal group of order $|G(f_r)|=2^{\alpha_r-1}$.

For any other primitive idempotent which is necessarily of the form $e=\bar f_1\dots\bar f_{r-1}=f_r$ and $|G(e)|=\varphi(p_r^{\alpha_r})$ we have (with $\beta_r=p_r^{\alpha_r-1}$)

$$\begin{aligned}U[x;G(e)]&=(f_1+\dots+f_{r-1})x^{|G(e)|}+f_r(x^{p_r-1}-1)^{|G(e)|/(p_r-1)}=\\&=\bar f_r\cdot x^{|G(e)|}+f_r(x^{p_r-1}-1)^{|G(e)|/(p_r-1)}=[\bar f_r\cdot x^{p_r-1}+f_r(x^{p_r-1}-1)]^{\beta_r}=\\&=[x^{p_r-1}-f_r]^{\beta_r}.\end{aligned}$$

Hence we state:

Corollary 3. *If f_i is a primitive idempotent $\in S_m$, then*

$$U[x;G(f_i)]=[x^{p_i-1}-f_i]^{\beta_i},\ \beta_i=p_i^{\alpha_i-1},$$

with the exception of the case that m is even, $f_i=[a\cdot m/2^{\alpha_i}]$, $\alpha_i\geqq 2$, $a\in G(1)$, *in which case*

$$U[x;G(f_i)]=(x^2-f_i)^{\gamma_i},\ \gamma_i=2^{\alpha_i-2}.$$

Remark 2. It is worth to note the following. Suppose, e. g., that p_i is odd. The group G_i and the group $G(f_i)$ are algebraically isomorphic, while

$$\prod_{v\in G_i}(x-v)=[(x-\bar{f}_i)^{p_i-1}-f_i]^{\beta_i},\ \beta_i=p_i^{\alpha_i-1},$$

$$\prod_{v\in G(f_i)}(x-v)=[x^{p_i-1}-f_i]^{\beta_i},$$

which are different polynomials (over S_m).

3. The product $U[x;P(e)]$

In the following we shall need a Lemma.

Denote $Z_\alpha=\prod_{h=1}^{p^{\alpha-1}}(x-hp)$. Note: If $V=\{0,1,\ldots,p^\alpha-1\}$, and $V^{(0)}=\{v\in V\,|\,(h,p)>1\}$, then $Z_\alpha\equiv\prod_{v\in V^{(0)}}(x-v)\ (\mathrm{mod}\ p^\alpha)$.

Lemma 2. a) *If* $p>2$, *then*

$$Z_\alpha\equiv x^{p^{\alpha-1}}\ (\mathrm{mod}\ p^\alpha).$$

b) *If* $p=2$, $\alpha\geqq 2$, *then*

$$Z_\alpha\equiv(x^2-2x)^{2^{\alpha-2}}\ (\mathrm{mod}\ p^\alpha).$$

Remark. The first part of this Lemma is implicitly contained in paper [3].

Proof. a) Suppose $p>2$, the Lemma is true for $\alpha=1$, since $Z_1=x-p\equiv x\ (\mathrm{mod}\ p)$. Suppose that $Z_\alpha\equiv x^{p^{\alpha-1}}\ (\mathrm{mod}\ p^\alpha)$, we prove $Z_{\alpha+1}\equiv x^{p^\alpha}\ (\mathrm{mod}\ p^{\alpha+1})$.

Now

$$Z_{\alpha+1}=\prod_{j=0}^{p-1}\left(\prod_{h=1}^{p^{\alpha-1}}(x-hp-jp^\alpha\right).$$

For a fixed j

$$\prod_{h=1}^{p^{\alpha-1}}(x-hp-jp^\alpha)\equiv\prod_{h=1}^{p^{\alpha-1}}(x-hp)+jp^\alpha\cdot g(x)\equiv Z_\alpha+jp^\alpha g(x)\ (\mathrm{mod}\ p^{\alpha+1}),$$

where $g(x)$ is a polynomial independent of j. This implies

$$Z_{\alpha+1}\equiv\prod_{j=0}^{p-1}(Z_\alpha+jp^\alpha g(x))\equiv Z_\alpha^p+Z_\alpha^{p-1}\cdot p^\alpha\cdot g(x)\cdot\sum_{j=0}^{p-1}j\equiv Z_\alpha^p\ (\mathrm{mod}\ p^{\alpha+1}).$$

Since by the inductive supposition $Z_\alpha = x^{p^{\alpha-1}} + p^\alpha \cdot g_1(x)$ (with a polynomial $g_1(x)$), we have

$$Z_{\alpha+1} \equiv [x^{p^{\alpha-1}} + p^\alpha \cdot g_1(x)]^p \equiv x^{p^\alpha} \pmod{p^{\alpha+1}}.$$

This proves our Lemma for $p>2$.

b) Suppose $p=2$. The statement holds for $\alpha=2$, since $Z_2 = x(x-2)$. We suppose that

$$Z_\alpha = \prod_{h=1}^{2^{\alpha-1}} (x-2h) \equiv (x^2-2x)^{2^{\alpha-2}} \pmod{2^\alpha},$$

we have to prove that $Z_{\alpha+1} \equiv (x^2-2x)^{2^{\alpha-1}} \pmod{2^{\alpha+1}}$. Now

$$Z_{\alpha+1} = \prod_{h=1}^{2^{\alpha-1}} (x-2h)(x-2(2^{\alpha-1}+h)) \equiv \prod_{h=1}^{2^{\alpha-1}} (x-2h-2^{\alpha-1})^2 \pmod{2^\alpha}$$

(since $2(\alpha-1) \geqq \alpha$ for $\alpha \geqq 2$). Further

$$\prod_{h=1}^{2^{\alpha-1}} (x-2h-2^{\alpha-1}) = Z_\alpha(x-2^{\alpha-1}) \equiv [(x-2^{\alpha-1})^2 - 2(x-2^{\alpha-1})]^{2^{\alpha-2}} \equiv$$

$$\equiv (x^2-2x)^{2^{\alpha-2}} \pmod{2^\alpha},$$

hence

$$\prod_{h=1}^{2^{\alpha-1}} (x-2h-2^{\alpha-1}) = (x^2-2x)^{2^{\alpha-2}} + 2^\alpha \cdot g(x),$$

where $g(x)$ is a polynomial. This implies finally

$$Z_{\alpha+1}(x) = [(x^2-2x)^{2^{\alpha-2}} + 2^\alpha g(x)]^2 \equiv (x^2-2x)^{2^{\alpha-1}} \pmod{2^{\alpha+1}}.$$

This completes the proof of Lemma 2.

The next theorem deals with the product $\prod_{v \in I_i} (x-v)$, where I_i has been defined in the introduction.

Theorem 4.

$$U[x:I_i] = \begin{cases} (x-f_i)^{|I_i|} & \text{if } p_i > 2, \\ (x^2 - [2]x + \bar{f}_i)^{\frac{1}{2}|I_i|} & \text{if } p_i^{\alpha_i} = 2^{\alpha_i},\ \alpha_i \geqq 2, \\ x - \bar{f}_i & \text{if } p_i^{\alpha_i} = 2, \end{cases}$$

where $|I_i| = p_i^{\alpha_i - 1}$.

Proof. Any element $v \in I_i$ is of the form $v = \bar{f}_i + hf_i$, $h \in V_i^{(0)}$. We have

$$x - v = (x-1)\bar{f}_i + (x-h)f_i,\ h \in V_i^{(0)},$$

$$U[x_i\,;\,I_i]=\prod_{v\in I_i}(x-v)=(x-1)^{|I_i|}\cdot\bar{f}_i+f_i\cdot\prod_{h\in V_i^{(0)}}(x-h).$$

a) If $p_i>2$, by Lemma 2 (since $[p_i^{\alpha_i}]f_i=[0]$)

$$U[x\,;\,I_i]=(x-1)^{|I_i|}\bar{f}_i+x^{|I_i|}f_i=[(x-1)\bar{f}_i+xf_i]^{|I_i|}=$$
$$=(x-\bar{f}_i)^{|I_i|}.$$

b) If $p^{\alpha_i}=2^{\alpha_i}$, $\alpha_i\geqq 2$, again by Lemma 2

$$U[x\,;\,I_i]=(x-1)^{|I_i|}\bar{f}_i+(x^2-2x)^{\frac{1}{2}|I_i|}f_i=$$
$$=[(x-1)^2\bar{f}_i+(x^2-2x)f_i]^{\frac{1}{2}|I_i|}=(x^2-[2]x+\bar{f}_i)^{\frac{1}{2}|I_i|}.$$

c) If $p_i^{\alpha_i}=2$, $V_i^{(0)}=\{0\}$, so that I_i reduces to $\bar{f}_i+[0]f_i=\bar{f}_i$, hence $U[x\,;\,I_i]=x-\bar{f}_i$.
This proves Theorem 4.

To find $U[x\,;\,P(e)]$ we may restrict ourselves to the case $e\neq[1]$ since $P(1)=G(1)$.

Let $e=\bar{f}_1\ldots\bar{f}_s$, $s\leqq r$, (and $s\geqq 1$). The semigroup $P(e)$ admits the following (internal) direct decomposition

$$P(e)=I_1\ldots I_sG_{s+1}\ldots G_r,$$

where if $s=r$, no G_i appears. Clearly $|P(e)|=|I_1|\ldots|I_s|\cdot|G_{s+1}|\ldots|G_r|$.

$U[x\,;\,P(e)]=\Pi(x-v_1\ldots v_sv_{s+1}\ldots v_r)$, where $v_k\in I_k$ for $k\leqq s$, and $v_k\in G_k$, for $k>s$.

We write again $U[x\,;\,P(e)]=\sum_{i=1}^{r}U[x\,;\,P(e)]\cdot f_i$.

Recall $v_k=\bar{f}_k+h_kf_k$, where $h_k\in V_k^{(0)}$ for $k\leqq s$ and $h_k\in V_k^{(1)}$ for $k>s$.

a) If $i\leqq s$, then $v_1\ldots v_r\cdot f_i=v_if_i$ for all possible $|P(e)/|I_i|$ values of the product $v_1\ldots v_{i-1}v_{i+1}\ldots v_r$, so that

$$U[x\,;\,P(e)]f_i=\prod_{v\in I_i}(x-v)^{|P(e)|\;|I_i|}f_i.$$

b) If $s<r$ and $i>s$, then again $v_1\ldots v_rf_i=v_if_i$ for all possible $|P(e)|/|G_i|$ choices of the remaining v_j, so that

$$U[x\,;\,P(e)]f_i=\prod_{v_i\in G_i}(x-v_i)^{|P(e)|\;|G_i|}.$$

Therefore:

$$U[x\,;\,P(e))]=\sum_{i=1}^{s}U(x\,;\,I_i)^{|P(e)|/|I_i|}f_i+\sum_{i=s+1}^{r}[U(x\,;\,G_i)]^{|P(e)\;|G_i|}f_i. \tag{4}$$

c) If $s=r$, the same formula holds if the last term to the right is omitted.

A) Suppose that $m=p_1^{\alpha_1}\dots p_r^{\alpha_r}$, $r\geqq 2$, where all $p_i^{\alpha_i}$ are odd or one of the factors is 2. Then (4), Theorem 1 and Theorem 3 imply

$$U[x;P(e)]=\sum_{i=1}^{s}(x-\bar{f}_i)^{|P(e)|}f_i+\sum_{i=s+1}^{r}[(x-\bar{f}_i)^{p_i-1}-f_i]^{|P(e)|/(p_i-1)}f_i=$$

$$=[f_1+\dots+f_s]x^{|P(e)|}+\sum_{i=s+1}^{r}f_i(x^{p_i-1}-1)^{|P(e)|/(p_i-1)}, \tag{5}$$

where if $s=r$, the second term should be omitted so that $U[x;P(e)]=x^{|P(e)|}$.

There remains the case that one of the factors of $m=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ is equal to 2^α, where $\alpha\geqq 2$. In this case it is necessary to consider several possibilities.

B) Suppose first that $m=2^{\alpha_1}\cdot p_2^{\alpha_2}\dots p_r^{\alpha_r}$, $\alpha_1\geqq 2$, and $r=s$, i. e. $e=[0]$ and $P(e)=P([0])=P(0)$.

Then

$$U[x;I_1]^{|P(e)|/|I_1|}f_1=(x^2-2x+\bar{f}_1)^{\frac{1}{2}|P(e)|}f_1=(x^2-2x)^{\frac{1}{2}|P(e)|}f_1,$$

and

$$U[x;P(0)]=(x^2-2x)^{\frac{1}{2}|P(0)|}f_1+(f_2+\dots+f_r)x^{|P(0)|}=$$

$$=(x^2-2x)^{\frac{1}{2}|P(0)|}f_1+\bar{f}_1x^{|P(0)|}=[(x^2-2x)f_1+\bar{f}_1x^2]^{\frac{1}{2}|P(0)|}=(x^2-2xf_1)^{\frac{1}{2}|P(0)|}.$$

Hereby $|P(0)|=2^{\alpha_1-1}p_2^{\alpha_2-1}\dots p_r^{\alpha_r-1}$.

C) Suppose $s<r$, $e=\bar{f}_1\dots\bar{f}_s$, and the maximal idempotent which is a multiple of $[2^\alpha]$ is a factor of $e=\bar{f}_1\dots\bar{f}_s$. Write $m=2^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$, so that $\bar{f}_1$ is a multiple of $[2^{\alpha_1}]$. We have again

$$U[x;I_1]^{\frac{|P(e)|}{|I_1|}}\cdot f_1=(x^2-2x)^{\frac{1}{2}|P(e)|}f_1.$$

But since $|P(e)|=2^{\alpha_1-1}\dots\varphi(p_r^{\alpha_r})$, $|P(e)|$ is divisible by 2^{α_1} and $\frac{1}{2}|P(e)|=$ $=2^{\alpha_1-1}\cdot u$, where u is an integer. Hence

$$(x^2-2x)^{\frac{1}{2}|P(e)|}f_1=x^{|P(e)|}f_1+f_1\cdot\sum_{k\geqq 1}(-1)^k\binom{\frac{1}{2}|P(e)|}{k}2^kx^{|P(e)|-k}=x^{|P(e)|}\cdot f_1,$$

since for $k\geqq 1$ the term $\binom{\frac{1}{2}|P(e)|}{k}2^k$ is divisible by 2^{α_1} and $[2^{\alpha_1}]f_1=[0]$. For $U[x;P(e)]$ we obtain the same result as in (5).

D) Suppose $s<r$, $e=\bar{f}_1\dots\bar{f}_s$, and write $m=p_1^{\alpha_1}\dots p_{r-1}^{\alpha_{r-1}}\cdot 2^{\alpha_r}$, $\alpha_r\geqq 2$, so that the maximal idempotent corresponding to $[2^{\alpha_r}]$ is not a factor of e.

By Theorem 1 we have

$$U[x;G_r]=[(x-\bar{f}_r)^2-f_r]^{\frac{1}{2}|G_r|},$$

and the last term in (4) is now

$$(U[x;G_r])^{|P(e)|\,|G_r|}\cdot f_r=[(x-f_r)^2-f_r]^{\frac{1}{2}|P(e)|}f_r=(x^2-1)^{\frac{1}{2}|P(e)}\cdot f_r.$$

D 1) If $s\leqq r-2$, then $|P(e)|$ is divisible by 2^{α_r}, hence $\frac{1}{2}$ $|P(e)|=2^{\alpha_r-1}\cdot u$, where u is an integer. In this case (with $\beta=2^{\alpha_r-1}\cdot u$)

$$(x^2-1)^{\frac{1}{2}|P(e)|}\cdot f_r=[(x-1)^2+2(x-1)]^{\beta}\cdot f_r,$$

and by the same argument as in the proof of Theorem 1 (case c) we obtain

$$(U[x;G_r])^{|P(e)|\,|G_r|}f_r=(x-1)^{|P(e)|},$$

so that the formula (5) holds.

D 2) If $s=r-1$, i. e. $P(e)=I_1\,\ldots\,I_{r-1}\cdot G_r$ and $|G_r|=2^{\alpha_r-1}$, the last term in (4) is $(x^2-1)^{\frac{1}{2}|P(e)|}f_r$, which cannot be directly reduced to a simpler form.

But in this case we have

$$U[x;P(e)]=(f_1+\ldots+f_{r-1})x^{|P(e)|}+(x^2-1)^{\frac{1}{2}|P(e)|}f_r=$$
$$=\bar{f}_rx^{|P(e)|}+(x^2-1)^{\frac{1}{2}|P(e)|}f_r=[\bar{f}_rx^2+(x^2-1)\cdot f_r]^{\frac{1}{2}|P(e)|}=(x^2-f_r)^{\frac{1}{2}|P(e)}.$$

Summarily we have proved the following two statements:

Theorem 5a. *Let $m=p_1^{\alpha_1}\ldots p_r^{\alpha_r}$, $r\geqq 2$. Then $U[x;P(0)]=x^{|P(0)|}$ with the exception of the case that m is even and one of the factors, say $p_r^{\alpha_r}$, is 2^{α_r} with $\alpha_r\geqq 2$. In this case $U[x;P(0)]=(x^2-2xf_r)^{\frac{1}{2}|P(0)|}$.*

Theorem 5b. *Let $m=p_1^{\alpha_1}\ldots p_r^{\alpha_r}$, $r\geqq 2$, and $e=\bar{f}_1\ldots\bar{f}_s\neq[0]$, Then $U[x;P(e)]=[f_1+\ldots+f_s]x^{|P(e)|}+\sum_{i=s+1}^{r}f_i(x^{p_i-1}-1)^{|P(e)|\,(p_i-1)}$, with the exception of the case that $s=r-1$ and $p_r^{\alpha_r}=2^{\alpha_r}$, $\alpha_r\geqq 2$,, in which case $U[x;P(e)]=(x^2-f_r)^{\frac{1}{2}|P(e)|}$.*

Remark 1. The second case in Theorem 5b corresponds to the case of $m=p_1^{\alpha_1}\ldots p_{r-1}^{\alpha_{r-1}}2^{\alpha_r}$, $\alpha_r\geqq 2$, and e is a primitive idempotent of the form $f_r=\left[\frac{m}{2^{\alpha_r}}\cdot a\right]$, $a\in G(1)$.

For any other primitive idempotent f_i of the form

$$e=f_i=\left[\frac{m}{p_i^{\alpha_i}}a_i\right],\ p_i\neq 2,\quad a_i\in G(1),$$

the formula (5) may be rewritten as follows:

$$U[x;P(f_i)]=\bar{f}_ix^{|P(e)|}+f_i(x^{p_i-1}-1)^{|P(e)|/(p_i-1)}=$$

$$=[\bar{f}_i \cdot x^{p_i-1}+f_i(x^{p_i-1}-1)]^{|P(f_i)|/(p_i-1)}=(x^{p_i-1}-f_i)^{|P(f_i)|/(p_i-1)}.$$

Corollary 4. *For a primitive idempotent we have*

$$U[x\,;\,P(f_i)]=(x^{p_i-1}-f_i)^{|P(f_i)|/(p_i-1)}$$

with the exception of the case that m is even, $f_i=\left[\frac{m}{2^{\alpha_i}}\,a\right]$, $\alpha_i \geqq 2$, $a \in G(1)$, *in which case*

$$U[x\,;\,P(f_i)]=(x^2-f_i)^{\frac{1}{2}|P(f_i)|}.$$

Remark 2. It seems to be worth to remark that $\Pi(x-v)$, v running through all elements $\in P(0)$ (i. e. all nilpotent elements $\in S_m$) is in "most cases" $x^{|P(0)|}$. But by Theorem 5 a this is not true if m is divisible by 2^{α_r}, $\alpha_r \geqq 2$. The corresponding result $(x^2-2xf_r)^{\frac{1}{2}|P(0)|}$ can be rewritten. Since $\binom{\frac{1}{2}P(0)}{k}2^k$ for $k \geqq 3$ is divisible by 2^{α_r}, at most three terms are $\neq [0]$ and a simple calculation shows that

$$U[x\,;\,P(0)]=\begin{cases} x^{|P(0)|}-|P(0)|f_r \cdot x^{|P(0)|-1} & \text{for } \alpha_r=2,\\ x^{|P(0)|}-|P(0)| \cdot f_r \cdot x^{|P(0)|-1}-|P(0)|f_r x^{|P(0)|-2} & \text{for } \alpha_r \geqq 3.\end{cases}$$

To have a numerical example consider, e. g., $m=5 \cdot 2^3=40$. Here $f_1=[16]$, $f_2=[25]$, $P(0)=\{[0], [10], [20], [30]\}$.

$$U[x\,;\,P(0)]=x(x-[10])(x-[20])(x-[30])=$$
$$=(x^2-2 \cdot [25]x)^2=x^4+[20]x^3+[20]x^2.$$

Theorems 3 and 5b lead to the following remarkable result:

Theorem 6. *Let* $m=p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $r \geqq 2$, *and* $e \neq [0]$. *Then*

$$U[x\,;\,P(e)]=U[x\,;\,G(e)]^L,$$

where $L=|P(e)|/|G(e)|$.

Proof. Due to the orthogonality of the set $\{f_i\}$, the formula of Theorem 3 implies for any integer $k \geqq 1$:

$$U[x\,;\,G(e)]^k=(f_1+\dots+f_s)^{k \cdot |G(e)|}+\sum_{i=s+1}^{r} f_i(x^{p_i-1}-1)^{k \cdot |G(e)|/(p_i-1)}$$

Putting $k=|P(e)|/|G(e)|$ the right-hand side gives exactly the formula of Theorem 5b.

Our statement holds also in the exceptional case mentioned in Theorem 3 and Theorem 5b, since in this case

$$U[x;G(e)]=(x^2-f_r)^{\frac{1}{2}|G(e)|},\ U[x;P(e)]=(x^2-f_r)^{\frac{1}{2}|P(e)|}.$$

Finally it is true also if $e=[1]$, since in this case $|P(e)|=|G(e)|$.

Remark. If $[e]=[0]$, $U[x:G(0)]=x$, so that Theorem 6 is true if m is odd or m is divisible by 2 but not by 4. In the exceptional case mentioned in Theorem 5a, the statement of Theorem 6 does not hold.

4. The product $U[x;S_m]$

In order to find the formula for the product $\Pi(x-v)$, where v runs trough the whole semigroup S_m, we recall that $S_m=T_1\ldots T_r$, where T_i has been defined in the introduction.

It is natural to find first the product $U[x;T_i]$.

Since $T_i=G_i\cup I_i$, we have $U[x;T_i]=U[x;G_i]\cdot U[x;I_i]$.

Theorem 7. a) *If* $p_i>2$, *then*

$$U[x;T_i]=[(x-\bar{f}_i)^{p_i}-xf_i]^{\beta_i},\beta_i=p_i^{\alpha_i-1}.$$

b) *If* $p_i=2$, $U[x;T_i]=(x-\bar{f}_i)(x-[1])$.

c) *If* $p_i^{\alpha_i}=2^{\alpha_i}$, $\alpha_i\geqq 2$, *then*

$$U[x;T_i]=(x^2-2x+\bar{f}_i)^{\gamma_i}\cdot[(x-\bar{f}_i)^2-f_i]^{\gamma_i},\ \gamma_i=2^{\alpha_i-2}.$$

Proof. By Theorem 1 and Theorem 4 we obtain for $p_i>2$

$$U[x;T_i]=(x-\bar{f}_i)^{\beta_i}\cdot[(x-\bar{f}_i)^{p_i-1}-f_i]^{\beta_i}=$$

$$=[(x-\bar{f}_i)^{p_i}-(x-\bar{f}_i)f_i]^{\beta_i}=[(x-\bar{f}_i)^{\beta_i}.$$

The remaining cases follow directly from the corresponding statements of Theorems 1 and 4.

Any element $v\in S_m$ can be written uniquely in the form $v=t_1t_2\ldots t_r$, with $t_i\in T_i$. For any $v\in S_m$ $v\cdot f_i=(t_1\ldots t_r)\cdot f_i=t_if_i$ independently of the $m/p_i^{\alpha_i}$ possible values of $t_1\ldots t_{i-1}t_{i+1}\ldots t_r$.

Hence

$$U[x;S_m]\cdot f_i=\prod_{v\in S_m}(xf_i-vf_i)=\prod_{t\in T_i}(xf_i-tf_i)^{u_i}=(U[x;T_i])^{u_i}\cdot f_i,$$

where $u_i=m/p_i^{\alpha_i}$

Since $U[x;S_m]=\sum_{i=1}^{r}U[x;S_m]\cdot f_i$, we have finally

$$U[x;S_m]=\sum_{i=1}^{r}U[x;T_i]^{u_i}f_i.$$

a) If $p_i>2$, we have (with $\beta_i=p_i^{\alpha_i-1}$)

$$U[x;T_i]^{u_i}\cdot f_i=([x^{p_i}-x]^{\beta_i}\cdot f_i)^{u_i}=(x^{p_i}-x)^{m\ p_i}\cdot f_i.$$

b) If $p_i = 2$,

$$U[x; T_i]^{m/2} f_i = [(x - \bar{f}_i)(x-1)f_i]^{m/2} = (x^2 - x)^{m/2} \cdot f_i.$$

c) If $p_i^{\alpha_i} = 2^{\alpha_i}$, $\alpha_i \geqq 2$, (with $v_i = m/2^{\alpha_i}$)

$$U[x; T_i]^{v_i} f_i = (x^2 - 2x)^{m/4} \cdot (x^2 - 1)^{m/4} \cdot f_i =$$
$$= [(x^2 - x)^2 - 2(x^2 - x)]^{m/4} \cdot f_i.$$

We have proved:

Theorem 8. *Let $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. If all p_i are odd or m is divisible by 2 but not by 4, then*

$$U[x; S_m] = \sum_{i=1}^{r} f_i \cdot (x^{p_i} - x)^{m/p_i}. \tag{6}$$

If $m = 2^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $\alpha_1 \geqq 2$, then

$$U[x; S_m] = [(x^2 - x)^2 - 2(x^2 - x)]^{m/4} f_1 + \sum_{i=2}^{r} f_i (x^{p_i} - x)^{m/p_i}. \tag{7}$$

Remark. The first term in (7) can be directly computed and we obtain (analogously to the Remark after Corollary 4):

$$[(x^2 - x)^2 - 2(x^2 - x)]^{m/4} f_1 = \begin{cases} (y^{m/2} + \frac{m}{2} y^{m/2-1}) \cdot f_1, & \text{for } \alpha_1 = 2, \\ (y^{m/2} + \frac{m}{2} y^{m/2-1} + \frac{m}{2} y^{m/2-2}) \cdot f_1, & \text{for } \alpha_1 \geqq 3, \end{cases}$$

where $y = x^2 - x$.

The formula (6) has been proved (in essential) by Vandiver. His formula for $U[x; S_m]$ in the case of m even (as reproduced in Dickson [1], p. 89) is not correct. The correct result is (7).

5. Concluding remarks

Theorems 1 and 4 enable to find also formulae for $U[x; G_1 \dots G_s]$, $U[x; I_1 \dots I_s]$, $U[x; T_1 \dots T_s]$ with $s < r$. We omit this since these products seem to be of minor interest.

There are several applications of the results obtained. We outline one of them.

Suppose, e. g., that m is odd (and $r \geqq 2$).

Let $e = \bar{f}_1 \dots \bar{f}_s$ be a non-primitive idempotent $\in S_m$ (i. e. $s \leqq r-2$). Then putting $x = 0$ in the formula of Theorem 3 we obtain

$$[-1]^{|G(e)|} \cdot \prod_{u \in G(e)} u = \prod_{u \in G(e)} u = f_{s+1} + \dots + f_r = 1 - f_1 - \dots - f_s = \bar{f}_1 \dots \bar{f}_s = e.$$

If $e = f_i$ is a primitive idempotent $\in S_m$, then Corollary 3 implies (with $\beta_i = p_i^{\alpha_i - 1}$):

$$[-1]^{|G(f_i)|} \prod_{u \in G(e)} u = \prod_{u \in G(e)} u = [-f_i]^{\beta_i} = -f_i = -e .$$

Hence (if m is odd) $\prod_{u \in G(e)} u$ is e for any non-primitive idempotent and $-e$ for any primitive idempotent $\in S_m$. By considering also the case of m even, we arrive at Theorem 8, 1 of paper [4], where the value of $\prod_{u \in G(e)} u$ has been derived directly. Also Theorem 8, 2 of paper [4] follows immediately from Theorem 6.

REFERENCES

[1] DICKSON, L. E.: History of the Theory of Numbers. Volume I. Stechert & Co, New York, 1934.

[2] HARDY, G. H.—WRIGHT, E. M.: An Introduction to the Theory of Numbers. Second edition. Clarendon Press, Oxford, 1945.

[3] LUBELSKI, S.: Zur Theorie der höheren Kongruenzen. J. reine und angew. Math. 162, 1930, 63—68.

[4] SCHWARZ, Š.: The role of semigroups in the elementary theory of numbers. Math. Slovaca 31, 1981, 369—395.

Received June 5, 1981

Matematický ústav SAV
Obrancov mieru 49
814 73 Bratislava

ОБОБЩЕНИЯ СРАВНЕНИЙ М. БАУЭРА

Štefan Schwarz

Резюме

Пусть S_m– мультипликативная полугруппа кольца классов вычетов (mod m). Пусть e – идемпотент $\in S_m$, $G(e)$ и $P(e)$ – максимальная группа и максимальная полугруппа принадлежащая и идемпотенту e. Целью статьи является вычисление произведения $\Pi(x - v)$, где v пробегает все элементы $\in G(e)$ и $\in P(e)$ соотвественно. Основными результатами являются формулы данные в Теореме 3, в Теоремах 5a, b и в Теореме 6.