MATEMATICKO-FYZIKÁLNY ČASOPIS SAV, X, 1-1960

O ROZKLADE POLOGRUPY ZVYŠKOV (mod m) NA DIREKTNÝ SÚČIN

BOHUMÍR PARÍZEK, Bratislava

Nech $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ je rozklad prirodzeného čísla $m > 1$ na súčin kladných prvočiniteľov. Nech $S(m)$ je pologrupa tried zvyškov (mod m), $G(m)$ nech je grupa tried zvyškov (mod m) nesúdeliteľných s číslom m. Grupa $G(m)$, ako je známe, má $\varphi(m)$ elementov, kde φ je Eulerova funkcia.

V práci nájdeme explicitnú metódu rozkladu pologrupy $S(m)$ na direktný súčin čiastočných pologrúp $T_1, T_2, \dots, T_r$ rádov $m_1 = p_1^{\alpha_1}$, $m_2 = p_2^{\alpha_2}, \dots$, $m_r = p_r^{\alpha_r}$ v tvare

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

Súčasne ukážeme, že táto metóda umožňuje nájsť rozklad grupy $G(m)$ na direktný súčin podgrúp v tvare

$$G(m) = G_1 . G_2 . \dots . G_r, \tag{2}$$

kde podgrupy G_i $(i = 1, 2, \dots, r)$ majú rád $\varphi(m_i)$ a $m_i = p_i^{\alpha_i}$.

Známa je veta (pozri napr. Parker [3], lemma na str. 613), ktorá hovorí, že pologrupa $S(m)$ je izomorfná s direktným súčinom pologrúp $S(m_i)$, kde $m_i = p_i^{\alpha_i}$ $(i = 1, 2, \dots, r)$, teda že platí $S(m) \cong S(m_1) \times \dots \times S(m_r)$. Táto veta má však existenčný charakter a neumožňuje bezprostredne nájsť rozklad pologrupy $S(m)$ na direktný súčin jej čiastočných pologrúp.

Rédei v knihe [4] (str. 186) dokazuje vetu o rozklade pologrupy $S(m)$ a grupy $G(m)$ na direktný súčin v tvare (1) a (2). Množiny T_i a G_i sú tu však popísané pomocou aditívnych vlastností okruhu tried zvyškov (mod m). V práci ukážeme, že množiny T_i a G_i možno charakterizovať i multiplikatívne, t. j. bez použitia aditívnych vlastností okruhu tried zvyškov (mod m).

1

Triedu prirodzených čísel (mod m), do ktorej patrí číslo a, budeme ako element pologrupy $S(m)$ označovať znakom $[a]$. Element $[1]$ je jednotkou pologrupy $S(m)$.

Nech E je množina všetkých idempotentov pologrupy $S(m)$. V práci [1] bolo dokázané, že E má (včítane $[0]$ a $[1]$) 2^r elementov.

Idempotent $e \neq [1]$ nazývame maximálnym, keď zo vzťahu $ef = e$,

$f \in E$, $f \neq [1]$ vyplýva $e = f$. V práci [1] bolo dokázané, že $S(m)$ má r maximálnych idempotentov a že každý z nich je tvaru $[p_i^{\alpha_i} a_i]$, kde a_i je vhodne zvolený (jednoznačne určený) prvok grupy $G(m)$. V ďalšom budeme používať označenie $e_i = [p_i^{\alpha_i} a_i]$, takže $e_1, e_2, \dots, e_r$ budú práve všetky maximálne idempotenty pologrupy $S(m)$.

V tomto odseku sa budeme zaoberať rozkladom pologrupy $S(m)$ na direktný súčin čiastočných pologrúp.

Veta 1. *Nech e_i je maximálny idempotent pologrupy $S(m)$. Potom množina*

$$T_i = \{[x] \mid [x] \in S(m),\ [x]\, e_i = e_i\}$$

je čiastočná pologrupa pologrupy $S(m)$ a $S(m)$ možno písať v tvare direktného súčinu

$$S(m) = T_1 . T_2 . \dots . T_r.$$

Dôkaz. Množina T_i je čiastočná pologrupa pologrupy $S(m)$, lebo keď $[x] \in T_i$, $[y] \in T_i$, je $[x]\, e_i = e_i$, $[y]\, e_i = e_i$ a teda aj $[x]\,[y]\, e_i = e_i$.

Trieda $[x] \in S(m)$ patrí do množiny T_i vtedy a len vtedy, keď $[x]\, e_i = e_i$, t. j. keď platí

$$[p_i^{\alpha_i} a_i]\,[x] = [p_i^{\alpha_i} a_i].$$

Pretože e_i je idempotent, je predošlá rovnica ekvivalentná s rovnicou

$$[p_i^{\alpha_i} a_i]\,[x] = [p_i^{\alpha_i} a_i]^2. \tag{3}$$

Číslo x patrí do triedy $[x]$ vyhovujúcej rovnici (3) vtedy a len vtedy, keď vyhovuje kongruencii

$$p_i^{\alpha_i} a_i x \equiv p_i^{2\alpha_i} a_i^2 \pmod{m},$$

t. j.

$$x \equiv p_i^{\alpha_i} a_i \left(\mathrm{mod}\ \frac{m}{p_i^{\alpha_i}}\right). \tag{4}$$

Každé (mod m) inkongruentné riešenie kongruencie (4) je tvaru $p_i^{\alpha_i} a_i + k \dfrac{m}{p_i^{\alpha_i}}$, kde $k = 0, 1, \dots, p_i^{\alpha_i} - 1$. To je dovedna $p_i^{\alpha_i}$ rôznych čísel. T_i má teda p_i^{α} prvkov a možno písať

$$T_i = \left\{\left[p_i^{\alpha_i} a_i + k \frac{m}{p_i^{\alpha_i}}\right],\quad k = 0, 1, \dots, p_i^{\alpha_i} - 1\right\}.$$

Keď dokážeme, že každý prvok $[x] \in S(m)$ možno písať jedným a len jedným spôsobom v tvare $[x] = \xi_1 . \xi_2 . \dots . \xi_r$, kde $\xi_i \in T_i$ $(i = 1, 2, \dots, r)$, bude veta dokázaná.

Súčin $T_1 . T_2 . \dots . T_r$ pozostáva z $p_1^{\alpha_1} . p_2^{\alpha_2} . \dots . p_r^{\alpha_r} = m$ elementov pologrupy $S(m)$. Stačí preto dokázať, že každé dva prvky tohoto súčinu sú navzájom rôzne.

Nech

$$\left[p_1^{\alpha_1}a_1 + k_1\frac{m}{p_1^{\alpha_1}}\right]\left[p_2^{\alpha_2}a_2 + k_2\frac{m}{p_2^{\alpha_2}}\right]\dots\left[p_r^{\alpha_r}a_r + k_r\frac{m}{p_r^{\alpha_r}}\right]$$

a

$$\left[p_1^{\alpha_1}a_1 + l_1\frac{m}{p_1^{\alpha_1}}\right]\left[p_2^{\alpha_2}a_2 + l_2\frac{m}{p_2^{\alpha_2}}\right]\dots\left[p_r^{\alpha_r}a_r + l_r\frac{m}{p_r^{\alpha_r}}\right]$$

sú dva prvky zo súčinu $T_1 . T_2 . \dots . T_r$; predpokladajme, že sú si rovné, t. j. že platí

$$\prod_{i=1}^{r}\left(p_i^{\alpha_i}a_i + k_i\frac{m}{p_i^{\alpha_i}}\right) \equiv \prod_{i=1}^{r}\left(p_i^{\alpha_i}a_i + l_i\frac{m}{p_i^{\alpha_i}}\right) \pmod{m}. \tag{5}$$

Z kongruencie (5) vyplýva

$$k_1\frac{m}{p_1^{\alpha_1}}\prod_{i=2}^{r}p_i^{\alpha_i}a_i \equiv l_1\frac{m}{p_1^{\alpha_1}}\prod_{i=2}^{r}p_i^{\alpha_i}a_i \pmod{p_1^{\alpha_1}},$$

a pretože $\frac{m}{p_1^{\alpha_1}}\prod_{i=2}^{r}p_i^{\alpha_i}a$ je nesúdeliteľné s $p_1^{\alpha_1}$, je

$$k_1 \equiv l_1 \pmod{p_1^{\alpha_1}}. \tag{6}$$

Keďže $0 \leqq k_1 \leqq p_1^{\alpha_1} - 1$, $0 \leqq l_1 \leqq p_1^{\alpha_1} - 1$, vyplýva z kongruencie (6) $k_1 = l_1$.
Analogicky dokážeme, že platí $k_2 = l_2$, $k_3 = l_3$, ..., $k_r = l_r$. Súčin $T_1 . T_2 . \dots . T_r$ pozostáva teda z m navzájom rôznych prvkov pologrupy $S(m)$ a rovná sa teda pologrupe $S(m)$. Tým je veta 1 dokázaná.

Príklad. Rozložme pologrupu $S(360)$ na direktný súčin čiastočných pologrúp v zmysle vety 1.

Pretože $360 = 2^3 . 3^2 . 5$, majú maximálne idempotenty tvar $e_1 = [8a_1]$, $e_2 = [9a_2]$, $e_3 = [5a_3]$, kde a_1, a_2, a_3 sú prirodzené čísla, menšie než 360 a nesúdeliteľné s číslom 360. Číslo a_1 určíme z podmienky $[8a_1] = [8a_1]^2$, ktorá je ekvivalentná s podmienkou $8a_1 \equiv 64a_1^2 \pmod{360}$ a táto s podmienkou $8a_1 \equiv 1 \pmod{45}$. Riešením tejto kongruencie je číslo $a_1 = 17$. Teda $e_1 = [136]$. Podobne nájdeme $e_2 = [81]$, $e_3 = [145]$.

Trieda $[x]$ patrí do pologrupy T_1 vtedy a len vtedy, keď číslo x je riešením kongruencie $136x \equiv 136 \pmod{360}$, t. j. kongruencie $x \equiv 1 \pmod{45}$. Z toho dostávame

$$T_1 = \{[1], [46], [91], [136], [181], [226], [271], 316]\}.$$

Analogicky nájdeme

$$T_2 = \{[1], [41], [81], [121], 161], [201], [241], [281], [321]\},$$
$$T_3 = \{[1], [73], [145], [217], [289]\}.$$

Hľadaný rozklad je

$$S(360) = T_1 . T_2 . T_3.$$

Naskytá sa otázka, či možno pologrupy T_i z rozkladu (1) ďalej direktne rozložiť. Ukážeme, že každá z tých pologrúp je direktne ireducibilná.
Najprv dokážeme túto pomocnú vetu:

Lemma 1. *Pologrupa T_i $(i = 1, 2, \dots, r)$ z rozkladu (1) je izomorfná s pologrupou $S(p_i^{\alpha_i})$.*

Dôkaz. Triedu prirodzených čísel (mod $p_i^{\alpha_i}$), do ktorej patrí číslo x, označíme v dôkaze tejto lemmy znakom $\langle x \rangle$ (na rozdiel od triedy prirodzených čísel (mod m), ktorú budeme i naďalej označovať znakom $[x]$).

Ku každému elementu $\left[p_i^{\alpha_i}a_i + k\frac{m}{p_i^{\alpha_i}}\right] \in T_i$, priraďme element $\left\langle k\frac{m}{p_i^{\alpha_i}}\right\rangle \in S(p_i^{\alpha_i})$. Dokážeme, že toto zobrazenie je izomorfizmus.

1° Nech $\left[p_i^{\alpha_i}a_i + k\frac{m}{p_i^{\alpha_i}}\right]$ a $\left[p_i^{\alpha_i}a_i + l\frac{m}{p_i^{\alpha_i}}\right]$, kde $k \neq l$, $0 \leqq k$, $l \leqq p_i^{\alpha_i} - 1$ sú dva rôzne prvky pologrupy T_i. Ich obrazy v pologrupe $S(p_i^{\alpha_i})$ sú elementy $\left\langle k\frac{m}{p_i^{\alpha_i}}\right\rangle$, $\left\langle l\frac{m}{p_i^{\alpha_i}}\right\rangle$. Keby platilo

$$\left\langle k\frac{m}{p_i^{\alpha_i}}\right\rangle = \left\langle l\frac{m}{p_i^{\alpha_i}}\right\rangle,$$

mali by sme

$$k\frac{m}{p_i^{\alpha_i}} \equiv l\frac{m}{p_i^{\alpha_i}} \pmod{p_i^{\alpha_i}},$$
$$k \equiv l \pmod{p_i^{\alpha_i}},$$

a to je spor s predpokladom, že $k \neq l$, $0 \leqq k$, $l \leqq p_i^{\alpha_i} - 1$. Naše zobrazenie je teda jednojednoznačné.

2° Obrazom súčinu dvoch prvkov $\left[p_i^{\alpha_i}a_i + k\frac{m}{p_i^{\alpha_i}}\right]\left[p_i^{\alpha_i}a_i + l\frac{m}{p_i^{\alpha_i}}\right] = \left[p_i^{\alpha_i}a_i + kl\left(\frac{m}{p_i^{\alpha_i}}\right)^2\right] \in T_i$ je prvok $\left\langle kl\left(\frac{m}{p_i^{\alpha_i}}\right)^2\right\rangle \in S(p_i^{\alpha_i})$. Zrejme je $\left\langle kl\left(\frac{m}{p_i^{\alpha_i}}\right)^2\right\rangle = \left\langle k\frac{m}{p_i^{\alpha_i}}\right\rangle\left\langle l\frac{m}{p_i^{\alpha_i}}\right\rangle$, teda obrazom súčinu dvoch prvkov pologrupy T_i v pologrupe $S(p_i^{\alpha_i})$ je súčin obrazov tých prvkov. Pretože naše zobrazenie má vlastnosti 1° a 2°, je to izomorfizmus.

Veta 2. *Nech $\alpha \geqq 1$ celé, p je kladné prvočíslo. Potom multiplikatívna pologrupa $S(p^\alpha)$ tried zvyškov* (mod p^α) *je direktne ireducibilná.*

Dôkaz. Predpokladajme, že existujú pologrupy $S_1 \neq \{[1]\}$, $S_2 \neq \{[1]\}$ také, že $S(p^\alpha)$ možno písať v tvare direktného súčinu $S(p^\alpha) = S_1 . S_2$.

Tvrdíme, že prvok $[0] \in S(p^\alpha)$ nie je obsiahnutý ani v S_1 ani v S_2. Keby napr. platilo $[0] \in S_1$, bolo by $[0] = [0] . S_2$ a vyjadrenie elementu $[0]$ ako súčinu jedného prvku z S_1 a jedného prvku z S_2 by nebolo jednoznačné.

Zo vzťahu $[0] \in S(p^\alpha)$ vyplýva však $[0] \in S_1 . S_2$. Existujú teda prvky $[ap^\mu] \in S_1$, $[bp^\nu] \in S_2$ také, že $[a] \in G(p^\alpha)$, $[b] \in G(p^\alpha)$, $\mu + \nu = \alpha$, $\mu \geqq 1$, $\nu \geqq 1$ celé. Pretože S_1 je pologrupa, vyplýva zo vzťahu $[ap^\mu] \in S_1$, $\mu \geqq 1$ vzťah $[ap^\mu]^\varrho \in S_1$ pre každé celé $\varrho \geqq 1$. Pre vhodne zvolené celé $\varrho \geqq 1$ je však $p^{\mu\varrho} > p^\alpha$, a teda $[ap^\mu]^\varrho = [0] \in S_1$, čo je spor s dokázaným tvrdením. Tým je naša veta dokázaná.

Priamym dôsledkom lemmy 1 a vety 2 je

Veta 3. *Každá pologrupa T_i ($i = 1, 2, \ldots, r$) v rozklade* (1) *pologrupy $S(m)$ na direktný súčin je direktne ireducibilná.*

2

V tomto odseku ukážeme, že podobne ako sme rozložili pologrupu $S(m)$ na direktný súčin pologrúp, možno rozložiť i grupu $G(m)$ tried zvyškov (mod m) nesúdeliteľných s číslom m na direktný súčin podgrúp grupy $G(m)$.

Veta 4. *Nech e_i je maximálny idempotent pologrupy $S(m)$. Potom množina*

$$G_i = \{[x] \mid [x] \in G(m), \quad [x]\, e_i = e_i\}$$

je podgrupou grupy $G(m)$ tried zvyškov (mod m) *nesúdeliteľných s číslom m a platí tento rozklad na direktný súčin podgrúp*

$$G(m) = G_1 . G_2 . \ldots . G_r .$$

Dôkaz. Množina G_i je podgrupou grupy $G(m)$. Keď totiž $[x] \in G_i$, $[y] \in G_i$, potom platí $[x]\, e_i = e_i$, $[y]\, e_i = e_i$ a teda i $[x][y]\, e_i = e_i$, t. j. $[x][y] \in G_i$. Nech ďalej je $[x] \in G_i$ a nech $[x]^{-1}$ je inverzný prvok k prvku $[x]$ v grupe $G(m)$. Potom zo vzťahu $[x]\, e_i = e_i$ vyplýva $[x]^{-1} e_i = e_i$, teda $[x]^{-1} \in G_i$. Teda G_i je podgrupa grupy $G(m)$.

Nech $e_i = [p_i^{\alpha_i} a_i]$ je maximálny idempotent pologrupy $S(m)$. Prvok $[x] \in G(m)$ patrí do podgrupy G_i vtedy a len vtedy, keď $[p_i^{\alpha_i} a_i]\,[x] = [p_i^{\alpha_i} a_i]$. Analogicky ako v dôkaze vety 1 ukážeme, že prvok $[x] \in G(m)$ patrí do podgrupy G_i vtedy a len vtedy, keď číslo x spĺňuje tieto dve podmienky:

1° x je nesúdeliteľné s číslom m,

2° x je riešenie kongruencie

$$x \equiv p_i^{\alpha_i} a_i \left(\mathrm{mod}\ \frac{m}{p_i^{\alpha_i}}\right).$$

Všetky (mod m) inkongruentné riešenia našej kongruencie sú čísla $b_k = p_i^{\alpha_i} a_i + k \dfrac{m}{p_i^{\alpha_i}}$, kde $k = 0, 1, 2, \ldots, p_i^{\alpha_i} - 1$. Nájdeme medzi nimi všetky tie, ktoré sú nesúdeliteľné s číslom m.

Ani jedno číslo b_k ($k = 0, 1, 2, \ldots, p_i^{\alpha_i} - 1$) nie je deliteľné niektorým z prvočísel $p_1, p_2, \ldots, p_{i-1}, p_{i+1}, \ldots, p_r$. Číslo b_k je deliteľné prvočíslom p_i vtedy a len vtedy, keď alebo platí $k = 0$, alebo k je celočíselným násobkom prvočísla p_i. Pre každé iné celočíselné k, kde $0 < k \leqq p_i^{\alpha_i} - 1$, je číslo b_k nesúdeliteľné s p_i a teda i s číslom m. Takých čísel k je zrejme $\varphi(p_i^{\alpha_i})$.

Podgrupa G_i pozostáva teda z tých a len tých prvkov $[b_k]$, pre ktoré platí: $b_k = p_i^{\alpha_i} a_i + k \dfrac{m}{p_i^{\alpha_i}}$, $0 < k \leqq p_i^{\alpha_i} - 1$, $(k, p_i) = 1$. Podgrupa G_i má $\varphi(p_i^{\alpha_i})$ prvkov.

Utvorme súčin podgrúp $G_1 . G_2 . \ldots . G_r$. Tento súčin obsahuje

$$\varphi(p_1^{\alpha_1}) . \varphi(p_2^{\alpha_2}) . \ldots . \varphi(p_r^{\alpha_r}) = \varphi(m_1) . \varphi(m_2) . \ldots . \varphi(m_r) = \varphi(m)$$

tried zvyškov (mod m), ktoré sú všetky prvkami pologrupy $S(m)$. Z dôkazu vety 1 vyplýva, že všetky tieto triedy sú navzájom rôzne. Ukážeme ešte, že tieto triedy sú všetky prvkami grupy $G(m)$ a tým bude naša veta dokázaná.

Stačí dokázať: Keď $[x] \in G_1 . G_2 . \ldots . G_r$, potom x je nesúdeliteľné s číslom m.

Každá trieda zo súčinu $G_1 . G_2 . \ldots . G_r$ má tvar

$$[\beta_{k_1, k_2, \ldots, k_r}] = \left[p_1^{\alpha_1} a_1 + k_1 \frac{m}{p_1^{\alpha_1}}\right]\left[p_2^{\alpha_2} a_2 + k_2 \frac{m}{p_2^{\alpha_2}}\right] \ldots \left[p_r^{\alpha_r} a_r + k_r \frac{m}{p_r^{\alpha_r}}\right],$$

kde k_i ($i = 1, 2, \ldots, r$) spĺňuje podmienky $0 < k_i \leqq p_i^{\alpha_i} - 1$, $(k_i, p_i) = 1$. Pre žiadne takéto $k_1, k_2, \ldots, k_r$ nie je však číslo $\beta_{k_1, k_2, \ldots, k_r}$ deliteľné ani jedným z prvočísel p_l ($l = 1, 2, \ldots, r$), lebo

$$\beta_{k_1, k_2, \ldots, k_r} \equiv k_l \frac{m}{p_l^{\alpha_l}} \prod_{i=1, i \neq l}^{r} p_i^{\alpha_i} a_i \ (\mathrm{mod}\ p_l^{\alpha_l}).$$

Pretože $\beta_{k_1, k_2, \ldots, k_r}$ nie je deliteľné číslom p_l ($l = 1, 2, \ldots, r$), je nesúdeliteľné i s číslom m. Tým je veta 4 dokázaná.

3

V tomto poslednom odseku rozoberieme otázku reducibility podgrúp G_i ($i = 1, 2, \ldots, r$) grupy $G(m)$ v rozklade (2). Výsledky tohto odseku sú známe (pozri napr. [5]). Nové je, že grupy U, V, o ktorých je v ďalšom reč, sú charakterizované multiplikatívne.

Lemma 2. *Grupa G_i ($i = 1, 2, \ldots, r$) v rozklade* (2) *je izomorfná s grupou $G(p_i^{\alpha_i})$ tried zvyškov* (mod $p_i^{\alpha_i}$) *nesúdeliteľných s číslom $p_i^{\alpha_i}$.*

Dôkaz. Podobne ako v dôkaze lemmy 1 označíme i v tomto dôkaze triedu prirodzených čísel (mod $p_i^{\alpha_i}$), do ktorej patrí číslo x znakom $\langle x \rangle$.

Ku každému elementu $\left[p_i^{\alpha_i} a_i + k \dfrac{m}{p_i^{\alpha_i}}\right] \in G_i$, kde $0 < k \leqq p_i^{\alpha_i} - 1$ a $(k, p_i) = 1$, priradíme prvok $\left\langle k \dfrac{m}{p_i^{\alpha_i}} \right\rangle \in G(p_i^{\alpha_i})$, kde k spĺňuje tie isté podmienky.

Celkom analogicky ako v dôkaze lemmy 1 ukážeme, že toto zobrazenie je izomorfizmus.

Riešenie otázky reducibility grupy G_i $(i = 1, 2, \ldots, r)$ z rozkladu (2) môžeme teda nahradiť riešením otázky reducibility grupy $G(p^\alpha)$, kde p je prvočíslo, α prirodzené číslo.

Je známe, že pre $\alpha = 1$, $p > 2$ je $G(p)$ cyklická grupa rádu $p - 1$. Vo všeobecnej teórii Abelových grúp sa dokazuje, že $G(p)$ možno rozložiť na súčin cyklických grúp, z ktorých každá má rád mocniny nejakého prvočísla. Tieto rozklady závisia od aritmetických vlastností čísla $p - 1$, teda od voľby čísla p. Pre $\alpha > 1$ môžeme však vysloviť všeobecné vety, platné pre každé p. Pritom treba rozlišovať prípady $p > 2$ a $p = 2$.

Veta 5. *Nech $p > 2$ je prvočíslo, $\alpha > 1$ prirodzené číslo. Nech $G(p^\alpha)$ je grupa tried zvyškov* (mod p^α) *nesúdeliteľných s číslom p^α. Potom množiny*

$$U = \{[x] \mid [x] \in G(p^\alpha),\ [x]\,[p^{\alpha-1}] = [p^{\alpha-1}]\}$$
$$V = \{[x] \mid [x] \in G(p^\alpha),\ [x]^{p-1} = [1]\}$$

sú netriviálne podgrupy grupy $G(p^\alpha)$ rôzne od jednotkovej grupy a platí tento rozklad na direktný súčin podgrúp:

$$G = U \,.\, V \tag{7}$$

Dôkaz. 1° Dokážeme najprv, že U je netriviálna podgrupa grupy $G(p^\alpha)$. Keď $[x] \in U$, $[y] \in U$, platí $[x]\,[p^{\alpha-1}] = [p^{\alpha-1}]$, $[y]\,[p^{\alpha-1}] = [p^{\alpha-1}]$, z čoho vyplýva $[x]\,[y]\,[p^{\alpha-1}] = [p^{\alpha-1}]$, teda $[x]\,[y] \in U$. Nech ďalej $[x] \in U$, $[x]^{-1} \in G(p^\alpha)$. Potom zo vzťahu $[x]\,[p^{\alpha-1}] = [p^{\alpha-1}]$ vyplýva $[p^{\alpha-1}] = [x]^{-1}\,[p^{\alpha-1}]$, teda $[x]^{-1} \in U$. Preto je U podgrupou grupy $G(p^\alpha)$.

Keď $[x] \in U$, potom pre číslo x, ktoré patrí do triedy $[x]$, vyplýva zo vzťahu $[x]\,[p^{\alpha-1}] = [p^{\alpha-1}]$ kongruencia $xp^{\alpha-1} \equiv p^{\alpha-1}$ (mod p^α), t. j. $x \equiv 1$ (mod p). Je teda $[x] \in U$ vtedy a len vtedy, keď $x = 1 + kp$, $k = 0, 1, \ldots, p^{\alpha-1} - 1$. Podgrupa U má $p^{\alpha-1}$ rôznych prvkov.

Grupa $G(p^\alpha)$ má však $p^{\alpha-1}(p-1)$ rôznych elementov a pre $p > 2$, $\alpha > 1$ je $1 < p^{\alpha-1} < p^{\alpha-1}(p-1)$. Je teda U netriviálnou podgrupou grupy $G(p^\alpha)$. Množina V je zrejme grupa.

2° Ukážeme, že každý element $[x] \in G(p^\alpha)$ možno napísať v tvare $[x] = [u]\,[v]$, kde $[u] \in U$, $[v] \in V$.

Nech je daný istý prvok $[x] \in G(p^\alpha)$. Zvoľme v grupe $G(p^\alpha)$ dva ďalšie prvky, a to $[u] = [x^{1-p^{\alpha-1}}]$, $[v] = [x^{p^{\alpha-1}}]$. Potom je skutočne $[x] = [u]\,[v]$.

Zo vzťahu $x \equiv x^p$ (mod p) vyplýva postupne $x \equiv x^p \equiv x^{p^2} \equiv \ldots \equiv x^{p^{\alpha-1}}$ (mod p), a keďže $G(p^\alpha)$ je grupa, $x^{1-p^{\alpha-1}} \equiv 1$ (mod p) čiže $u \equiv 1$ (mod p). Po násobení $p^{\alpha-1}$ máme $u\,p^{\alpha-1} \equiv p^{\alpha-1}$ (mod p^α), teda $[u]\,[p^{\alpha-1}] = [p^{\alpha-1}]$, čo znamená, že $[u] \in U$.

Ďalej platí $[v]^{p-1} = [x^{p^{\alpha-1}}]^{p-1} = [x]^{p^{\alpha-1}(p-1)} = [x]^{\varphi(p^\alpha)} = [1]$, takže $[v] \in V$ a tým je naše tvrdenie dokázané.

Z dokázaného súčasne vyplýva, že V je netriviálna podgrupa grupy $G(p^\alpha)$.

3° Nakoniec dokážeme, že $U \cap V = [1]$. Nech $[x] \in U \cap V$. Potom x spĺňuje súčasne dve podmienky:

$$x = 1 + kp, \qquad 0 \leqq k \leqq p^{\alpha-1} - 1, \tag{8}$$
$$x^{p-1} \equiv 1 \pmod{p^\alpha}. \tag{9}$$

Zo vzťahov (8) a (9) vyplýva

$$(1 + kp)^{p-1} \equiv 1 \pmod{p^\alpha},$$

t. j.

$$1 + \binom{p-1}{1} kp + \binom{p-1}{2} (kp)^2 + \ldots + (kp)^{p-1} \equiv 1 \pmod{p^\alpha}.$$

Z toho vzťahu vyplýva $(p-1)\,kp \equiv 0$ (mod p^2), teda $k \equiv 0$ (mod p). Preto $k = k'p$ a teda z (8) máme

$$x = 1 + k'p^2, \tag{10}$$

kde $k' \geqq 0$ je celé číslo. Dosadením do (9) dostávame

$$(1 + k'p^2)^{p-1} \equiv 1 \pmod{p^\alpha}$$

a z toho opäť

$$1 + \binom{p-1}{1} k'p^2 + \binom{p-1}{2} (k'p^2)^2 + \ldots + (k'p^2)^{p-1} \equiv 1 \pmod{p^\alpha},$$

teda

$(p-1)\,k'p^2 \equiv 0$ (mod p^3), t. j. $k' \equiv 0$ (mod p). Preto $k' = k''p$, kde $k'' \geqq 0$ je celé číslo a z (10) vyplýva

$$x = 1 + k''p^3.$$

Opakovaním tohoto postupu dostaneme $k = k'p = k''p^2 = \ldots = k^{(\alpha)}p^\alpha$, kde $k, k', \ldots, k^{(\alpha)}$ sú celé čísla $\geqq 0$. Pretože $0 \leqq k \leqq p^{\alpha-1} - 1$ platí $k = 0$. Teda $[1]$ je jediný element, ktorý leží v $U \cap V$.

Z platnosti tvrdení 2° a 3° vyplýva, že $G(p^\alpha)$ je direktným súčinom podgrúp U a V. Tým je veta 5 dokázaná.

Nakoniec sa budeme zaoberať otázkou reducibility grupy $G(2^\alpha)$, $\alpha > 1$, celé. Pretože $G(2^2)$ nemá netriviálne podgrupy a je teda direktne ireducibilná, budeme sa otázkou reducibility grupy $G(2^\alpha)$ zaoberať pre $\alpha > 2$ celé.

Veta 6. *Nech $\alpha > 2$ je celé číslo a nech $G(2^\alpha)$ je grupa tried zvyškov* (mod 2^α) *nesúdeliteľných s číslom 2^α. Potom množiny*

$$U = \{[x] \mid [x] \in G(2^\alpha),\ [x]\,[2^{\alpha-2}] = [2^{\alpha-2}]\},$$
$$V = \{[1], [2^\alpha - 1]\}$$

sú netriviálne podgrupy grupy $G(2^\alpha)$ rôzne od jednotkovej grupy a platí tento rozklad na direktný súčin:

$$G = U \, . \, V. \tag{11}$$

Dôkaz. 1° Predovšetkým, podobne ako v dôkaze vety 5 zo vzťahov $[x] \in U$, $[y] \in U$ vyplýva $[x]\,[y] \in U$ a zo vzťahov $[x] \in U$, $[x]^{-1} \in G(2^\alpha)$ vyplýva $[x]^{-1}\,[2^{\alpha-2}] = [2^{\alpha-2}]$, teda U je podgrupa grupy $G(2^\alpha)$.

Keď $[x] \in U$, potom pre číslo x, ktoré patrí do triedy $[x]$, platí $x\,2^{\alpha-2} \equiv 2^{\alpha-2} \pmod{2^\alpha}$, z čoho vyplýva $x \equiv 1 \pmod 4$. Poslednej kongruencii vyhovujú všetky čísla $x = 1 + 4k$, kde $k = 0, 1, 2, \ldots, 2^{\alpha-1} - 1$. Ľahko zistíme, že medzi týmito číslami je iba $2^{\alpha-2}$ navzájom rôznych reprezentantov tried grupy $G(2^\alpha)$ a teda i podgrupy U. Keď totiž $0 \leqq k$, $l \leqq 2^{\alpha-2} - 1$, vyplýva z kongruencie $1 + 4k \equiv 1 + 4l \pmod{2^\alpha}$ kongruencia $(k - l) \equiv 0 \pmod{2^{\alpha-2}}$, t. j. $k = l$, lebo $|k - l| \leqq 2^{\alpha-2} - 1$. Teda pre $k = 0, 1, \ldots, 2^{\alpha-2} - 1$, $x = 1 + 4k$ sú všetky prvky $[x]$ navzájom rôzne. Keď však $k = l + 2^{\alpha-2}$, kde $0 \leqq l \leqq 2^{\alpha-2} - 1$, je $1 + 4k = 1 + 4l + 2^\alpha$, t. j. $1 + 4k \equiv 1 + 4l \pmod{2^\alpha}$. Keď teda $x = 1 + 4k$, $k = 2^{\alpha-2}, 2^{\alpha-2} + 1, \ldots, 2^{\alpha-1} - 1$, je každý prvok $[x] \in U$ totožný s jedným prvkom pre $0 \leqq k \leqq 2^{\alpha-2} - 1$. Podgrupa U má práve $2^{\alpha-2}$ rôznych prvkov a je teda netriviálnou podgrupou grupy $G(2^\alpha)$, ktorá má $2^{\alpha-1}$ prvkov.

Ďalej je $[2^\alpha - 1]^2 = [2^\alpha(2^\alpha - 2) + 1] = [1]$. Množina V je teda tiež netriviálnou podgrupou grupy $G(2^\alpha)$.

2° Platnosť vzťahu $U \cap V = [1]$ je zrejmá z toho, že $[2^\alpha - 1]$ non $\in U$. Keby totiž platil opak, bolo by $[2^\alpha - 1]\,[2^{\alpha-2}] = [2^{\alpha-2}]$, t. j. bola by správna kongruencia $(2^\alpha - 1)\,2^{\alpha-2} \equiv 2^{\alpha-2} \pmod{2^\alpha}$, z ktorej vyplýva $2^{\alpha-1} \equiv 1 \pmod 2$, čo nie je pravda.

3° Pre dokončenie dôkazu stačí už iba ukázať, že každý prvok $x \in G(2^\alpha)$ možno písať v tvare $[x] = [u]\,[v]$, kde $[u] \in U$, $[v] \in V$. Nato stačí dokázať, že platí

$$G(2^\alpha) = U \, . \, [1] \cup U \, . \, [2^\alpha - 1],$$

kde na pravej strane je množinový súčet. Tento rozklad grupy $G(2^\alpha)$ na triedy podľa podgrupy U je iste správny, lebo — ako sme videli — prvok $[2^\alpha - 1] \in G(2^\alpha)$ nepatrí do podgrupy U a obe disjunktné triedy na pravej strane majú úhrnom $2^{\alpha-1}$ elementov.

Tým je veta 6 úplne dokázaná.

Príklad. Nájsť rozklad grupy $G(360)$ na direktný súčin v zmysle vety 4 a rozklad jednotlivých súčiniteľov v zmysle vety 5 a 6.

Riešenie. Grupa $G(360)$ je rádu $\varphi(360) = 96$. Maximálne idempotenty pologrupy $S(360)$ sú $e_1 = [136]$, $e_2 = [81]$ a $e_3 = [145]$. Prvkami grupy G_1 sú tie a len tie riešenia rovnice $[x]\,[136] = [136]$, ktoré sú prvkami grupy $G(360)$. Dostaneme ich tak, že z pologrupy T_1 vynecháme všetky prvky, ktorých reprezentanti sú čísla súdeliteľné s číslom 360. Takto dostaneme:

$$G_1 = \{[1], [91], [181], [271]\}$$

a analogicky:

$$G_2 = \{[1], [41], [121], [161], [241], [281]\},$$
$$G_3 = \{[1], [73], [217], [289]\}.$$

Hľadaný rozklad je:

$$G(360) = G_1 \, . \, G_2 \, . \, G_3 \, .$$

Nájdime teraz izomorfizmus $G_1 \cong G(2^3)$. Triedu prirodzených čísel (mod 8), do ktorej patrí číslo x, označme $\langle x \rangle$. Podľa lemmy 2 je

$$[1] \longleftrightarrow \langle 1 \rangle;\ [91] \longleftrightarrow \langle 91 \rangle = \langle 3 \rangle,\ [181] \longleftrightarrow \langle 181 \rangle = \langle 5 \rangle,\ [271] \longleftrightarrow \langle 271 \rangle = \langle 7 \rangle$$

a podľa vety 6 je

$$G_1 = U_1 \, . \, V_1,$$

kde

$$U_1 = \{[1], [181]\}, \qquad V_1 = \{[1], [271]\}.$$

Analogicky nájdeme izomorfizmus $G_2 \cong G(3^2)$ a podľa vety 5 zostrojíme množiny $U_2 = \{[1], [121], [241]\}$, $V_2 = \{[1], [161]\}$. Potom $G_2 = U_2 \, . \, V_2$.

O podgrupe $G_3 \cong G(5)$ veta 5 nič nehovorí, je však priamo zrejmé, že je direktne ireducibilná.

Úhrnom je

$$G(360) = \{[1], [181]\} \, . \, \{[1], [271]\} \, . \, \{[1], [121], [241]\} \, . \, \{[1], [161]\} \, . \, \{[1], [73], [217], [289]\}.$$

V našom prípade sú náhodou všetky faktory na pravej strane direktne nerozložiteľné.

LITERATÚRA

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

[2] Vandiver H. S.—Weawer M. W., Introduction to arithmetic factorization and congruences from the standpoint of abstract algebra, Amer. Math. Monthly 65 (1958), No. 8 (Part II), 1—53.

[3] Parker E. T., On multiplicative semigroups of residue classes, Proc. Amer. Math. Soc. 5 (1954), 612—616.

[4] Rédei L., *Algebra* I, Budapest 1954.

[5] Hasse H., *Lekciji po teoriji čisel* (preklad z nemčiny), Moskva 1953.

Došlo 1. októbra 1959.

Katedra matematiky Slovenskej vysokej školy technickej v Bratislave

О РАЗЛОЖЕНИИ ПОЛУГРУППЫ КЛАССОВ ВЫЧЕТОВ (mod m) В ПРЯМОЕ ПРОИЗВЕДЕНИЕ

БОГУМИР ПАРИЗЕК

Выводы

Пусть $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ разложение натурального числа $m > 1$ на простые множители и $S(m)$ полугруппа классов вычетов (mod m). Пусть $G(m)$ группа классов вычетов (mod m) взаимно простых с m. Класс натуральных чисел (mod m) содержащих число a обозначим $[a]$. Мы скажем, что идемпотент $e \neq [1]$ максимальный, если $ef = e \Rightarrow e = f$ для всякого идемпотента $f \neq [1]$.

В работе [1] показано, что $S(m)$ содержит r максимальных идемпотентов $e_1, e_2, \dots, e_r$ и что они обладают свойством $e_i = [p_i^{\alpha_i} a_i]$, где $[a_i] \in G(m)$, $(i = 1, 2, \dots, r)$.

В настоящей работе доказывается, что полугруппа $S(m)$ допускает разложение в прямое произведение r частичных полугрупп $S(m) = T_1 . T_2 \dots T_r$. Полугруппы $T_i (i = 1, 2, \dots, r)$ характеризуются соотношениями $T_i = \{[x] \mid [x] \in S(m), [x]\, e_i = e_i\}$ где e_i — максимальный идемпотент. В статье показано, что полугруппы T_i имеют вид $T_i = \left\{\left[p_i^{\alpha_i} a_i + k \frac{m}{p_i^{\alpha_i}}\right], k = 0, 1, 2, \dots, p_i^{\alpha_i} - 1\right\}$ и что они не допускают разложение в прямое произведение.

Во второй части работы аналогично построено разложение группы $G(m)$ в прямое произведение r подгрупп $G = G_1 . G_2 \dots G_r$. Подгруппы $G_i (i = 1, 2, \dots, r)$ характеризируются соотношениями $G_i = \{[x] \mid [x] \in G_m, [x]\, e_i = e_i\}$ где e_i, максимальной идемпотент. Подгруппы G_i выражаются в виде $G_i = \left\{\left[p_i^{\alpha_i} a_i + k \frac{m}{p_i^{\alpha_i}}\right], k = 0, 1, \dots, p_i^{\alpha_i} - 1, (k, p_i) = 1\right\}$.

В последней части показывается, что подгруппы G_i этого разложения изоморфны группам $G(p_i^{\alpha_i})$. Но может случиться, что эти группы допускают разложение в прямое произведение. Для $p_i > 2, \alpha_i > 1$ имеем $G(p_i^{\alpha_i}) = U_i V_i$, где $U_i = \{[x] \mid [x] \in G(p_i^{\alpha_i}), [x]\,[p_i^{\alpha_i - 1}] = [p_i^{\alpha_i - 1}]\}$, $V_i = \{[x] \mid [x] \in G(p_i^{\alpha_i}), [x]^{\alpha_i - 1} = [1]\}$. Для $p_i = 2, \alpha_i > 2$ имеем $G(p_i^{\alpha_i}) = U_i V_i$, где $U_i = \{[x] \mid [x] \in G(2^{\alpha_i}), [x]\,[2^{\alpha_i - 2}] = [2^{\alpha_i - 2}]\}$, $V_i = \{[1], [2^{\alpha_i} - 1]\}$. Поэтому тоже подгруппы $G_i (i = 1, 2, \dots, r)$ в показанных случаях допускают разложение в прямое произведение и факторы разложения изоморфны U_i и V_i.

ON THE DECOMPOSITION OF THE SEMIGROUP OF RESIDUE CLASSES (mod m) INTO A DIRECT PRODUCT

BOHUMÍR PARÍZEK

Summary

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ be the factorization of the integer $m > 1$ into different primes, $S(m)$ be the multiplicative semigroup of residue classes mod(m) and $G(m)$ be the group of classes relatively prime to m. The class containing the integer a will be denoted by $[a]$. An idempotent $e \in S(m)$, $e \neq [1]$ is called maximal, if $ef = e$ with an idempotent $f \neq [1]$ implies $e = f$. In the paper [1] we proved that $S(m)$ contains exactly r maximal idempotents $e_1, e_2, \dots, e_r$ and $e_i = [p_i^{\alpha_i} a_i]$ holds with a suitably chosen $[a_i] \in G(m)$, $(i = 1, 2, \dots, r)$.

In this paper we give first a decomposition of $S(m)$ into a direct product of subsemigroups: $S(m) = T_1 . T_2 \dots T_r$. The subsemigroup T_i is characterized by the property $T_i = \{[x] \mid [x] \in S(m), [x]\, e_i = e_i\}$ where e_i is a maximal idempotent of $S(m)$. It is shown that the subsemigroups T_i can be explicitly written in the form $T_i = \left\{\left[p_i^{\alpha_i} a_i + k \frac{m}{p_i^{\alpha_i}}\right], k = 0, 1, 2, \dots, p_i^{\alpha_i} - 1\right\}$ and that they are directly indecomposable.

In the second part of the paper we construct by an analogous method a decomposition of $G(m)$ into a direct produkt of subgroups: $G(m) = G_1 . G_2 \dots G_r$. The subgroups $G_i (i = 1, 2, \dots, r)$ are characterized by the property $G_i = \{[x] \mid [x] \in G(m), [x]\, e_i = e_i\}$ where e_i is a maximal idempotent. The explicit form of G_i is given by $G_i = \left\{\left[p_i^{\alpha_i} a_i + k \frac{m}{p_i^{\alpha_i}}\right], k = 0, 1, 2, \dots, p_i^{\alpha_i} - 1; (k, p_i) = 1\right\}$.

In the last section we show first that the subgroups G_i in this decomposition are isomorphic to the groups $G(p_i^{\alpha_i})$. These groups may be directly decomposable. For $p_i > 2$, $\alpha_i > 1$ we have $G(p_i^{\alpha_i}) = U_i . V_i$, where $U_i = \{[x] \mid [x] \in G(p_i^{\alpha_i}), [x]\,[p_i^{\alpha_i - 1}] = [p_i^{\alpha_i - 1}]\}$, $V_i = \{[x] \mid [x] \in G(p_i^{\alpha_i}), [x]^{p_i - 1} = [1]$. For $p_i = 2, \alpha_i > 2$ we have $G(p_i^{\alpha_i}) = U_i . V_i$ where $U_i = \{[x] \mid [x] \in G(2^{\alpha_i}), [x]\,[2^{\alpha_i - 2}] = [2^{\alpha_i - 2}]$, $V_i = \{[1], [2^{\alpha_i} - 1]\}$. Hence in these cases also the subgroups G_i are directly decomposable and the direct factors are isomorphic to the groups U_i and V_i.