O MULTIPLIKATÍVNEJ POLOGRUPE ZVYŠKOVÝCH TRIED (mod m)

BOHUMÍR PARÍZEK a ŠTEFAN SCHWARZ, Bratislava

Nech $m > 0$ je prirodzené číslo, S_m množina tried zvyškov (mod m). Ak pokladáme S_m za okruh s obvyklými operáciami sčítania a násobenia, je štruktúra S_m dobre známa a možno ju nájsť v mnohých učebniciach algebry. Nie je bez zaujímavosti vyšetrovať množinu S_m, ak potlačíme operáciu sčítania a vyšetrujeme iba multiplikatívne vlastnosti jej elementov.

Úlohou tejto práce je vyšetriť štruktúru multiplikatívnej pologrupy S_m metódami teórie pologrúp.

Takto postavená otázka je zaujímavá i z hľadiska elementárnej teórie čísel. Je všeobecne známe, že sa v číselnej teórii zapodievame takmer výhradne vlastnosťami grupy G_1 tried zvyškov (mod m) nesúdeliteľných s m. Rovnako je známe, že existujú niektoré dôležité vety z teórie čísel, ktoré možno odvodiť čisto metódami teórie grúp. Pologrupa S_m obsahuje však vo všeobecnosti oveľa viac navzájom disjunktných podgrúp. Význam týchto podgrúp pre problémy číselnej teórie zdá sa dosiaľ nedostatočne osvetlený. To je jedna z príčin, pre ktorú sa budeme nastolenou otázkou v ďalšom podrobne zapodievať.

1

Pre pohodlie čitateľa pripomenieme v tomto úvodnom odseku niektoré fakty z teórie konečných pologrúp, ktoré platia celkom všeobecne, nezávisle od špeciálneho charakteru pologrupy S_m. Dôkazy týchto viet nájde čitateľ v práci [1].

Nech S je konečná (nie nevyhnutne komutatívna) pologrupa. Nech $a \in S$. Postupnosť

$$a,\ a^2,\ a^3 \ldots \tag{1}$$

má iba konečný počet rôznych elementov. Je známe, že keď ϱ, σ, $\varrho < \sigma$ sú najmenšie prirodzené čísla, pre ktoré platí $a^\varrho = a^\sigma$, potom (1) obsahuje presne $\sigma - 1$ rôznych elementov, a to:

$$a,\ \ldots,\ a^{\varrho-1} \mid a^\varrho,\ \ldots,\ a^{\sigma-1}.$$

Množina $\mathfrak{G}_a = \{a^\varrho, \ldots, a^{\sigma-1}\}$ je cyklická grupa. Ak $\tau \geqq \sigma$, je $a^\tau \in \mathfrak{G}_a$.

Množina (1) má jediný idempotent e, a to jednotkový element grupy $\mathfrak{G}_a$. Budeme hovoriť, že a patrí k idempotentu e.

Nech P_e je množina všetkých elementov pologrupy S, ktoré patria k pevne zvolenému idempotentu e. Pretože každý prvok pologrupy S patrí iba k jedinému idempotentu e, možno písať S ako súčet disjunktných množín $S = \sum_e P_e$, kde e prebieha všetky idempotenty pologrupy S. Množina P_e nemusí byť pologrupa. Ak však S je komutatívna pologrupa, je i P_e pologrupa. V tomto prípade budeme P_e nazývať maximálnou pologrupou, ktorá patrí k idempotentu e.

Ku každému idempotentu e existuje okrem toho jedna a len jedna maximálna grupa G_e, ktorá má e za jednotkový element. Je zrejmé, že $G_e \subseteq P_e$. Maximálne gruppy patriace k rôznym idempotentom sú teda navzájom disjunktné. Grupa G_e je množina tých elementov $x \in P_e$, pre ktoré platí $ex = xe = x$. Preto $P_e e = eP_e = G_e$.

Nakoniec poznamenajme: Keď S má jednotkový prvok e_1, platí $P_{e_1}e_1 = P_{e_1} = G_{e_1}$, t. j. maximálna pologrupa, ktorá patrí k jednotkovému prvku, je grupa.

Uvedené fakty budeme v ďalšom bežne používať. Ostatné pomocné vety, ktoré budeme potrebovať, si odvodíme.

2

V tomto odseku si odvodíme dve vety, ktoré majú všeobecný charakter. Pritom nebudeme ani predpokladať, že pologrupa, o ktorej uvažujeme, je konečná.

Lemma 1. *Nech S je pologrupa, ktorá má jednotkový element e_1, a nech G je grupa, ktorá leží v S a obsahuje e_1. Nech x, y sú dva ľubovoľné prvky pologrupy S. Množiny xG a yG sú alebo disjunktné, alebo totožné. Pologrupu S možno teda písať ako súčet disjunktných množín v tvare*

$$S = \bigcup_i x_i G, \tag{2}$$

kde x_i sú vhodne zvolené elementy pologrupy S.

Poznámka. Rozklad (2), ktorý je okrem poradia sčítancov zrejme jednoznačný, budeme nazývať rozkladom pologrupy S modulo G. Množiny x_iG budeme nazývať triedami modulo G.

Dôkaz. Pretože pre každý prvok $z \in S$ platí $z = ze_1 \in zG$, je každý element $z \in S$ v nejakej triede. Množina všetkých tried mod G pokrýva celé S.

Predpokladajme, že pre dva elementy x, $y \in S$ platí $xG \cap yG \neq \emptyset$. Potom existujú také prvky a, $b \in G$, že $xa = yb$. Nájdime v grupe G element a^{-1}, pre ktorý platí $aa^{-1} = e_1$. Potom $xaa^{-1} = yba^{-1}$, $x = yba^{-1}$. Pretože ba^{-1} je prvok grupy G, máme

$$xG = yba^{-1}G = y(ba^{-1}G) = yG.$$

Triedy xG a yG sú totožné, č. b. t. d.

Poznámka. Lemma 1 je v podstate známa; implicitne ju obsahuje práca [2].

Lemma 2. *Nech sú splnené predpoklady lemmy 1 a nech S je komutatívna pologrupa. Trieda xG, ktorá obsahuje idempotent, je grupa.*

Dôkaz. Z dôkazu lemmy 1 vyplýva, že triedu, ktorá obsahuje idempotent e, možno písať v tvare eG. Keď máme dokázať, že eG je grupa, stačí dokázať, že ku každým dvom prvkom ea, eb, kde $a, b \in G$, existuje taký prvok $\xi \in eG$, že platí $ea\xi = eb$. Nájdime v grupe G taký element c, že $ac = b$. To je možné. Položme $\xi = ec \in eG$. Potom je skutočne $ea\xi = eaec = eac = eb$, č. b. t. d.

Poznámka. Pojem maximálnej grupy, ktorá patrí k danému idempotentu, možno definovať v každej pologrupe. Poznamenajme tu výslovne, že grupa eG z lemmy 2 nemusí byť vo všeobecnosti maximálnou grupou, ktorá patrí k e, a to ani vtedy, keď G je maximálna grupa patriaca k e_1.

3

Odteraz až do konca tejto práce budeme používať toto označenie: Číslo m je prirodzené číslo väčšie ako 1. Jeho rozklad na kladné prvočinitele je $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $\alpha_1 \geqq 1$, $\alpha_2 \geqq 1, \dots, \alpha_r \geqq 1$.

S_m značí multiplikatívnu pologrupu tried zvyškov (mod m). Triedu (mod m), do ktorej patrí číslo a, budeme označovať znakom $[a]$. Keď $a \equiv b \pmod m$, platí $[a] = [b]$. Zrejme platí $[a]\,[b] = [ab]$. Element $[1]$ je jednotkovým prvkom pologrupy S_m.

Grupu tried zvyškov (mod m) nesúdeliteľných s číslom m, označíme znakom G_1. Je známe, že táto grupa má $\varphi(m)$ elementov, kde φ je Eulerova funkcia. Prvkami grupy G_1 sú teda tie a len tie elementy $[a]$, pre ktoré platí $(a, m) = 1$. Grupa G_1 je zrejme maximálna grupa, ktorá patrí k elementu $[1]$.

Poznamenajme ešte, že každý prvok $[x] \in S_m$ možno písať v tvare $[x] = [p_1^{l_1} p_2^{l_2} \dots p_r^{l_r} a]$, kde $l_1 \geqq 0, \dots, l_r \geqq 0$ a $[a]$ je vhodne zvolený prvok grupy G_1.

Našou prvou úlohou je študovať rozklad pologrupy S_m modulo G_1 vo zmysle odseku 2.

Lemma 3. *Nech $c = p_1^{l_1} p_2^{l_2} \dots p_r^{l_r} a$, $(a, m) = 1$. Označme $\gamma_i = \min(\alpha_i, l_i)$. Potom $[c]$ patrí do triedy*

$$[p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r}] G_1.$$

Dôkaz. Ak pre všetky $i = 1, 2, \dots, r$ je $l_i \leqq \alpha_i$, patrí $[c]$ do triedy $[p_1^{l_1} p_2^{l_2} \dots p_r^{l_r}] G_1$ a nemáme čo dokazovať.

Ak pre všetky $i = 1, 2, \dots, r$ je $l_i \geqq \alpha_i$, platí $[c] = [0]$, a teda

$$[c] \in [p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}] G_1 = [0].$$

Preto stačí, keď sa budeme zapodievať iba tým prípadom, že aspoň pre jeden index j platí $l_j > \alpha_j$. Bez ujmy na všeobecnosti predpokladajme, že platí

$$l_1 > \alpha_1, \dots, l_s > \alpha_s, l_{s+1} = \alpha_{s+1}, \dots, l_t = \alpha_t, l_{t+1} < \alpha_{t+1}, \dots, l_r < \alpha_r,$$

kde $1 \leqq s < t \leqq r$. Takéto usporiadanie možno vždy dosiahnuť vhodnou zámenou poradia prvočísel p_i. Napíšme číslo c v tvare

$$c = p_1^{\alpha_1} \dots p_s^{\alpha_s} p_{s+1}^{l_{s+1}} \dots p_t^{l_t} p_{t+1}^{l_{t+1}} \dots p_r^{l_r} (p_1^{l_1 - \alpha_1} \dots p_s^{l_s - \alpha_s}) a.$$

Zrejme platí

$$[c] = [p_1^{\alpha_1} \dots p_s^{\alpha_s} p_{s+1}^{l_{s+1}} \dots p_t^{l_t} p_{t+1}^{l_{t+1}} \dots p_r^{l_r} (p_1^{l_1 - \alpha_1} \dots p_s^{l_s - \alpha_s} + p_{s+1}^{\alpha_{s+1}} \dots p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1} - l_{t+1}} \dots p_r^{\alpha_r - l_r}) a],$$

lebo v hranatej zátvorke na pravej strane sme pričítali celistvý násobok čísla m. Označme

$$b = p_1^{l_1 - \alpha_1} \dots p_s^{l_s - \alpha_s} + p_{s+1}^{\alpha_{s+1}} \dots p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1} - l_{t+1}} \dots p_r^{\alpha_r - l_r}.$$

Pretože b nie je deliteľné žiadnym z prvočísel $p_1, p_2, \dots, p_r$, platí $(b, m) = 1$. Preto je $[b] \in G_1$ a platí

$$[c]\, G_1 = [p_1^{\alpha_1} \dots p_s^{\alpha_s} p_{s+1}^{l_{s+1}} \dots p_t^{l_t} p_{t+1}^{l_{t+1}} \dots p_r^{l_r} ba]\, G_1 = [p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r}]\, [ab]\, G_1 = [p_1^{\gamma_1} \dots p_r^{\gamma_r}] G_1,$$

t. j. $[c] \in [p_1^{\gamma_1} \dots p_r^{\gamma_r}] G_1$, č. b. t. d.

Veta 1. *Rozklad pologrupy S_m modulo G_1 má $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$ tried. Každú takúto triedu možno písať v tvare*

$$[p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}] G_1, \tag{3}$$

kde $0 \leqq k_i \leqq \alpha_i (i = 1, 2, \dots, r)$ a všetky napísané triedy modulo G_1 sú navzájom disjunktné.

Dôkaz. Podľa lemmy 3 patrí každý prvok $[c] \in S_m$ do niektorej z tried (3). Čísel tvaru $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ s podmienkou $0 \leqq k_i \leqq \alpha_i$ je zrejme $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$. Treba ešte dokázať, že všetky triedy tvaru (3) sú navzájom rôzne, alebo — čo je podľa lemmy 1 to isté — že sú navzájom disjunktné.

Predpokladajme, že platí

$$[p_1^{k_1} \dots p_r^{k_r}] G_1 \cap [p_1^{l_1} \dots p_r^{l_r}] G_1 \neq \emptyset \quad (0 \leqq k_i \leqq \alpha_i, 0 \leqq l_i \leqq \alpha_i),$$

pričom aspoň pre jeden index j platí $k_j \neq l_j$. Nech teda pre určité j platí $0 \leqq k_j < l_j \leqq \alpha_j$. Z nášho predpokladu vyplýva, že existujú také prvky $[a]$, $[b] \in G_1$, že platí

$$p_1^{k_1} \dots p_r^{k_r} a \equiv p_1^{l_1} \dots p_r^{l_r} b \pmod m.$$

Vezmime túto kongruenciu $(\mathrm{mod}\ p_j^{\alpha_j})$ a deľme ju číslom $p_j^{k_j}$. Máme:

$$p_1^{k_1} \dots p_{j-1}^{k_{j-1}} p_{j+1}^{k_{j+1}} \dots p_r^{k_r} a \equiv$$
$$\equiv p_1^{l_1} \dots p_{j-1}^{l_{j-1}} p_j^{l_j - k_j} p_{j+1}^{l_{j+1}} \dots p_r^{l_r} b \,(\mathrm{mod}\ p_j^{\alpha_j - k_j}).$$

Pretože $\alpha_j - k_j \geqq 1$ a $l_j - k_j \geqq 1$, je takýto vzťah nemožný, lebo ľavá strana nie je deliteľná číslom p_j. Máme spor a veta je dokázaná.

Veta 2. *Trieda* $[p_1^{k_1} \dots p_r^{k_r}] G_1$, $0 \leqq k_i \leqq \alpha_i$ $(i = 1, 2, \dots, r)$ má

$$\varphi(p_1^{\alpha_1 - k_1} p_2^{\alpha_2 - k_2} \dots p_r^{\alpha_r - k_r})$$

rôznych elementov.

Dôkaz. Dva prvky

$$[p_1^{k_1} \dots p_r^{k_r} a], [p_1^{k_1} \dots p_r^{k_r} b], [a], [b] \in G_1,$$

sú totožné vtedy a len vtedy, keď

$$p_1^{k_1} \dots p_r^{k_r} a \equiv p_1^{k_1} \dots p_r^{k_r} b \,(\mathrm{mod}\ m),$$

t. j. keď

$$a \equiv b \,(\mathrm{mod}\ p_1^{\alpha_1 - k_1} p_2^{\alpha_2 - k_2} \dots p_r^{\alpha_r - k_r}). \tag{4}$$

Nech $[a]$ je ľubovoľný (pevne zvolený) prvok grupy G_1, pre ktorý platí $0 < a < p_1^{\alpha_1 - k_1} \dots p_r^{\alpha_r - k_r}$. Označme $n = p_1^{k_1} \dots p_r^{k_r}$. Každý z prvkov

$$[a + l p_1^{\alpha_1 - k_1} \dots p_r^{\alpha_r - k_r}],\ l = 0, 1, \dots, (n-1), \tag{5}$$

násobený $[p_1^{k_1} \dots p_r^{k_r}]$, dáva ten istý element $[p_1^{k_1} \dots p_r^{k_r} a] \in S_m$. Ak z týchto n elementov patrí $\tau = \tau(a)$ elementov do G_1, existuje presne τ elementov grupy G_1, ktoré, násobené prvkom $[p_1^{k_1} \dots p_r^{k_r}]$, dávajú element $[p_1^{k_1} \dots p_r^{k_r} a]$. (Vzhľadom na vzťah (4) je zrejmé, že žiadne iné elementy grupy G_1 nemôžu mať túto vlastnosť.)

V ďalšom uvidíme, že číslo τ nezávisí od a, t. j. že je pre každé zvolené a rovnaké. Z toho ihneď vyplýva, že trieda $[p_1^{k_1} \dots p_r^{k_r}] G_1$ má presne $\frac{\varphi(m)}{\tau}$ rôznych elementov.

Pre jednoduchosť rozoznávajme v ďalšom dva prípady:

a) Nech $k_1 < \alpha_1$, $k_2 < \alpha_2$, $\dots$, $k_r < \alpha_r$. Potom každý z n prvkov (5) padne do G_1, a to nezávisle od a. Táto skutočnosť vyplýva z toho, že číslo a je nesúdeliteľné číslom m, zatiaľ čo druhý sčítanec $l p_1^{\alpha_1 - k_1} \dots p_r^{\alpha_r - k_r}$ je deliteľný každým z prvočísel $p_1, p_2, \dots, p_r$. Trieda $[p_1^{k_1} \dots p_r^{k_r}] G_1$ má teda

$$\frac{\varphi(m)}{n} = \frac{\varphi(p_1^{\alpha_1} \dots p_r^{\alpha_r})}{p_1^{k_1} \dots p_r^{k_r}} = \varphi(p_1^{\alpha_1 - k_1} \dots p_r^{\alpha_r - k_r})$$

rôznych elementov.

b) V druhom prípade môžeme bez ujmy na všeobecnosti predpokladať, že platí

$$k_1 = \alpha_1, \dots, k_t = \alpha_t, k_{t+1} < \alpha_{t+1}, \dots, k_r < \alpha_r,$$

kde $t \geqq 1$. V tomto prípade treba úvahu trocha modifikovať.

Žiadne z čísel

$$a + l p_{t+1}^{\alpha_{t+1} - k_{t+1}} \dots p_r^{\alpha_r - k_r},\ l = 0, 1, \dots, (n-1) \tag{6}$$

nie je deliteľné prvočíslami $p_{t+1}, \dots, p_r$. Ak chceme zistiť, koľko elementov (5) patrí do G_1, stačí určiť, koľko z čísel (6) nie je deliteľných žiadnym z prvočísel $p_1, p_2, \dots, p_t$.

Zistíme, koľko z čísel (6) je deliteľných prvočíslom p_1, t. j. koľko je tých l, $0 < l < n$, pre ktoré platí

$$a + l p_{t+1}^{\alpha_{t+1} - k_{t+1}} \dots p_r^{\alpha_r - k_r} \equiv 0 \,(\mathrm{mod}\ p_1).$$

Táto kongruencia má jediné riešenie l_1, pre ktoré platí $0 < l_1 < p_1$. Medzi číslami (6) je teda presne $\frac{n}{p_1}$ čísel deliteľných p_1. Podobne je medzi nimi $\frac{n}{p_2}$ čísel deliteľných číslom p_2 atď. a konečne $\frac{n}{p_t}$ čísel deliteľných číslom p_t.

Obvyklý postup ukazuje, že rôznych čísel množiny (6), nesúdeliteľných číslom $p_1^{k_1} \dots p_t^{k_t} = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, je

$$n - \sum_{i=1}^{t} \frac{n}{p_i} + \sum_{\substack{i,k=1 \\ i \neq k}}^{t} \frac{n}{p_i p_k} - \dots = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right) =$$
$$= \varphi(p_1^{\alpha_1} \dots p_t^{\alpha_t}) p_{t+1}^{k_{t+1}} \dots p_r^{k_r}.$$

Toto číslo nezávisí od a. Počet rôznych elementov triedy $[p_1^{k_1} \dots p_r^{k_r}] G_1$ rovná sa teda číslu

$$\frac{\varphi(m)}{\varphi(p_1^{\alpha_1} \dots p_t^{\alpha_t}) p_{t+1}^{k_{t+1}} \dots p_r^{k_r}} = \varphi(p_{t+1}^{\alpha_{t+1} - k_{t+1}} \dots p_r^{\alpha_r - k_r}) =$$
$$= \varphi(p_1^{\alpha_1 - k_1} \dots p_r^{\alpha_r - k_r}).$$

Tým je veta 2 dokázaná.

4

V tomto odseku si všimneme idempotenty pologrupy S_m.

Veta 3. *Trieda* $[p_1^{k_1} \dots p_r^{k_r}] G_1$ *obsahuje idempotent vtedy a len vtedy, ak pre každé* $i = 1, 2, \dots, r$ *je alebo* $k_i = 0$, *alebo* $k_i = \alpha_i$. *Každá takáto trieda obsahuje jeden a len jeden idempotent.*

Dôkaz.

a) Ak má trieda $[p_1^{k_1} \dots p_r^{k_r}]G_1$ obsahovať idempotent, musí existovať také $[a] \in G_1$, že

$$(p_1^{k_1} \dots p_r^{k_r}a)^2 \equiv p_1^{k_1} \dots p_r^{k_r}a \pmod m,$$

t. j.

$$p_1^{k_1} \dots p_r^{k_r}a \equiv 1 \pmod{p_1^{\alpha_1-k_1} \dots p_r^{\alpha_r-k_r}}.$$

Nech pre nejaké i je $\alpha_i - k_i > 0$. Potom z kongruencie

$$p_1^{k_1} \dots p_i^{k_i} \dots p_r^{k_r}a \equiv 1 \pmod{p_i^{\alpha_i-k_i}}$$

vyplýva, že nemôže byť $k_i > 0$, lebo by sme mali $0 \equiv 1 \pmod{p_i}$, a to nie je pravda. Ak teda $\alpha_i - k_i > 0$, je nevyhnutne $k_i = 0$. Tým je nevyhnutnosť podmienky vo vete 3 dokázaná.

b) Dokážeme, že podmienka je i postačujúca. Ak pre všetky $i = 1, 2, \dots, r$ platí $k_i = \alpha_i$, je naše tvrdenie zrejmé, lebo potom trieda pozostáva z jediného elementu [0]. Ak pre všetky $i = 1, 2, \dots, r$ platí $k_i = 0$, je trieda totožná s grupou G_1 a táto grupa obsahuje idempotent [1]. Bez ujmy na všeobecnosti môžeme teda predpokladať, že existuje také t, $1 \leqq t < r$, že $k_1 = \alpha_1, \dots, k_t = \alpha_t$, $k_{t+1} = \dots = k_r = 0$. Takéto poradie môžeme vždy dosiahnuť vhodnou zámenou indexov prvočísel p_i. Dokážeme, že trieda $[p_1^{\alpha_1} \dots p_t^{\alpha_t}]G_1$ obsahuje idempotent.

Nájdime také a_1, pre ktoré platí

$$p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1 \equiv 1 \pmod{p_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r}}.$$

Také a_1 existuje. Potom platí $p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1 = 1 + lp_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r}$, kde l je celé číslo. Pre číslo $p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1$ platí:

$$(p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1)^2 = p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1 =$$
$$= p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1(1 + lp_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r}) \equiv p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1 \pmod m.$$

Element $[p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1] \in [p_1^{k_1} \dots p_r^{k_r}]G_1$ je teda idempotent, č. b. t. d.

c) Dokážme nakoniec, že trieda $[p_1^{\alpha_1} \dots p_t^{\alpha_t}]G_1$ má jediný idempotent. Keď $[p_1^{\alpha_1} \dots p_t^{\alpha_t}a]$ je idempotent, platí podľa odseku a):

$$p_1^{\alpha_1} \dots p_t^{\alpha_t}a \equiv 1 \pmod{p_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r}}.$$

Všetky riešenia tejto kongruencie sú $a = a_1 + lp_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r}$, kde l je celé číslo. Ale

$$[p_1^{\alpha_1} \dots p_t^{\alpha_t}a] = [p_1^{\alpha_1} \dots p_t^{\alpha_t}(a_1 + lp_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r})] = [p_1^{\alpha_1} \dots p_t^{\alpha_t}a_1].$$

Tým je veta 3 úplne dokázaná. Jej priamym dôsledkom je:

Veta 4. *Pologrupa S_m obsahuje 2^r idempotentov. Každý idempotent $e \neq [1]$ možno písať v tvare $e = [p_{i_1}^{\alpha_{i_1}} \dots p_{i_s}^{\alpha_{i_s}}a]$, kde $\{i_1, i_2, \dots, i_s\}$ je pevne zvolená podmnožina množiny indexov $\{1, 2, \dots, r\}$ a kde $[a]$ je vhodne zvolený element grupy G_1.*

Poznámka. Skutočnosť, že S_m má 2^r idempotentov vyplýva, pravda, celkom elementárne z toho, že kongruencia $x^2 \equiv x \pmod m$ má $2^r \pmod m$ inkongruentných riešení. Naše odvodenie má tú výhodu, že nás informuje i o tvare idempotentov. Idempotenty pologrupy S_m sú obsiahnuté v týchto triedach modulo G_1:

$$[1]G_1,$$
$$[p_1^{\alpha_1}]G_1, [p_2^{\alpha_2}]G_1, \dots, [p_r^{\alpha_r}]G_1,$$
$$[p_1^{\alpha_1}p_2^{\alpha_2}]G_1, [p_1^{\alpha_1}p_3^{\alpha_3}]G_1, \dots, [p_{r-1}^{\alpha_{r-1}}p_r^{\alpha_r}]G_1,$$
$$[p_1^{\alpha_1} \dots p_r^{\alpha_r}]G_1 = [0].$$

Do množiny všetkých idempotentov každej komutatívnej pologrupy možno zaviesť čiastočné usporiadanie, ktoré je niekedy užitočné.

Definícia. *Nech S je komutatívna pologrupa, e_i, e_k dva idempotenty pologrupy S. Budeme písať $e_i \leqq e_k$ vtedy a len vtedy, ak $e_ie_k = e_i$.*

Relácia $\leqq$ definuje čiastočné usporiadanie množiny všetkých idempotentov pologrupy S. Ak e', e'' sú dva ľubovoľné idempotenty pologrupy S, platí $e'e'' \leqq e'$, $e'e'' \leqq e''$.

Zaveďme reláciu $\leqq$ do množiny E všetkých idempotentov pologrupy S_m. Nech e', e'' sú dva idempotenty pologrupy S_m. Podľa vety 3 možno písať:

$$e' = [p_1^{l_1}p_2^{l_2} \dots p_r^{l_r}a], \text{ kde } [a] \in G_1, l_i = 0 \text{ alebo } l_i = \alpha_i \ (i = 1,2, \dots, r),$$
$$e'' = [p_1^{k_1}p_2^{k_2} \dots p_r^{k_r}b], \text{ kde } [b] \in G_1, k_i = 0 \text{ alebo } k_i = \alpha_i \ (i = 1, 2 \dots, r).$$

Pre súčin $e'e''$ dostávame

$$e'e'' = [p_1^{l_1+k_1}p_2^{l_2+k_2} \dots p_r^{l_r+k_r}ab] \in [p_1^{l_1+k_1} \dots p_r^{l_r+k_r}]G_1.$$

Podľa lemmy 3 je $e'e'' \in [p_1^{\gamma_1}p_2^{\gamma_2} \dots p_r^{\gamma_r}]G_1$, kde $\gamma_i = \min(\alpha_i, k_i + l_i)$. Keďže l_i, k_i nadobúdajú len hodnotu 0 alebo α_i, platí $\min(\alpha_i, k_i + l_i) = \max(k_i, l_i)$. Teda

$$e'e'' = [p_1^{\max(l_1,k_1)} \dots p_r^{\max(l_r,k_r)}c], \text{ kde } [c] \in G_1.$$

Z toho vyplýva: Relácia $e' = [p_1^{l_1}p_2^{l_2} \dots p_r^{l_r}a] \leqq e'' = [p_1^{k_1}p_2^{k_2} \dots p_r^{k_r}b]$ platí vtedy a len vtedy, keď pre každé $i = 1, 2, \dots, r$ platí $k_i \leqq l_i$.

Definujme na množine E dve operácie $\wedge$ a $\vee$ tak, že elementom e', e'' priradíme elementy $e' \wedge e''$, $e' \vee e''$ podľa tohto predpisu:

$$e' \wedge e'' = e'e'' = [p_1^{\max(l_1,k_1)} \dots p_r^{\max(l_r,k_r)}c], [c] \in G_1,$$
$$e' \vee e'' = [p_1^{\min(l_1,k_1)} \dots p_r^{\min(l_r,k_r)}d], [d] \in G_1.$$

Je zrejmé, že $e' \wedge e''$ je najväčší element $\leqq$ ako e' a e'' a $e' \vee e''$ je najmenší element $\geqq$ ako e' a e''. Množina E tvorí teda vzhľadom na reláciu $\leqq$ sväz, ktorý je — ako bezprostredne vidno — dokonca Boolovou algebrou. V tejto algebre komplementom k elementu $[p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$ je element $[p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r} b]$ s vhodne volenými a jednoznačne určenými $[a], [b] \in G_1$. Tým sme dokázali nasledujúcu vetu:

Veta 5. *Vzhľadom na zavedené čiastočné usporiadanie tvorí množina všetkých idempotentov pologrupy S_m Boolovu algebru.*

Definícia. *Idempotent $e \neq [0]$ nazývame primitívnym, ak zo vzťahu $ef = f$, $f \neq [0]$, kde f je idempotent, vyplýva $e = f$. Idempotent $e \neq [1]$ nazývame maximálnym, ak zo vzťahu $ef = e$, $f \neq [1]$, kde f je idempotent, vyplýva $f = e$.*

Z predošlých vývodov je zrejmá táto veta:

Veta 6. *Pologrupa S_m má presne r primitívnych idempotentov. Sú to všetky idempotenty tvaru $[p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_r^{\alpha_r} a_i]$, $(i = 1, 2, \dots, r)$, kde $[a_i] \in G_1$. S_m má r maximálnych idempotentov. Sú to všetky idempotenty tvaru $[p_i^{\alpha_i} a_i]$, $a_i \in G_i$, pre $i = 1, 2, \dots, r$.*

5

V tomto odseku budeme sa zapodievať maximálnou pologrupou a maximálnou grupou, ktorá patrí k danému idempotentu $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$, $[a] \in G_1$, $1 \leqq s \leqq r$. Ak $e \neq [1]$, môžeme vhodnou zámenou indexov prvočísel v každom prípade docieliť, že e má takýto tvar.

Ktoré elementy pologrupy S_m patria k idempotentu e?

Nech $[x] = [p_1^{l_1} p_2^{l_2} \dots p_r^{l_r} b]$, $[b] \in G_1$ je ľubovoľný element pologrupy S_m. Tento element patrí k e vtedy a len vtedy, keď existuje také celé číslo $\varrho \geqq 1$, že $[x]^\varrho = e$, t. j. keď

$$(p_1^{l_1} \dots p_r^{l_r} b)^\varrho \equiv p_1^{\alpha_1} \dots p_s^{\alpha_s} a (\mathrm{mod}\ m).$$

Keby pre $i = s+1, s+2, \dots, r$ bolo $l_i > 0$, vyplývalo by z tohto vzťahu $0 \equiv p_1^{\alpha_1} \dots p_s^{\alpha_s} a (\mathrm{mod}\ p_i)$, čo nie je pravda. Preto keď $s < r$, je nevyhnutne $l_{s+1} = l_{s+2} = \dots = l_r = 0$.

Uvažujme teraz o ľubovoľnom prvku $[y] = [p_1^{l_1} \dots p_s^{l_s} b]$, $[b] \in G_1$, kde $l_1 > 0, \dots, l_s > 0$. Označme $\alpha = \alpha_1 \alpha_2 \dots \alpha_s$. Prvok $[y]^\alpha = [p_1^{\alpha l_1} \dots p_s^{\alpha l_s} b^\alpha]$ patrí podľa lemmy 3 do triedy $[p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}] G_1$. Podľa vety 3 je táto trieda grupou, ktorá má jednotkový prvok e. Existuje teda také číslo β, že $[y]^{\alpha\beta} = e$, t. j. $[y]$ patrí k idempotentu e.

Tým sme dokázali túto vetu:

Veta 7. *Maximálna pologrupa P_e, ktorá patrí k idempotentu $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$, $[a] \in G_1$, je množinovým súčtom všetkých tried tvaru*

$$[p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}] G_1,$$

kde $1 \leqq l_1 \leqq \alpha_1, \dots, 1 \leqq l_s \leqq \alpha_s$. P_e je teda súčtom $\alpha_1 \alpha_2 \dots \alpha_s$ tried modulo G_1.

Podľa vety 2 počet rôznych elementov triedy $[p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}] G_1$ rovná sa číslu

$$\varphi(p_1^{\alpha_1 - l_1} \dots p_s^{\alpha_s - l_s} p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1 - l_1} \dots p_s^{\alpha_s - l_s})\, \varphi(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}).$$

Počet elementov pologrupy P_e je teda

$$\sum_{l_1, \dots, l_s} \varphi(p_1^{\alpha_1 - l_1} \dots p_s^{\alpha_s - l_s})\, \varphi(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}),$$

kde $l_1, l_2, \dots, l_s$ prebiehajú nezávisle od seba čísla, ktoré vyhovujú nerovnostiam $1 \leqq l_1 \leqq \alpha_1, \dots, 1 \leqq l_s \leqq \alpha_s$. Tento výraz možno zrejme napísať v tvare

$$\varphi(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}) \prod_{i=1}^{s} [\varphi(1) + \varphi(p_i) + \dots + \varphi(p_i^{\alpha_i - 1})] =$$
$$= p_1^{\alpha_1 - 1} \dots p_s^{\alpha_s - 1} \varphi(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}).$$

Tým sme dokázali vetu 8:

Veta 8. *Maximálna pologrupa P_e, ktorá patrí k idempotentu $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$, $[a] \in G_1$ má $p_1^{\alpha_1 - 1} \dots p_s^{\alpha_s - 1} \varphi(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r})$ rôznych prvkov.*

Dôsledok. *Pologrupa S_m má $p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_s^{\alpha_s - 1}$ nilpotentných prvkov.*

Pýtajme sa, koľko elementov má maximálna grupa G_e, ktorá patrí k idempotentu $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$, $[a] \in G_1$, $1 \leqq s \leqq r$.

V lemme 2 sme dokázali, že trieda, ktorá obsahuje idempotent e, t. j. trieda eG_1 je grupa. Ukážeme najprv, že táto grupa je totožná s maximálnou grupou, ktorá patrí k idempotentu e. Keďže grupa eG_1 má jednotkový element e, je nevyhnutne $eG_1 \leqq G_e$. Stačí teda dokázať, že $G_e \leqq eG_1$.

Nech $[x]$ je ľubovoľný element grupy G_e. Pretože $[x] \in P_e$, platí $[x] = [p_1^{l_1} \dots p_s^{l_s} b]$, $l_1 > 0, \dots, l_s > 0$, $[b] \in G_1$. Tento element patrí do G_e vtedy a len vtedy, keď $[x]\, e = [x]$, t. j. keď platí:

$$p_1^{l_1} \dots p_s^{l_s} b p_1^{\alpha_1} \dots p_s^{\alpha_s} a \equiv p_1^{l_1} \dots p_s^{l_s} b (\mathrm{mod}\ m),$$
$$p_1^{\alpha_1} \dots p_s^{\alpha_s} a \equiv 1 (\mathrm{mod}\ p_1^{\alpha_1 - l_1} \dots p_s^{\alpha_s - l_s} p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}).$$

Z toho vyplýva, že $\alpha_1 = l_1, \dots, \alpha_s = l_s$. Keby totiž pre nejaké i platilo $\alpha_i - l_i > 0$, mali by sme $0 \equiv 1 (\mathrm{mod}\ p_i)$, čo nie je možné. Prvok $[x]$ možno teda napísať v tvare $[x] = [p_1^{\alpha_1} \dots p_s^{\alpha_s} b]$, $[b] \in G_1$, t. j. $[x] \in eG_1$. Dokázali sme nasledujúcu vetu:

Veta 9. *Nech e je idempotent pologrupy S_m. Maximálna grupa, ktorá patrí k idempotentu e, je daná vzorcom $G_e = eG_1$. (G_e je teda totožná s tou triedou modulo G_1, ktorá obsahuje idempotent e.)*

Poznámka. Veta 9 je veľmi pozoruhodná. Hovorí: Keď poznáme maximálnu grupu G_1 a všetky idempotenty, poznáme i všetky maximálne grupy. Keď chceme nájsť všetky maximálne grupy, nemusíme poznať dokonca ani konkrétny tvar idempotentov. Keď totiž $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$, $[a] \in G_1$, potom $eG_1 = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a] G_1 = [p_1^{\alpha_1} \dots p_s^{\alpha_s}] G_1$. Každú maximálnu grupu, ktorá nie je totožná s grupou G_1, dostaneme teda takto: Zvolíme ľubovoľný prvok tvaru $[p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}]$, $1 \leqq s \leqq r$ a utvoríme $[p_1^{\alpha_1} \dots p_s^{\alpha_s}] G_1$. To už je maximálna grupa pologrupy S_m. Napríklad maximálne grupy, ktoré patria k primitívnym idempotentom, sú tieto grupy:

$$[p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r}] G_1, [p_1^{\alpha_1} p_3^{\alpha_3} \dots p_r^{\alpha_r}] G_1, \dots, [p_1^{\alpha_1} \dots p_{r-1}^{\alpha_{r-1}}] G_1.$$

Z vety 2 vyplýva ihneď:

Veta 10. *Maximálna grupa G_e, ktorá patrí k idempotentu $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$, $[a] \in G_1$, $s < r$, má $\varphi(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r})$ rôznych prvkov.*

Vieme, že $G_e \subseteq P_e$. Rovnosť $G_e = P_e$ platí vtedy a len vtedy, ak obe napísané množiny majú rovnaký počet elementov. Keď $e = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$, $[a] \in G_1$, zo vzťahu $P_e = G_e$ vyplýva

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

t. j. $\alpha_1 = \alpha_2 = \dots = \alpha_s = 1$.

Špeciálne: Keď e_i je primitívny idempotent $[p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_s^{\alpha_s} a]$, $[a] \in G_1$, je P_{e_i} grupa vtedy a len vtedy, keď $\alpha_1 = \dots = \alpha_{i-1} = \alpha_{i+1} = \dots = \alpha_r = 1$. Keď e_i je maximálny idempotent $e_i = [p_i^{\alpha_i} a]$, $[a] \in G_1$, je P_{e_i} grupa vtedy a len vtedy, keď $\alpha_i = 1$.

Z toho dostávame:

Dôsledok 1. *Pologrupa S_m je množinovým súčtom disjunktných grúp vtedy a len vtedy, keď $\alpha_1 = \alpha_2 = \dots = \alpha_r = 1$.*

Dôsledok 2. *S_m je súčtom disjunktných grúp vtedy a len vtedy, keď maximálne pologrupy, ktoré patria k primitívnym idempotentom, sú grupy.*

Dôsledok 3. *S_m je súčtom disjunktných grúp vtedy a len vtedy, keď maximálne pologrupy, ktoré patria k maximálnym idempotentom, sú grupy.*

Dôsledok 4. *S_m je súčtom disjunktných grúp vtedy a len vtedy, keď neobsahuje nilpotentný element.*

Poznámka. Výsledky, ktoré sme práve odvodili, dávajú nový dôkaz vety dokázanej v práci [3].

Nakoniec dokážeme túto vetu:

Veta 11. *Nech $e' < e''$. Počet elementov pologrupy $P_{e'}$ nie je väčší ako počet elementov pologrupy $P_{e''}$ a počet elementov grupy $G_{e'}$ nie je väčší ako počet elementov grupy $G_{e''}$. Ak m je nepárne, možno slová „nie je väčší“ nahradiť slovami „je menší“.*

Dôkaz. Nech $e'' = [p_1^{\alpha_1} \dots p_s^{\alpha_s} a]$, $[a] \in G_1$, $0 \leqq s < r$, pričom pre $s = 0$ nech $e'' = [1]$. Potom e' má nevyhnutne tvar $e' = [p_1^{\alpha_1} \dots p_s^{\alpha_s} p_{s+1}^{\alpha_{s+1}} \dots p_t^{\alpha_t} b]$, $[b] \in G_1$, kde $s < t \leqq r$.

Počet elementov pologrupy $P_{e''}$ podľa vety 8 je

$$p_1^{\alpha_1 - 1} \dots p_s^{\alpha_s - 1} \varphi(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}) = \frac{m}{p_1 p_2 \dots p_r} (p_{s+1} - 1) \dots (p_r - 1),$$

počet elementov pologrupy $P_{e'}$ je

$$p_1^{\alpha_1 - 1} \dots p_t^{\alpha_t - 1} \varphi(p_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r}) = \frac{m}{p_1 p_2 \dots p_r} (p_{t+1} - 1) \dots (p_r - 1).$$

Pretože $(p_{s+1} - 1)(p_{s+2} - 1) \dots (p_t - 1) \geqq 1$, je prvá časť našej vety zrejmá. Znamienko rovnosti v poslednom vzťahu platí vtedy a len vtedy, keď $t - s = 1$ a jedno z čísel $p_{s+1}, \dots, p_t$ rovná sa 2. Znamienko rovnosti nemôže teda platiť, ak m je nepárne.

Počet elementov grupy $G_{e''}$ podľa vety 10 je $\varphi(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r})$, počet elementov grupy $G_{e'}$ je $\varphi(p_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r})$. Pretože

$$\varphi(p_{s+1}^{\alpha_{s+1}} \dots p_t^{\alpha_t}) = p_{s+1}^{\alpha_{s+1} - 1} \dots p_t^{\alpha_t - 1} (p_{s+1} - 1) \dots (p_t - 1) \geqq 1,$$

je prvá časť tvrdenia opäť zrejmá. V poslednom vzťahu platí znamienko rovnosti vtedy a len vtedy, keď $t - s = 1$, jedno z čísel $p_{s+1} \dots, p_t$, napr. $p_i (s + 1 \leqq i \leqq t)$ rovná sa číslu 2, a súčasne $\alpha_i = 1$. Znamienko nerovnosti platí teda iste vtedy, ak m je nepárne. Tým je veta 11 dokázaná.

6

Ilustrujme odvodené výsledky na špeciálnom prípade $r = 3$. Tu je $m = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$, $\alpha_1, \alpha_2, \alpha_3 > 0$. Maximálna grupa, ktorá patrí k idempotentu [1], nech je G_1.

Všetky maximálne grupy sú:

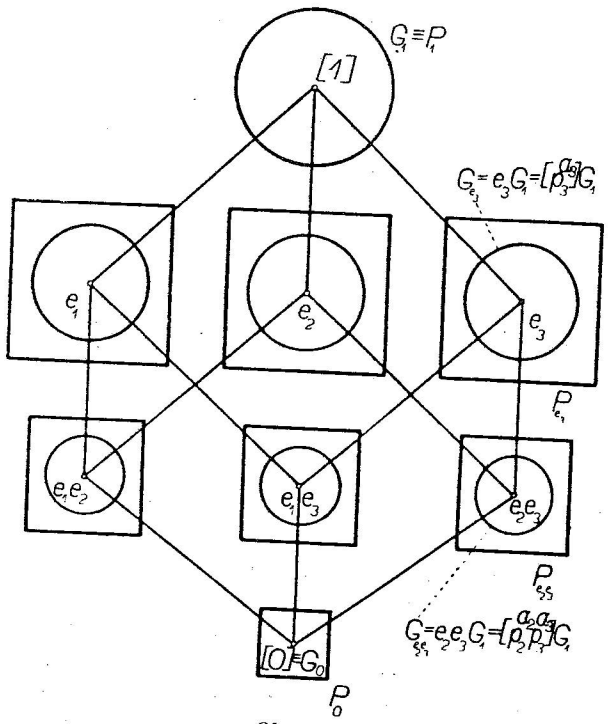
$$G_1,$$

$$[p_1^{\alpha_1}] G_1, [p_2^{\alpha_2}] G_1, [p_3^{\alpha_3}] G_1,$$

$$[p_1^{\alpha_1} p_2^{\alpha_2}] G_1, [p_1^{\alpha_1} p_3^{\alpha_3}] G_1, [p_2^{\alpha_2} p_3^{\alpha_3}] G_1,$$

$$[0].$$

Označme idempotent, ktorý leží v grupe $[p_i^{\alpha_i}]\,G_1$, znakom e_i. Idempotent, ktorý leží v grupe $[p_i^{\alpha_i}p_k^{\alpha_k}]\,G_1$, je e_ie_k. Boolova algebra idempotentov je znázornená na schematickom diagrame.



Obr. 1.

Maximálna grupa, ktorá patrí napr. k idempotentu e_3, je e_3G_1 a má $\varphi(p_1^{\alpha_1}p_2^{\alpha_2})$ elementov. Maximálna grupa $e_2e_3G_1$ patriaca k idempotentu e_2e_3 má $\varphi(p_1^{\alpha_1})$ elementov.

Maximálna pologrupa P_{e_3}, ktorá patrí k e_3, má $p_3^{\alpha_3-1}\varphi(p_1^{\alpha_1}p_2^{\alpha_2})$ elementov. Pologrupa P_{e_3} sama je množinovým súčtom α_3 tried modulo G_1, totiž $P_{e_3} = [p_3]\,G_1 \cup [p_3^2]\,G_1 \cup \ldots \cup [p_3^{\alpha_3}]\,G_1$. Maximálna pologrupa $P_{e_2e_3}$, ktorá patrí k primitívnemu idempotentu e_2e_3, má $p_2^{\alpha_2-1}p_3^{\alpha_3-1}\varphi(p_1^{\alpha_1})$ elementov. Je súčtom $\alpha_2\alpha_3$ tried $P_{e_2e_3} = [p_2p_3]\,G_1 \cup [p_2^2p_3]\,G_1 \cup [p_3p_3^2]\,G_1 \cup \ldots \cup [p_2^{\alpha_2}p_3^{\alpha_3}]\,G_1$.

V zmysle čiastočného usporiadania, ktoré sme zaviedli v texte, je napr. $[1] > e_3 > e_2e_3 > [0]$. Preto počet elementov pologrúp G_1, P_{e_3}, $P_{e_2e_3}$, P_0, resp. grúp G_1, G_{e_3}, $G_{e_2e_3}$, $[0]$ (napísaných v tomto poradí) postupne nerastie a v prípade, že m je nepárne, klesá.

Pri zostrojení schematického diagramu sme rešpektovali všetky tieto okolnosti.

LITERATÚRA

[1] Št. Schwarz, К теории периодических полугрупп, Чех. мат. журнал 3 (78), (1953), 7—21.

[2] H. S. Vandiver, The elements of a theory of abstract discrete semigroups, Vierteljschr. Naturforsch. Ges. Zürich 85 (1940), 71—86.

[3] B. Parízek, Poznámka o štruktúre multiplikatívnej pologrupy zvyškových tried, Mat. fyz. čas. SAV 7 (1957), 183—185.

Došlo 20. 11. 1957.

Katedra matematiky SVŠT
v Bratislave

О МУЛТИПЛИКАТИВНОЙ ПОЛУГРУППЕ КЛАССОВ ВЫЧЕТОВ (mod m)

БОГУМИЛ ПАРИЗЕК И ШТЕФАН ШВАРЦ

Выводы

Пусть $m = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, $\alpha_1 \geqq 1$, $\alpha_2 \geqq 1$, $\ldots$, $\alpha_r \geqq 1$ — разложение целого числа $m > 1$ на простые множители и S_m — мультипликативная полугруппа классов вычетов по модулю m. Класс, содержащий число a обозначим $[a]$, полугруппу классов взаимнопростых с m обозначим G_1.

Известно, что S_m можно писать как прямое произведение r полугрупп порядка $p_i^{\alpha_i}(i = 1, 2, \ldots, r)$. Целью этой работы является изучение множества S_m из другой точки зрения именно, из точки зрения существования групп в полугруппе S_m.

Некоторые результаты: Полугруппа S_m содержит 2^r идемпотента (включительно [0] и [1]). Каждый идемпотент $e \neq [1]$ можно писать в виде $e = [p_{i_1}^{\alpha_{i_1}} \ldots p_{i_s}^{\alpha_{i_s}}a]$, где $\{i_1, i_2, \ldots, i_s\}$ — непустое подмножество множества $\{1, 2, \ldots, r\}$ и, где $[a]$ удобно выбранный элемент $\in G_1$. Говорим, что элемент $x \in S_m$ принадлежит к идемпотенту e, если существует целое число $\varrho > 0$ такое, что $x^\varrho = e$. Множество всех элементов $\in S_n$, принадлежащих к e образует полугруппу P_e. Полугруппа S_m является очевидно суммой таких непересекающихся частичных полугрупп $S_m = \sum_e P_e$. Полугруппа P_e, принадлежащая к идемпотенту $e = [p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_s^{\alpha_s}a]$ содержит точно $p_1^{\alpha_1-1} \ldots p_s^{\alpha_s-1}\varphi(p_{s+1}^{\alpha_{s+1}} \ldots p_r^{\alpha_r})$ разных элементов. Максимальная группа G_e содержащая e в качестве единицы (и которая является подмножеством полугруппы P_e) равна G_1e и содержит точно $\varphi(p_{s+1}^{\alpha_{s+1}} \ldots p_r^{\alpha_r})$ разных элементов.

Подробнее изучается разложение полугруппы S_m modulo G_1 и приведены другие результаты, касающиеся структуры полугруппы S_m.

ON THE MULTIPLICATIVE SEMIGROUP OF RESIDUE CLASSES (mod m)

BOHUMÍR PARÍZEK and ŠTEFAN SCHWARZ

Summary

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $\alpha_1 \geqq 1, \dots \alpha_r, \geqq 1$, be the factorization of the 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 $[a]$. By G_1 we denote the subgroup of classes relatively prime to m.

It is well-known that S_m can be written as a direct product of r semigroups of prime-power orders. The purpose of this paper is to study the set S_m from an other point of view, namely from the stand-point of the existence of groups in S_m.

Some results: The semigroup S_m contains 2^r idempotents (including $[0]$ and $[1]$). Each idempotent $e \neq [1]$ can be written in the form $e = \left[p_{i_1}^{\alpha_{i_1}} \dots p_{i_s}^{\alpha_{i_s}} a\right]$, where $\{i_1, i_2, \dots, i_s\}$ is a non-empty subset of $\{1, 2, \dots, r\}$ and $[a]$ is a suitably chosen element $\in G_1$. We say that an element $x \in S_m$ belongs to the idempotent e, if there is an integer $\varrho > 0$ with $x^\varrho = e$. The set of all elements $\in S_m$ belonging to e forms a semigroup P_e. Clearly S_m is a disjoint sum of such subsemigroups: $S_m = \sum_e P_e$. The semigroup P_e belonging to $e = \left[p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} a\right]$ contains exactly $p_1^{\alpha_1 - 1} \dots p_s^{\alpha_s - 1} \varphi\left(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}\right)$ different elements. The maximal group G_e containing e as unity element (which is a subset of P_e) is equal to $G_1 e$ and it contains exactly $\varphi\left(p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}\right)$ different elements.

The decomposition of S_m modulo G_1 is studied in a greater detail and some other results concerning the structure of S_m are given.