POZNÁMKA O ŠTRUKTÚRE MULTIPLIKATÍVNEJ POLOGRUPY ZVYŠKOVÝCH TRIED

BOHUMÍR PARÍZEK
Katedra matematiky Slovenskej vysokej školy technickej v Bratislave

Nech S_m značí multiplikatívnu pologrupu zvyškových tried (mod m). Bez obavy z nedorozumenia budeme elementy pologrupy S_m označovať znakmi $1, 2, \ldots, m$. Účelom tejto poznámky je zistiť, kedy je takáto pologrupa súčtom disjunktných grúp.

V súhlase s prácou [1] budeme hovoriť, že prvok x nejakej pologrupy S je konečného rádu, ak existujú celé čísla $h > 0$, $k > 0$ také, že platí

$$x^{h+k} = x^h. \tag{1}$$

Ak h je najmenšie číslo, ktoré splňuje vzťah (1) a ak $h > 1$, budem hovoriť, že prvok $x \in S$ má predperiódu.

V práci [1] dokázal Š. Schwarz vetu:

Nech S je pologrupa, ktorej každý prvok je konečného rádu. Potom S je súčtom svojich maximálnych grúp vtedy a len vtedy, ak žiaden element z S nemá predperiódu.

Dokážme túto vetu:

Veta. *Nech $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, kde p_i $(i = 1, 2, \ldots, r)$ sú od seba rôzne kladné prvočísla, α_i $(i = 1, 2, \ldots, r)$ sú celé kladné čísla. Potom pologrupa S_m je súčtom svojich maximálnych grúp vtedy a len vtedy, ak $\alpha_i = 1$ pre všetky i $(i = 1, 2, \ldots, r)$.*

Dôkaz.

a) Tvrdím: Ak aspoň pre jedno celé i $(1 \leqq i \leqq r)$ je $\alpha_i > 1$, existuje aspoň jeden element $z \in S_m$, ktorý má predperiódu.

Pre dôkaz tvrdenia predpokladajme, že pre určité celé i $(1 \leqq i \leqq r)$ je $\alpha_i > 1$. Zvoľme $z = p_i$. Pretože v S_m je každý prvok konečného rádu, existujú celé čísla $h > 0$, $k > 0$ také, že pre prvok p_i platí vzťah (1), ktorý môžeme napísať v tvare

$$p_i^{h+k} \equiv p_i^h \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i} \ldots p_r^{\alpha_r}}. \tag{2}$$

Dokážem, že $h > 1$. Keby bolo $h = 1$, muselo by existovať také celé číslo $k > 0$, že by platilo

$$p_i^{1+k} \equiv p_i \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i} \ldots p_r^{\alpha_r}}.$$

Z toho by však vyplývalo

$$p_i^k \equiv 1 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i - 1} \dots p_r^{\alpha_r}}$$

a tým skôr

$$p_i^k \equiv 1 \pmod{p_i^{\alpha_i - 1}}.$$

Muselo by teda existovať celé číslo $c \geqq 0$ také, že by platilo

$$p_i^k - 1 = c p_i^{\alpha_i - 1},$$

teda

$$p_i^k - c p_i^{\alpha_i - 1} = 1. \tag{3}$$

Pretože je $\alpha_i - 1 > 0$, $c \geqq 0$, neexistuje celé číslo $k > 0$, ktoré by vyhovovalo rovnici (3). Ak teda h je najmenšie celé kladné číslo, ktoré spĺňuje vzťah (2), je $h > 1$ a prvok $p_i \in S_m$ má predperiódu.

b) Dokážem: Ak pre všetky celé i $(1 \leqq i \leqq r)$ je $\alpha_i = 1$, žiaden prvok $z \in S_m$ nemá predperiódu.

Nech $m = p_1 p_2 \dots p_r$.

α) Ak $z = 1$ alebo $z = m$, pre každé celé $k > 0$ je

$$z^{1+k} \equiv z \pmod{m}.$$

β) Ak $z \in S_m$ je nesúdelné s m, je známe, že existuje celé číslo $k = \varphi(m)$ (φ je Eulerova funkcia) také, že

$$z^k \equiv 1 \pmod{m}$$

a teda i

$$z^{1+k} \equiv z \pmod{m}.$$

γ) Ak $z \in S_m$ je súdeliteľné s m, potom

$$z = n p_1^{\beta_1} p_2^{\beta_2} \dots p_l^{\beta_l},$$

kde n je alebo 1, alebo celé kladné číslo nesúdeliteľné s m a l, β_i sú celé čísla, spĺňujúce vzťahy $1 \leqq l \leqq r$, $\beta_i > 0$ $(i = 1, 2, \dots, l)$.

1° Keď $l = r$, je $z \equiv m \pmod{m}$ a máme prípad α).

2° Keď $1 \leqq l < r$, existuje celé číslo $k = \varphi(p_{l+1} \dots p_r) > 0$ (φ je Eulerova funkcia) také, že

$$(n p_1^{\beta_1} p_2^{\beta_2} \dots p_l^{\beta_l})^k \equiv 1 \pmod{p_{l+1} \dots p_r}.$$

Z toho

$$(n p_1^{\beta_1} p_2^{\beta_2} \dots p_l^{\beta_l})^{1+k} \equiv n p_1^{\beta_1} p_2^{\beta_2} \dots p_l^{\beta_l} \pmod{n p_1^{\beta_1} p_2^{\beta_2} \dots p_l^{\beta_l} p_{l+1} \dots p_r}$$

a tým skôr

$$(n p_1^{\beta_1} p_2^{\beta_2} \dots p_l^{\beta_l})^{1+k} \equiv n p_1^{\beta_1} p_2^{\beta_2} \dots p_l^{\beta_l} \pmod{p_1 p_2 \dots p_l p_{l+1} \dots p_r},$$

teda

$$z^{1+k} \equiv z \pmod{m}.$$

Úhrnom: Ku každému $z \in S_m$ existuje celé číslo $k > 0$ také, že

$$z^{1+k} \equiv z \pmod{m}.$$

To znamená: Ak h je najmenšie celé kladné číslo, pre ktoré platí vzťah (1), pre každý prvok $z \in S_m$ je $h = 1$, teda žiaden prvok $z \in S_m$ nemá predperiódu, č. b. t. d.

LITERATÚRA

1. Schwarz Š., Teória pologrúp, Sborník prác Prírodovedeckej fakulty Slovenskej univerzity v Bratislave, VI, 1943, 7—15.

Došlo 12. 4. 1957.

ЗАМЕТКА О СТРУКТУРЕ МУЛЬТИПЛИКАТИВНЫХ ПОЛУГРУПП

БОГУМИР ПАРИЗЕК

Выводы

В статье доказывается следующая теорема:

Пусть S_m мултипликативная полугруппа классов вычетов по модулю m. Если $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, где p_i $(i = 1, 2, \dots, r)$ разные простые числа и α_i натуральные числа $(i = 1, 2, \dots, r)$, то S_m является суммой непересекающихся своих максимальных групп тогда и только тогда, когда $\alpha_i = 1$ для всех $i = 1, 2, \dots, r$.

NOTE ON STRUCTURE OF MULTIPLICATIVE SEMIGROUP OF RESIDUE CLASSES

BOHUMÍR PARÍZEK

Summary

In this paper the following theorem is showed.

Let S_m be the multiplicative semigroup of residue classes (mod m). If $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where p_i $(i = 1, 2, \dots, r)$ are distinct primes and α_i $(i = 1, 2, \dots, r)$ are positive integers, then S_m is a disjunct summ of its maximal groups if and only if $\alpha_i = 1$ for all i $(i = 1, 2, \dots, r)$.