Algebra a diskrétna matematika
Prehľad z 13. týždňa
Polia - pokračovanie

**Pole** je množina $F$ s dvoma binárnymi operáciami $\oplus, \otimes$, pričom
- $(F, \oplus)$ a $(F - \{0\}, \otimes)$ tvoria komutatívne grupy,
- V poli $F$ platí distributívny zákon

$\forall\ a, b, c \in F: \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

**Tvrdenie:** Rád konečného poľa je mocnina prvočísla.

Príklad 1: Vypočítajte aditívne a mutliplikatívne rády prvkov $2, 3$ v poli $\mathbb{Z}_{11}$.

Odpoveď: Aditívny rád prvku 2 je 11, pretože najmenšie $n$, ktoré vyhovuje rovnici $n \cdot 2 \equiv 0 \pmod{11}$, je $n = 11$. To isté platí pre prvok 3.
Multiplikatívny rád prvku 2 je 10, pretože $2^{10} \equiv 1 \pmod{11}$ a 10 je najmenšia taká kladná mocnina.
Prvok 3 má multiplikatívny rád 5, lebo $3^5 \equiv 1 \pmod{11}$ a 5 je najmenšia taká kladná mocnina.

Príklad 2: Ktorý prvok generuje pole $\mathbb{Z}_{17}$?

Odpoveď: Ak prvok $x$ je generátor v $\mathbb{Z}_{17}$, potom platí
$x^{16} \equiv 1$ a $x^8 \equiv -1 \pmod{16}$.
Postupne ideme overovať mocniny prvkov v $\mathbb{Z}_{17}$.
$2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16 \equiv -1, 2^8 \equiv 1$, teda 2 nie je generátor $\mathbb{Z}_{17}$.
$3^2 \equiv 9, 3^3 \equiv 10, 3^4 \equiv 13, 3^5 \equiv 5, 3^6 \equiv 15, 3^7 \equiv 11, 3^8 \equiv 16 \equiv -1,$
$3^9 \equiv 3 \cdot 3^8 \equiv -3 \equiv 14, 3^{10} \equiv -3 \cdot 3 \equiv 8, 3^{11} \equiv 7, 3^{12} \equiv 4, 3^{13} \equiv 12, 3^{14} \equiv 2, 3^{15} \equiv 6, 3^{16} \equiv 1.$
Prvok 3 je generátor poľa $\mathbb{Z}_{17}$.

Grupa je cyklická, ak je generovaná jedným prvkom.

**Veta:** Multiplikatívna grupa každého *konečného* poľa je **cyklická**.

Každý generátor multiplikatívnej grupy poľa nazývame **primitívny prvok**.

Nájsť primitívny prvok v poli nie je triviálne, ak ide o pole veľkého rádu.

Príklad 3: V poli $\mathbb{Z}_{23}$ nájdite primitívny prvok.

Odpoveď: Hľadáme prvok $x$ v $\mathbb{Z}_{23}$, pre ktorý $x^{22} \equiv 1 \pmod{23}$ a tiež $x^{11} \equiv -1 \equiv 22 \pmod{23}$.

$2^{11} \equiv 1 \pmod{23}$, 2 nie je generátor. To isté platí pre 4.

Overíme prvok 3.
$3^3 \equiv 4$, takže $3^{33} \equiv (3^3)^{11} \equiv 4^{11} \equiv 1 \pmod{23}$ (*)
Ale potom ak by 3 bol primitívny prvok, tak $3^{11}$ by musel byť $-1 \pmod{23}$, a teda
$3^{33} = 3^{22} \cdot 3^{11} \equiv 1.(-1) \equiv -1 \bmod 23$, čo je v rozpore s (*).
Ani 3 nie je primitívnym prvkom v $\mathbb{Z}_{23}$.

Overme prvok 5.
$5^2 \equiv 2, 5^{10} \equiv 2^5 \equiv 9, 5^{11} \equiv 9 \cdot 5 \equiv -1 \pmod{23}$.
Prvok 5 je primitívny v poli $\mathbb{Z}_{23}$.

**Počet primitívnych prvkov**

Pole rádu $p$ má $\varphi(p-1)$ primitívnych prvkov, kde $\varphi$ je Eulerova funkcia (počet kladných čísel menších ako $p-1$ a nesúdeliteľných s $p-1$).

Ak prirodzené číslo $n$ má prvočíselný rozklad $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$, potom

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

Príklad 4: Určte počet primitívnych prvkov v poliach $\mathbb{Z}_{11}, \mathbb{Z}_{17}, \mathbb{Z}_{19}$.

Odpoveď:

$\varphi(10) = 10(1-\frac{1}{2})(1-\frac{1}{5}) = 4$
$\varphi(16) = 16(1-\frac{1}{2}) = 8$
$\varphi(18) = 18(1-\frac{1}{2})(1-\frac{1}{3}) = 6$
V poli $\mathbb{Z}_{11}$ sú 4 primitívne prvky, v poli $\mathbb{Z}_{17}$ je ich 8 a pole $\mathbb{Z}_{19}$ ich má 6.

Príklad 5: Určte, ktoré prvky majú v poli $\mathbb{Z}_{19}$ druhé odmocniny.

Odpoveď: Najprv je potrebné nájsť primitívny prvok v $\mathbb{Z}_{19}$. Sú nimi napríklad prvky 2 a 3. Potom všetky prvky, ktoré sú párne mocniny primitívneho prvku, majú v $\mathbb{Z}_{19}$ druhú odmocninu.
Túto množinu tvoria prvky $1, 4, 5, 6, 7, 9, 11, 16, 17$.

Príklad 6: Riešte rovnicu $x^3 = 1$ v poli $\mathbb{Z}_7$ a v poli $\mathbb{Z}_{11}$.

Odpoveď: V $\mathbb{Z}_7$ sú korene $x_1 = 1, x_2 = 2, x_3 = 4$.
V poli $\mathbb{Z}_{11}$ je iba jeden koreň $x = 1$, pretože $11 - 1$ nie je deliteľné číslom 3.

**Malá Fermatova veta:** Nech $p$ je prvočíslo a nech $a$ je celé číslo nesúdeliteľné s $p$. Potom platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dôkaz: Budeme dokazovať ekvivalentné tvrdenie $a^p \equiv a \pmod{p}$.
Matematickou indukciou vzhľadom na $a$, pričom $p$ je prvočíslo a $p \nmid a$.
1. $a = 2$

$$2^p = (1+1)^p = \binom{p}{0} + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} + \binom{p}{p} = 2 \pmod{p}$$

Využili sme tu fakt, že pre $k < p$ je $\binom{p}{k} \equiv 0 \pmod{p}$.
2. Predpokladajme, že platí $a^p \equiv a \pmod{p}$.
Ukážeme, že platí aj $(a+1)^p \equiv a + 1 \pmod{p}$.

$$(a+1)^p = \binom{p}{0} a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + \binom{p}{p} \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

Príklad 7: Bez použitia kalkulačky vypočítajte

a) $19669^{28} \pmod{29}$

b) $4324^{3323} \pmod{3323}$

c) $11^{209458} \pmod{104729}$

Odpoveď: Keďže každé z čísel $29, 3323, 104729$ je prvočíslo, je možné aplikovať Malú Fermatovu vetu.

a) $19669^{28} \equiv 1 \pmod{29}$

b) $4324^{3323} \equiv 4324 \equiv 1001 \pmod{3323}$

c) $11^{209458} = (11^{104728})^2 \cdot 11^2 \equiv 121 \pmod{104729}$

**Veľká Fermatova veta:** Pre žiadne nenulové celé čísla $a, b, c$ a $n > 2$ *neplatí*

$$a^n + b^n = c^n$$

Považuje sa za jeden z najťažších matematických problémov.
V roku 1637 Fermat napísal toto tvrdenie na okraj jedného listu Diofantovej Aritmetiky (3. st. pnl) s tým, ze údajný dôkaz sa mu tam už nezmestil.
Prvý dôkaz publikoval v roku 1995 anglický matematik Andrew Wiles.
V tom istom roku s Richardom Taylorom odstránili medzeru v dôkaze.