Algebra a diskrétna matematika
Prehľad z 12. prednášky
Polia

Medzi slávne antické problémy, ktoré sa viac ako dvetisíc rokov nedarilo vyriešiť patria:

• *Problém trisekcie uhla* – Pomocou pravítka a kružidla zostrojte uhol, ktorý je tretinou daného uhla.

• *Problém kvadratúry kruhu* – Pomocou pravítka a kružidla zostrojte štvorec, ktorý má rovnaký obsah ako daný kruh.

• *Problém zdvojenia kocky* – Pomocou pravítka a kružidla zostrojte kocku, ktorá má dvojnásobný objem ako daná kocka.

Odpoveď o ich neriešiteľnosti priniesla až moderná algebra v 19. storočí. Pomocou prostriedkov algebry sa dá dokázať, že pomocou pravítka a kružidla nedokážeme žiadnou konštrukciou
− rozdeliť daný uhol na tri rovnaké časti,
− zostrojiť z úsečky dĺžky 1 úsečku dĺžky π,
− zostrojiť z úsečky dĺžky a úsečku dĺžky $a\sqrt[3]{2}$.

Dôležitá algebraická štruktúra v tomto dôkaze je **pole**.

Pole je množina F s dvoma binárnymi operáciami $\oplus, \otimes$, pričom sú splnené nasledujúce podmienky

• $(F, \oplus)$ a $(F - \{0\}, \otimes)$ tvoria komutatívne grupy,

• Na F platí distributívny zákon

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

Operácie $\oplus, \otimes$ zvyčajne nazývame *sčitovanie* a *násobenie.*

Pole potom jednoducho zapisujeme $(F, +, \cdot)$.
Grupa $(F, +)$ sa nazýva *aditívnou* grupou poľa, skrátene F^+.
Grupa $(F - \{0\}, \cdot)$ sa nazýva *multiplikatívnou* grupou poľa, skrátene $F^\times$.

Príklad 1: Najznámejšie nekonečné polia sú $(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$.

Príklad 2: Príklad konečného poľa je $(\mathbb{Z}_5,+,\cdot)$.
Jeho aditívny neutrálny prvok je 0 a inverzné prvky v aditínej grupe sú $-1=4,-2=3,-3=2,-4=1$.
Multiplikatívny inverzný prvok je 1 a inverzné prvky v multiplikatívnej grupe sú $2^{-1}=3,3^{-1}=2,4^{-1}=4$.
Rovnicu $3x+4\equiv 1$ v $\mathbb{Z}_5$ riešime nasledovne

$$\begin{aligned}3x+4+1 &= 1+1\\ 3x &= 2\\ 3^{-1}\cdot 3x &= 3^{-1}\cdot 2\\ 2\cdot 3x &= 2\cdot 2\\ x &= 4\end{aligned}$$

Príklad 3: V poli $(\mathbb{Z}_{11},+,\cdot)$ riešte rovnicu

$$4x+5=7$$

Odpoveď: $x=6$

Príklad 4: V poli $(\mathbb{Z}_{19},+,\cdot)$ riešte rovnicu

$$3x+8=13$$

Odpoveď: $x=8$

Príklad 5: V poli $(\mathbb{Z}_5,+,\cdot)$ riešte rovnicu

$$x^2+4x+3=0$$

Odpoveď: $x_1=2,x_2=4$

Príklad 6: V poli $(\mathbb{Z}_7,+,\cdot)$ riešte rovnicu

$$x^2+5x+2=0$$

Odpoveď: nemá riešenie

Príklad 7: V poli $(\mathbb{Z}_{11},+,\cdot)$ riešte rovnicu

$$x^2+3x+7=0$$

Odpoveď: $x_1=1,x_2=7$

Príklad 8: V poli $\mathbb{Z}_5$ riešte sústavu rovníc

$$\begin{aligned} 3x + y &= 3 \\ x + 3y &= 2 \end{aligned}$$

Odpoveď: $x = 4, y = 1$

Príklad 9: V poli $\mathbb{Z}_7$ riešte sústavu rovníc

$$\begin{aligned} x + z &= 0 \\ 2x + y + 3z &= 4 \\ 5x + y + z &= 5 \end{aligned}$$

Odpoveď: $x = 3, y = 0, z = 4$

Príklad 10: V $\mathbb{Z}_6$ rovnica $3x + 4 = 2$ nemá riešenie, lebo k 3 neexistuje multiplikatívny inverz. $\mathbb{Z}_6$ nie je pole!

Tvrdenie 1: Ak p je prvočíslo, tak pre každé $x \in \mathbb{Z}_p - \{0\}$ existuje $y \in \mathbb{Z}_p - \{0\}$ také, že $x \cdot y \equiv 1 \pmod{p}$.

Rád poľa je počet prvkov poľa.

Tvrdenie 2: Rád konečného poľa je mocnina prvočísla.

Tvrdenie 3: Pre každé prvočíslo p a prirodzené číslo n existuje práve jedno (až na izomorfizmus) pole rádu $p^n = q$.

Príklad 11: Ktorý prvok generuje pole $\mathbb{Z}_{17}$?

Odpoveď: Ak prvok x je generátor v $\mathbb{Z}_{17}$, potom platí
$x^{16} \equiv 1$ a $x^8 \equiv -1$ (mod 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 $\mathbb{Z}_{17}$.

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

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

Príklad 12: 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 $\mathbb{Z}_{23}$.

Príklad 13: 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 $1, 4, 5, 6, 7, 9, 11, 16, 17$.

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

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

Príklad 14: Bez použitia kalkulačky vypočítajte

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

b) $3324^{3323} \pmod{3323}$

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) $3324^{3323} \equiv 1 \pmod{3323}$

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