Okruhy celých čísel a deliteľnosť

17. októbra 2024

Okruh celých čísel

Chceme:

- Povedať niečo o deliteľnosti.
- Povedať ako vyzerajú ideály v $\mathbb{Z}$.
- Podobné veci nás budú zaujímať pre okruh $F[x]$ (okruh polynómov nad poľom F).

Veta o delení so zvyškom

Tvrdenie (Veta o delení so zvyškom)

Nech $a, b \in \mathbb{Z}$ a $b \neq 0$. Potom existujú celé čísla q, r také, že platí

$$a = q \cdot b + r, \qquad 0 \leq r < |b|.$$

Navyše čísla q a r sú týmito podmienkami jednoznačne určené. Číslo q nazývame podiel a číslo r zvyšok čísla a po delení číslom b. Pre zvyšok budeme používať označenie $r = a \bmod b$.

Deliteľnosť

Definícia

Ak $a, b \in \mathbb{Z}$ tak hovoríme, že a *delí* b, ak existuje celé číslo q také, že $b = qa$. Označujeme $a \mid b$.

- $1 \mid a$, $a \mid 0$;
- Ak $0 \mid a$, tak $a = 0$.
- $a \mid a$;
- Ak $a \mid b$ aj $b \mid a$, tak $a = \pm b$
- Ak $a \mid b$ a $b \mid c$, tak aj $a \mid c$.
- Ak $a \mid b$ aj $a \mid c$, tak $a \mid b \pm c$.
- Ak $a \mid b$ aj $a \mid c$, tak platí $a \mid bx + cy$ pre ľubovoľné $x, y \in \mathbb{Z}$.
- Ak $a, b \in \mathbb{N}$, tak z $a \mid b$ vyplýva $a \leq b$.
- Ak $a \mid b$ a $b \neq 0$, tak $|a| \leq |b|$.

Každý ideál v $\mathbb{Z}$ je hlavný

Tvrdenie

Nech $I \subseteq \mathbb{Z}$ je ideál v okruhu $(\mathbb{Z}, +, \cdot)$. Potom existuje $a \in \mathbb{Z}$ také, že

$$I = (a) = \{ax; x \in \mathbb{Z}\}.$$

Ak navyše pridáme podmienku $a \geq 0$, tak číslo a je jednoznačne určené.

Stručné zhrnutie dôkazu: Celý dôkaz sa stručne dá zhrnúť tak, že:

- Zoberieme si najmenšie kladné a patriace do ideálu I.
- Ukážeme, že všetky ostatné prvky v I sú násobky čísla a.

Ideály a deliteľnosť

Pre $a, b \in \mathbb{Z}$ sú tieto podmienky ekvivalentné:

- $a \mid b$
- $b \in (a)$
- $(b) \subseteq (a)$.

Najväčší spoločný deliteľ

Definícia

Nech $a, b \in \mathbb{Z}$. Celé číslo $d \geq 0$ nazveme *najväčší spoločný deliteľ* čísel a, b ak $d \geq 0$ a platí:

(i) $d \mid a$, $d \mid b$ (T.j. d je súčasne deliteľ a aj deliteľ b.)

(ii) Pre každé $c \in \mathbb{Z}$ také, že $c \mid a$, $c \mid b$ platí aj $c \mid d$.

Označujeme: $d = \gcd(a, b)$.

Najväčší spoločný deliteľ

Tvrdenie

Nech $a, b \in \mathbb{Z}$. Potom množina

$$(a, b) = \{ax + by; x, y \in \mathbb{Z}\}$$

je ideál v $\mathbb{Z}$.
Navyše ak $d \geq 0$ je celé číslo také, že $(d) = (a, b)$, tak d je najväčší spoločný deliteľ (a, b).

Dôsledok (Bézoutova identita)

Ak $d = \gcd(a, b)$ tak existujú $x, y \in \mathbb{Z}$ také, že

$$d = ax + by.$$

Nesúdeliteľné čísla

Definícia

Celé čísla a, b nazývame *nesúdeliteľné*, ak $\gcd(a, b) = 1$.

Dôsledok

Ak $a, b \in \mathbb{Z}$ sú nesúdeliteľné celé čísla, tak existujú $x, y \in \mathbb{Z}$ také, že

$$ax + by = 1.$$

Prvočísla

Definícia

Prirodzené číslo $p > 1$ sa nazýva prvočíslo ak pre jeho ľubovoľný zápis v tvare $p = a \cdot b$ platí $a = 1$ alebo $b = 1$.

Veta (Základná veta aritmetiky)

Pre každé prirodzené číslo $n > 1$ existujú prvočísla $p_1, p_2, \ldots, p_k$ také, že

$$n = p_1 \cdot p_2 \cdots p_k.$$

Navyše takýto zápis je určený jednoznačne až na poradie.

Prvočísla

Tvrdenie

Nech p je prvočíslo, a, b sú celé čísla. Ak $p \mid ab$, tak $p \mid a$ alebo $p \mid b$.

$$p \mid ab \qquad \Rightarrow \qquad p \mid a \vee p \mid b$$

$$\begin{aligned} \gcd(p, a) &= 1 \\ px + ay &= 1 \\ pbx + aby &= b \end{aligned}$$

$$\left.\begin{matrix} p \mid p \\ p \mid ab \end{matrix}\right\} \Rightarrow \left.\begin{matrix} p \mid pbx \\ p \mid aby \end{matrix}\right\} \Rightarrow p \mid pbx + aby = b.$$

Nesúdeliteľné čísla

Tvrdenie

Nech p je prvočíslo, a, b sú celé čísla. Ak $p \mid ab$, tak $p \mid a$ alebo $p \mid b$.

$$p \mid ab \qquad \Rightarrow \qquad p \mid a \vee p \mid b$$

Tvrdenie

Ak pre celé čísla a, b, c platí $a \mid bc$ a $\gcd(a, b) = 1$, tak $a \mid c$.

Kongruencie

Definícia

Ak $a, b, n \in \mathbb{Z}$, tak hovoríme, že čísla a, b sú kongruentné modulo n, ak platí

$$n \mid a - b.$$

Označujeme $a \equiv b \pmod{n}$.

$$a \equiv b \pmod{n} \qquad \Leftrightarrow \qquad n \mid a - b$$

$$\begin{aligned} a \equiv b \pmod{n} \qquad &\Leftrightarrow \qquad a \equiv b \pmod{-n} \\ a \equiv b \pmod{0} \qquad &\Leftrightarrow \qquad a = b \\ a \equiv b \pmod{1} \qquad &\Leftrightarrow \qquad a, b \in \mathbb{Z} \end{aligned}$$

Kongruencia je relácia ekvivalencie

Tvrdenie

Nech $a, b, c, n \in \mathbb{Z}$. *Potom platí:*

(i) $a \equiv a \pmod{n}$

(ii) *Ak* $a \equiv b \pmod{n}$, *tak aj* $b \equiv a \pmod{n}$.

(iii) *Ak platí* $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, *tak aj* $a \equiv c \pmod{n}$.

Sčitovanie a násobenie kongruencií

Tvrdenie

Nech $a, b, c, d, n \in \mathbb{Z}$. *Ak*

$$a \equiv c \pmod{n}$$
$$b \equiv d \pmod{n}$$

tak platí aj

$$a + b \equiv c + d \pmod{n}$$
$$a \cdot b \equiv c \cdot d \pmod{n}$$

Okruh $\mathbb{Z}/(n)$

Kongruencia modulo n je relácia ekvivalencie.

$$\overline{a} = [a] = \{x \in \mathbb{Z}; x \equiv a \pmod{n}\}$$

$$\mathbb{Z}/(n) = \{\overline{a}; a \in \mathbb{Z}\}$$

$$\overline{x} + \overline{y} = \overline{x + y}$$
$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Sčitovanie a násobenie sú dobre definované

Tvrdenie

Nech $n \in \mathbb{Z}$, $n \neq \pm 1$. Potom vzťahy

$$\overline{x} + \overline{y} = \overline{x + y}$$
$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

určujú dobre definované binárne operácie na množine $\mathbb{Z}/(n)$. Množina $\mathbb{Z}/(n)$ s týmito operáciami tvorí komutatívny okruh s jednotkou.

Pole $\mathbb{Z}/(p)$

Tvrdenie

Ak (p) je prvočíslo, tak $(\mathbb{Z}/(p), +, \cdot)$ je pole.

$$ax + py = 1$$

$$ax \equiv 1 \pmod{p}$$

$$\overline{a} \cdot \overline{x} = \overline{1}$$