LINEÁRNE KONGRUENCIE A DIOFANTICKÉ ROVNICE

Lineárna kongruencia je vzťah

$$ax \equiv b \ (\mod m)$$

s neznámou x a danými $a, b, m \in \mathbb{Z}$. Celé čísla x, ktoré vyhovujú tejto kongruencii nazývame riešeniami.

Veta 1. *Kongruencia* $ax \equiv b \ (\mod m)$ *má riešenie práve vtedy, keď* $d = (a, m)$ *delí* b. *Riešením sú práve tie* $x \in \mathbb{Z}$, *ktoré spĺňajú podmienku*

$$x \equiv \frac{b}{d} u \ (\mod \frac{m}{d}),$$

kde $d = au + mv \ (u, v \in \mathbb{Z})$.

Riešenie lineárnych kongruencií ilustrujeme na príklade

$$15x \equiv 7 \ (\mod 37).$$

Platí $(15, 37) = 1$, Euklidovým algoritmom dostaneme $1 = 15 \cdot 5 - 37 \cdot 2$, teda $u = 5$ a kongruencia má riešenie

$$x \equiv 7 \cdot u = 35 \ (\mod 37).$$

Veta o delení so zvyškom dovoľuje zapísať riešenie aj v parametrickom tvare

$$x = 37k + 35, \quad k \in \mathbb{Z}.$$

Ako príklad lineárnej kongruencie, ktorá nemá riešenie uveďme

$$21x \equiv 16 \ (\mod 33).$$

Skutočne, $(21, 33) = 3$ a 3 nedelí 16.

Nasledujúce tvrdenie je známe ako *Čínska veta o zvyškoch.*

Veta 2. *Nech $m_1, \ldots, m_n$ sú navzájom nesúdeliteľné celé čísla. Nech $c_1, \ldots, c_n$ sú ľubovoľné celé čísla. Potom existuje $x \in \mathbb{Z}$ tak, že*

$$x \equiv c_i \ (\mod m_i)$$

pre každé i.

Bez predpokladu nesúdeliteľnosti modulov veta neplatí: nie je problém nájsť dve kongruencie, z ktorých každá má riešenie, ale spoločné riešenie nemajú.

Diofantické rovnice sú vo všeobecnosti rovnice s viacerými neznámymi, kde hľadáme celočíselné riešenia. My sa budeme venovať iba najjednoduchšiemu typu, a to sú lineárne rovnice s dvoma neznámymi. Pri riešení takých

rovníc sa uplatnia lineárne kongruencie. Postup ukážeme na príklade.

Hľadajme celočíselné riešenia rovnice

$$18x - 23y = 10.$$

Vyjadríme

$$x = \frac{23y + 10}{18}.$$

Pretože x má byť celé číslo, musí $23y+10$ byť deliteľné 18, čo sa dá vyjadriť kongruenciou

$$23y \equiv -10 \ (\mod 18),$$

ktorá má riešenie

$$y \equiv 16 \ (\mod 18).$$

Parametrický tvar $y = 18k + 16$ nám teraz dovoľuje dopočítať x:

$$x = \frac{23(18k + 16) + 10}{18} = \frac{23 \cdot 18k + 378}{18} = 23k + 21.$$

Takže riešením pôvodnej rovnice sú všetky dvojice tvaru $[23k+21, 18k+16]$, kde $k \in \mathbb{Z}$. Napríklad pre $k = 0$ máme riešenie $x = 21$, $y = 16$, voľba $k = -1$ dáva $x = -2$, $y = -2$.

Kontrolný test

Začiatok testu (4 body) :

1. Kongruencia $5x \equiv b \pmod{43}$ riešenie

- ☐ určite má;
- ☐ určite nemá;
- ☐ závisí to od b.

2. Kongruencia $15x \equiv 36 \pmod{48}$ riešenie

- ☐ nemá
- ☐ má a je to trieda kongruencie modulo 3;
- ☐ má a je to trieda kongruencie modulo 16;
- ☐ má a je to trieda kongruencie modulo 48.

3. Rovnica $18x - 22y = 7$ v $\mathbb{Z}$

- ☐ nemá riešenie;
- ☐ má jediné riešenie;
- ☐ má nekonečne veľa riešení.

4. Označte pravdivé výroky.

- ☐ Každá lineárna kongruencia má riešenie.
- ☐ Ak dve kongruencie majú riešenie, tak majú aj spoločné riešenie.
- ☐ Ak dve kongruencie s nesúdeliteľnými modulmi majú riešenie, tak majú aj spoločné riešenie.
- ☐ Ak tri kongruencie s navzájom nesúdeliteľnými modulmi majú riešenie, tak majú aj spoločné riešenie.

Koniec testu Správne odpovede

Získané body:

Úspešnosť: