Dělitelnost

$a \mid b \iff b = k \cdot a, \quad k \in \mathbb{Z}$

(dělitel, násobek)

Operace vs Relace

$: \mathbb{Z} \times \mathbb{Z} \setminus \{0\} \to \mathbb{Q} \qquad | \subset \mathbb{Z} \times \mathbb{Z}$

Vlastnosti |

- $a \neq 0 \quad a \mid b \wedge a \mid c \Rightarrow a \mid (ra + sc), \quad r, s \in \mathbb{Z}$
- $\forall a, b \in \mathbb{Z}, \exists q, r \in \mathbb{Z} : a = q \cdot b + r \wedge 0 \leq r < b$

(dělenec, dělitel, podíl, zbytek)

$a \text{ div } b = \text{podíl} \qquad a \bmod b = \text{zbytek}$

$7 \text{ div } 2 = 3 \qquad 7 \bmod 2 = 1$

Kongruence

$a \equiv b \pmod m \iff a \bmod m = b \bmod m$

$a \equiv b \pmod m \iff m \mid b - a$

tj. $\exists k \in \mathbb{Z}, b = a + km$

Počítání se zbytkovými třídami

$a +_m b = (a + b) \bmod m \qquad 8 +_{12} 7 = 15 \bmod 12 = 3$

$a \cdot_m b = (a \cdot b) \bmod m \qquad 3 \cdot_5 4 = 12 \bmod 5 = 2$

- NSD(a, b) - definice
- Euklidův Algoritmus + Bezoutova věta

$\exists r, s \in \mathbb{Z}, \ NSD(a, b) = r \cdot a + s \cdot b$

Lineární kongruence: $ax \equiv b \pmod m, \quad x = ?$

Příklady:

1.) Určete zbytek po dělení čísla 589 číslem 8.

- $589 = q \cdot 8 + r, \quad 0 \leq r < 8$

  (589 dělenec, 8 dělitel, q podíl, r zbytek)

$$\frac{589}{8} = 73{,}625 \Rightarrow q = 73, \; r = ?$$

$$589 - 73 \cdot 8 = 589 - 584 = 5 = r$$

pomocí kalkulačky →

jiné řešení →

- $589 = 560 + 29 \equiv 29 \pmod 8$

  $29 = 24 + 5 \equiv 5 \pmod 8$

  $\Rightarrow 589 \equiv 5 \pmod 8$

  tj. $589 = q \cdot 8 + \underline{5} = r$

2.) Určete zbytek po dělení čísla 4774 číslem 6.

„4774 mod 6" = ? $\qquad 4774 = q \cdot 6 + r, \quad 0 \leq r < 6$

$4774 = 4800 - 26 \equiv -26 \pmod 6$

$-26 = -30 + 4 \equiv 4 \pmod 6$

$4774 \equiv \underbrace{4}_{= r} \pmod 6 \qquad \underbrace{0 \leq 4 < 6}_{r}$

$r = 4$

$4774 \bmod 6 = 4$

3) Určete zbytek po dělení čísla 5891 číslem 11.

$5891 \bmod 11 = ? \qquad 5891 = q \cdot 11 + r, \quad 0 \leq r < 11$

$5891 = 5500 + 391 \equiv 391 \pmod{11}$

$391 = 330 + 61 \equiv 61 \pmod{11}$

$61 = 55 + 6 \equiv 6 \pmod{11}$

$5891 \equiv 6 \pmod{11}$ $\quad 5891 \bmod 11 = 6$

$r = 6$

Je 4321 prvočíslo? (Hledáme dělitele)

zbytek po dělení: 2, 3, 5, 7, 11, 13

$2 \nmid 4321$ $\quad 2 \mid 4321$

$3 \nmid 4321$

$5 \nmid 4321$

$7 \mid 4321$

$11 \nmid 4321$

$4321 \equiv 4200 + 121 \pmod 7$

$121 = 70 + 51 \equiv 51 \pmod 7$

$51 = 49 + 2 \equiv 2 \pmod 7$

$4321 = 4400 - 79 \equiv -79 \pmod{11}$

$-79 = -77 - 2 \equiv -2 \pmod{11}$

$-2 = -11 + 9 \equiv 9 \pmod{11}$

Eukleidův algoritmus $NSD(a,b)$ a Bezoutova věta

+ zpětné dosazení

$NSD(a,b) = r \cdot a + s \cdot b$

pro řešení kongruencí.

Př. Určete největšího spol. dělitele 589 a 8.

$NSD(589, 8) = 1$

Eukleidovým algoritmem.

postup:

dělitele dělíme zbytkem

$589 = 73 \cdot 8 + 5$

$q \quad r$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$ $= NSD(589, 8)$

$2 = 2 \cdot 1 + 0$

Př.: Eukl. alg. určete $NSD(123, 277)$

$277 = 2 \cdot 123 + 31$

$123 = 3 \cdot 31 + 30$

$31 = 1 \cdot 30 + 1$ $= NSD(123, 277) = 1$

$30 = 30 \cdot 1 + 0$

nesoudělná čísla.

Zpětný chod Eu. Alg.

Podle Bezout. věty

$NSD(123, 277) = r \cdot 123 + s \cdot 277$

$1 = 1 \cdot 31 - 1 \cdot 30 = 1 \cdot 31 - 1 \cdot (123 - 3 \cdot 31) =$

$= 4 \cdot 31 - 1 \cdot 123 = 4 \cdot (277 - 2 \cdot 123) - 1 \cdot 123 =$

$= 4 \cdot 277 - 9 \cdot 123$

$1 = -9 \cdot 123 + 4 \cdot 277$

" $r = -9$ " $s = 4$

Př.: Eukl. algoritmem najděte $NSD(a, b)$

a také najděte Bezoutovy koeficienty.

$NSD(14039, 1529) = ?$ $= r \cdot 14039 + s \cdot 1529$

$r = ?, s = ?$

$$14039 = 9 \cdot 1529 + 278$$
$$1529 = 5 \cdot 278 + 139$$
$$278 = 2 \cdot 139 + 0$$

$$NSD(14039, 1529) = 139 = 1529 - 5 \cdot 278 =$$
$$= 1529 - 5 \cdot (14039 - 9 \cdot 1529) =$$
$$= \underbrace{-5}_{\parallel} \cdot 14039 + \underbrace{46}_{\parallel} \cdot 1529$$
$$r = (-5) \qquad s = 46$$

Dále
- Eukleidův Algoritmus
- Bezoutovy koeficienty
- Hledání inverze
- Řešení lin. kongruencí
- Aplikace
  - rodné číslo
  - UPC kód
  - ISBN 10 kód
  - a jiné kódy.

Př.: Najděte NSD(196, 14) a zapište jej jako lineární kombinaci 196 a 14.

$196 = 140 + 56 = 10 \cdot 14 + 4 \cdot 14 = 14 \cdot 14$

$NSD(196, 14) = 14 = r \cdot 196 + s \cdot 14$

$= \underline{0} \cdot 196 + \underline{1} \cdot 14$

lin. kombinace s koef. 0 a 1.

Př.: Najděte NSD(196, 112) a zapište jej jako lineární kombinaci 196 a 112.

Eukleidův algoritmus

$196 = 1 \cdot 112 + 84$

$112 = 1 \cdot 84 + 28$

$84 = 3 \cdot 28 + 0$

$NSD(196, 112) = 28$

chceme zapsat

$28 = r \cdot 196 + s \cdot 112$

hledáme r a s

Nalezení bezoutových koeficientů r, s zpětným dosazením z Eukleid alg.

$28 = 112 - 1 \cdot 84 =$

$= 112 - 1 \cdot (196 - 1 \cdot 112) =$

$= 112 - 196 + 112 = \underbrace{(-1)}_{r} \cdot 196 + \underbrace{2}_{s} \cdot 112 = 28$

Poznámka: $k \cdot 196 + l \cdot 112 = 28 \cdot (k \cdot 7 + l \cdot 4)$

$NSD(196, 112) = 28$ je nejmenší z lin. kombinací, kde k a l jsou bezoutovy koeficienty.

Př: Najděte NSD(228, 54) + koeficienty

$228 = 4 \cdot 54 + 12$

$54 = 4 \cdot 12 + 6$

$12 = 2 \cdot 6 + 0$

$NSD(228, 54) = 6$

$6 = r \cdot 228 + s \cdot 54$

zpětným dosazením

$6 = 54 - 4 \cdot 12 = 54 - 4 \cdot (228 - 4 \cdot 54) =$

$= 54 + 16 \cdot 54 - 4 \cdot 228 = \underbrace{-4}_{r} \cdot 228 + \underbrace{17}_{s} 54$

Př: Najděte inverzi k číslu 5 modulo 13.

Inverze k a je $\bar{a}$ takové, že $a \cdot \bar{a} \equiv 1 \pmod m$.

Platí: $\bar{a}$ existuje jestliže $NSD(a, m) = 1$

z Bezout. věty je-li $NSD(13, 5) = 1$ pak

$r \cdot 13 + s \cdot 5 = 1 \Rightarrow s \cdot 5 \equiv 1 \pmod{13}$

a tedy koef. s je inverze.

Eukl. alg.

$13 = 2 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$NSD(13, 5) = 1$

$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) =$

$= 2 \cdot 3 - 1 \cdot 5 = 2 \cdot (13 - 2 \cdot 5) - 1 \cdot 5 =$

$= \underbrace{-5}_{s} 5 + \underbrace{2}_{r} 13$

$-5 \cdot 5 + 2 \cdot 13 \equiv 1 \pmod{13}$

$-5 \cdot 5 \equiv 1 \pmod{13}$

$13 \cdot 5 - 5 \cdot 5 \equiv 1 \pmod{13}$

$8 \cdot 5 \equiv 1 \pmod{13}$ $\Rightarrow$ inverze k 5 je 8. mod 13

Zk: $5 \cdot 8 = 40$, $40 = 3 \cdot 13 + 1$

Poz.: možné úpravy kongruencí: sčítat, násobit prostějším, dělit číslem nesoudělným s m, dělit číslem soudělným s m včetně m. (podrobněji viz přednáška)

Př.: Najděte inverzi čísla 68 mod 17.

tj. $\bar{a} = ?$ takové, že $\bar{a} \cdot 68 \equiv 1 \pmod{17}$

ale $68 = 17 \cdot 4$ a nelze zjednodušit kongruenci

$\bar{a} \cdot 17 \cdot 4 \equiv 1 \pmod{17}$ ← kongruence nemá řešení.

$\bar{a}$ - neexistuje

$NSD(68, 17) = 17$

$\forall k \in \mathbb{Z}$ platí $k \cdot 17 \cdot 4 \equiv 0 \pmod{17}$

Platí, je-li $NSD(a, b) \neq 1$ $\Rightarrow$ $\bar{a}$ modulo b neexistuje.

Př.: Najděte $\bar{a}$ k $a = 68$ modulo 16.

$a = 68$, $m = 16$ pak $NSD(68, 16) = 4$

$68 = 4 \cdot 16 + 4$

$16 = 4 \cdot 4 + 0$

$\bar{a} \cdot 68 \equiv 1 \pmod{16}$

$\bar{a}(4 \cdot 16 + 4) \equiv 1 \pmod{16}$

$\bar{a} \cdot 4 \not\equiv 1 \pmod{16}$

násobky 4 - vždy sudé číslo mod sudé číslo sudé zbytky

Př.: Najděte inverzi k 68 mod 15.

$NSD(68, 15) = 1 \Rightarrow$ ā existuje

Potř. bezout. koef.

$68 = 4 \cdot 15 + 8$

$15 = 1 \cdot 8 + 7$

$8 = 1 \cdot 7 + 1$

$7 = 7 \cdot 1 + 0$

zpětné dosazení

$1 = 8 - 1 \cdot 7 = 8 - 1 \cdot (15 - 1 \cdot 8) =$

$= 2 \cdot 8 - 1 \cdot 15 = 2 \cdot (68 - 4 \cdot 15) - 1 \cdot 15 =$

$= 2 \cdot 68 - 9 \cdot 15$

ā

$2 \cdot 68 - 9 \cdot 15 \equiv 1 \pmod{15}$

$2 \cdot 68 \equiv 1 \pmod{15}$

68, 8 – stejná zb. tř. modulo 15

$2 \cdot (4 \cdot 15 + 8) \equiv 1 \pmod{15} \Rightarrow 2 \cdot 8 \equiv 1 \pmod{15}$

zkouška: $2 \cdot 68 = 136 \doteq 120 + 16 \equiv 16 \pmod{15}$

$16 = 15 + 1 \equiv 1 \pmod{15}$

tj. 2 je $\overline{68} \pmod{15}$

a stejně 2 je $\bar{8} \pmod{15}$

Lineární kongruence

$ax \equiv b \pmod{m}$

$x = ?$

Př.: Najděte řešení kongruence

$x \equiv 21 \pmod{9}$

Můžeme zjednodušit.

$x \equiv 2 \cdot 9 + 3 \pmod{9}$

$x \equiv 3 \pmod{9}$

$x = \ldots -24, -15, -6, 3, 12, 21, 30, 39, \ldots$

stručnější zápis $x = 9 \cdot k + 3, \; k \in \mathbb{Z}$

Př.: Vyřešte kongruenci

$x \equiv -93 \pmod{11}$

$x \equiv -99 + 6 \pmod{11}$

$x \equiv 6 \pmod{11}$

Řešení:

$x = \ldots -16, -5, 6, 17, 28, 39$

$x = 11 \cdot k + 6, \quad k \in \mathbb{Z}$

Př.: Řešte kongruenci

a) $2x \equiv 34 \pmod{8}$

lze dělit 2 (včetně modulu)

$x \equiv 17 \pmod{4}$

$x \equiv 16 + 1 \pmod{4}$

$x \equiv 4 \cdot 4 + 1 \pmod{4}$

$x \equiv 1 \pmod{4} \Rightarrow x = 4k + 1, \quad k \in \mathbb{Z}$

$a \cdot c \equiv b \cdot c \pmod{m \cdot c}$

$a \cdot c \equiv b \cdot c \pmod{m}$ pro $NSD(c, m) = 1$

b) $2x \equiv 33 \pmod{8}$

Krátit nelze, zjednodušíme:

$2x \equiv 32 + 1 \pmod{8}$

$2x \equiv 4 \cdot 8 + 1 \pmod{8}$

$2x \equiv 1 \pmod{8}$ → řešením by bylo x takové, že $2 \cdot x \equiv 1$ tj. $x = \bar{2}$ ← inverze

Ale $\bar{2} \pmod{8}$ neexistuje, protože $NSD(8, 2) = 2 \neq 1$

Kongruence nemá řešení!