Celá čísla a dělitelnost

- dělitelnost, dělení se zbytkem
- největší společný dělitel, Euklidův alg.
- Bezoutova věta
- nesoudělnost
- prvočísla, rozklad na prv.

Diofantické rovnice

$$2k + 5l = n \qquad n \text{ pevné}, k, l \text{ prom.}$$

k, l hledáme celočíselné

$n = 1: \; k = -2, l = 1; \; k = 3, l = -1; \; \ldots$

$n = 2: \; k = 1, l = 0;$

Dělitelnost

a, b celá čísla

a <u>dělí</u> b $\quad a|b$ .... existuje celé c tak, že $ac = b$

($a|0$ vždy, i když $a = 0$)

$a|b \wedge b|c \Rightarrow a|c, \quad a|a$

$a|b \wedge a|c \Rightarrow a|b+c, \; a|b-c$

$a|b \Rightarrow a|-b, \; -a|b, \; -a|-b$

$c \neq 0 \Rightarrow (a|b \Leftrightarrow ac|bc)$

Př. Pro která $n \in \mathbb{N}$ platí, že n^2+1 je dělitelné 3?

$3k = n^2+1$

$n = 3l$ $\quad 3k = (3l)^2+1 = \underbrace{9l^2}+1$

$3(k-3l^2) = 1$

nemá řešení

$n = 3l+1$ $\quad 3k = (3l+1)^2+1 = 3(\ldots)+2$

$n = 3l+2$ $\quad 3k = (3l+2)^2+1 = 3(\ \ )+5$ $\quad \uparrow 3+2$

V. (o dělení se zbytkem)
Pro lib. čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$ a $r \in \{0, 1, \ldots, m-1\}$ taková, že $a = qm + r$.

D. Indukcí, postupné odečítání m

I. $a < m \Rightarrow r = a,\ q = 0$

II. $a - m$ ✓, dokážeme pro a

q .... (neúplný) podíl
r .... zbytek

Největší společný dělitel

Pro a, b definujeme NSD jako číslo $m \geq 0$:

- $m | a$, $m | b$
- $n | a \wedge n | b \Rightarrow n | m$

Pozn. NSD je určen jednoznačně.

Označení: (a,b)

Nejmenší společný násobek $[a,b] = m \geq 0$

- $a|m$, $b|m$
- $a|n \wedge b|n \Rightarrow m|n$

Rozšíření pro více čísel:

$$(a_1, a_2, \dots, a_n) = ((a_1, a_2), a_3, \dots, a_n) =$$
$$= (((a_1, a_2), a_3), a_4, \dots, a_n)$$
$$(a,b) = (b,a)$$
$$((a,b),c) = (a,(b,c))$$

Eukleidův algoritmus pro nalezení NSD

- vstup a, b, $|a| \geq |b|$
- počítáme zbytek po $a:b$ $\quad b, r$
- konec $r=0$, NSD je předposlední člen posloupnosti

$a = 10175$, $b = 2277$ $\qquad 4b = 9108$

$r_3 = 6 r_4 + 0$

$a = 4b + 1067 \leftarrow r_1$ $\qquad 2r_1 = 2134$

$b = 2r_1 + 143 \leftarrow r_2$ $\qquad 7r_2 = 1001$ $\qquad (a,b) = 11$

$r_1 = 7r_2 + 66 \leftarrow r_3$ $\qquad 2 \cdot 66 = 132$

$r_2 = 2r_3 + 11 \leftarrow r_4$ $\qquad 6 \cdot 11 = 66$

$r_1 = a - 4b$

$r_2 = b - r_1 = b - (a - 4b)$
$= 5b - a$

$\vdots$

Bezoutova věta Pro lib. $a,b \in \mathbb{Z}$ existuje jejich NSD a čísla $k,l \in \mathbb{Z}$ tak, že $ak + bl = (a,b)$

Nejmenší společný násobek: $(a,b)\cdot[a,b] = |a \cdot b|$

náznak důkazu:

$$a = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot \ldots \cdot p_m^{\alpha_m}$$
$$b = p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot \ldots \cdot p_m^{\beta_m}$$
$$(a,b) = p_1^{\min(\alpha_1,\beta_1)}\cdot \ldots \cdot p_m^{\min(\alpha_m,\beta_m)}$$
$$[a,b] = p_1^{\max(\alpha_1,\beta_1)}\cdot \ldots \cdot p_m^{\max(\alpha_m,\beta_m)}$$

nesoudělnost a,b nesoud. .... $(a,b)=1$

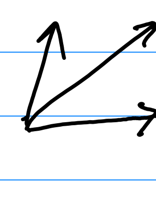
$a_1,\ldots,a_m$ nesoud. ... $(a_1,\ldots,a_m)=1$

-||- podvou nesoud.: $(a_i,a_j)=1$ pro lib. $i \neq j$ z $\{1,\ldots,m\}$

$2,6,9$ $\quad (2,6,9) = (2,9) = 1$

$(2,6) = 2 \neq 1$

$(6,9) = 3 \neq 1$



- $(ac,bc) = (a,b)\cdot c$
- $a|bc \wedge (a,b)=1 \Rightarrow a|c$
- $d=(a,b) \Leftrightarrow \exists q_1,q_2 \in \mathbb{N}$ $a=dq_1, b=dq_2$, $(q_1,q_2)=1$

Prvočísla #1

- přirozené číslo, které je dělitelné pouze sebou samým a jedničkou (má právě 2 dělitele)
- je jich ∞ mnoho

  $p_1 p_2 \dots p_n + 1$ je to zase prvočíslo
  spor

Základní věta aritmetiky

Libovolné přirozené číslo $n \geq 2$ lze jednoznačně vyjádřit jako součin prvočísel.

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$$

$$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$$

$$\underbrace{(1,3,2)} \rightsquigarrow 2^1 \cdot 3^3 \cdot 5^2 = \dots$$

$$\underset{1}{+}, \underset{2}{\forall}, \underset{3}{(}, \dots ?$$