MATH 4. 3. 2011

Počítání v celých číslech = počítání v $\mathbb{Z}$

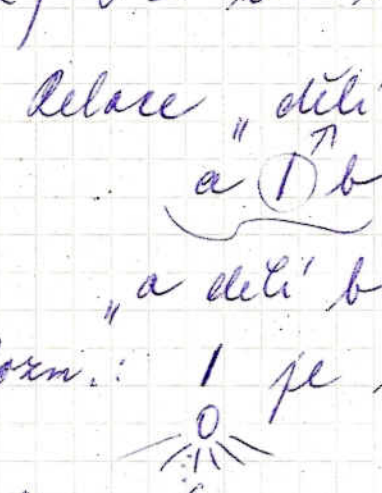
V: o dělení se zbytkem pro libovolná $a, b \in \mathbb{Z}$, $b \neq 0$
existuje jediné $q, r \in \mathbb{Z}$ tak, že
1) $a = q \cdot b + r$
2) $0 \leq r < b$

Def Relace „dělí" v $\mathbb{Z}$

$$a \mid b \text{ iff } a = k \cdot b \text{ pro } k \in \mathbb{Z}$$

„a dělí b beze zbytku"

Pozn.: $\mid$ je relace uspořádání na $\mathbb{N}$



nula je nejvyšší ← je dělitelná všem

nejmenší společný dělitel

prvočísla

nejnižší

Def: Prvočíslo ~~p ∈~~ je $p \in \mathbb{N}$, $p \geq 2$, kde pouze $1 \mid p$ a $p \mid p$

V: Každé $n \geq 2$ lze napsat ~~jednozn~~ jednoznačně jako součin prvočísel

$$n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}, \quad \underbrace{p_1 < p_2 < p_3 < \ldots p_r}_{\text{prvočísla}}$$

Dk existence prvočíselného rozkladu

provádí se silnou indukcí

1) $n = 2$ to je prvočíslo

2) indukč. předpokl. - pro všechna k, $2 \le k < n$ existuje prvočís. rozklad

chci rozložit n

$n = (n-1) + 1$ tento rozklad (= slabá indukce) nestačí

$n =$ $= p$ je prvočíslo $\Rightarrow$ hotovo

$= a \cdot b$, tj. složené číslo, $2 \le a \le b < n$

$\Rightarrow$ dle ind. p. $a = \prod p_i^{k_i}$, $b = \prod q_i^{k_i}$

$n = \left(\prod p_i^{k_i}\right)\left(\prod q_i^{k_i}\right)$

= dám stejná prvočísla k sobě a mám prvočís. rozklad pro n.

jednoznačnost - bez Dk

Def) nejmenší společný násobek pro a, b
největší společný dělitel pro a, b (GCD)

GCD (a, b) = d takové, že 1) $d | a$, $d | b$
2) když $c | a$, $c | b$, pak $c | d$
3) $d > 0$, $d \in \mathbb{N}$ (protože $-d$ také splňuje 1) a 2))

Jak najít GCD(a, b), $b \leq a$?

1) přes prvočíselný rozklad = součin společných prvočísel ve společné mocnině

$$\left.\begin{array}{l} a = 2^2 \cdot 5 \\ b = 2^3 \cdot 7 \end{array}\right\} \rightarrow GCD = 2^2$$

Pro velká čísla je to v dohledném čase nepoužitelné, protože najít ~~najít~~ prvočís. rozklad je exponenciálně náročné (v závislosti na počtu cifer v n)

2) Eukleidův algoritmus
- je rekurzivní a) přímý výpočet, když
$a = k \cdot b \rightarrow b = GCD(a, b)$
ANO, protože $b | b$ a nic víc b nedělí.
b) rekurzivní volání, když
$a = kb + r$, $0 < r < b$
hledám GCD (b, r)

PROČ to funguje?
Protože dvojice a, b má společné dělitele (všechny) jako dvojice b, z.
Tedy i GCD je stejné.
Např. pokud $2/a$, $2/b$ $\Rightarrow$
$z = a - kb = \text{sudé} \Rightarrow 2/z$

sudé sudé

a naopak.

- Terminace $= b > z_1 > z_2 \ldots \geq 0$
  jednou prostě zbyde 0
- Parciální korektnost - slabá indukce
  podle počtu kroků v algoritmu
  1 krok - viz přímý výpočet
  indukč. předp. pro libovolný ~~alg~~ algoritmus v k krocích počítá GCD
  k + 1 kroků → 1 rekurz. volání zachová GCD (viz rekurz. volání)

Časová složitost - průměrná (= lineární)
Počet kroků ≤ 5. počet cifer menšího čísla.
(=lineární 5.n)

PŘ GCD $(121, 38)$

① $121 = \underline{\;3\;} \cdot 38 + \underline{\;7\;}$

② $38 = \underline{\;5\;} \cdot 7 + \underline{\;3\;}$

③ $7 = \underline{\;2\;} \cdot 3 + \underline{\;1\;}$

④ $3 = \underline{\;3\;} \cdot 1 + \underline{\;0\;}$ STOP

GCD $= 1$ → říkáme, že čísla jsou <u>nesoudělná</u>

V: <u>Bezoutova věta</u>

~~GCD je~~ GCD(a,b) je celočíselnou kombinací a, b.

$$GCD(a,b) = k \cdot a + l \cdot b, \quad k, l \in \mathbb{Z}$$

Dk: Zpětné použití rovnic Euklid. algoritmu viz PŘ GCD$(121, 38)$

$$1 = GCD(121,38) \underset{③}{=} 7 - 2 \cdot 3 \underset{②}{=} 7 - 2(38 - 5 \cdot 7) =$$

$$= (-2) \cdot 38 + 11 \cdot 7 \underset{①}{=} (-2) \cdot 38 + 11(121 - 3 \cdot 38) =$$

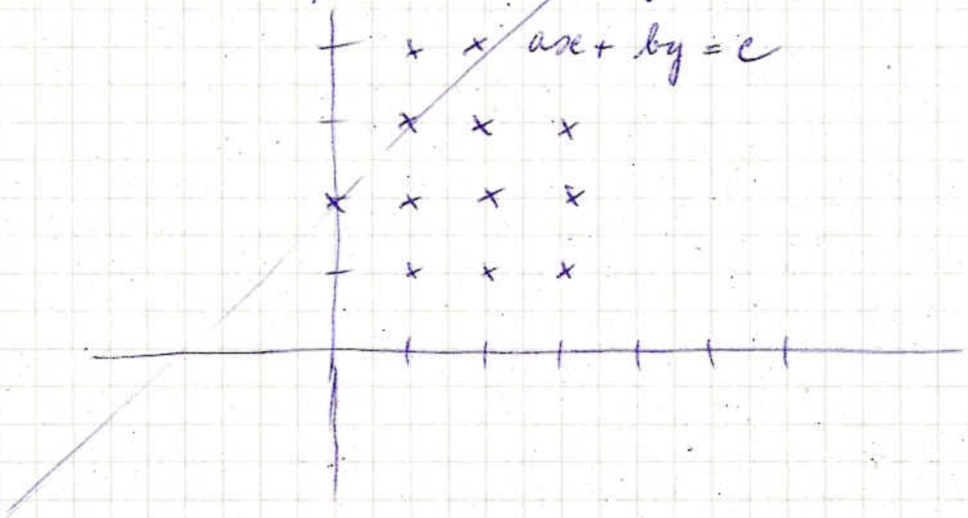
$$= \underbrace{11}_{k} \cdot 121 - \underbrace{35}_{l} \cdot 38$$

našli jsme 1 celočíselné řešení $121x + 38y = 1$.

Diofantés → <u>Diofantické rovnice</u>

$ax + by = c$, kde $a, b, c \in \mathbb{Z}$
hledá se x, y v oboru $\mathbb{Z}$

Protne přímka body $[x, y]$ s celočísel. souřadnicemi?



ne vždy $\quad 2x + 4y = 7$
pro $x, y \in \mathbb{Z}$ je nalevo sudé číslo $\neq 7$

→ aby exist. řešení v $\mathbb{Z}$, tak musí $GCD(a, b)$ dělit c
Když $GCD(a, b) \mid c$, tak najdeme celočís. řešení přes Euklid. alg.

Tvrzení: $ax + by = c$ má řešení v $\mathbb{Z}$ iff $GCD(a, b) \mid c$, pak je nekonečně řešení v $\mathbb{Z}$ tvarem

$$(x, y) = \underbrace{(x_p, y_p)}_{\text{partikul. řešení Euklid}} + k\underbrace{(x_0, y_0)}_{\text{řeš. hom. rov. nesoudělné (= nejkratší celočíselný směrový vektor)}}$$

(PŘ) Řešte v $\mathbb{Z}$ $54x + 150y = 18$

1. krok $GCD(54, 150)$ ← Eukleid

① $150 = 2 \cdot 54 + 42$

② $54 = 42 + 12$

③ $42 = 12 \cdot 3 + 6$

④ $12 = 6 \cdot 2 + 0$ STOP

$6 / 18$ → bude exist. řešení v $\mathbb{Z}$

Rozšířený Euklidův algoritmus (pro $GCD(a, b)$)
- v každém kroku vyjádříme ~~aktuá~~ aktuální zbytek jako kombinaci a, b
⇝ v posledním kroku nakombinuji GCD

$a = 150, \; b = 54$

① $42 = a - 2b$ $\cancel{(150 - 2 \cdot 54)}$

② $12 = 54 - 42 = b - (a - 2b) = (-a) + 3b$

③ $GCD = 6 = 42 - 3 \cdot 12 = (a - 2b) - 3(-a + 3b)$
$= 4a - 11b$

Výhoda - stačí si pamatovat kombinaci dvou předchozích zbytků.

Partikul. řešení $18 = 3 \cdot 6 = 3(4a - 11b) = 12a - 33b$
$= \underbrace{12}_{y_p} \cdot \underbrace{150}_{} - \underbrace{33}_{x_p} \cdot \underbrace{54}_{}$

$(x_p, y_p) = (-33, 12)$

nesoudělné řeš. homog. rov.

$$54x + 150y = 0 \quad / : GCD = 6$$
$$9x + 25y = 0$$
$$(x_0, y_0) = (25, -9)$$

nesoudělné

všechna řešení v $\mathbb{Z}$

$$(x, y) = (-33, 12) + k(25, -9), \text{ kde } k \in \mathbb{Z}$$

Pozn. $3x + 4y = 2$

shodou $GCD(3, 4) = 1$

$1 | 2 \rightarrow$ existuje řeš. v $\mathbb{Z}$

partik. řeš. $x_p = 2$, $y_p = -1$

$\rightsquigarrow$ netřeba Eukleid

nesouděl. homog. rov. $x_0 = 4$, $y_0 = -3$

všechna řešení $(x, y) = (2, -1) + k(4, -3)$, $k \in \mathbb{Z}$