$3^2 + 4^2 = 9 + 16 = 25 = 5^2$

Definice $a, b \in \mathbb{Z}$

$a \mid b$, jestliže $\exists k \; b = ka$

$a \mid 0$ 0 dělí pouze 0

$a \mid b \wedge b \mid c \Rightarrow a \mid c$

$b = ka \wedge c = lb \Rightarrow c = lb = lka$

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

$b = ka$ $\quad$ $bc = lac$

(2)

Dělitelnost n^2+1 číslem 3

$n = 3k + r \qquad r = 0, 1, 2$

$n^2+1 = (3k+r)^2 + 1 = \underbrace{9k^2 + 6kr}_{\text{dělitelné } 3} + \underbrace{r^2+1}$

$0 + 1$
$1 + 1$
$4 + 1$

n^2+1 není nikdy dělitelné 3

Pro které n platí $n-1 \mid n^2+1$.

$n^2+1 = n^2 - 1 + 2 = \underbrace{(n-1)(n+1)}_{\text{dělitelné } n-1} + 2$

2/10

$n-1 \mid n^2+1 \iff n-1 \mid 2 \qquad n = 2 \text{ nebo } 3$

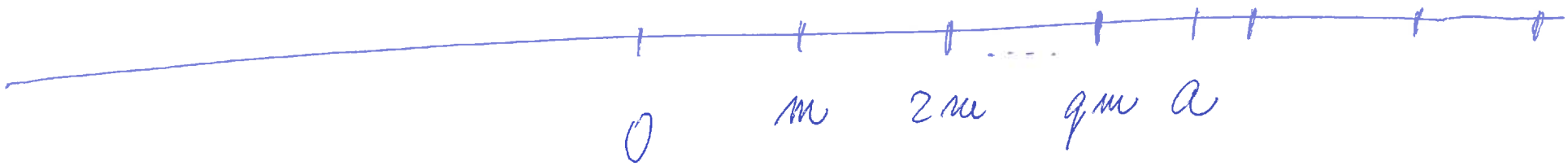
a, m

$\exists! q \in \mathbb{Z} \quad \exists! r \in [0, m-1] \cap \mathbb{Z}$

$a = q m + r$ → zbytek

↓

celočíselný podíl



q největší takové, že $qm \leq a$

$r = a - qm$

$r = 0, 1, \ldots m-1$

$$a = qm + r$$

$$\frac{a}{m} = q + \frac{r}{m} \qquad \frac{r}{m} \in [0,1)$$

Příklad

$$a = q_1 m + 1$$

$$b = q_2 m + 1$$

$$ab = (q_1 m + 1)(q_2 m + 1) = q_1 q_2 m^2 + (q_1 + q_2) m + 1$$

Největší společný dělitel čísel a_1, a_2

značení (a_1, a_2) gcd

d je společný dělitel čísel a_1, a_2

$$d \mid a_1 \wedge d \mid a_2$$

d je největší spol. dělitel čísel a_1, a_2, jestliže každý další dělitel

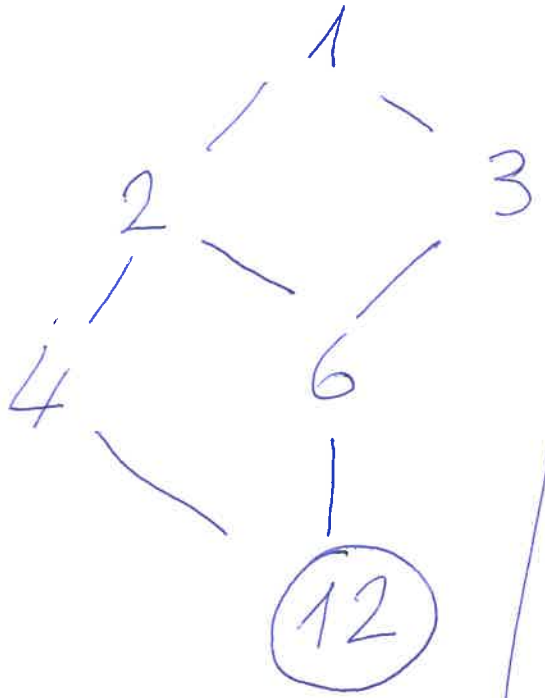
$$d_1 \mid a_1 \wedge d_1 \mid a_2 \Rightarrow d_1 \mid d$$

$a_1 = 36 \qquad a_2 = 24$

společní dělitelé

$1, 2, 3, 4, 6, 12,$

$(36, 24) = 12$



$\Leftarrow \quad \geq$

$a_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

$a_2 = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$

$(a_1, a_2) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots$

Nejmenší společný násobek

Nejmenší společný násobek přirozených čísel a_1, a_2

a_1 / m a a_2 / m

Nejmenší společný násobek přirozených čísel m, které dělí všechny ostatní společné násobky

$[a_1, a_2]$

$[24, 36] = 12 \cdot 6 = 72$

$12 \cdot 2 \quad 12 \cdot 3$

$(a_1, a_2) \cdot [a_1, a_2] = a_1 \cdot a_2$.

$a_1 = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$

$a_2 = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$

$[a_1, a_2] = p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n, \beta_n)}$

$p_1^{\alpha_1+\beta_1} \, p_2^{\alpha_2+\beta_2} \cdots = a_1 \cdot a_2$.

Euklidův algoritmus

Řešíme (a_1, a_2)

$$a_1 = q_1 a_2 + a_3 \qquad 0 \le a_3 \le a_2 - 1$$

$$a_2 = q_2 a_3 + a_4 \qquad 0 \le a_4 \le a_3 - 1$$

$$a_{k-1} = q_{k-1} a_k + a_{k+1}$$

$$a_k = q_k \boxed{a_{k+1}} + a_{k+2}$$

$$\| \; 0$$

Tvrzení $a_{k+1} = (a_1, a_2)$

Důkaz: $d \mid a_1 \wedge d \mid a_2 \Rightarrow d \mid a_3 \Rightarrow d \mid a_4 \Rightarrow \dots d \mid a_{k+1}$

$a_{k+1} \mid a_k \Rightarrow a_{k+1} \mid a_{k-1} \Rightarrow \dots\dots a_{k+1} \mid a_2 \Rightarrow a_{k+1} \mid a_1$

$(10175, 2277)$

$10175 = 4 \cdot 2277 + 1067$

$2277 = 2 \cdot 1067 + 143$

$1067 = 7 \cdot 143 + 66$

$143 = 2 \cdot 66 + 11$

$66 = 6 \cdot \boxed{11} + 0$

10 175
9 108

1067
2277
2134

143

1001

$(10175, 2277) = 11$ Zkrácení

$(10175, 2277) = (2277, 1067) = (1067, 143) =$

$= (143, 66) = (66, 11) = 11$

$$(a, b) = (b, a - kb)$$

Euklidův algoritmus je nejčastější důkazem existence NSD.

Bezoutova věta

a, b celá čísla $k \in \mathbb{Z}$ a $l \in \mathbb{Z}$,

pak $ak + bl = (a, b)$

$$a_1 = q_1 a_2 + a_3$$

$$a_2 = q_2 a_3 + a_4$$

$$\vdots$$

$$a_{k-2} = q_{k-2} a_{k-1} + a_k$$

$$a_{k-1} = q_{k-1} a_k + \boxed{a_{k+1}}$$

$$a_k = q_k a_{k+1}$$

$$\| \quad (a_1, a_2)$$

$$a_{k+1} = -q_{k-1} a_k + a_{k-1}$$

$$= -q_{k-1}(a_{k-2} - q_{k-2} a_{k-1}) + a_{k-1}$$

$$= k_1 a_{k-2} + l_1 a_{k-1}$$

$$\vdots$$

$$(a_1, a_2) = a_{k+1} = k a_1 + l a_2$$

Praktický výpočet

$(\underset{a}{999}, \underset{b}{598})$

k	l	ka + lb
1	0	999
0	1	598
1	-1	401
-1	2	197
3	-5	7
-61	102	57
-85	142	1

$-61 - 24$

$102 + 40$

$(-85) \cdot 999 + 142 \cdot 598 = 1$

$$[a, b] \cdot (a, b) = |a \cdot b|$$

$a > 0, b > 0$

a. Důkaz

Dokážeme, že $\frac{a \cdot b}{(a,b)}$ je ~~nejm.~~ nejm. spol. nás.

$(a,b) = d \qquad a = kd, \quad b = ld$

$$ab = kld^2$$

$$\frac{ab}{d} = kld$$

$a \mid kld$

$b \mid kld$

$\frac{a \cdot b}{d}$ je společný násobek.

Нехай n је произвољан природан број такав да $\frac{ab}{d} \mid n$.

$ak + bl = d$ Безуова једнакост

$b \mid n$ и $a \mid n$

$$\mathbb{Z} \ni \underbrace{\frac{n}{b}}_{\in\mathbb{Z}} k + \underbrace{\frac{n}{a}}_{\in\mathbb{Z}} l = \frac{nak + nbl}{ab} = \frac{n(ak+bl)}{ab} = \frac{n}{\frac{ab}{d}} \in \mathbb{Z}$$

$(ak+bl = d)$

$\frac{ab}{d} \mid n$

a, b nesoudělná

$$(a, b) = 1$$

$a_1, a_2, \ldots a_n$ nesoudělná

$$(a_1, a_2, \ldots a_n) = 1$$

$a_1, a_2, \ldots a_n$ po dvou nesoudělná

$$(a_i, a_j) = 1 \text{ pro } i \neq j$$

$$(ac, bc) = c(a, b)$$

$$(a, b) = ak + bl$$

$$c(a, b) = cak + cbl$$

$$c(a, b) \mid (ac, bc)$$

$(a, b) \mid a$, $(a, b) \mid b$ $\Rightarrow$ $c(a, b) \mid ac$

$c(a, b) \mid bc$

$c(a, b)$ je spol. delitelj čísel ac, bc

$$(a, b) = ak + bl$$

$$\boxed{c(a, b) = \textcircled{a}ck + \textcircled{b}cl} \Rightarrow c(a, b) = NSD$$

ac, bc

Jednině

$a \mid bc \wedge (a,b) = 1 \Rightarrow a \mid c$

$1 = ak + bl \quad / \cdot c$

$c = ack + bcl$

$a \mid ac \quad a \mid bc \Rightarrow a \mid c$

Adam Spencer

Why I fell in love with maths

prime numbers

2013

Eukleidova věta o prvočíslech

$p \geq 2$ je prvočíslo $\Leftrightarrow$ $\forall a, b \in \mathbb{Z}$

$p \mid ab \Rightarrow p \mid a$ nebo $p \mid b$

$\Rightarrow$ p je prvočíslo

$p \mid ab$ p nedělí a $(a, p) = 1$

$kp + la = 1 \quad / \cdot b$

$kbp + lab = b$

dělitelné p $\quad$ $p \mid ab$ $\Rightarrow$ $p \mid b$

$\Leftarrow$ Ovemo ekv. še p je praštevilo

$p = ab \Rightarrow p \mid ab \Rightarrow p \mid a \;\vee\; p \mid b$

$p = a \qquad p = b$

$a, b > 0$

$b = 1 \qquad a = 1$

p ~~ab~~ je očitno res tako $p \cdot 1$.

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ jednoznačno

$= p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} \Rightarrow \alpha_1 = \beta_1$

$\alpha_2 = \beta_2$

$p_2 (\quad)$