$6 = 1+2+3$

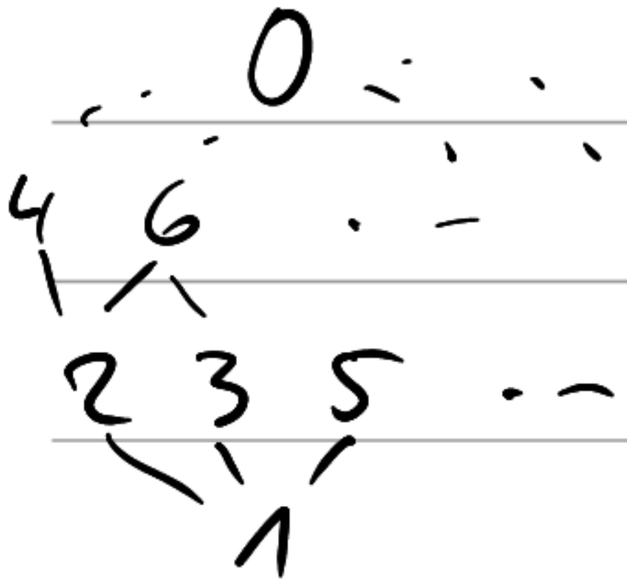
$28 = 1+2+4+7+14$

$16 \cdot 31 = \ldots$

$x^2+y^2=z^2$ $\quad$ $3^2+4^2=5^2$

$a|b$ $\quad$ a dělí b $\quad$ b je dělitelné a

b je násobek a



$n = 3k \Rightarrow n^2+1 = (3k)^2+1$

$= 9k^2+1$

$= 3(3k^2)+1$ Zb. 1

$n = 3k+1 \Rightarrow n^2+1 = (3k+1)^2+1$

$= 9k^2+6k+1+1$

$= 3(3k^2+2k)+2$ Zb. 2

$n = 3k+2 \Rightarrow n^2+1 = (3k+2)^2+1$

$= 9k^2+12k+4+1$

$= 3(3k^2+4k+1)+2$ Zb. 2

$n+1 \mid n^2+1$

$n+1 \mid n^2-1$ $\quad n \in \mathbb{Z}$ $\Rightarrow$ $n+1 \mid (n^2+1)-(n^2-1) = 2$

$n+1 \in \{-2,-1,1,2\}$

$n \in \{-3,-2,0,1\}$

$(-2) \mod 5$ $\qquad -2 = (-1)\cdot 5 + 3$

$a = q \cdot m + r$ $\qquad \frac{a}{m} = q + \frac{r}{m}$

$\frac{-2}{5} = -1 + \frac{3}{5}$

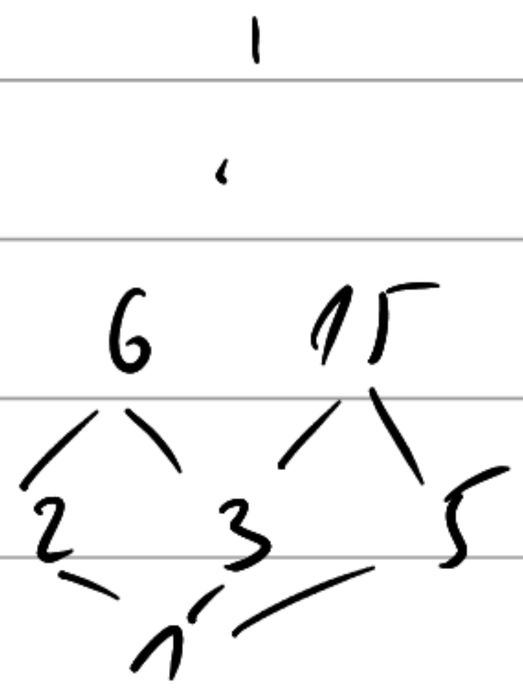
$a = k \cdot m + r$

$b = l \cdot m + s$

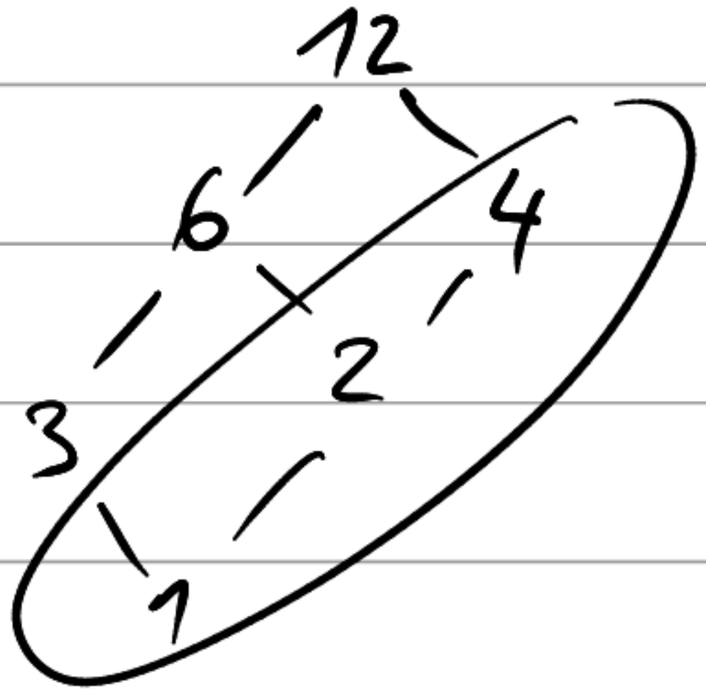
$\Rightarrow \quad a \cdot b = (k \cdot m + r) \cdot (l \cdot m + s)$

$= k \cdot l \cdot m^2 + k \cdot m \cdot s + l \cdot m \cdot r + rs$

$= (k \cdot l \cdot m + k \cdot s + l \cdot r) \cdot m + rs$



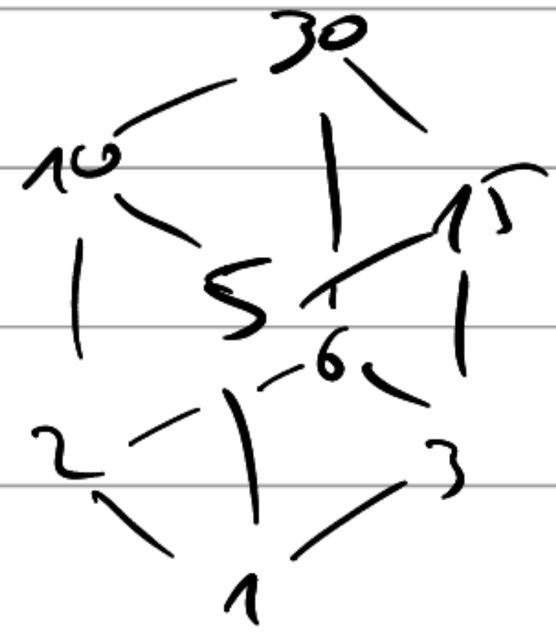
$12 = 2^2 \cdot 3$



(926)

$64 = 2^6$

$30 = 2 \cdot 3 \cdot 5$



$(10175, 2277) = ?$

$10175 = 4 \cdot 2277 + 1067$

$2277 = 2 \cdot 1067 + 143$

$1067 = 7 \cdot 143 + 66$

$143 = 2 \cdot 66 + 11$

$66 = 6 \cdot 11 + 0$

$\Rightarrow 11 = 1 \cdot 143 - 2 \cdot 66$

$= 1 \cdot 143 - 2 \cdot (1067 - 7 \cdot 143)$

$= -2 \cdot 1067 + 15 \cdot 143$

$= -2 \cdot 1067 + 15 \cdot (2277 - 2 \cdot 1067)$

$= 15 \cdot 2277 - 32 \cdot 1067$

$= 15 \cdot 2277 - 32 \cdot (10175 - 4 \cdot 2277) = -32 \cdot 10175 + 143 \cdot 2277$

NSD = 11

$(a, b) = (a, b - a) = \dots = (a, b - q \cdot a)$

$(n^2 + 1, n + 1) = (2n + 1) = \{1, 2\}$

GCD, prosze

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

$= (66, 143) = (66, 11) = (0, 11) = 11$

$$p_1^{a_1} \cdots p_k^{a_k} \mid p_1^{b_1} \cdots p_k^{b_k}$$

$$\Leftrightarrow a_1 \le b_1 \ \& \ \cdots \ \& \ a_k \le b_k$$

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

$a \mid ac$

$a \mid k \cdot ac + \ell \cdot bc = (\underbrace{ka + \ell b}_{\text{mize byt } 1})c$

Jiná organizace výpočtu (10175, 2277):

10175	2277			
1	0	10175	I	$10175 = 4 \cdot 2277 + 1067$
0	1	2277	II	
1	−4	1067	III	$= I - 4 \cdot II$
−2	9	143	IV	$= II - 2 \cdot III$
15	−67	66	V	$= III - 7 \cdot IV$
−32	143	11	VI	$= IV - 2 \cdot V$
←	✱	0		

$6 = 2 \cdot 3 = 3 \cdot 2$

$= 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3$

$p_1 \mid p_1 \cdots p_r = q_1 \cdots q_n \Rightarrow p_1 \mid q_1 \Rightarrow p_1 = q_1$