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

$n^2-1 = (n+1)(n-1)$

$n+1 \mid 2 = (n^2+1)-(n^2-1)$

$\Rightarrow n+1 = 2$

2 22-13:55

$a = q_1 m + r_1 = q_2 m + r_2$

$(q_1 - q_2)m = r_2 - r_1 = 0$

$\Downarrow$

$q_1 - q_2 = 0$

$r_2 - r_1 \in (-m, m)$

$\Downarrow$ dělí m

$r_2 - r_1 = 0$

2 22-14:16

$m_1 \mid m_2$ a $m_2 \mid m_1$

$m_2 = k m_1$ a $m_1 = \ell m_2$

$m_2 = k m_1 = k\ell m_2$

$\Downarrow m_2 \neq 0$

$1 = k\ell \Rightarrow k = \ell = \pm 1$

2 22-14:26

$3476 = a_1$ $3201 = a_2$

$3476 = 1 \cdot 3201 + 275$ (a_2, a_0)

$3201 = 11 \cdot 275 + 176$

$275 = 1 \cdot 176 + 99$ (a_3, a_4)

$176 = 1 \cdot 99 + 77$

$99 = 1 \cdot 77 + 22$

$77 = 3 \cdot 22 + \boxed{11}$

$22 = 2 \cdot 11$ (a_{k-1})

2 22-14:33

"zbytek" $-\frac{m}{2} < r \leq \frac{m}{2}$

$\Rightarrow$ potřeba pouze lin. mnoho kroků

2 22-14:39

$11 = 1 \cdot 7 + 4$

$7 = 1 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$3 = 3 \cdot 1$

$1 = 1 \cdot 4 - 1 \cdot 3$

$= 1 \cdot 4 - 1 \cdot (7-4)$

$= -1 \cdot 7 + 2 \cdot 4$

$= -1 \cdot 7 + 2 \cdot (11-7)$

$= 2 \cdot 11 - 3 \cdot 7$

2 22-14:45

$(a_1, a_2) = k_1 a_1 + k_2 a_2$

$k(a_1, a_2) = k k_1 a_1 + k k_2 a_2$

naopak: $n = k_1 a_1 + k_2 a_2$

násobky (a_1, a_2)

$\Rightarrow (a_1, a_2) \mid n$

2 22-14:49

chceme: $q = \frac{a_1 \cdot a_2}{(a_1, a_2)}$ je lcm a_1, a_2

$q = a_1 \cdot \frac{a_2}{(a_1, a_2)} \in \mathbb{N}$

$= \frac{a_1}{(a_1, a_2)} \cdot a_2$ ... společný násobek

nechť n je spol. nás. a_1, a_2

ukážeme $q \mid n$

$\frac{a_1 \cdot a_2}{(a_1, a_2)} \mid n \iff a_1 a_2 \mid n \cdot (a_1, a_2)$

Ale $n \cdot (a_1, a_2) = n \cdot (k_1 a_1 + k_2 a_2)$

$= k_1 a_1 n + k_2 a_2 n$

q ... násobek a_2 nás. a_1, a_2

+ sym $\Rightarrow$ platí

2 22-14:53

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

chceme $a \mid c$

$c = c \cdot 1 = c \cdot (k \cdot a + l \cdot b)$ (Bez. lem. na a, b)

$= k \cdot c \cdot a + l \cdot c \cdot b$

dělí a dělí a

tedy $a \mid c$

2 22-15:07

p není prvočíslo

$p = k \cdot l$ $\quad k \neq p$, $k \neq 1$

$p \mid k \cdot l$, ale

$p \nmid k$, $p \nmid l$, protože

$p > k$, $p > l$

2 22-15:17

$p_1 \cdots p_m = q_1 \cdots q_s \quad (*)$

$p_1 \mid p_1 \cdots p_m = q_1 \cdots q_s$

$\Rightarrow p_1 \mid q_i$ pro nějaké i

$p_1 \neq 1 \Rightarrow p_1 = q_i$

$(*)$ vydělíme $p_1 = q_i$

a použijeme indukci

$p_2 \cdots p_m = q_1 \cdots q_{i-1} q_{i+1} \cdots q_s$

2 22-15:25