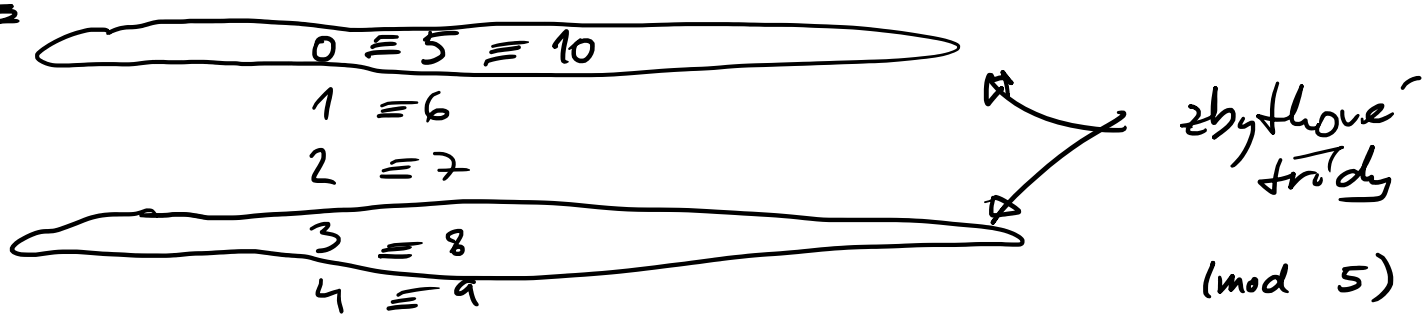


$\equiv$ mod 47 ..... $-21 \equiv 26 \quad (47)$ (+47)

$90 \equiv 43 \quad (47)$

$\equiv$ $m \mid a_1 - b_1$, $m \mid a_2 - b_2$

$\Rightarrow m \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$

$\equiv$ $a_1 = b_1 \rightarrow a_1 a_2 \equiv b_1 a_2 \equiv b_1 b_2$

① · a_2 b_1 · ②

$\equiv$ $a = b \pmod m$ $\xrightarrow{(a,m)=1}$ $a^k \equiv b^k \pmod m$

$k = l \pmod{\varphi(m)}$

0

$\equiv$ $2 \cdot 0 \equiv 2 \cdot 2 \pmod 4 \not\Rightarrow 0 \equiv 2 \pmod 4$

$\Leftarrow$ $m \mid k \cdot a - k \cdot b = k \cdot (a-b) \rightarrow m \mid a-b$

$\uparrow$

$(m, k) = 1$

$\Leftrightarrow$

$a \equiv b \quad (112) \quad \Leftrightarrow \quad a \equiv b \quad (7)$

$a \equiv b \quad (16)$

$112 \mid a-b \quad \Leftrightarrow \quad 7 \mid a-b$

$16 \mid a-b$

$\Leftrightarrow$

$112 \mid (835^5 + 6)^{18} - 1$

$\Leftrightarrow \quad (835^5 + 6)^{18} \equiv 1 \quad (112)$

zjedn. $\Leftrightarrow \quad (835^5 + 6)^{18} \equiv 1 \quad (7)$

$(835^5 + 6)^{18} \equiv 1 \quad (16)$

$835 \equiv 2 \quad (7)$

$835^5 \equiv 2^5 \equiv 32 \equiv 4 \quad (7)$

$835^5 + 6 \equiv 4 + 6 \equiv 3 \quad (7)$

$(835^5 + 6)^{18} \equiv 3^{18} \equiv ((3^2)^3)^3 \quad (7)$

$\equiv (9^3)^3 \equiv (2^3)^3 \equiv 1 \quad (7)$

$\Rightarrow$

$5^{20} \equiv ? \quad (26)$

$5^2 \equiv 25 \equiv -1 \quad (26)$

$5^{20} \equiv (5^2)^{10} \equiv (-1)^{10} \equiv 1 \quad (26)$

$\equiv$

$(a+b)^2 = a^2 + 2ab + b^2 \equiv a^2 + b^2 \quad (2)$

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \equiv a^3 + b^3 \quad (3)$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1

$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{k} a^{p-k} b^k + \dots + b^p$

Chceme: $p \mid \binom{p}{k}$ pro $k = 1, \dots, p-1$

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$$

$=$

$39 \cdot x = 1 \quad (47)$

pouřijeme $(39, 47) = 1$

1	0	47
0	1	39
1	-1	8
-4	5	7
5	-6	1

$5 \cdot 47 - 6 \cdot 39 = 1 \quad / \text{mod } 47$

$5 \cdot \underbrace{47}_{\equiv 0} - 6 \cdot 39 \equiv 1 \quad (47)$

$-6 \cdot 39 \equiv 1 \quad (47)$

$x \equiv -6 \equiv 41$

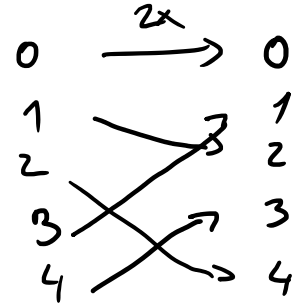
$47x \equiv 0 \quad (47)$ ← platí vždy

$39x \equiv 1 \quad (47)$

$8x \equiv -1$

$7x \equiv 5$

$x \equiv -6$



$(\text{mod } 5)$

$2x \equiv 2y \quad (5)$

$\Rightarrow x \equiv y$

$39x \equiv 41 \quad (47) \qquad / \cdot 39^{-1} \equiv -6$

$(-6) \cdot \underbrace{39} \cdot x \equiv (-6) \cdot 41 \quad (47)$

1

$x \equiv (-6) \cdot 41 \equiv \dots \pmod{47}$

Jinak: $47x \equiv 0 \pmod{47}$

$39x \equiv 41 \equiv -6$

$8x \equiv 6$

$7x \equiv -30 \equiv 17$

$x \equiv -11$

$\Rightarrow$

$8x \equiv 10 \pmod{14}$

$\Rightarrow$

$14x \equiv 0 \pmod{14}$

$8x \equiv 10 \pmod{14}$

$6x \equiv 4 \pmod{14}$

$2x \equiv 6 \pmod{14} \iff x \equiv 3 \pmod{7}$

$0x \equiv -14 \equiv 0 \qquad x \equiv 3 \pmod{14}$

nebo $x \equiv 10 \pmod{14}$