JAKUB LEVÝ

ÚLOHA č. 3

Zvolme $k=2$, $n_1=2$, $n_2=4$. Čísla n_1 a n_2 jsou soudělná $GCD(2,4)=2$.
$n=8$, $H: \mathbb{Z}_8 \to \mathbb{Z}_2 \times \mathbb{Z}_4$, $H(a)=(a \bmod 2, a \bmod 4)$.

$$\left.\begin{array}{ll} H(0)=(0,0) & H(4)=(0,0)=H(0) \\ H(1)=(1,1) & H(5)=(1,1)=H(1) \\ H(2)=(0,2) & H(6)=(0,2)=H(2) \\ H(3)=(1,3) & H(7)=(1,3)=H(3) \end{array}\right\} \text{H není prostá}$$

H není ani „na". $\nexists a \in \mathbb{Z}_8 : H(a) \in \{(0,1),(0,3),(1,0),(1,2)\}$.

ÚLOHA č. 1

Nejprve si převedeme jednotlivé rovnice na kongruence.
$a \bmod 3 = 2 \iff 3 \mid a-2 \iff a \equiv 2 \pmod 3$. Obdobným způsobem pro všechny ostatní rovnice. Dostaneme:

$$\begin{array}{ll} a \equiv 2 \pmod 3 & b \equiv 0 \pmod 3 \\ a \equiv 4 \pmod 5 & b \equiv 2 \pmod 5 \\ a \equiv 4 \pmod 8 & b \equiv 2 \pmod 8 \\ a \equiv 11 \pmod{13} & b \equiv 11 \pmod{13} \end{array}$$

Snadno ověříme, že $\forall x,y \in \{3,5,8,13\}, x \neq y : GCD(x,y)=1$. Tedy můžeme využít Čínskou větu o zbytcích. Nejprve vyřešíme a.

$$a = \underbrace{5\cdot 8\cdot 13}_{\bmod 3} + \underbrace{3\cdot 8\cdot 13}_{\bmod 5} + \underbrace{3\cdot 5\cdot 13}_{\bmod 8} + \underbrace{3\cdot 5\cdot 8}_{\bmod 13}$$

$a \equiv 5\cdot 8\cdot 13 \pmod 3 \iff a \equiv 520 \pmod 3 \iff a \equiv 1 \pmod 3$

$$a = \underbrace{5\cdot 8\cdot 13\cdot 2}_{\bmod 3} + \underbrace{3\cdot 8\cdot 13}_{\bmod 5} + \underbrace{3\cdot 5\cdot 13}_{\bmod 8} + \underbrace{3\cdot 5\cdot 8}_{\bmod 13}$$

$a \equiv 3\cdot 8\cdot 13 \pmod 5 \iff a \equiv 312 \pmod 5 \iff a \equiv 2 \pmod 5$

$$a = \underbrace{5\cdot 8\cdot 13\cdot 2}_{\bmod 3} + \underbrace{3\cdot 8\cdot 13\cdot 2}_{\bmod 5} + \underbrace{3\cdot 5\cdot 13}_{\bmod 8} + \underbrace{3\cdot 5\cdot 8}_{\bmod 13}$$

$a \equiv 3\cdot 5\cdot 13 \pmod 8 \iff a \equiv 195 \pmod 8 \iff a \equiv 3 \pmod 8$

$$a = \overset{\text{mod } 3}{5 \cdot 8 \cdot 13 \cdot 2} + \overset{\text{mod } 5}{3 \cdot 8 \cdot 13 \cdot 2} + \overset{\text{mod } 8}{3 \cdot 5 \cdot 13 \cdot 4} + \overset{\text{mod } 13}{3 \cdot 5 \cdot 8}$$

$$a \equiv 3 \cdot 5 \cdot 8 \pmod{13} \iff a \equiv 120 \pmod{13} \iff a \equiv 3 \pmod{13}$$

$$a = 5 \cdot 8 \cdot 13 \cdot 2 + 3 \cdot 8 \cdot 13 \cdot 2 + 3 \cdot 5 \cdot 13 \cdot 4 + 3 \cdot 5 \cdot 8 \cdot 8 = 3404.$$

Chceme řešení $a \in \mathbb{Z}_{1560}$ a tedy $a = 3404 \bmod 1560 = 284$.

Zbývá vyřešit b.

$$b = \overset{\text{mod } 3}{5 \cdot 8 \cdot 13} + \overset{\text{mod } 5}{3 \cdot 8 \cdot 13} + \overset{\text{mod } 8}{3 \cdot 5 \cdot 13} + \overset{\text{mod } 13}{3 \cdot 5 \cdot 8}$$

$$b \equiv 1 \pmod{3}, \quad b \equiv 2 \pmod{5}, \quad b \equiv 3 \pmod{8}, \quad b \equiv 3 \pmod{13}$$

$$b = \overset{\text{mod } 3}{5 \cdot 8 \cdot 13 \cdot 3} + \overset{\text{mod } 5}{3 \cdot 8 \cdot 13} + \overset{\text{mod } 8}{3 \cdot 5 \cdot 13 \cdot 14} + \overset{\text{mod } 13}{3 \cdot 5 \cdot 8 \cdot 8} = 5562.$$

Chceme řešení $b \in \mathbb{Z}_{1560}$ a tedy $b = 5562 \bmod 1560 = 882$.

$$a + b = 284 + 882 = \underline{1166}$$

ÚLOHA č. 2

$$x^2 \equiv y^2 \pmod{p} \iff p \mid x^2 - y^2 \iff p \mid (x-y) \cdot (x+y) \Rightarrow$$

$$\Rightarrow p \mid x-y \ \vee \ p \mid x+y \iff x \equiv y \pmod{p} \ \vee \ x \equiv -y \pmod{p}$$

Tedy řešením je dvojce (x, y) splňující $x = y$ nebo $x = -y$ $(x, y \in \mathbb{Z}_p)$. Žádné další řešení neexistuje, protože $x + y \in \{0, \dots, p-1\}$, $x - y \in \{0, \dots, p-1\}$ a musí platit, že $p \mid x-y$ nebo $p \mid x+y$. Jediná možnost, aby toto platilo je, že $p \mid \underbrace{x-y=0}_{x=y}$ nebo $p \mid \underbrace{x+y=0}_{x=-y}$.