

$3x \equiv 11 \pmod{5}$   
 $3x \equiv 1 \pmod{5}$   
 ~~$x \equiv 2 \pmod{5}$~~

$6x \equiv 2 \pmod{10}$   
 $3x \equiv 1 \pmod{5}$

$\{x \equiv 2 \pmod{5}\}$  není systémový  
 $\Rightarrow$  řešení jedno řešení.  
 $3^{-1}$  existuje mod 5  
 $3^{-1} \equiv 2 \Rightarrow 3x = a \quad | \cdot 3^{-1}$   
 $2 \cdot 3x = x \equiv 2a$

Řešení v  $\mathbb{Z}$ :  $\{5t + 2; t \in \mathbb{Z}\}$

bře 12-14:01

$2x \equiv 3 \pmod{3}$   
 ~~$0 \equiv 3 \pmod{3}$~~

$10x \equiv 15 \pmod{15}$   
 $2x \equiv 0 \pmod{3}$

$10x \equiv b \pmod{15}$      $\gcd(10, 15) = 5 = d$   
 je dělitelné  $\Downarrow$   
 $2x \equiv b/d \pmod{3} \Rightarrow x = 2 \cdot b/5$

bře 12-14:15

$39x \equiv 41 \pmod{47}$   
 $\gcd(39, 47) = 1 \Rightarrow \exists!$  řešení

$39^{-1} = ? \pmod{47}$   
 Euler  $39^{\varphi(47)} = 1 = 39^{\varphi(47)-1} \cdot 39$   
 $\varphi(47) = 46$      $39^{45} \equiv \dots \equiv 36$

2) Bezout  $1 = a \cdot 39 + b \cdot 47 \quad | \pmod{47}$   
 $1 + 8x = +6 \Leftrightarrow 4x \equiv 3 \Leftrightarrow 4x \equiv -44$   
 $\Leftrightarrow x \equiv -11 \equiv 36 \quad \checkmark$

bře 12-14:22

$n = 5$   
 $(n-1)! = 24 \equiv -1 \pmod{5}$

Fejthabó lema:  $x \equiv c_i \pmod{m_i}$

Příklad:  $x \equiv 8 \pmod{12}$   
 $\rightarrow x \equiv 2 \pmod{6}$

$x = 6t + 2$ ;  $6t + 2 \equiv 8 \pmod{12}$   
 $6t \equiv 6 \pmod{12} \Rightarrow t \equiv 1 \pmod{2}$   
 $t = 1 + 2s \Rightarrow x = 6(1 + 2s) + 2 = 12s + 8$

bře 12-14:33

$x \equiv a_1 \pmod{m_1}$   
 $x \equiv a_2 \pmod{m_2}$

Bezout:  $1 = m_1 m_2 + m_2 m_1$

$M = m_1 \cdot \dots \cdot m_k$   
 $M_i = M/m_i$   
 $1 = \gcd(m_i, M_i)$

řešení:  $x = a_1 M_2 + a_2 M_1$   
 $\equiv 1 \pmod{m_1}$      $\equiv 0 \pmod{m_2}$   
 $\equiv 0 \pmod{m_2}$

po  $\&$  kongruenci: obdobně

bře 12-14:50

počet modulu: 3, 5, 7, 11, 13  
 $3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 15015$

$1234 \times 5678$

$3: \begin{cases} 1 \times 2 = 2 \\ 4 \times 3 = 2 \\ 2 \times 1 = 2 \\ 13: -1 \times 10 = 3 \end{cases}$

$x = 2 + 3t$   
 $2 + 3t \equiv 2 \pmod{5}$   
 $3t \equiv 0 \pmod{5}$   
 $t = 5s$   
 $x = 2 + 3 \cdot 5s = 2 + 15s \equiv 2 \pmod{7}$   
 $15s \equiv 0 \pmod{7}$   
 $s = 7z$

$x = 2 + 7 \cdot 15z \equiv 4 \pmod{11} \Rightarrow 7 \cdot 15z \equiv 2 \pmod{11}$   
 $7 \cdot 15z \equiv 2 \pmod{11} \Rightarrow 7z \equiv 2 \pmod{11}$   
 $z \equiv 4 \pmod{11} \Rightarrow x = 2 + 7 \cdot 15 \cdot (4 + 11e)$   
 $= 2 + 7 \cdot 15 \cdot 4 + 7 \cdot 15 \cdot 11e \equiv 3 \pmod{13}$

bře 12-15:05