

$39 \equiv -2 \pmod{41}$

$x^2 + 13 = x - 17 \pmod{3}$

lineární kongruence

$17x = 11 \pmod{5}$

$2x = 1$

$x \equiv 2^{-1} \equiv 2^3 \equiv 3$

$2 \cdot 3 \equiv 1 \pmod{5}$

$x \equiv 3 \pmod{5}$

Endev: $a^{\varphi(m)} = 1 \pmod{m}$
 $(a, m) = 1$
 $a^{\varphi(m)-1} = a^{-1} \pmod{m}$

bře 12-14:03

$\boxed{10}x \equiv \frac{25}{b} \pmod{\boxed{15}}$

$10x - 15 \equiv 0 \pmod{15}$

↑
dělitel 5

relativně prímé

$\boxed{2}x \equiv 5 \pmod{\boxed{3}}$

$x \equiv 2 \cdot 5 \equiv 1$

$x = a^{\varphi(m)-1} \cdot b \pmod{m}$

$2 \equiv 2^{-1} \pmod{3}$

bře 12-14:20

$39x \equiv 41 \pmod{47}$

1) $(39, 47) = 1$ ✓ $\varphi(47) = 46$
 $x \equiv 39^{-1} \cdot 41 \equiv 39 \cdot 41 \equiv 39^{45} \cdot 41$

2) $(39, 47) = 1 = a \cdot 39 + b \cdot 47 \equiv 36$
 $\equiv a \cdot 39 \pmod{47}$

$47 = 1 \cdot 39 + 8$
 $39 = 4 \cdot 8 + 7$
 $8 = 1 \cdot 7 + 1$

$1 = 8 - 1 \cdot 7$
 $= 8 - 1 \cdot (39 - 4 \cdot 8)$
 $= 5 \cdot 8 - 1 \cdot 39$
 $= 5 \cdot (47 - 1 \cdot 39) - 1 \cdot 39$
 $= -6 \cdot 39 + 5 \cdot 47$

$-6 \cdot 41 \equiv -246 \equiv 36 \pmod{47}$
 $\equiv -11$ ✓

bře 12-14:27

$n=2 \quad (n-1)! = 1 \equiv -1 \pmod{2}$ ✓
 $n=5 \quad 4! = 24 \equiv -1 \pmod{5}$ ✓
 $n=6 \quad 5! = 120 \equiv 0 \pmod{6}$ ✓ NE
 $n=7 \quad 6! = 720 \equiv -1 \pmod{7}$ ✓
 $n=8 \quad 7! = 5040 \equiv 0 \pmod{8}$ U NE

$a) x \equiv b_i \pmod{m_i} \quad i=1, 2, \dots$

↑
 $x \equiv c_i \pmod{m_i}$

bře 12-14:40

$x \equiv 1 \pmod{10}$
 $x \equiv 5 \pmod{18}$
 $x \equiv -4 \pmod{25}$

$(10, 18) = 2$
 $5 - 1 \equiv 0 \pmod{2}$

1. Kongruence $\Rightarrow x = 1 + 10t \quad t \in \mathbb{Z}$

2. Kongruence $\Rightarrow 1 + 10t \equiv 5 \pmod{18}$
 $\Rightarrow 10t \equiv 4 \pmod{18} \Rightarrow 5t \equiv 2 \pmod{9}$
 $\Rightarrow t \equiv 2 \cdot 5^{-1} \equiv 1 \cdot 5^{-1} \equiv 7^2 \equiv 4 \pmod{9}$
 $\varphi(9) = 3 \cdot 2 = 6$

3. $\Rightarrow t \equiv 4 + 9s \Rightarrow 1 + 10(4 + 9s) = 41 + 90s$

$[10, 18] = 2 \cdot 5 \cdot 9 = 90$
 $x \equiv 41 \pmod{90}$

4. $41 + 90s \equiv -4 \pmod{25}$, tj. $90s \equiv -45 \equiv 5 \pmod{25}$

bře 12-14:48

$90s \equiv 5 \pmod{25} \quad (90, 25) = 5$
 $18s \equiv 1 \pmod{5}$
 $3s \equiv 1 \pmod{5}$
 $s \equiv 2 \pmod{5} \Rightarrow s = 2 + 5r$

$x = 41 + 90(2 + 5r) = 221 + 450r$

$x \equiv 221 \pmod{450}$

$[10, 18, 25] = 2 \cdot 9 \cdot 25 = 450$
 $2 \cdot 5 \quad 2 \cdot 3 \cdot 3 \quad 5 \cdot 5$

bře 12-15:00

$23941x \equiv 915 \pmod{4}$
 $1 \cdot x \equiv 3 \pmod{4}$

$23941x \equiv 915 \pmod{81}$
 \parallel
 $23941 : 81 = 295$
 \parallel
 $\begin{array}{r} 162 \\ 727 \\ 727 \\ \hline 151 \\ 105 \\ \hline 46 \end{array}$

$46x \equiv 24 \pmod{81}$
 $x \equiv 37 \cdot 24 \pmod{81}$
 $\equiv 888 \equiv -3 \pmod{81}$

$81 = 46 + 35$
 $46 = 35 + 11$
 $35 = 3 \cdot 11 + 2$
 $11 = 5 \cdot 2 + 1$
 $1 = 11 - 5 \cdot 2$
 $= 11 - 5(35 - 3 \cdot 11)$
 $= 16 \cdot 11 - 5 \cdot 35$
 $= 16 \cdot (46 - 35) - 5 \cdot 35$
 $= -21 \cdot 35 + 16 \cdot 46$
 $= -21(81 - 46) + 16 \cdot 46$
 $\equiv 57 \pmod{81}$

bře 12-15:16