

$f(x) \equiv 0 \pmod{m}$?
 $x^5 + 7x^2 + 14 \equiv 0 \pmod{3}$
 $x^5 + x^2 + 2 \equiv 0 \pmod{3}$

x	0	1	2
x^5	0	1	2
x^2	0	1	1
$x^5 + x^2 + 2$	2	2	1

\Rightarrow NEJAKÁ ŘEŠENÍ!

$x^5 + 7x^2 + 14 \equiv 0 \pmod{3}$ po zjedl. v
 no řešení?
 $1: 1+7+14=1$
 $0: -1$
 $=$

3 13-16:04

$x^5 + 1 \equiv 0 \pmod{5}$ 1 řešení

x^5	0	1	2	3	4
$x^5 + 1$	1	2	4	3	0

$3^2 = -1$ $3^3 = 1$ $3^5 = 3$
 $4^2 = 1$ $4^3 = 1$ $4^5 = 4 = -1$

$\Rightarrow x \equiv 4 \pmod{5}$
 $x = 4 + 5t$

$x^2 + 1 \equiv 0 \pmod{5}$ 2 řešení!
 $\Rightarrow x \equiv 3$ $x = 3 + 5t$
 $x \equiv 2$ $x = 2 + 5t$
 $2x \equiv 3 \pmod{3}$
 $\Rightarrow x \equiv 3t$

3 13-16:17

$2x \equiv 5 \pmod{4}$ NEJAKÁ ŘEŠENÍ!
 $\equiv 1$

$d = (2, 4)$ $ax = b \pmod{m}$
 $d = (a, m)$

Ex \Leftrightarrow d | b

$2x \equiv 6 \pmod{4}$
 $2x \equiv 2 \pmod{2}$
 $x \equiv 1 \pmod{2}$

3 13-16:28

$39x \equiv 41 \pmod{47}$ $x = 39^{-1} \cdot 41$

$d = (39, 47) = 1$
 $\Rightarrow 39^{-1} \pmod{47} = 1$
 $39^{-1} \pmod{47} = 39$

$x = 39 \cdot 41 \pmod{47}$

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

$\Rightarrow 1 = 41 \cdot 39 \pmod{47}$
 $x = 41 \cdot 39 \pmod{47} = 36$

3 13-16:31

10.52: $23 \cdot 941 x \equiv 915 \pmod{3567}$

\Rightarrow řešit lze po jedné normované faktory:

$m_1 = 4, m_2 = 81, m_3 = 11$

$x \equiv 3 \pmod{4} \Rightarrow x = 3 + 4t$
 $x \equiv -3 \pmod{81} \Rightarrow 3 + 4t \equiv -3 \pmod{81} \Rightarrow 4t \equiv -6 \pmod{81} \Rightarrow 4t \equiv 75 \pmod{81} \Rightarrow t \equiv 39 \pmod{81}$
 $x = 3 + 4(39 + 81s) = 159 + 324s$
 $x \equiv -4 \pmod{11} \Rightarrow 159 + 324s \equiv -4 \pmod{11} \Rightarrow 159 + 324s \equiv 7 \pmod{11} \Rightarrow 159 \equiv 4 \pmod{11} \Rightarrow 4 + 324s \equiv 7 \pmod{11} \Rightarrow 324s \equiv 3 \pmod{11} \Rightarrow 9s \equiv 3 \pmod{11} \Rightarrow s \equiv 18 \pmod{11}$

3 13-16:42

$x - x \equiv c_1 - c_2 \pmod{d} \Leftrightarrow c_1 \equiv c_2 \pmod{d}$

$(10, 32) \rightarrow$ (1) $x \equiv 1 \pmod{10}$
 (2) $x \equiv 5 \pmod{18}$
 (3) $x \equiv -4 \pmod{25}$

$x \equiv 221 \pmod{450}$

1) řešitelná? Ano $\{x = 2 + 5t \Rightarrow x = 41 + 90(2 + 5t) = 221 + 450t$

2) $x = 1 + 10s \Rightarrow 1 + 10s \equiv 5 \pmod{18} \Rightarrow 10s \equiv 4 \pmod{18} \Rightarrow 5s \equiv 2 \pmod{9} \Rightarrow s = 4 + 9k \Rightarrow x = 1 + 10(4 + 9k) = 41 + 90k$

$41 + 90k \equiv -4 \pmod{25} \Rightarrow 90k \equiv -45 \pmod{25} \Rightarrow 90k \equiv 5 \pmod{25} \Rightarrow 18k \equiv 1 \pmod{5} \Rightarrow k \equiv 2 \pmod{5}$

3 13-16:46

m_1, m_2, \dots, m_k pairweise uesondig :
 $x \equiv a_1 \pmod{m_1}$
 \vdots
 $x \equiv a_k \pmod{m_k}$

$x \equiv 2 \pmod{3}$
 $x \equiv 3 \pmod{5}$
 $x \equiv 2 \pmod{7}$

3 13-17:02

$M := m_1 \cdot \dots \cdot m_k$ $m_i := M / m_i$
 ex. $\exists!$ $b_i, b_i \cdot m_i \equiv 1 \pmod{m_i}$

$x \equiv a_1 \pmod{m_1}$
 \vdots
 $x \equiv a_k \pmod{m_k}$

$x = a_1 b_1 m_1 + a_2 b_2 m_2 + \dots + a_i b_i m_i$
 \uparrow
 $\equiv a_i \pmod{m_i}$
 $\equiv 0 \pmod{m_j}$ $i \neq j$

3 13-17:07