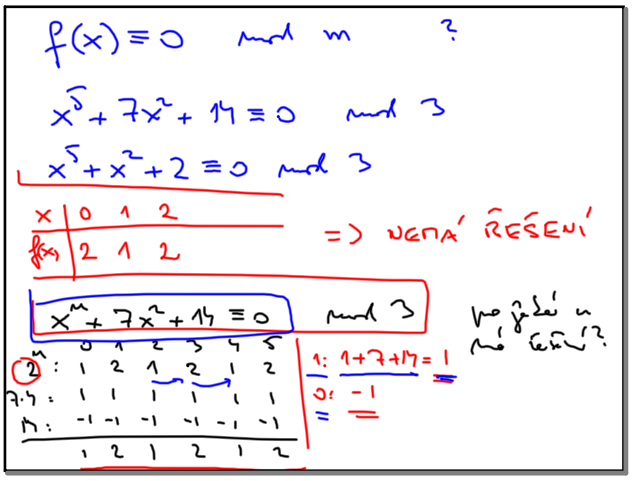
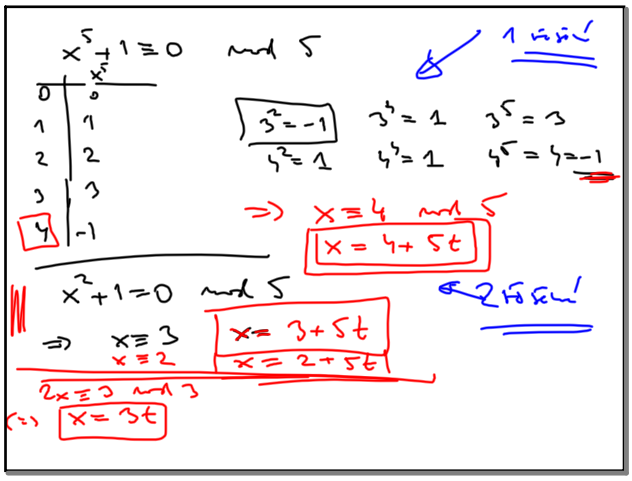
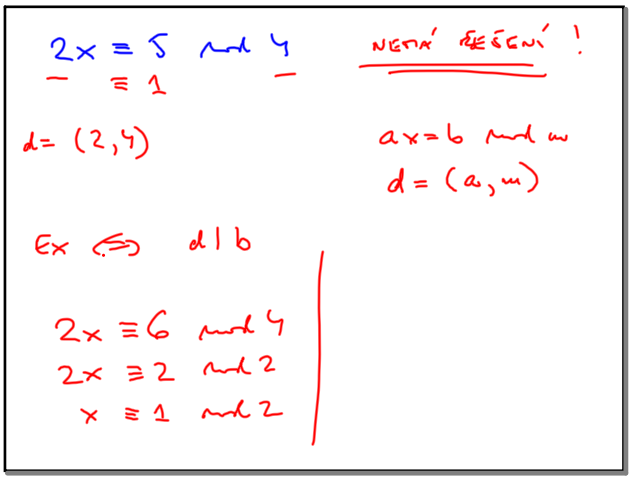


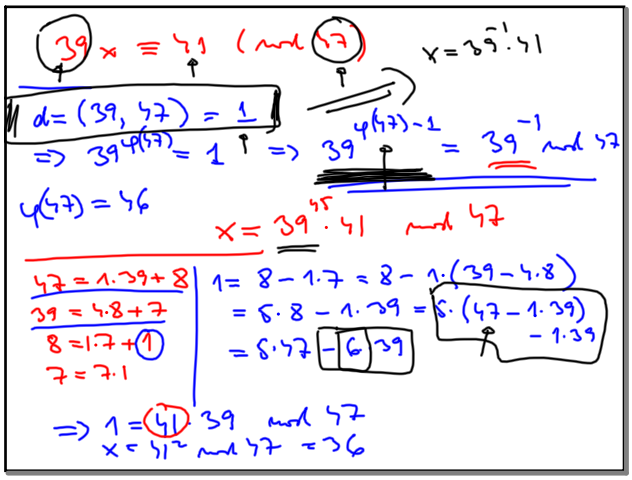
3 13-16:04



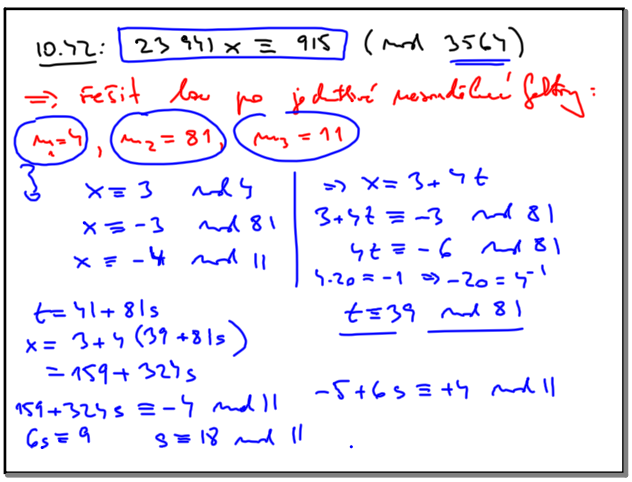
3 13-16:17



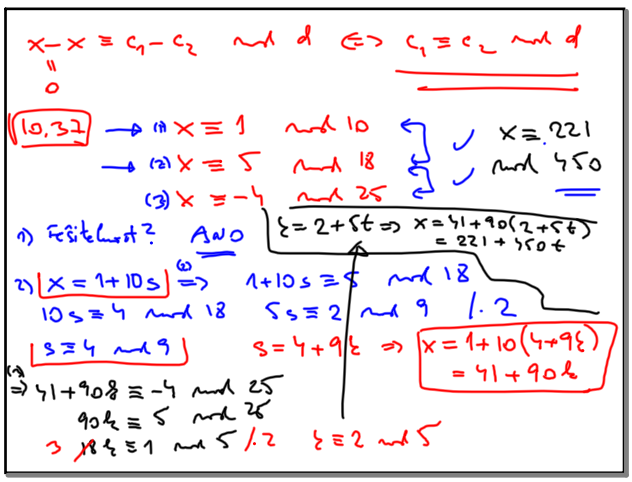
3 13-16:28



3 13-16:31



3 13-16:42



3 13-16:46

$m_1, m_2, \dots, m_k$ nesoudělné (po dvou):

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

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

3 13-17:02

$M := m_1 \cdot \dots \cdot m_k \qquad M_i := M / m_i$

ex. čísla b_i, $b_i M_i \equiv 1 \pmod{m_i}$

$$x = a_1 b_1 M_1 + a_2 b_2 M_2 + \dots + a_k b_k M_k$$

$$\equiv a_1 \pmod{m_1}$$
$$\equiv 0 \pmod{m_i}, \quad i \neq 1$$

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

3 13-17:07