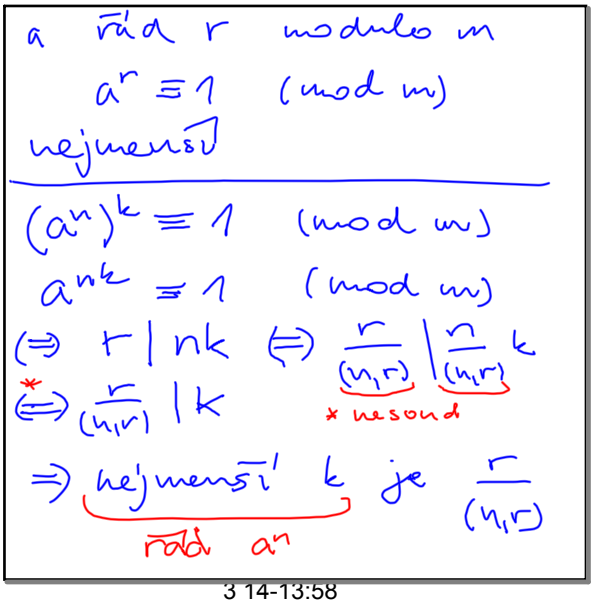
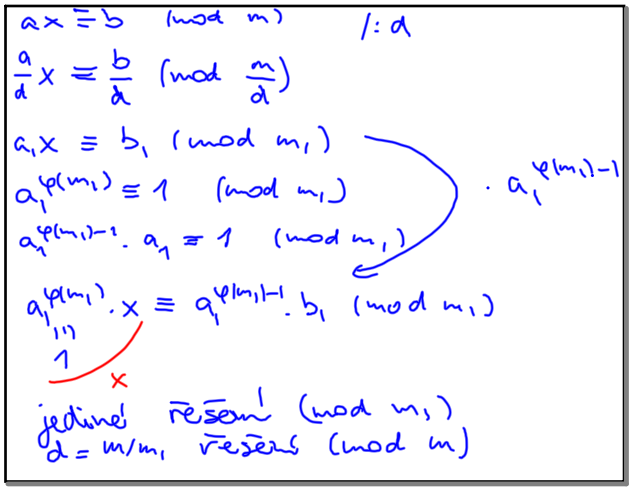
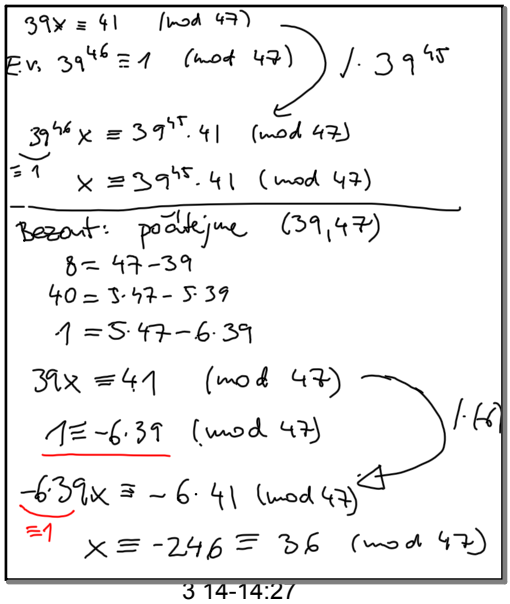


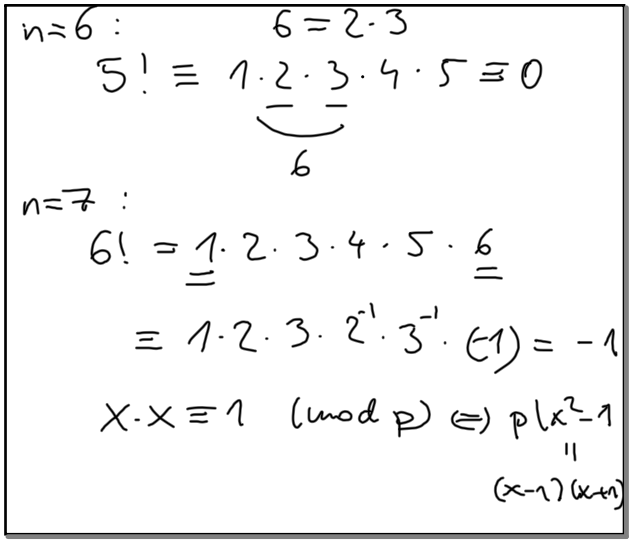
3 14-13:58



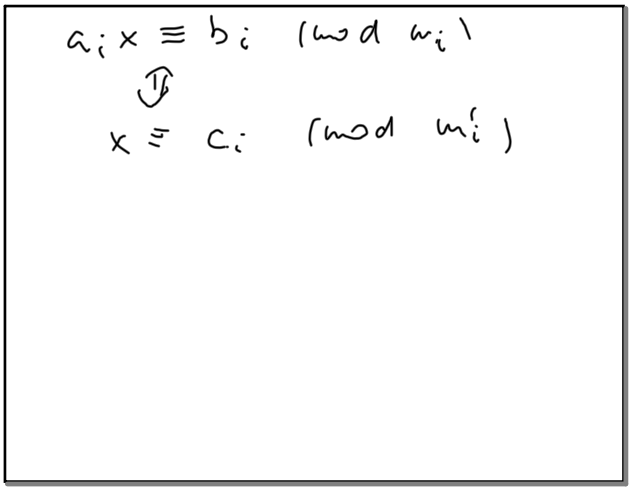
3 14-14:21



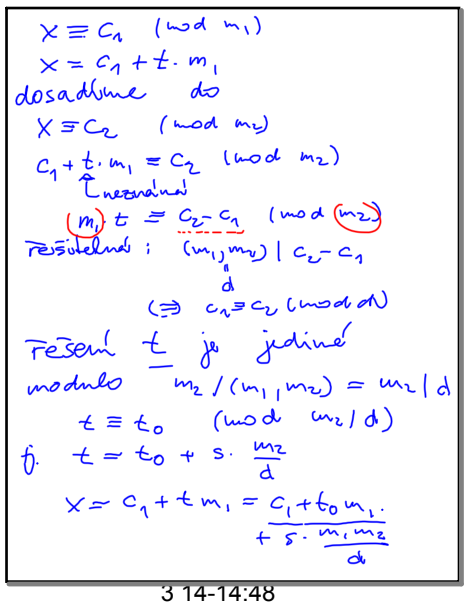
3 14-14:27



3 14-14:39



3 14-14:44



3 14-14:48

$x = 1+10y \Leftarrow x \equiv 1 \pmod{10}$

$1+10y \equiv 5 \pmod{18}$

$10y \equiv 4 \pmod{18} \quad /:2$

$5y \equiv 2 \pmod{9}$

$y \equiv 10y \equiv 4 \pmod{9}$

$y = 4+9z \Rightarrow x = 1+10y$

$= 41+90z$

$41+90z \equiv -4 \pmod{25}$

$90z \equiv 5 \pmod{25} \quad /:5$

$3z \equiv 18z \equiv 1 \pmod{5}$

$z \equiv 6z \equiv 2 \pmod{5}$

$z = 2+5t \Rightarrow x = 41+90z$

$= 221+450t$

3 14-14:57

$x \equiv 7 \pmod{27} \quad /\cdot 11$

$x \equiv -3 \pmod{11} \quad /\cdot 27$

$11x \equiv 77 \pmod{27\cdot 11}$

$27x \equiv -81 \pmod{27\cdot 11}$

$= 297$

$1 = 5\cdot 11 - 2\cdot 27$

$x = (5\cdot 11 - 2\cdot 27)x = 5\cdot 11x - 2\cdot 27x$

$= 5\cdot 77 - 2\cdot(-81) = 547 \equiv 250 \pmod{297}$

3 14-15:07

$x^3 \equiv 3 \pmod{18}$

$x = 3y$

$27y^3 \equiv 3 \pmod{18} \quad /:3$

$9y^3 \equiv 1 \pmod{6}$

$3 \mid 6, \; 3 \mid 9y^3 \Rightarrow 3 \mid 1$ .... nemá řešení

3 14-15:25

$a^{\varphi(m)} \equiv 1 \pmod{m}$

řád a dělí $\varphi(m)$

$x \longmapsto$ zbytek g^x po dělení m

$0 \le x < \varphi(m)$ — $0 \le \dots < m$

$\varphi(m)$ prvků — nesoud. s m $\varphi(m)$ prvků

3 14-15:29

$x^n \equiv a \pmod{m} \quad (n, \varphi(m)) = 1$

$x^{\varphi(m)} \equiv 1 \pmod{m}$

$k\cdot n + l\cdot\varphi(m) = 1$

$x = x^{k\cdot n + l\cdot\varphi(m)} = (x^n)^k \cdot (x^{\varphi(m)})^l$

$\equiv a^k \cdot 1^l \equiv a^k \pmod{m}$

3 14-15:37