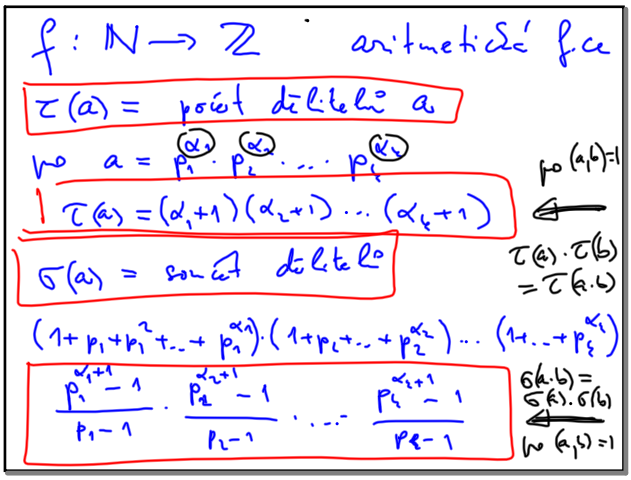
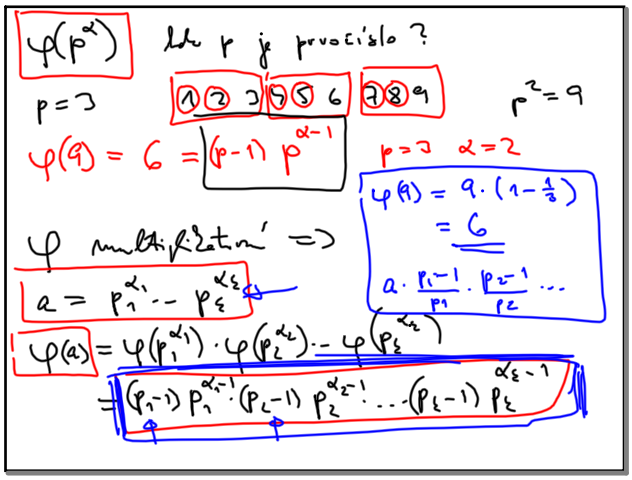
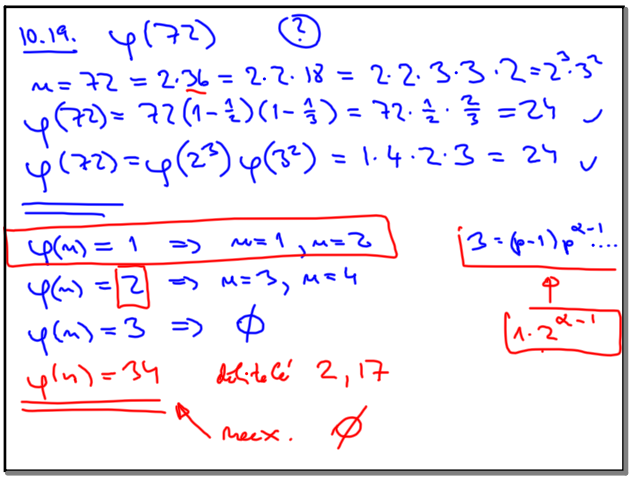


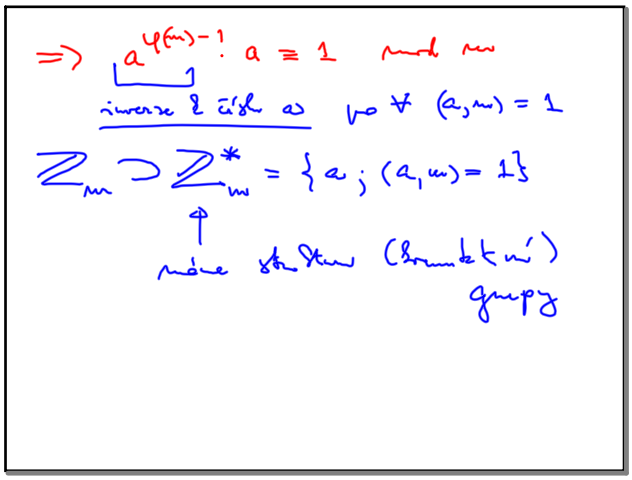
3 6-16:01



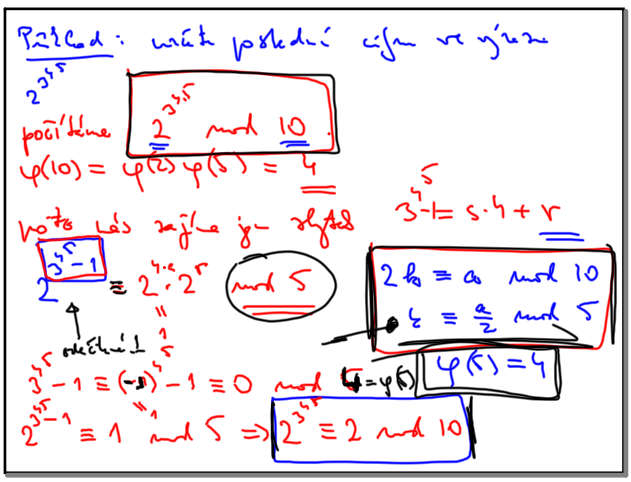
3 6-16:24



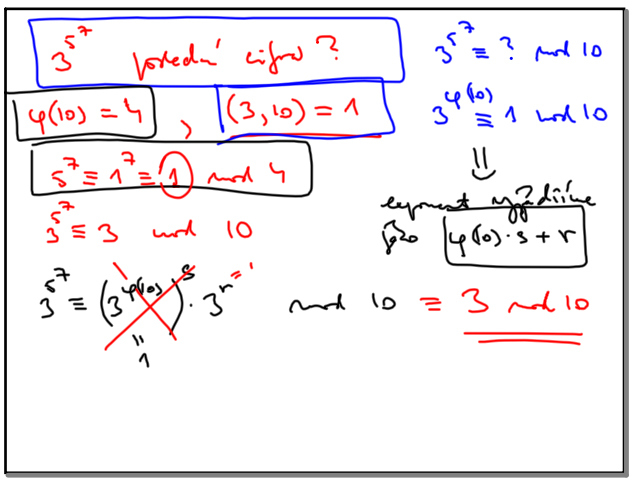
3 6-16:36



3 6-16:49



3 6-16:55



3 6-17:04

$2^{50}+3^{50}+4^{50} \equiv m \pmod{17}$

$2^{16} \equiv 1 \quad 3^{16} \equiv 1 \quad 4^{16} \equiv 1$

$50 \equiv 2 \pmod{16}$

$m \equiv 2^2+3^2+4^2 \equiv 12 \pmod{17}$

$2^{181}+3^{181}+5^{181} \equiv m \pmod{37}$

$1 \equiv 2^{36} \equiv 3^{36} \equiv 5^{36} \pmod{37}$

$181 \equiv 1 \pmod{36}$

$\Rightarrow m \equiv 2+3+5 = 10 \pmod{37}$

3 6-17:17

$\mathbb{Z}_5^*$: otázka: nejmenší mocnina $a^n = 1$ je řád a mod m.

$1^1 = 1$

$2^2 \equiv -1 \pmod 5$

$2^4 \equiv 1 \pmod 5$ ← první $\Rightarrow$ řád 2 je 4

$3^2 \equiv -1 \pmod 5$

$3^4 \equiv 1 \Rightarrow$ řád 3 je 4

$4^2 \equiv 1 \Rightarrow$ řád 4 je 2

$2, 4, 3, 1$ ... pořadí hodnot

řád r vždy dělí $\varphi(m)$

3 6-17:24

10.28 (ii) $15^{14^{13}} \equiv m \pmod{11}$

$\varphi(11) = 10$ $14^{13} \bmod 10$?

řád r čísla 15 je $r \in \{\cancel{1}, 5, 10\}$

$15 \equiv 4 = 2^2 \pmod{11}$

řád 2: $2, 4, 8, 5, 1, -1 \Rightarrow$ řád 2 = 10

$\Rightarrow$ řád 4 je 5

$14^{13} \equiv ? \pmod 5$

$(-1)^{13} \equiv -1 \pmod 5$

$\equiv 4$

$\Rightarrow m \equiv 4^4 = 2^8 = 256$

$\equiv 2+6-5 = 3 \pmod{11}$

$\equiv 4^{-1} \equiv 3$

3 6-17:31