$t \equiv s \pmod{\varphi(m)}$
$a \equiv b \pmod{m}$ $\Rightarrow$ $a^t \equiv b^s \pmod{m}$

$(a,m) = 1$

$a^{18} \equiv 1$ $\qquad$ $(a^3)^6 \equiv 1$

$a^s \equiv 1$ $\qquad$ $b^t \equiv 1$

$(ab)^{st} = a^{st} \cdot b^{st} \equiv 1 \cdot 1 \equiv 1$

$a^s \equiv 1$ $\qquad$ $b^t \equiv 1$

$s = 2^2 \cdot 3 \cdot 5 \cdot 7^0$ $\qquad$ $t = 2 \cdot 3^2 \cdot 5 \cdot 7$

a^{15} mai mic 2^2 $\qquad$ b^2 mai mic $3^2 \cdot 5 \cdot 7$

$a^{15} \cdot b^2$ mai mic $2^2 \cdot 3^2 \cdot 5 \cdot 7$

$$px^2 - p \equiv 0 \pmod{p}$$

Eulerova věta: $a^{\varphi(35)} \equiv 1 \pmod{35}$

$$\varphi(35) = \varphi(5 \cdot 7) = (5-1)(7-1) = \underline{\underline{24}}$$

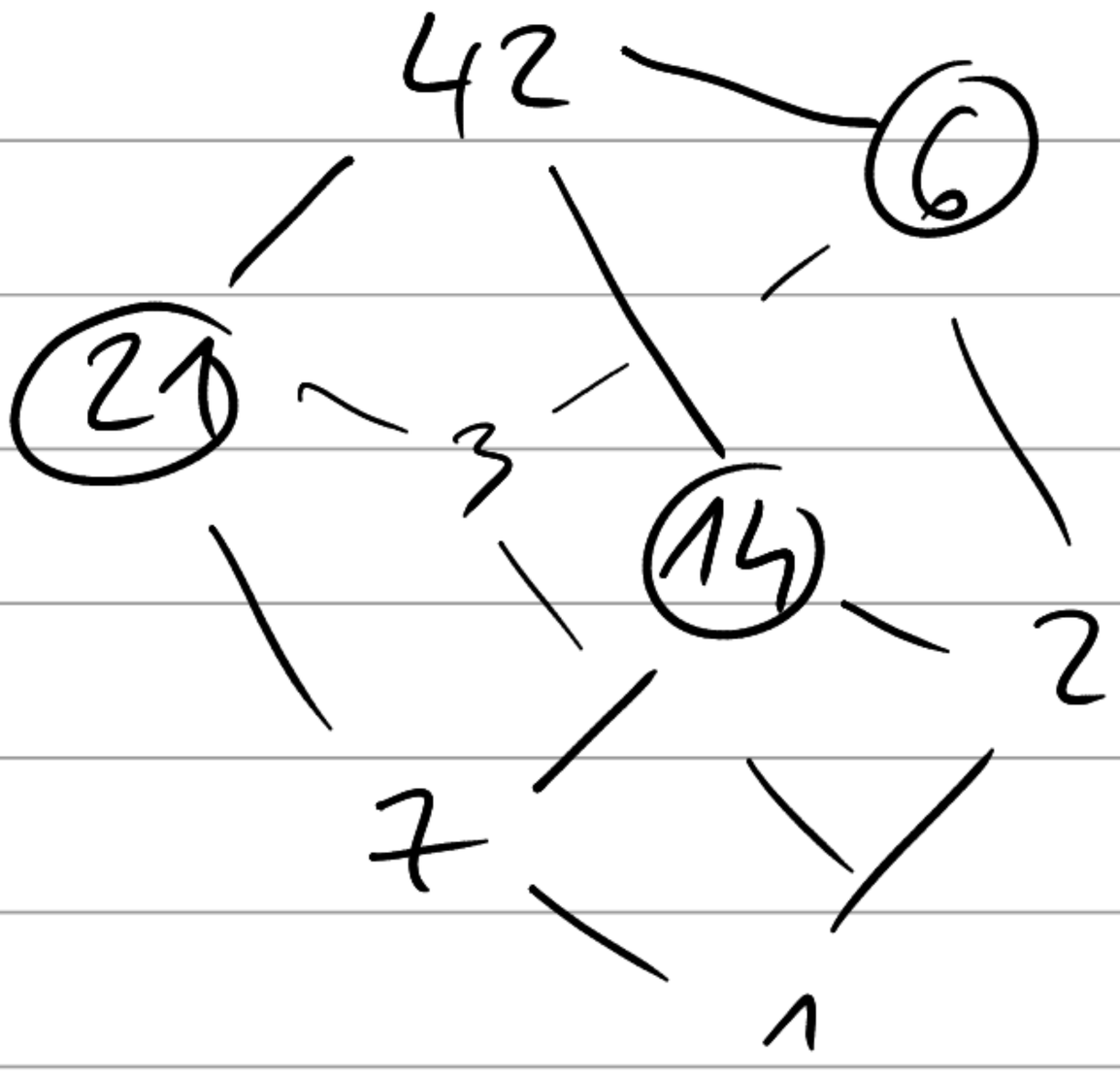
$$f(x) = (x-a) \cdot g(x) + r$$

$$f(a) = 0 \cdot g(a) + r$$

$$f(a) \equiv 0 \pmod{p}$$
$$\| \quad r$$

$$a \cdot b \equiv 0 \pmod{p}$$
$$\Rightarrow a \equiv 0 \pmod{p} \text{ nebo } b \equiv 0 \pmod{p}$$

$\varphi(43) = 42$



zvolme $a \neq 0$

počítáme a^6, a^{14}, a^{21}

$\alpha \longmapsto g^\alpha$

$\log_g a \longleftarrow\!\shortmid\ a$

n	0	1	2	3	4	5	6	7	8	9
$2^n \pmod{11}$	1	2	4	-3	5	-1	-2	-4	3	5

$x^2 \equiv a \pmod{p}$

mal resen($\Rightarrow$ a je kvadr. zb.

je 2 kvadr. zb. mod 11?

$2^{\frac{11-1}{2}} \equiv 2^5 \equiv -1 \pmod{11}$

E. v. $a^{p-1} \equiv 1 \pmod{p}$

$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$

$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$

$$(ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}}$$

$$(-1)^P \cdot (-1)^Q = (-1)^{P+Q}$$

$$= (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$$

$$\left(\frac{219}{383}\right) = \left(\frac{383}{219}\right)(-1) = (-1)\left(\frac{164}{219}\right)$$

$$(-1)^{\frac{n^2-1}{8}} = \begin{cases} +1 & n \equiv 1,7 \ (8) \\ -1 & n \equiv 3,5 \ (8) \end{cases}$$

$$383 \equiv 3 \quad (4)$$

$$219 \equiv 3 \quad (4)$$

$$= (-1)\left(\frac{2}{219}\right)\left(\frac{2}{219}\right)\left(\frac{41}{219}\right)$$

$$219 \equiv 3 \quad (8) \longrightarrow -1$$

$$41 \equiv 1 \quad (4)$$

$$= (-1)(-1)(-1) \cdot \left(\frac{219}{41}\right) \cdot (+1)$$

$$= (-1) \cdot \left(\frac{14}{41}\right) = (-1)\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)$$

$$41 \equiv 1 \quad (8) \longrightarrow +1$$

$$= (-1)(+1)\left(\frac{41}{7}\right) \cdot (+1)$$

$$= (-1)\left(\frac{6}{7}\right) = (-1)\left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = (-1)\left(\frac{7}{3}\right)(-1)$$

$$= (+1) \cdot \left(\frac{1}{3}\right) = \underline{\underline{+1}} \qquad +1$$

$$\left(\frac{219}{383}\right) = +1 \quad \text{a} \quad 383 \quad \text{prvočíslo}$$
$$\equiv 219^{191} \pmod{383}$$

$$\Rightarrow x^2 \equiv 219 \pmod{383} \quad \text{má řešení}$$

vynásobíme $219^{191} \equiv 1$

$$x^2 \equiv 219 \cdot 219^{191} \equiv 219^{192} \pmod{383}$$

$$x \equiv \pm 219^{96} \pmod{383}$$

$$x^2 \equiv a \pmod{p}$$
$$x^2 \equiv a \cdot a^{\frac{p-1}{2}} \equiv a^{\frac{p+1}{2}} \pmod{p}$$
$$x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$$

! $p \equiv 3 \pmod{4}$