$$(a\cdot b)^{rs} \equiv (a^r)^s \cdot (b^s)^r \equiv 1^s \cdot 1^r \equiv 1$$

$$(a\cdot b)^{\delta} \equiv 1 \quad \Rightarrow \quad ((a\cdot b)^{\delta})^r \equiv 1$$

$$\Rightarrow \quad b^{\delta\cdot r} \equiv 1 \pmod m$$

$$\Rightarrow \quad s \mid \delta r \quad \Rightarrow \quad s \mid \delta$$

Symetricky $r \mid \delta$ $\xrightarrow{(s,r)=1}$ $r\cdot s \mid \delta$

$a^s \equiv 1 \qquad s = 2^3 \cdot 3^2 \cdot 5 \Rightarrow s' = 2^3 \cdot 5$

$b^t \equiv 1 \qquad t = 2^2 \cdot 3^2 \cdot 7 \Rightarrow t' = 3^2 \cdot 7$

$a^{s/s'}$ má řád s'
$b^{t/t'}$ má řád t'
} nesoudělná

$a^9 \cdot b^4$ má řád $2^3 \cdot 3^2 \cdot 5 \cdot 7$

společný řád | $[\varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})]$

$\varphi(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}) \wedge \cdots \wedge \varphi(p_r^{\alpha_r})$

$f(a) \equiv 0 \pmod p$

$g^0, g^1, \dots, g^{p-2}$ ← různé zbytky

$\equiv 1, 2, \dots, p-1$ v jiném pořadí

$(g^a)^r \equiv 1 \equiv g^0 \pmod p \iff ar \equiv 0 \pmod{p-1}$

Pokud $(a, p-1) = 1$

$r \equiv 0$

g prim. kořen

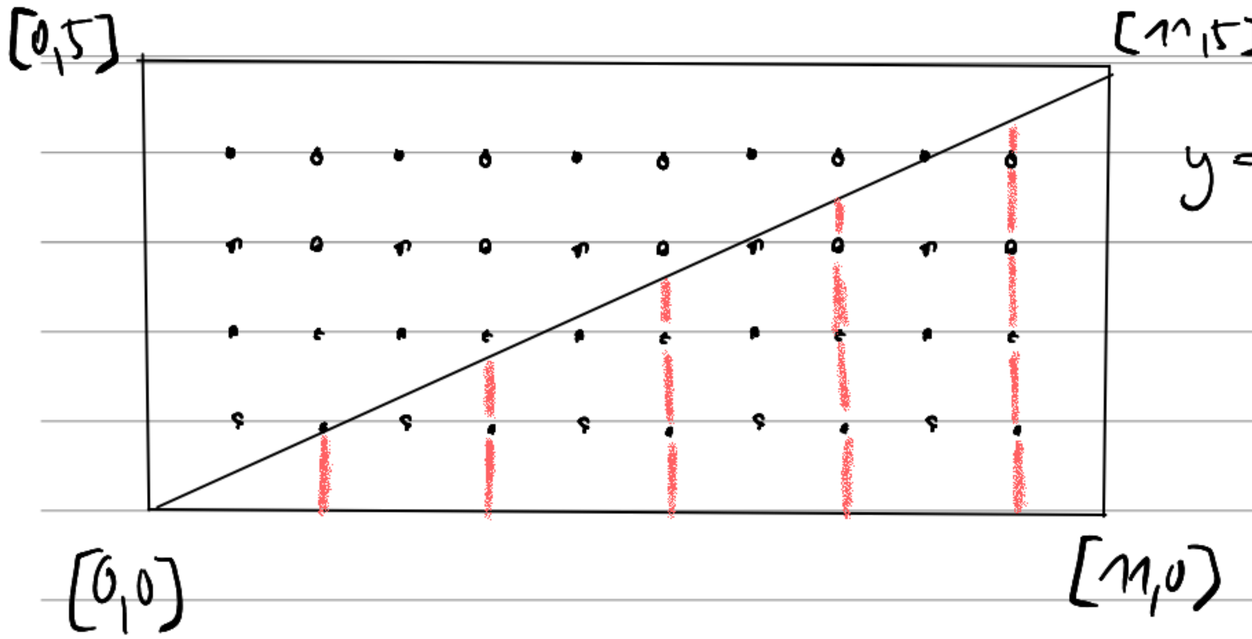
$a \pmod{\varphi(m)} \longmapsto g^a \pmod m$

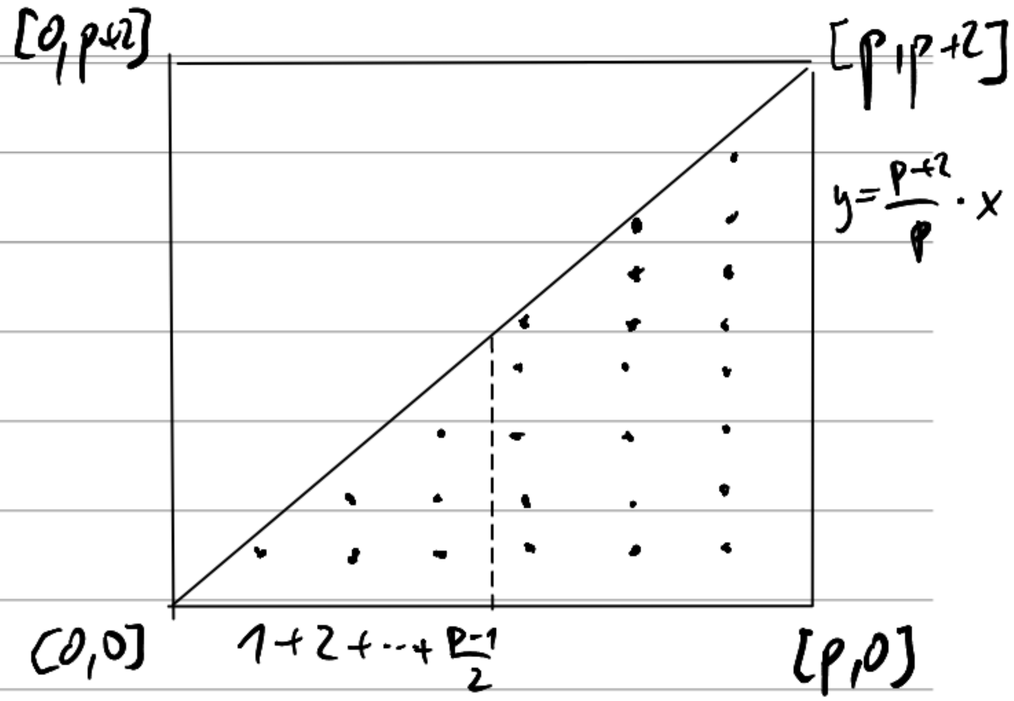
$\longleftarrow \log_g$ diskrétní logaritmus

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

$\frac{p-1}{2}$ sudé $\rightarrow +1$

$\frac{p-1}{2}$ liché $\rightarrow -1$





$5 \cdot 1 \equiv 5$

$5 \cdot 2 \equiv -1$

$5 \cdot 3 \equiv 4$

$5 \cdot 4 \equiv -2$

$5 \cdot 5 \equiv 3$

$\frac{5}{11} \cdot 1 = 0 + \frac{5}{11}$

$\frac{5}{11} \cdot 2 = 0 + \frac{10}{11}$

$\frac{5}{11} \cdot 4 = 2 - \frac{2}{11}$

$\frac{5}{11} \cdot 8 = 3 + \frac{7}{11}$

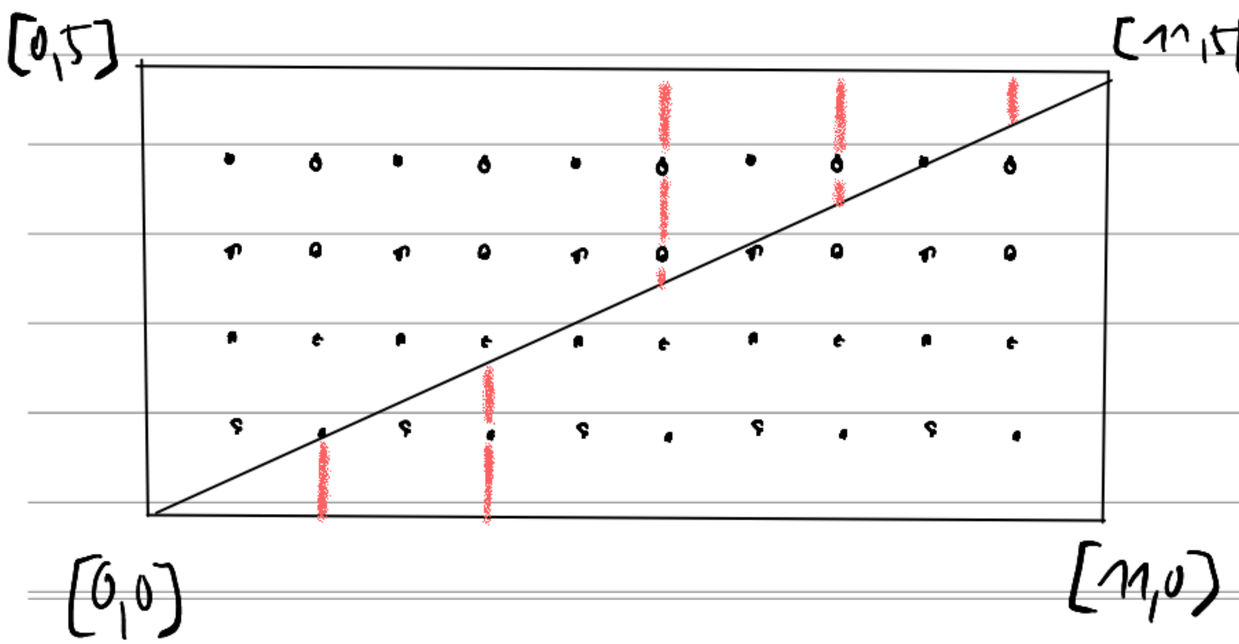
×2

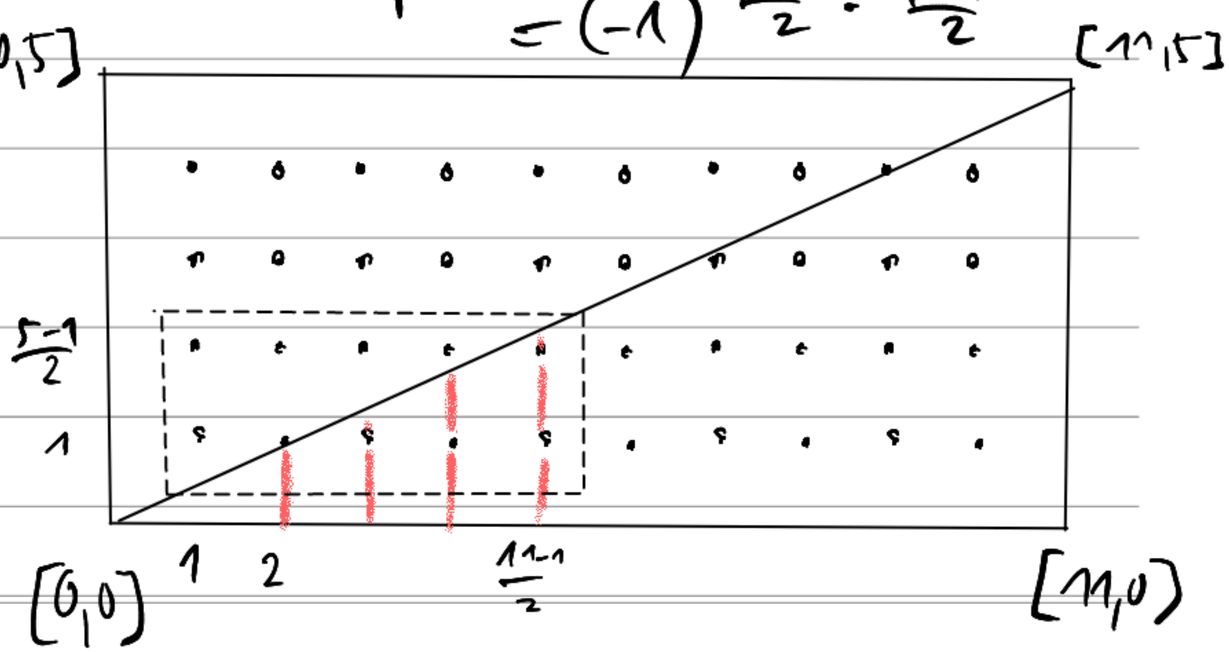
×2

$5^{\frac{11-1}{2}} \equiv (-1)^{\text{počet čísel}}$

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\text{pod}} \cdot (-1)^{\text{vlevo}}$

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





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

$219 \equiv 3 \quad (4)$
$383 \equiv 3 \quad (4)$
$219 \equiv 3 \quad (8)$
$41 \equiv 1 \quad (4)$
$41 \equiv 1 \quad (8)$
$7 \equiv 3 \quad (4)$

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

$$= (-1)(-1)^{\frac{3^2-1}{8}}(-1)^{\frac{3^2-1}{8}}\left(\frac{41}{219}\right)$$

$$= (-1)(-1)^{1\cdot 0}\left(\frac{219}{41}\right)$$

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

383 je prvočíslo

$x^2 \equiv 219 \quad (383)$
má řešení

$$= (-1)(-1)^{\frac{1^2-1}{8}}\left(\frac{7}{41}\right)$$

$$= (-1)(-1)^{0\cdot 1}\left(\frac{41}{7}\right)$$

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

$$= (-1)\cdot 1\cdot(-1) \equiv +1 \pmod 7$$

$$\left(\frac{3}{p}\right) = \begin{cases} p\equiv 1(4) & \left(\frac{p}{3}\right) = \begin{cases} p\equiv 1(3) & \left(\frac{1}{3}\right) = +1 \quad p\equiv 1 \ (12) \\ p\equiv 2(3) & \left(\frac{2}{3}\right) = -1 \quad p\equiv 5 \ (12) \end{cases} \\ p\equiv 3(4) & -\left(\frac{p}{3}\right) = \begin{cases} p\equiv 1(3) & -\left(\frac{1}{3}\right) = -1 \quad p\equiv 7 \ (12) \\ p\equiv 2(3) & -\left(\frac{2}{3}\right) = +1 \quad p\equiv 11 \ (12) \end{cases} \end{cases}$$