$a = p_1^{n_1} \cdots p_k^{n_k} \Rightarrow$ dělitelé tvaru

$b = p_1^{m_1} \cdots p_k^{m_k}$ $\quad 0 \le m_1 \le n_1 \quad \cdots \quad (n_1+1)$ možností

$\vdots$

$0 \le m_k \le n_k \quad (n_k+1)$

$\Rightarrow$ počet dělitelů $(n_1+1) \cdots (n_k+1) = \tau(a)$

$$\sigma(a) = (1 + p_1 + \cdots + p_1^{n_1}) \cdots (1 + p_k + \cdots + p_k^{n_k})$$

$$= \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{n_k+1} - 1}{p_k - 1}$$

$\sigma(a) = 2a \quad ; \; a = 2^k \cdot \ell$ — liché

$(2^{k+1}-1)\,\sigma(\ell) = 2 \cdot 2^k \cdot \ell \qquad \sigma(a) = (2^{k+1}-1) \cdot \sigma(\ell)$

$2^{k+1}-1 \mid 2^{k+1} \cdot \ell$ ale nesoudělné s 2^{k+1}

$\Rightarrow \; 2^{k+1}-1 \mid \ell$

$\cancel{(2^{k+1}-1)}\,\sigma((2^{k+1}-1) \cdot m) = \qquad a = 2^k \cdot (2^{k+1}-1) \cdot m$

$= 2^{k+1}\,\cancel{(2^{k+1}-1)} \cdot m \qquad$ chceme $m = 1$

$\sigma((2^{k+1}-1) \cdot m) = 2^{k+1} \cdot m$

má dva dělitele $(2^{k+1}-1) \cdot m$ & m

součet je $2^{k+1} \cdot m \Rightarrow$ žádný další

$\Rightarrow m = 1$ & je $2^{k+1}-1$ je prvočíslo

$2 \cdot 3 \cdot 5 \cdots p + 1 = q_1 \cdots q_k$

$q_i \notin \{2, 3, 5, \ldots, p\}$ protože $q_i \equiv 1 \pmod{p}$

$2 \cdot 3 \cdot 5 + 1 = 31$

$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$

$n! - 1$ je děl. nejaším p

$3k$; $3k+1$; $3k+2$

$\cancel{\infty}$ ∞ ∞

$4k$ $4k+1$ $4k+2$ $4k+3$

$\cancel{\infty}$ ∞ $\cancel{\infty}$ ∞

$\pi(x) = \# \{ 2 \le p \le x \mid p \text{ prvočíslo} \}$

$5^{30} \pmod{91}$

n	0	1	2	3	4	5	6
$5^n \pmod{91}$	1	5	25	34	79	31	64

7	8	9	10	11	12
47	53	83	51	73	1

$a^t \equiv a^s \pmod{m} \iff r \mid s-t \iff s \equiv t\ (r)$

(||| $a \equiv b \pmod{m}$

b^t)

$a \equiv b\ (m)$

$s \equiv t\ (r)$ $\Rightarrow$ $a^s \equiv b^t\ (m)$

$100 \equiv 9\ (13)$

$100 \equiv 4\ (12)$

$\boxed{\text{Pr}}$ $100^{100} \equiv 9^4 \quad (13)$

r řád a = řád b; $(a,m)=1$

$f: \mathbb{N} \to \mathbb{Z}$ nebo něco

$$f(a) = f(p_1^{n_1} \cdots p_k^{n_k}) = f(p_1^{n_1}) \cdot f(p_2^{n_2} \cdots p_k^{n_k})$$

$$\cdots = f(p_1^{n_1}) \cdot \ldots \cdot f(p_k^{n_k})$$

$\Rightarrow$ závisí pouze na hodnotách $\underline{f(p^n)}$

$$\varphi(n) = \{ a \pmod n \mid (a,n) = 1 \}$$

$$= \{ \text{invertibilní } a \pmod n \}$$

$n=6$

$\cancel{0}$	1	$\cancel{2}$	$\cancel{3}$	$\cancel{4}$	5
$\cancel{6}$	7	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$	11

$1 \cdot 1 \equiv 1 \quad (6)$

$5 \cdot 5 \equiv 1 \quad (6)$

$\varphi(6) = 2$

$n=9$ $\quad 1^{-1}=1 \quad 2^{-1}=5 \quad 4^{-1}=7 \quad 5^{-1}=2 \quad 7^{-1}=4 \quad 8^{-1}=8$

$\cancel{0} \quad 1 \quad 2 \quad \cancel{3} \quad 4 \quad 5 \quad \cancel{6} \quad 7 \quad 8$

$\varphi(9)=6$

$\varphi(p)=p-1$ — pouze $0 \pmod p$ neinvertibilní

$$\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}=p^{\alpha-1}(p-1)=p^\alpha\left(1-\frac{1}{p}\right)$$

$$\underbrace{1\cdot p \pmod{p^\alpha},\ 2\cdot p \pmod{p^\alpha},\ \dots,\ p^{\alpha-1}\cdot p \pmod{p^\alpha}}_{p^{\alpha-1}\text{ zb. tříd}}$$

$$\varphi(p_1^{\alpha_1}\cdots p_k^{\alpha_k})=\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})=p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)$$

n

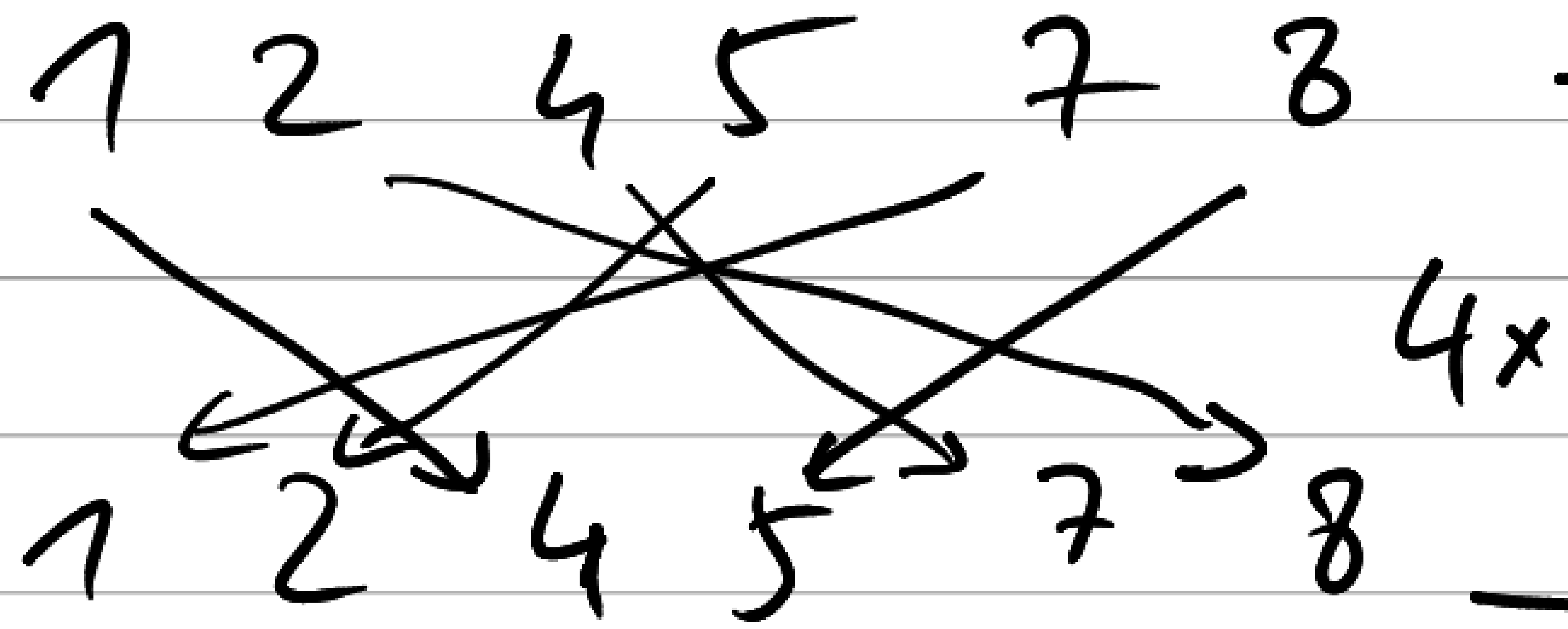
$x \cdot y \equiv 1 \ (a \cdot b)$ $\quad x \cdot z \equiv 1 \ (a) \quad x \cdot w \equiv 1 \ (b)$

$\longleftarrow \quad z \equiv y \equiv w \ (a \cdot b)$

$$\varphi(72) = \varphi(2^3 \cdot 3^2) = (2^3 - 2^2)(3^2 - 3^1)$$
$$= (8-4)(9-3) = 24$$

$$\varphi(4n+2) = \varphi(2n+1)$$
$$\| $$
$$\varphi(2 \cdot (2n+1))$$
$$\| $$
$$1 = \varphi(2) \cdot \varphi(2n+1)$$

$$\varphi(91) = \varphi(7 \cdot 13)$$
$$= (7-1)(13-1) = 72$$



$\longrightarrow$ součin $\quad 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \pmod 9$

$\longrightarrow$ součin $\quad (4\cdot 1)\cdot(4\cdot 2)\cdot(4\cdot 4)\cdot(4\cdot 5)\cdot(4\cdot 7)\cdot(4\cdot 8) \equiv 1\cdot 2\cdot 4\cdot 5\cdot 7\cdot 8$

$$\Downarrow \quad \pmod 9$$

$$4^6 \equiv 1 \pmod 9$$

n	0	1	2	3
$2^n \pmod 7$	$\underline{1}$	2	4	$\underline{1}$

řád 2 mod 7 je $\underline{\underline{3}}$ $\Rightarrow$ 2 není prim. kořen mod 7