$\varphi(n)$ ... počet čísel $q \in \mathbb{N}$ takových, že n a q jsou nesoudělná

p prvočíslo $\Rightarrow \varphi(p) = p-1$

$p = q^r$, q prvočíslo $\Rightarrow \varphi(p) = q^r - q^{r-1}$

$2^3 = 8$: 1, 3, 5, 7

$2^3 - 2^2 = 4$ ✓

Lemma $p = q \cdot r$, q, r nesoudělná $\Rightarrow$

$\varphi(p) = \varphi(q) \cdot \varphi(r)$

Důk. s dělí $p \Rightarrow$ buď dělí q nebo dělí r ✓

$p = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ prvočíselný rozklad

$\Rightarrow \varphi(p) = \prod_{i=1}^{s} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$

3 26-18:00

$\mathbb{Z}_{\varphi(n)} \ni e, e^{-1}$

$M \mapsto M^e \in \mathbb{Z}_{\varphi(n)}$

$(M^e)^d = M \pmod{\varphi(n)}$

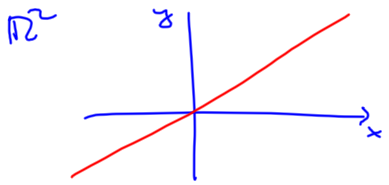
$e^{\varphi(n)} = 1 \pmod{n}$

$\mathbb{Z}_n$ má méně $\varphi(n)$ prvků

3 26-18:21

$C_2 = M \cdot h^y = M \cdot (g^x)^y = M \cdot g^{(x \cdot y)}$

$C_2 = M \cdot g^{x \cdot y} \cdot (g^y)^{-x} = M \cdot g^0 = M$



3 26-18:27

$\{d, d^2 = a\} = H$

$[a] = \{d, a\} = H$

$[b] = \{b, f\} = b \cdot H$

$[c] = \{c, e\} = c \cdot H$

$[a] = \{d, a\} = H$

$[b] = \{e, b\} = H \cdot b$

$[c] = \{f, c\} = H \cdot c$

3 26-18:53

$\Sigma_3 \xrightarrow{\text{vn.}} \mathbb{Z}_2$

	a	b	c	d	e	f
a						
b						
c						
d						
e						
f						

$\{c, \textcircled{b}, c\beta\} = H$

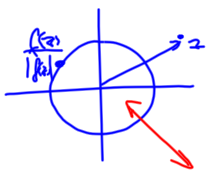
$\{\textcircled{d}, e, f\} = L$

3 26-19:01

$x^2 + 1 = 0$ $\quad \mathbb{R} \mapsto \mathbb{R} + i\mathbb{R}$

$z \mapsto \frac{f(z)}{|f(z)|}$

z^d



3 26-19:10