

## Definice

- Přes kořenové činitele: Necht'  $\omega_n = e^{\frac{2\pi i}{n}}$  a  $N_n$  je množina, přirozených čísel menších nebo rovných  $n$  nesoudělných s  $n$ . Pak

$$\Phi_n(x) = \prod_{k \in N_n} (x - \omega_n^k).$$

- Přes nejmenší společný násobek: Necht'  $\gcd$  značí největší společný násobek polynomů. Pak

$$\Phi_n(x) = \frac{x^n - 1}{\gcd_{d < n, d|n} (x^d - 1)}.$$

- Rekurentně:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d < n, d|n} \Phi_d(x)}.$$

## Vlastnosti

- $\Phi_n(x)$  je polynom stupně  $\phi(n)$  (eulerova funkce) s celočíselnými koeficienty.
- $\Phi_n(x)$  je nerozložitelný v racionálních číslech, tedy v racionálních číslech se  $x^n - 1$  rozkládá na

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

- Uvažme přirozené číslo  $n$  a dělitele  $d | n$ ,  $d < n$ . Pokud je  $p$  společný prvočíselný dělitel  $\Phi_n(x)$  a  $\Phi_d(x)$  pro pevné  $x$ , tak  $p | n$ .
- Pokud jsou čísla  $\Phi_a(x)$  a  $\Phi_b(x)$  soudělná, tak  $a/b$  je tvaru  $p^k$  pro prvočíslo  $p$  a celé číslo  $k$ .
- Pro liché  $n$  je po vynásobení dvěma  $\Phi_{2n}(x) = \Phi_n(-x)$ .
- Po pronásobení prvočíslem  $p$  lze spočítat

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{pro } p | n, \\ \frac{\Phi_n(x^p)}{\Phi_n(x)} & \text{pro } p \nmid n. \end{cases}$$

## Příklady

- $\Phi_1(x) = x - 1$ ,
- $\Phi_2(x) = x + 1$ ,
- $\Phi_{2^n}(x) = x^{2^{n-1}} + 1$ ,
- pro prvočíslo  $p$  je  $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1$ ,
- pro prvočíslo  $p > 2$  je  $\Phi_{2p}(x) = x^{p-1} - x^{p-2} + \dots - x + 1$ ,
- $\Phi_{12}(x) = \frac{x^{12} - 1}{(x^6 - 1) \cdot \Phi_4(x)} = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1$ .
- $\Phi_n(0) = \begin{cases} -1 & \text{pro } n = 1, \\ 1 & \text{jinak.} \end{cases}$
- $\Phi_n(1) = \begin{cases} 0 & \text{pro } n = 1, \\ p & \text{pro } n = p^k, \text{ kde } p \text{ je prvočíslo,} \\ 1 & \text{jinak.} \end{cases}$