Cyklotomické polynomy

Pro každé $n \in \mathbb{N}$ je *cyklotomický polynom* $t_n \in \mathbb{C}[X]$ definován jako

$$t_n := \prod_{k \in \mathbb{Z}_n^*} (x - \omega_n^k).$$

Jinými slovy, je to polynom, jehož kořeny jsou právě všechny primitivní n-té odmocniny z jedné. Např.

$$\begin{aligned} t_1 &= x - 1, \\ t_2 &= x + 1, \\ t_6 &= (x - \omega_6)(x - \omega_6^{-1}) = x^2 + x(\omega_6 + \omega_6^{-1}) + 1. \end{aligned}$$

V posledním případě platí, že $\omega_6 + \omega_6^{-1} = 1$, protože imaginární části se odečtou a $\mathrm{Re}(\omega_6) = \frac{1}{2}$, což je vidět např. z toho, že body 0, 1 a ω_6 komplexní roviny tvoří rovnostranný trojúhelník. Také t_6 je tedy celočíselný. Ukážeme, že ve skutečnosti jsou všechny cyklotomické polynomy prvky $\mathbb{Z}[x]$ a jsou tam ireducibilní.

Věta. Cyklotomické polynomy jsou celočíselné.

Důkaz. Poznamenejme nejprve, že všechny cyklotomické polynomy jsou zjevně monické. Protože každá n-tá odmocnina z jedné je d-tá primitivní odmocnina z jedné pro nějaké $d \mid n$, dostáváme

$$\prod_{d \mid n} t_d = \prod_{k \in \mathbb{Z}_n} (x - \omega_n^k) = x^n - 1.$$

Pokud tedy použijeme indukční předpoklad, že t_d je celočíselný pro všechna $d < n$ (přičemž pro t_1 to platí) dostaneme, že i t_n je celočíselný (součin neceločíselného polynomu a celočíselného monického polynomu nemůže být celočíselný). □

Větě o ireducibilitě cyklotomických polynomů předešleme následující pomocné tvrzení, které využívá pojem *formální derivace* polynomu. Formální derivace polynomu a je definována stejně jako derivace v analýze a značí se rovněž a'. Formální se jí říká proto, že od ní nečekáme žádné topologické (limita) ani geometrické (směrnice tečny) vlastnosti. Je to prostě jen zobrazení $R[x] \to R[x]$, které je užitečné tím, že splňuje

$$\begin{aligned} (a + b)' &= a' + b' \\ (ab)' &= a'b + b'a. \end{aligned}$$

Lemma. Nechť p je prvočíslo, které nedělí n. Pak je polynom $x^n - 1$ v $\mathbb{Z}_p[x]$ bezčtvercový, tj. není dělitelný čtvercem žádného nekonstatntního polynomu.

Důkaz. Předpokládejme, že $x^n - 1 = a^2 \cdot b$. Pak zderivováním obou stran dostáváme

$$nx^{n-1} = a(ab' + 2a'b).$$

Polynom $x^n - 1$ a jeho derivace nx^{n-1} jsou nesoudělné, jak je vidět např. z rovnosti:

$$n = x(nx^{n-1}) - n(x^n - 1).$$

Dosazením dostáváme

$$n = a \cdot (xab' + 2xa'b - nab),$$

z čehož plyne, že a je konstanta (protože $n \neq 0$ v $\mathbb{Z}_p$). □

Věta. Cyklotomický polynom t_n je ireducibilní v $\mathbb{Z}[x]$.

Důkaz. Nechť f je ireducibilní monický celočíselný dělitel t_n, který má v $\mathbb{C}$ kořen α. Nechť je dále p prvočíslo nesoudělné s n. Ukážeme, že pak i α^p je kořenem f.

Protože p nedělí n, je α^p, podobně jako α, primitivní n-tou odmocninou z jedné, a tedy kořenem t_n. Předpokládejme, pro spor, že α^p není kořenem f. Pak je v $\mathbb{C}$ kořenem polynomu $g := t_n/f$, což je podle Gaussova lemmatu celočíselný monický polynom. Uvažujme polynom $g(x^p)$, který vznikne z g nahrazením členů $g_k x^k$ členy $g_k x^{kp}$. Ten má podobně jako f kořen α, a je s ním tedy soudělný. Protože je ale f ireducibilní, musí f dělit $g(x^p)$.

> V pozadí je fakt, že Eukleidův algoritmus prováděný v $\mathbb{C}[x]$ je současně Eukleidovým algoritmem v $\mathbb{Q}[x]$, a tudíž dostaneme racionální největší společný dělitel f a $g(x^p)$ stupně alespoň jedna. Podle Gaussova lemmatu je tento společný dělitel dokonce celočíselný.

Celkem tedy platí

$$t_n = f \cdot g, \qquad\qquad g(x^p) = f \cdot h,$$

kde $h = g(x^p)/f$ je celočíselný polynom. Nyní přejdeme do $\mathbb{Z}_p[x]$ pomocí zobrazení $\pi_x : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, které spočívá v redukci koeficientů modulo p. Toto zobrazení je homomorfismem, a máme tedy

$$\overline{t_n} = \overline{f} \cdot \overline{g}, \qquad\qquad \overline{g(x^p)} = \overline{f} \cdot \overline{h},$$

kde pruhem označujeme příslušné polynomy po redukci. Klíčovým bodem důkazu nyní je fakt, že v $\mathbb{Z}_p[x]$ platí

$$\overline{g(x^p)} = \overline{g}^{\,p}.$$

Protože $\overline{f}$ dělí $\overline{g}^{\,p}$, není $\overline{t_n}$ bezčtvercový. Vskutku, každý ireducibilní faktor r polynomu $\overline{f}$ dělí $\overline{g}^{\,p}$ a tedy $\overline{g}$ (protože $\mathbb{Z}_p[x]$ je obor jednoznačné faktorizace), a tudíž s^2 dělí $\overline{t_n}$.

To je ovšem spor, protože $x^n - 1$ je podle předchozího lemmatu v $\mathbb{Z}_p[x]$ bezčtvercový a je dělitelný $\overline{t_n}$. Tím je dokončen důkaz tvrzení, že f má pro každý kořen α a každé p nedělící n také kořen α^p.

Ireducibilita t_n už plyne snadno: pro každou faktorizaci t_n musí mít faktor s kořenem ω_n také všechny kořeny ω_n^k, $k \in \mathbb{Z}_n^*$. Takový faktor je tedy roven samotnému t_n, a faktorizace je triviální. □