PENTRU CERCURILE DE ELEVI

POLINOAME CICLOTOMICE

MARCEL ŢENA[1)]

Pentru $n \in \mathbb{N}^*$, notăm:

$$U_n = \{x \in \mathbb{C} \mid x^n = 1\} = \left\{ \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n} \,\middle|\, k = \overline{0, n-1} \right\}.$$

Mulţimea U_n se numeşte *mulţimea rădăcinilor de ordin n ale unităţii.* Notând $\zeta = \cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n}$, datorită formulei lui *Moivre*, avem:

$$U_n = \left\{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\right\}. \tag{1}$$

Propoziţia 1. *$(U_n, \cdot)$ este un subgrup al grupului abelian $(\mathbb{C}^*, \cdot)$.*

Demonstraţie. Pentru orice $x, y \in U_n$, avem $x^n = y^n = 1$, prin urmare $\left(xy^{-1}\right)^n = x^n \left(y^n\right)^{-1} = 1 \cdot 1^{-1} = 1$, deci $xy^{-1} \in U_n$.

Datorită egalităţii (1) putem afirma că grupul U_n este chiar ciclic, iar ζ este un generator al său. Ne propunem acum să vedem cum arată toţi generatorii acestui grup. Avem în acest sens:

Propoziţia 2. *$x \in U_n$ este un generator al grupului U_n (i.e. $U_n = \{1, x, x^2, ..., x^{n-1}\}$) dacă şi numai dacă $x = \zeta^k$, cu $0 \le k \le n-1, (k, n) = 1$.*

Demonstraţie. Presupunem că $x \in U_n$ este un generator. Fie $x = \zeta^k$, cu $0 \le k \le n-1$, ceea ce este clar, în baza lui (1). Rămâne să arătăm că $(k, n) = 1$. Deoarece $\zeta \in U_n$, avem $\zeta = x^q$, pentru un $q \in \{0, 1, ..., n-1\}$, deci $\zeta = \zeta^{kq}$. Este uşor de văzut că pentru $i, j \in \mathbb{Z}$, avem $\zeta^i = \zeta^j$ dacă şi numai dacă $i \equiv j \pmod n$ şi atunci, din egalitatea obţinută, deducem că $kq \equiv 1 \pmod n$, de unde $(k, n) = 1$. Reciproc, fie $x = \zeta^k$, cu $0 \le k \le n-1, (k, n) = 1$. Avem evident:

$$\left\{1, x, x^2, \ldots, x^{n-1}\right\} \subseteq U_n$$

şi pentru a dovedi egalitatea, este suficient să arătăm că elementele $1, x, x^2, \ldots, x^{n-1}$ sunt distincte două câte două. Într-adevăr: $x^i = x^j$ $(0 \le i, j \le n-1) \Leftrightarrow \zeta^{ki} = \zeta^{kj} \Leftrightarrow ki \equiv kj \pmod n \Leftrightarrow i \equiv j \pmod n)$, unde, pentru ultima echivalenţă, am ţinut seama de faptul că $(k, n) = 1$. Dar $i \equiv j \pmod n$ şi $0 \le i, j \le n-1$ conduc la $i = j$.

Definiţie. *Generatorii grupului U_n i.e. $\zeta^k = \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n}$ cu $(k, n) = 1$ se numesc rădăcini primitive de ordinul n ale unităţii.*

Notăm:

$$P_n = \{\zeta^k | 0 \le k \le n-1, (k, n) = 1\}. \tag{2}$$

[1)] Prof. dr., Colegiul Naţional „Sf. Sava“, Bucureşti

Mulţimea P_n are $\varphi(n)$ elemente, unde φ este indicatorul lui *Euler*. Deşi, în (2), ζ are semnificaţia de până acum şi anume $\zeta = \cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n}$, este uşor de dovedit că (2) rămâne adevărată, dacă ζ este oricare din elementele mulţimii P_n.

Propoziţia 3. *Familia de mulţimi (P_d), unde d parcurge divizorii naturali ai lui n, este o partiţie a mulţimii U_n, adică*:

1. $\bigcup_{d|n} P_d = U_n$;
2. $d_1 \neq d_2 \Rightarrow P_{d_1} \cap P_{d_2} = \emptyset$ (d_1, d_2 *divizori ai lui* n).

Demonstraţie. 1.„$\subseteq$“ Pentru fiecare divizor d al lui n, avem $P_d \subseteq U_d \subseteq U_n$, deci $\bigcup_{d|n} P_d \subseteq U_n$; am folosit faptul, aproape evident, că $d \mid n \Leftrightarrow U_d \subseteq U_n$.

„$\supseteq$” Fie $x \in U_n, x = \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n}$, cu $0 \leq k \leq n-1$. Scriind fracţia $\frac{k}{n}$ în forma ireductibilă $\frac{k'}{d'}$, avem $x = \cos\frac{2k'\pi}{d'} + \mathrm{i}\sin\frac{2k'\pi}{d'} \in P_{d'}$ cu $d' \mid n$. Cum $P_{d'} \subseteq \bigcup_{d|n} P_d$, rezultă că $U_n \subseteq \bigcup_{d|n} P_d$.

2. Dacă $\zeta \in P_{d_1} \cap P_{d_2}$, atunci:

$$\zeta = \cos\frac{2k_1\pi}{d_1} + \mathrm{i}\sin\frac{2k_1\pi}{d_1} = \cos\frac{2k_2\pi}{d_2} + \mathrm{i}\sin\frac{2k_2\pi}{d_2},$$

cu $(k_1, d_1) = (k_2, d_2) = 1$, de unde $k_1 = k_2$ şi $d_1 = d_2$.

Definiţie. *Pentru $n \in \mathbb{N}^*$, polinomul $\Phi_n(X) = \prod_{\zeta \in P_n} (X - \zeta)$ se numeşte al n-lea polinom ciclotomic.*

Polinomul $\Phi_n(X)$ este monic (unitar), are gradul $\varphi(n)$ şi, deocamdată, $\Phi_n(X)$ are coeficienţi complecşi. Vom arăta că $\Phi_n(X)$ are chiar coeficienţi întregi.

Teorema 4. (*Dedekind*) *Pentru $n \in \mathbb{N}^*$, are loc egalitatea*:

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{3}$$

Demonstraţie.

$$X^n - 1 = \prod_{\zeta \in U_n} (X - \zeta) = \prod_{\zeta \in \bigcup_{d|n} P_d} (X - \zeta) = \prod_{d|n} \left(\prod_{\zeta \in P_d} (X - \zeta) \right) = \prod_{d|n} \Phi_d(X).$$

Exemple de polinoame ciclotomice. Pentru $n = 1$, $\Phi_1(X) = X - 1$.

Pentru $n = p$ (număr prim), din $X^p - 1 = \Phi_1(X)\Phi_p(X)$, rezultă că:

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1.$$

Astfel, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$.
Pentru $n = 4$, avem:

$$\Phi_4(X) = \frac{X^4 - 1}{\Phi_1(X)\Phi_2(X)} = \frac{X^4 - 1}{(X - 1)(X + 1)} = X^2 + 1.$$

Teorema 5. (*Möbius*) *Pentru $n \in \mathbb{N}^*$, avem egalitatea*:

$$\Phi_n(X) = \prod_{d|n} \left(X^d - 1\right)^{\mu\left(\frac{n}{d}\right)}, \tag{4}$$

unde μ este funcţia lui Möbius.

Demonstraţie. Dacă $(G, \cdot)$ este un grup abelian şi $f, g : \mathbb{N}^* \to G$ două funcţii, atunci există formula de inversiune a lui *Möbius*:

$$g(n) = \prod_{d|n} f(d),\ \forall\, n \in \mathbb{N}^* \Leftrightarrow f(n) = \prod_{d|n} g(d)^{\mu\left(\frac{n}{d}\right)},\ \forall n \in \mathbb{N}^*.$$

Luând în rolul lui G grupul multiplicativ al fracţiilor raţionale nenule (rapoarte de polinoame nenule), formula (4) este echivalenta formulei (3), în baza formulei de inversiune a lui *Möbius*.

Propoziţia 6. *Polinoamele ciclotomice au coeficienţi întregi, adică $\Phi_n(X) \in \mathbb{Z}[X]$.*

Demonstraţie. Prin inducţie după n. Pentru $n = 1$, avem $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Să presupunem că $\Phi_k(X) \in \mathbb{Z}[X]$, pentru toţi $1 \leq k < n$ şi să arătăm că $\Phi_n(X) \in \mathbb{Z}[X]$. Din formula (3), avem că:

$$\Phi_n(X) = \frac{X^n - 1}{\prod\limits_{d|n, d<n} \Phi_d(X)}.$$

Conform ipotezei de inducţie, polinomul de la numitor este monic şi are coeficienţi întregi. Ţinând seama de algoritmul împărţirii, deducem că polinomul cât $\Phi_n(X)$ are coeficienţi întregi.

Teorema 7. (*Gauss-Dedekind*) *Polinomul $\Phi_n(X)$ este ireductibil în inelul de polinoame $\mathbb{Z}[X]$.*

Demonstraţie. Ne vom baza pe următorul rezultat important, a cărui demonstraţie se poate vedea în [1].

Lemă. (*Mertens*) *Dacă $f \in \mathbb{Z}[X]$ admite ca rădăcină o rădăcină primitivă de ordin n a unităţii ζ, atunci f admite ca rădăcini toate rădăcinile primitive de ordin n ale unităţii, adică $f(\zeta^k) = 0$, pentru $0 \leq k \leq n - 1$, $(k, n) = 1$.*

Să demonstrăm acum teorema. Evident, $\zeta = \cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n}$ este o rădăcină a polinomului $\Phi_n(X)$. Fie $f(X) \in \mathbb{Z}[X]$ acel factor ireductibil monic din descompunerea lui $\Phi_n(X)$ care are rădăcina ζ. Conform lemei lui *Mertens*, polinomul $f(X)$ are ca rădăcini toate ζ^k cu $0 \leq k \leq n-1, (k,n) = 1$. Rezultă că $f(X) = \Phi_n(X)$ şi, cum $f(X)$ este ireductibil în $\mathbb{Z}[X]$, rezultă că polinomul $\Phi_n(X)$ este ireductibil în inelul $\mathbb{Z}[X]$.

Alte rezultate privind polinoamele ciclotomice (pentru care se poate vedea [1]).

Teorema 8. *Dacă $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ este descompunerea canonică a lui n, atunci*:

$$\Phi_n(X) = \Phi_{p_1 \cdot \ldots \cdot p_k}\left(X^{\frac{n}{p_1 \cdot \ldots \cdot p_k}}\right).$$

Altfel spus, este suficient să cunoaştem polinoamele $\Phi_n(X)$, cu n liber de pătrate.

Propoziţia 9. *Dacă*:

$$\Phi_n(X) = c_0 X^{\varphi(n)} + c_1 X^{\varphi(n)-1} + \ldots + c_{\varphi(n)-1} X + c_{\varphi(n)},$$

atunci $c_i = c_{\varphi(n)-i}$, pentru $i = \overline{0, \varphi(n)}$, adică polinomul $\Phi_n(X)$ este reciproc.

Teorema 10. (*Schur*) *Mulţimea coeficienţilor polinoamelor $\Phi_n(X)$, când n parcurge $\mathbb{N}^*$, este mulţimea $\mathbb{Z}$ a numerelor întregi.*

Teorema 11. (*Migotti*) *Dacă p, q sunt numere prime distincte, polinomul $\Phi_{pq}(X)$ are coeficienţii în mulţimea $\{-1, 0, 1\}$.*

Reamintim definiţia funcţiei μ a lui *Möbius* $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$:

$$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^k, & n = p_1 \cdot \ldots \cdot p_k \ (p_1 < p_2 < \ldots < p_k \text{ prime}) \\ 0, & n \text{ se divide cu } p^2 \ (p \text{ prim}) \end{cases}.$$

Prelungim această funcţie la $\mathbb{Q}_+$, astfel:

$$\overline{\mu} : \mathbb{Q}_+ \to \{-1, 0, 1\}, \qquad \overline{\mu}(x) = \begin{cases} \mu(x), & x \in \mathbb{N}^* \\ 0, & x \in \mathbb{Q}_+ \backslash \mathbb{N}^* \end{cases}.$$

Prelungim şi coeficienţii binomiali prin egalităţile:

$$\binom{a}{k} = \frac{a(a-1) \cdot \ldots \cdot (a-k+1)}{k!}, \text{ unde } a \in \mathbb{Z}, k \in \mathbb{N}^*;$$

$$\binom{a}{0} = 1, \text{ unde } a \in \mathbb{Z}.$$

Cu notaţiile de mai sus, avem:

Teorema 12. (*Möller-Endo*) *Dacă*:

$$\Phi_n(X) = X^{\varphi(n)} + c_1 X^{\varphi(n)-1} + c_2 X^{\varphi(n)-2} + \ldots + c_{\varphi(n)},$$

atunci:

$$c_k = \sum_{\substack{i_1+2i_2+\ldots+ki_k=k \\ i_1\geq 0, i_2\geq 0, \ldots, i_k\geq 0}} (-1)^{i_1+i_2+\ldots+i_k} \binom{\overline{\mu}(n)}{i_1} \binom{\overline{\mu}\left(\frac{n}{2}\right)}{i_2} \cdot \ldots \cdot \binom{\overline{\mu}\left(\frac{n}{k}\right)}{i_k},$$

pentru $1 \leq k \leq \varphi(n)$, *deci coeficienţii celui de-al n-lea polinom ciclotomic se pot calcula efectiv.*

BIBLIOGRAFIE

[1] M. Ţena, *Rădăcinile unităţii*, Societatea de Ştiinţe Matematice din România, Bucureşti, 2005.