

Koliko ničel leži na enotski krožnici?

Sodobni trendi v izobraževanju matematike

Barbara Bone in Lucija Bogataj
Fakulteta za matematiko in fiziko
Oddelek za matematiko

28. marec 2022

Gradivo prirejeno po [1].

Opomba: Besedilo v modri barve te po kliku na to besedilo odpelje na neko spletno stran.

[Za uvod v temo si poglej video.](#)

V gradivu obravnavamo polinome oblike

$$p(z) = z^n + z^k - 1$$

nad poljem kompleksnih števil, kjer je $n, k \in \mathbb{N}$ in $1 \leq k \leq n-1$. Polinom ima n ničel (sledi iz osnovnega izreka algebre), nas pa zanima, katere od teh ničel ležijo na enotski krožnici. Spomnimo se še, da število na enotski krožnici po de Moivreovi formuli lahko zapišemo kot $e^{i\varphi}$, kjer je $\varphi \in [0, 2\pi]$.

Definicija 1 *Unimodularne ničle so tiste ničle, ki ležijo na enotski krožnici v kompleksni ravnini.*

1 Potrebni in zadostni pogoji

Unimodularne ničle lahko označimo z $e^{i\varphi}$. Denimo, da polinom $p(z) = z^n + z^k - 1$ ima neko unimodularno ničlo. Potem velja:

$$e^{in\varphi} + e^{ik\varphi} = 1.$$

To nam pove, da sta člena v vsoti unimodularni kompleksni števili, katerih vsota je natanko 1 (tudi unimodularno število). S konjugiranjem enakosti

dobimo tudi $e^{-in\varphi} + e^{-ik\varphi} = 1$. Edini tak par je $\frac{1}{2} \pm i\sqrt{\frac{3}{2}} = e^{\pm i\pi/3}$. Izrazimo sedaj n in k ;

$$\begin{aligned} n\varphi &= \pm \frac{\pi}{3} + 2\pi\alpha \\ k\varphi &= \mp \frac{\pi}{3} + 2\pi\beta, \end{aligned}$$

za $\alpha, \beta \in \mathbb{Z}$. Izrazimo kot φ iz posamezne enačbe, enačimo in računamo:

$$\begin{aligned} \pm \frac{\pi}{3n} + \frac{2\pi\alpha}{n} &= \mp \frac{\pi}{3k} + \frac{2\pi\beta}{k} \\ \frac{\pm\pi + 6\pi\alpha}{3n} &= \frac{\mp\pi + 6\pi\beta}{3k} \\ 3k(\pm\pi + 6\pi\alpha) &= 3n(\mp\pi + 6\pi\beta) \\ \pm 3\pi(k + n) &= 6\pi \cdot 3(-k\alpha + n\beta) \\ n + k &= \pm 6(n\beta - k\alpha) \end{aligned}$$

S tem smo izpeljali lemo, ki nam pove potrebne pogoje za unimodularne ničle polinoma:

Lema 1 Naj bosta $n, k \in \mathbb{N}$, $1 \leq k \leq n - 1$. Če polinom $p(z) = z^n + z^k - 1$ ima unimodularne ničle, potem $n + k \equiv 0 \pmod{6}$.

To je potreben pogoj, ni pa zadosten. Nadaljuj z ogledom [videa](#) in pozorno poslušaj razlago v njem.

Obrazložitev k videu, dodana 25. 3. 2022, 13.27: Opozorjeni sva bili na napako v izračunu ničel za $u^2 + u - 1 = 0$. Dejanski ničli sta: $u_{1,2} = \frac{-1 \pm \sqrt{5}}{2}$, torej brez imaginarne enote. Ničle polinoma p izračunamo kot $\pm \sqrt{u_{1,2}}$. Sledi, da je $z_{1,2} = \pm \sqrt{u_1}$; $u_1 = \frac{-1 - \sqrt{5}}{2}$, pri čemer korenimo negativno število in tukaj dobimo imaginarno enoto. Še vedno pa velja, da so $z_{1,2,3,4}$ kompleksna števila, ki ne ležijo na enotski krožnici. Za napako se opravičujeva.

Lema 2 Naj bosta $n, k \in \mathbb{N}$, $1 \leq k \leq n - 1$ in $g = \gcd(n, k)$. Potem ima polinom $p(z) = z^n + z^k - 1$ unimodularne ničle, če in samo če ima $q(z) = z^{n/g} + z^{k/g} - 1$ unimodularne ničle.

Dokaz. Denimo, da je z_0 unimodularna ničla polinoma p . Tudi z_0^g je unimodularno število (to hitro vidimo, če uporabimo deMoirov zapis za kompleksno število). Računajmo: $g(z_0^g) = (z_0^g)^{n/g} + (z_0^g)^{k/g} - 1 = p(z_0) = 0$. Denimo še, da je w_0 unimodularna ničla polinoma q . Označimo z ω kompleksno število, da velja $\omega^g = w_0$. Računajmo: $p(\omega) = \omega^n + \omega^k - 1 = (\omega^g)^{\frac{n}{g}} + (\omega^g)^{\frac{k}{g}} - 1 =$

$$q(w_0) = 0.$$

□

Po tej lemi lahko obravnavamo le polinome $p(z) = z^n + z^k - 1$, kjer sta n in k tuja (v tuji literaturi *relatively prime*).

Spomnimo se rezultata iz teorije števil za rešitve diofantskih enačb:

Trditev 1 *Celoštevilska enačba $ax + by = c$ za par (x, y) ima rešitve natanko tedaj, ko $g = \gcd(a, b)$ deli c . Še več, če je (x_0, y_0) partikularna rešitev, potem ostale rešitve dobimo z*

$$x = x_0 + m\frac{b}{g}, y = y_0 - m\frac{a}{g},$$

za $m \in \mathbb{Z}$.

Lema 3 *Če velja $n + k \equiv 0 \pmod{6}$ in $\gcd(n, k) = 1$, potem sta $e^{\pm i\pi/3}$ edini unimodularni ničli polinoma $p(z) = z^n + z^k - 1$.*

Dokaz. Iz predpostavk o številih n in k sledi, da obe števili nista deljivi niti z 2 niti s 3. Denimo, da $2|n$. Potem je $n = 2m$ in $k = 2l + 1$, saj sta števili tuji. Ker je njuna vsota deljiva s 6, je deljiva tudi z 2 in s 3. Iz prej povedanega pa sledi $n + k = 2(m + l) + 1$ in smo prišli v protislovje. Podoben razmislek je za deljivost n s 3. Za izpeljavo lastnosti za število k vlogi n in k v napisanem razmisleku obrnemo.

Iz nedeljivosti števil z dva in s tri, sledi, da sta števili kongruentni $\pm 1 \pmod{6}$. Torej obstajata števili $s, t \in \mathbb{Z}_+$, da je $n = 6s \pm 1$ in $k = 6t \mp 1$. Vzemimo $n = 6s + 1$ in $k = 6t - 1$, dokazovanje za obraten primer je podobno. Imamo torej:

$$p(z) = z^{6s+1} + z^{6t-1} - 1 = z^{6s}z + z^{6t}\frac{1}{z} - 1.$$

Hiter račun pokaže, da velja $p(e^{\pm i\pi/3}) = 0$.

Denimo sedaj, da obstaja nek φ , da $p(e^{i\varphi}) = 0$, torej, da ima polinom p neko unimodularno ničlo. Pokazali bomo, da je $\varphi = \pm \frac{\pi}{3}$, morda še prištejemo večkratnik 2π . Po lemi 1 sledi, da za potence velja $n + k \equiv 0 \pmod{6}$. Enakost lahko zapišemo kot dve linearni (neodvisni) diofantski enačni:

$$-6k\alpha + 6n\beta = n + k$$

$$6k\alpha - 6n\beta = n + k,$$

kjer sta α, β celotševilski neznanki v enačbah. Oglejmo si rešitve posamezne enačbe. Po trditvi 1 iz teorije števil o obstoju rešitve linearne difonatske enačbe le v primeru, ko največji skupni delitelj koeficientov pri neznankah

deli prosti člen sledi, da mora $\gcd(6n, 6k)$ deliti $n + k$. Ker $\gcd(n, k) = 1$, je $\gcd(6k, 6n) = 6$ in velja $6|(n + k)$ po lemi 1.

Očitno par $\alpha = s, \beta = t$ reši prvo enačbo, kjer sta s, t iz prej predpisane oblike števil n, k ; $n = 6s + 1, k = 6t - 1$. Par $\alpha = n - s, \beta = k - t$ pa reši drugo enačbo. Po trditvi 1 so rešitve prve enačbe oblike

$$\alpha = s + m \cdot n, \beta = t + m \cdot k,$$

kjer je $m \in \mathbb{Z}$. Rešitve druge enačbe pa so oblike

$$\alpha = n - s - m \cdot n, \beta = k - t - m \cdot k,$$

kjer je $m \in \mathbb{Z}$.

Pri izpeljavi leme 1 smo uporabili izražavi:

$$n\varphi = \pm \frac{\pi}{3} + 2\pi\alpha$$

$$k\varphi = \mp \frac{\pi}{3} + 2\pi\beta,$$

Enačbi seštejemo in uporabimo $n = 6s + 1$ in $k = 6t - 1$.

$$\varphi(n + k) = 2\pi(\alpha + \beta)$$

$$\varphi(6s + 6t) = 2\pi(\alpha + \beta)$$

$$\varphi = \frac{\pi}{3} \frac{\alpha + \beta}{s + t}$$

Dobili smo izražavo za kot, ki predstavlja unimodularno ničlo $e^{i\varphi}$. Če uporabimo rešitev prve linearne diofantske enačbe dobimo:

$$\varphi = \frac{\pi}{3} \cdot \frac{s + t}{s + t} = \frac{\pi}{3}, \text{ oziroma } e^{i\pi/3}.$$

Uporabimo še rešitev druge linearne difonatske enačbe za $m = 1$ in dobimo:

$$\varphi = \frac{\pi}{3} \cdot \frac{-s - t}{s + t} = -\frac{\pi}{3}, \text{ oziroma } e^{-i\pi/3}.$$

Res smo dobili $\varphi \equiv \pm \frac{\pi}{3} \pmod{2\pi}$. □

Oglej si še zadnji del [videa](#).

2 Glavni rezultat

Izrek 1 Naj bo $p(z) = z^n + z^k - 1$, $1 \leq k \leq n-1$, in označimo $g = \gcd(n, k)$ največjega skupnega delitelja eksponentov. Če 6 deli $\frac{n}{g} + \frac{k}{g}$, potem ima p natanko $2 \cdot g$ unimodularnih ničel, ki so konjugirani pari $z_m, \bar{z}_m$, definirani kot

$$z_m = \exp \left[i \left(\frac{\pi}{3g} + \frac{2\pi m}{g} \right) \right] = \exp \left[i \frac{1}{g} \left(\frac{\pi}{3} + 2\pi m \right) \right],$$

kjer $0 \leq m \leq g-1$.

Dokaz. Dokaz preprosto sledi iz prejšnjih lem; polinom $q(z) = z^{n/g} + z^{k/g} - 1$ zadostuje pogojem leme 3 in ima zato natanko dve unimodularni ničli oblike $\omega_0 = e^{\pm i\pi/3}$, tj. pri kotu $\varphi = \pm \frac{\pi}{3}$. Iz dokaza leme 2 sledi, da so ničle ω polinoma p take, da velja $\omega^g = \omega_0$, torej g -ti koreni ničle ω_0 , ki jih znamo rešiti s pomočjo de Moivreovega zapisa kompleksnega števila. $\varphi = \frac{\pi}{3g} + \frac{2\pi}{g} \cdot m$, kjer je $m \in \{0, 1, \dots, g-1\}$. $\square$

3 Vaje

Naloga 1 V motivaciji v videu je prikazan primer polinoma $p(z) = z^7 + z^5 - 1$, za katerega smo iz animacije v GeoGebri razbrali, da ima natanko dve unimodularni ničli. Najdi ti ničli! Zakaj pri ostalih polinomih iz družine $p(z) = z^7 + z^k - 1$, $1 \leq k \leq 6$ ni unimodularnih ničel?

Naloga 2 Najdimo unimodularne ničle v družini polinomov $p(z) = z^{70} + z^k - 1$, $1 \leq k \leq 69$. Za lažje računanje si pomagaj s programom, ki ti izračuna primerne k .

Naloga 3 Vzemimo splošen primer, ko je $p \geq 5$ praštevilo in k omejen z 1 in $p-1$. Kdaj so zadoščeni pogoji za glavni rezultat predavanja? Koliko ničel dobimo v primeru, ko je zadoščeno tem pogojem?

Naloga 4 Poiščimo unimodularne ničle polinoma $p(z) = z^5 + z^1 - 1$ in sklepajmo na ničle polinoma $q(z) = z^{5m} + z^{1m} - 1$.

Literatura

- [1] Michael Brilleslyper in Beth Schaubroeck. "Locating Unimodular Roots". V: *The College Mathematics Journal* 45.3 (2014), str. 162–168. ISSN: 07468342, 19311346. URL: <http://www.jstor.org/stable/10.4169/college.math.j.45.3.162>.