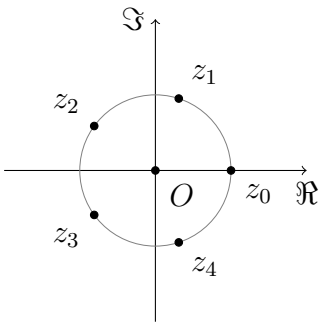
Zimska radionica - Filtar korijena iz jedinice

Adrian Beker

12. siječnja 2024.

1 Uvod

Kada kao funkciju izvodnicu imamo polinom, čiji koeficijenti predstavljaju određene kombinatorne informacije od interesa (npr. broj podskupova/nizova s određenim svojstvom), često nam se javlja potreba da "profiltriramo" članove stupnja djeljivog nekim danim prirodnim brojem. Metoda filtra korijena iz jedinice omogućit će nam da učinimo upravo to. S obzirom da se ona uvelike oslanja na računanje s korijenima iz jedinice, prisjetimo se za početak njihove definicije i osnovnih svojstava.



Slika 1: 5-ti korijeni iz jedinice u kompleksnoj ravnini

Neka je n prirodan broj. Kompleksan broj z je *n-ti korijen iz jedinice* ako zadovoljava $z^n = 1$. Za n-ti korijen iz jedinice z kažemo da je *primitivan* ukoliko ne postoji prirodan broj $n' < n$ takav da $z^{n'} = 1$. Na ovom predavanju, za primitivan n-ti korijen jedinice rezervirat ćemo oznaku ξ. Sljedećom propozicijom dana je osnovna karakterizacija (primitivnih) korijena iz jedinice.

Propozicija 1. *Za prirodan broj n:*

(i) postoji točno n različitih n-tih korijena iz jedinice – oni su upravo $e^{\frac{2\pi ik}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$ za $k \in \{0, 1, \ldots, n-1\}$;

(ii) $e^{\frac{2\pi ik}{n}}$ primitivan je n-ti korijen iz jedinice ako i samo ako je k relativno prost s n.

Primitivni korijeni iz jedinice značajni su iz sljedećeg razloga: ako je ξ primitivan n-ti korijen iz jedinice, tada brojevi ξ^k za $k \in \{0, 1, \ldots, n-1\}$ čine popis svih n-tih korijena iz jedinice. Drugim riječima, sve n-te korijene iz jedinice možemo dobiti potenciranjem primitivnog korijena iz jedinice. U sljedećoj lemi dana su neka osnovna pravila kojima se koristimo pri računanju s korijenima iz jedinice.

Lema 2. *Za n-ti korijen iz jedinice z vrijedi:*

(i) $|z| = 1$ *te je* $\overline{z} = z^{-1}$ *također n-ti korijen iz jedinice;*

(ii) za cijele brojeve k, l *vrijedi* $z^k = z^l$ *ako* $k \equiv l \pmod{n}$*, a obrat vrijedi ukoliko je* z *primitivan.*

Posebno, n-ti korijeni iz jedinice čine vrhove pravilnog n-terokuta upisanog u jediničnu kružnicu u kompleksnoj ravnini, s tim da se jedan vrh nalazi u točki 1. Slika 1 prikazuje situaciju za $n = 5$.

Izdvojimo sada jednu jednostavnu činjenicu koja predstavlja temelj za metodu kojom ćemo se baviti.

Lema 3. *Za* n*-ti korijen iz jedinice* z *vrijedi*

$$\sum_{j=0}^{n-1} z^j = \begin{cases} n & \text{ako } z = 1 \\ 0 & \text{inače} \end{cases}.$$

Posebno, za $n > 1$*, suma svih* n*-ti korijena iz jedinice jednaka je* 0*.*

Dokaz. Ako je $z = 1$, tada je $z^j = 1$ za sve $j \in \{0, 1, \ldots, n-1\}$ pa tvrdnja slijedi. U suprotnom, primjenom formule za sumu geometrijskog niza dobivamo

$$\sum_{j=0}^{n-1} z^j = \frac{1 - z^n}{1 - z} = 0.$$

Posebno, za $n > 1$ možemo kao z uzeti neki primitivan korijen iz jedinice te zaključiti da je suma svih n-tih korijena iz jedinice jednaka 0. □

Ono što u užem smislu smatramo filtrom korijena iz jedinice precizno je formulirano u sljedećem rezultatu.

Propozicija 4. *Neka je* $f(X) = \sum_{k=0}^{d} a_k X^k$ *polinom s kompleksnim koeficijentima. Tada za prirodan broj* n *vrijedi*

$$\sum_{n|k} a_k = \frac{1}{n} \sum_{j=0}^{n-1} f(\xi^j)$$

gdje je ξ *primitivan* n*-ti korijen iz jedinice.*

Dokaz. Dokaz se svodi na jednostavnu zamjenu sumacije i korištenje Leme 3. Konkretno, imamo

$$\sum_{j=0}^{n-1} f(\xi^j) = \sum_{j=0}^{n-1} \sum_{k=0}^{d} a_k (\xi^j)^k = \sum_{k=0}^{d} a_k \sum_{j=0}^{n-1} (\xi^k)^j.$$

Kako je ξ primitivan, iz dijela (ii) Leme 2 slijedi $\xi^k = 1$ ako i samo ako n dijeli k. Dakle, iz Leme 3 slijedi

$$\sum_{j=0}^{n-1} (\xi^k)^j = \begin{cases} n & \text{ako } n \mid k \\ 0 & \text{inače} \end{cases},$$

odakle slijedi željena tvrdnja. □

Dakle, Propozicija 4 govori da, za dani polinom, sumu koeficijenata članova stupnja djeljivog s n možemo dobiti uprosječivanjem njegovih vrijednosti u n-tim korijenima iz jedinice. S posljedicama ove činjenice u zadacima iz kombinatorike i teorije brojeva upoznat ćemo se u sljedećem poglavlju.

Za kraj, spomenimo još da ova metoda jednako dobro funkcionira i kada koeficijenti našeg polinoma pripadaju bilo kojem polju koje sadrži n različitih korijena iz jedinice. Ovdje pojam *polje* označava algebarsku strukturu u kojem možemo obavljati sve osnovne računske operacije (zbrajanje, oduzimanje, množenje, dijeljenje) te pritom one imaju odgovarajuća svojstva (postojanje neutralnih elemenata, komutativnost, asocijativnost, distributivnost). U velikoj većini primjena, nas će zanimati polje kompleksnih brojeva $\mathbb{C}$. Tek će u ponekom zadatku biti potrebno gledati polje $\mathbb{F}_p$ ostataka modulo p, gdje je p prost broj. U takvom polju možemo primijeniti opisanu metodu kada god je $p \equiv 1 \pmod{n}$. Zaista, tada možemo uzeti primitivni korijen g modulo p te će tada $\xi = g^{\frac{p-1}{n}}$ biti primitivni n-ti korijen iz jedinice u $\mathbb{F}_p$, a n-ti korijeni iz jedinice bit će ξ^k za $k \in \{0, 1, \ldots, n-1\}$. Lema 3 te Propozicija 4 ostaju valjani u ovim okolnostima, s istovjetnim dokazima.

2 Primjeri

Primjene započinjemo jednim poznatim primjerom.

Primjer 1. Koliko ima podskupova skupa $\{1, 2, \ldots, 2024\}$

(a) parne veličine;

(b) veličine kongruentne 1 modulo 3?

Rješenje. Promotrimo polinom $f(X) = (1+X)^{2024} = \sum_{k=0}^{2024} a_k X^k$, gdje je $a_k = \binom{2024}{k}$ broj podskupova veličine k. Kako je -1 primitivan drugi korijen iz jedinice, iz Propozicije 4 slijedi da je broj podskupova parne veličine jednak

$$\sum_{2|k} a_k = \frac{1}{2}(f(-1) + f(1)) = \frac{(1-1)^{2024} + (1+1)^{2024}}{2} = 2^{2023}.$$

Za dio (b), trebat ćemo se mrvicu više pomučiti s računanjem, no princip je isti. Neka je $\xi = e^{\frac{2\pi i}{3}}$ primitivan treći korijen iz jedinice. Tada je broj podskupova veličine kongruentne 1 modulo 3 jednak

$$\sum_{k \equiv 1 \pmod 3} a_k = \sum_{3|k} \langle X^k \rangle (X^2 f(X)),$$

pri čemu s $\langle X^k \rangle g(X)$ označavamo koeficijent uz X^k u polinomu $g(X)$. Dakle, prema Propoziciji 4, traženi je broj jednak

$$\begin{aligned}
\frac{1}{3}(\xi^0 f(\xi^0) + \xi^2 f(\xi^1) + \xi^1 f(\xi^2)) &= \frac{(1+1)^{2024} + \xi^2(1+\xi)^{2024} + \xi(1+\xi^2)^{2024}}{3} \\
&= \frac{2^{2024} + \xi^2(-\xi^2)^{2024} + \xi(-\xi)^{2024}}{3} \\
&= \frac{2^{2024} + 2}{3},
\end{aligned}$$

pri čemu smo u drugoj jednakosti koristili činjenicu da vrijedi $1+\xi+\xi^2=0$, koja slijedi iz Leme 3 za $n=3$. $\square$

Napomena 1. U Primjeru 1, dio (a) nije teško riješiti i kombinatorno tako da pronađemo bijekciju između podskupova parne i neparne veličine, npr. možemo gledati preslikavanje koje mijenja pripadnost određenog elementa danom podskupu. Međutim, dio (b) već je dosta teže riješiti kombinatornim pristupom, dok se metoda filtra korijena iz jedinice generalizira bez puno dodatnog napora.

Sljedeći primjer također je klasičan.

Primjer 2. (IMC 1999.) Ako igraću kocku bacimo n puta, koja je vjerojatnost da će zbroj dobivenih brojeva biti djeljiv s 5?

Rješenje. Tražena je vjerojatnost jednaka omjeru broja povoljnih ishoda i ukupnog broja ishoda:

$$p(n)=\frac{|\{(x_1,\ldots,x_n)\in\{1,\ldots,6\}^n \mid x_1+\ldots+x_n\equiv 0 \pmod 5\}|}{6^n}. \qquad (1)$$

Dakle, zanima nas funkcija izvodnica za broj nizova duljine n s elementima iz skupa $\{1,\ldots,6\}$ koji imaju danu sumu. U tu svrhu promotrimo polinom $f(X)=(X^1+X^2+\ldots+X^6)^n$. Primijetimo da će broj spomenutih nizova sa sumom točno s biti upravo $\langle X^s\rangle f(X)$: član X^s dobivamo tako da prilikom razvijanja polinoma f, za svaki $i\in\{1,\ldots,n\}$ iz i-te zagrade odaberemo član X^{x_i} za neki $x_i\in\{1,\ldots,6\}$, na način da pritom vrijedi $x_1+\ldots+x_n=s$. Dakle, označimo li $\xi=e^{\frac{2\pi i}{5}}$, iz Propozicije 4 slijedi da je brojnik u razlomku (1) jednak

$$\begin{aligned}\frac{1}{5}\sum_{j=0}^{4} f(\xi^j) &= \frac{1}{5}\left(6^n+\sum_{j=1}^{4}\left(\xi^j\cdot\frac{1-(\xi^j)^6}{1-\xi^j}\right)^n\right)\\ &= \frac{1}{5}\left(6^n+\sum_{j=1}^{4}\xi^{jn}\right)\\ &= \frac{1}{5}\left(6^n-1+\sum_{j=0}^{4}(\xi^n)^j\right).\end{aligned}$$

Konačno, sada slijedi da je tražena vjerojatnost jednaka

$$p(n)=\begin{cases}\frac{1}{5}\left(1+\frac{4}{6^n}\right) & \text{ako } 5\mid n\\ \frac{1}{5}\left(1-\frac{1}{6^n}\right) & \text{inače}\end{cases},$$

pri čemu smo ponovo iskoristili Lemu 3. $\square$

3 Zadaci

Zadaci su odabrani tako da se u njima treba koristiti barem jedan od rezultata koji čine srž metode filtra korijena iz jedinice (Lema 3 i Propozicija 4), a najčešće i oba. Prilikom biranja poretka zadataka, glavno je nastojanje bilo da se tematski slični zadaci nalaze jedan do drugoga. Također, težina zadataka ugrubo raste od početka prema kraju.

1. Koliko ima n-znamenkastih brojeva sa znamenkama iz skupa $\{1, 3, 4, 6, 7, 9\}$ kojima je zbroj znamenaka djeljiv sa 7?

2. (RMM 2017.)

   (a) Dokaži da se svaki prirodan broj n može jedinstveno napisati u obliku

   $$n = \sum_{j=1}^{2k+1} (-1)^{j-1} 2^{m_j},$$

   gdje su $k \geq 0$ te $0 \leq m_1 < m_2 < \ldots < m_{2k+1}$ cijeli brojevi. Broj k nazivamo *težina* broja n.

   (b) Odredi (u zatvorenom obliku) razliku između brojeva prirodnih brojeva manjih od ili jednakih 2^{2017} parne i neparne težine.

3. (IMO Shortlist 2007.) Odredi sve prirodne brojeve n takve da je elemente skupa $[n] = \{1, \ldots, n\}$ moguće obojati crveno i plavo na način da postoji točno 2007 trojki $(x, y, z) \in [n]^3$ takvih da su x, y, z iste boje te n dijeli $x + y + z$.

4. (Kineski TST 2010.) Svaki element skupa $[n] = \{1, \ldots, n\}$ obojan je crveno, bijelo ili plavo. Za trojku $(x, y, z) \in [n]^3$ kažemo da je *dobra* ukoliko n dijeli $x+y+z$. Neka je A skup svih dobrih trojki (x, y, z) takvih da su x, y, z iste boje, a B skup svih dobrih trojki (x, y, z) takvih da su x, y, z u parovima različitih boja. Dokaži da vrijedi $|B| \leq 2|A|$.

5. (IMO 1995.) Neka je $p > 2$ prost broj. Koliko ima p-članih podskupova skupa $\{1, 2, \ldots, 2p\}$ kojima je zbroj elemenata djeljiv s p?

6. Dokaži da je broj podskupova skupa $\{1, \ldots, n\}$ čiji je zbroj elemenata djeljiv s n jednak

   $$\frac{1}{n} \sum_{\substack{d \mid n \\ 2 \nmid d}} \varphi(d) 2^{\frac{n}{d}}.$$

7. Ploča dimenzija $m \times n$ može se popločati koristeći pločice oblika $1 \times a$ i $b \times 1$. Dokaži da se ona može popločati koristeći pločice samo jednog od tih oblika.

8. Je li moguće popločati ploču dimenzija 13×13 bez središnjeg polja pločicama oblika 1×4 i 4×1?

9. (IMO Shortlist 2002.) Neka su $m, n > 1$ prirodni brojevi. Neka su $a_1, \ldots, a_n$ cijeli brojevi koji nisu djeljivi s m^{n-1}. Dokaži da postoje cijeli brojevi $e_1, \ldots, e_n$ po apsolutnoj vrijednosti manji od m takvi da nisu svi 0 te m^n dijeli $\sum_{j=1}^{n} e_j a_j$.

10. (IMC 2022.) Neka je p prost broj. U ishodištu brojevnog pravca nalazi se buha. Svake minute, ona ima tri mogućnosti: ostati na mjestu, pomaknuti se za 1 ulijevo ili udesno. Nakon $p - 1$ minuta, buha se želi vratiti u ishodište. Neka je $f(p)$ broj načina na koje ona to može ostvariti (npr. $f(3) = 3$: buha se može uopće ne pomaknuti, pomaknuti za 1 ulijevo pa udesno ili za 1 udesno pa ulijevo). Odredi ostatak pri dijeljenju $f(p)$ s p.

11. (USA TST 2010.) Postoji li prirodan broj k takav da je $p = 6k + 1$ prost te vrijedi
$$\binom{3k}{k} \equiv 1 \pmod{p}?$$

12. (IMO Shortlist 1999.) Neka je $p > 3$ prost broj. Za $T \subseteq \{0, 1, \ldots, p-1\}$ definiramo $E(T)$ kao skup nizova $(x_1, \ldots, x_{p-1}) \in T^{p-1}$ takvih da p dijeli $\sum_{j=1}^{p-1} jx_j$. Dokaži da vrijedi
$$|E(\{0, 1, 3\})| \geq |E(\{0, 1, 2\})|$$
te da se jednakost postiže ako i samo ako je $p = 5$.

13. (IMC 2016.) Za prirodan broj n, neka S_n označava skup svih permutacija skupa $\{1, \ldots, n\}$. Za permutaciju $\pi \in S_n$, neka $\text{inv}(\pi)$ označava broj inverzija u π, odnosno broj parova (i, j) takvih da je $1 \leq i < j \leq n$ te $\pi(i) > \pi(j)$. Neka je $f(n)$ broj permutacija $\pi \in S_n$ takvih da $n + 1$ dijeli $f(n)$. Dokaži da postoji beskonačno mnogo prostih brojeva p takvih da $f(p-1) > \frac{(p-1)!}{p}$ te beskonačno mnogo prostih brojeva p takvih da $f(p-1) < \frac{(p-1)!}{p}$.

14. (USA TSTST 2018.) Neka je $S = \{1, \ldots, 100\}$ te za prirodan broj n, neka je
$$T_n = \{(a_1, \ldots, a_n) \in S^n \mid a_1 + \ldots + a_n \equiv 0 \pmod{100}\}.$$
Odredi sve n takve da vrijedi: kako god obojali točno 75 elemenata skupa S crveno, barem pola n-torki iz T_n ima paran broj crvenih koordinata.