Tema br. 2:

Analitičke metode u kombinatorici

Vjekoslav Kovač, 18. 3. 2022.

Ova tema obrađuje dvije tehnike za detekciju ili enumeraciju kombinatornih objekata: *funkcije izvodnice* i (konačnu) *Fourierovu analizu.*

1 Funkcije izvodnice

Funkcije izvodnice su korisno analitičko oruđe za proučavanje nizova, posebno onih koji dolaze iz raznih kombinatornih problema prebrojavanja. Kao što ćemo vidjeti, usko su povezane uz rekurzivne relacije, traženje zatvorenih formula te ispitivanje asimptotskog ponašanja.

Obična funkcija izvodnica (ili samo *funkcija izvodnica*) niza $(a_n)_{n=0}^{\infty}$ je red potencija

$$A(x) := \sum_{n=0}^{\infty} a_n x^n.$$

Eksponencijalna funkcija izvodnica niza $(a_n)_{n=0}^{\infty}$ je obična funkcija izvodnica od $\big(\frac{a_n}{n!}\big)_{n=0}^{\infty}$, tj.

$$E(x) := \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}.$$

Ako niz $(a_n)_{n=0}^{\infty}$ raste "razumno brzo", tada su funkcije A i E dobro definirane na nekom intervalu $\langle -r, r\rangle$ makar samo za dovoljno mali $r > 0$ i ponekad se mogu izračunati eksplicitne formule za $A(x)$ i $E(x)$. "Razumno brzo" u slučaju obične funkcije izvodnice znači: ne brže od svakog geometrijskog niza. Posebno je fascinantno što u nekim slučajevima imamo vrlo lijepe formule za $A(x)$ ili $E(x)$ makar je teško (ili čak nemoguće) napisati zatvorenu formulu za a_n. Obratno, iz formule za $A(x)$ ili $E(x)$ se razvojem u red potencija (barem načelno) mogu iščitati koeficijenti te dobiti formula za a_n. Ako je $A(x) = \sum_{n=0}^{\infty} a_n x^n$, tada obratno pišemo

$$a_n = [x^n]A(x),$$

tj. $[x^n]A(x)$ nam označava koeficijent uz x^n u razvoju od $A(x)$.

Slijede neki poznati razvoji koji se mogu koristiti.

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \text{za } x \in \mathbb{R}$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \ldots = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}, \quad \text{za } x \in \mathbb{R}$$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}, \quad \text{za } x \in \mathbb{R}$$

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots = \sum_{n=0}^{\infty} x^n, \quad \text{za } |x| < 1$$

$$\frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + 4x^3 + \ldots = \sum_{n=0}^{\infty} (n+1)x^n, \quad \text{za } |x| < 1$$

$$\frac{1}{(1-x)^{k+1}} = \sum_{n=0}^{\infty} \binom{n+k}{k} x^n, \quad \text{za } |x| < 1,\ k \in \mathbb{N}_0$$

$$(1+x)^\alpha = 1 + \binom{\alpha}{1} x + \binom{\alpha}{2} x^2 + \ldots = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n, \quad \text{za } |x| < 1,$$

$$\text{pri čemu je } \binom{\alpha}{n} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$$

$$\ln(1+x) = \frac{x}{1} - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n}, \quad \text{za } |x| < 1$$

$$\operatorname{arctg} x = \frac{x}{1} - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{2n+1}, \quad \text{za } |x| < 1$$

Primjer 1. Koja je obična funkcija izvodnica niza zadanog formulom $a_n = n^2$? Koja je eksponencijalna funkcija izvodnica tog istog niza?

Rješenje.

$$\begin{aligned} A(x) &= \sum_{n=0}^{\infty} n^2 x^n = x^2 \sum_{n=2}^{\infty} n(n-1)x^{n-2} + x \sum_{n=1}^{\infty} n x^{n-1} \\ &= x^2 \sum_{n=0}^{\infty} \underbrace{(n+2)(n+1)}_{2\binom{n+2}{2}} x^n + x \sum_{n=0}^{\infty} (n+1)x^n \\ &= \frac{2x^2}{(1-x)^3} + \frac{x}{(1-x)^2} = \frac{x(1+x)}{(1-x)^3} \end{aligned}$$

$$\begin{aligned} E(x) &= \sum_{n=0}^{\infty} n^2 \frac{x^n}{n!} = \sum_{n=1}^{\infty} \frac{n x^n}{(n-1)!} = \sum_{n=1}^{\infty} \frac{\big((n-1)+1\big)x^n}{(n-1)!} \\ &= \sum_{n=2}^{\infty} \frac{x^n}{(n-2)!} + \sum_{n=1}^{\infty} \frac{x^n}{(n-1)!} = x^2 \sum_{n=0}^{\infty} \frac{x^n}{n!} + x \sum_{n=0}^{\infty} \frac{x^n}{n!} = x(1+x)e^x. \end{aligned}$$

Primjer 2. Koliko ima permutacija skupa $\{1, 2, \ldots, n\}$ koje imaju najviše jedan "pad"? Dakle, traži se broj permutacija $p_1, p_2, \ldots, p_n$ od $1, 2, \ldots, n$ takvih da vrijedi $p_1 < \cdots < p_k$ i $p_{k+1} < \ldots < p_n$ za neki indeks k.

Rješenje. Označimo traženi broj s a_n. Očigledno je $a_1 = 1$, $a_2 = 2$. Kasnije ćemo vidjeti da je praktično staviti $a_0 = 1$.

Svaka permutacija od $1, 2, \ldots, n, n+1$ s opisanim svojstvom je ili identiteta ili ima točno jedan pad. Uzmemo li neku permutaciju od $1, 2, \ldots, n, n+1$ s najviše jednim padom i uklonimo element $n+1$, dobit ćemo permutaciju od $1, 2, \ldots, n$ koja opet ima najviše jedan pad. Ako ta permutacija ima točno jedan pad, tada broj $n+1$ možemo staviti na dva dozvoljena načina. Ako je pak ta permutacija identiteta, tada broj $n+1$ možemo staviti bilo gdje, tj. na $n+1$ načina. Dobili smo

$$a_{n+1} = 2(a_n - 1) + n + 1,$$

tj. rekurzivnu relaciju

$$a_{n+1} = 2a_n + n - 1.$$

Pomnožimo rekurziju s x^{n+1} i prosumirajmo po $n \in \mathbb{N}_0$.

$$\sum_{n=0}^{\infty} a_{n+1} x^{n+1} = 2x \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} (n-1) x^{n+1}$$

$$\sum_{n=1}^{\infty} a_n x^n = 2x \sum_{n=0}^{\infty} a_n x^n - x + x^3 \sum_{n=0}^{\infty} (n+1) x^n$$

Označimo li funkciju izvodnicu s $A(x)$, dobili smo (zbog $a_0 = 1$):

$$A(x) - 1 = 2xA(x) - \frac{x(1-2x)}{(1-x)^2},$$

tj.

$$A(x) = \frac{1}{1-2x} - \frac{x}{(1-x)^2}.$$

Rastav na parcijalne razlomke daje

$$A(x) = \frac{1}{1-2x} + \frac{1}{1-x} - \frac{1}{(1-x)^2}$$

te razvojem u red potencija dobivamo

$$A(x) = \sum_{n=0}^{\infty} 2^n x^n + \sum_{n=0}^{\infty} x^n - \sum_{n=0}^{\infty} (n+1) x^n = \sum_{n=0}^{\infty} (2^n - n)\, x^n.$$

Zato je konačno

$$a_n = [x^n]A(x) = 2^n - n.$$

Primjer 3. Na koliko načina se novčanica od 10 kuna može razmijeniti u kovanice?

Rješenje. Pretvorimo sve iznose u lipe, kako bi bili cjelobrojni. Zapravo tražimo koeficijent uz x^{1000} u produktu

$$\begin{aligned} f(x) = {} & \underbrace{(1 + x + x^2 + x^3 + \cdots)}_{\text{kovanice od 1 lp}} \underbrace{(1 + x^2 + x^4 + x^6 + \cdots)}_{\text{kovanice od 2 lp}} \\ & \cdot \underbrace{(1 + x^5 + x^{10} + x^{15} + \cdots)}_{\text{kovanice od 5 lp}} \underbrace{(1 + x^{10} + x^{20} + x^{30} + \cdots)}_{\text{kovanice od 10 lp}} \\ & \cdot \underbrace{(1 + x^{20} + x^{40} + x^{60} + \cdots)}_{\text{kovanice od 20 lp}} \underbrace{(1 + x^{50} + x^{100} + x^{150} + \cdots)}_{\text{kovanice od 50 lp}} \\ & \cdot \underbrace{(1 + x^{100} + x^{200} + x^{300} + \cdots)}_{\text{kovanice od 1 kn}} \underbrace{(1 + x^{200} + x^{400} + x^{600} + \cdots)}_{\text{kovanice od 2 kn}} \\ & \cdot \underbrace{(1 + x^{500} + x^{1000} + x^{1500} + \cdots)}_{\text{kovanice od 5 kn}}, \end{aligned}$$

koji se izračuna kao

$$\begin{aligned} & (1-x)^{-1}(1-x^2)^{-1}(1-x^5)^{-1}(1-x^{10})^{-1}(1-x^{20})^{-1} \\ & \cdot (1-x^{50})^{-1}(1-x^{100})^{-1}(1-x^{200})^{-1}(1-x^{500})^{-1}. \end{aligned}$$

Ako želimo razviti $f(x)$ u red potencija do člana x^{1000}, možemo u Mathematici koristiti naredbu

$$\text{Series}[f[x], \{x, 0, 1000\}]\,.$$

Ovdje "0" naprosto znači da se razvija oko nule, tj. u potencije $(x-0)^n = x^n$, što ćemo mi uvijek raditi. Očitavanje koeficijenta uz x^{1000} daje

$$[x^{1000}]f(x) = 327631321.$$

Primjer 4. (*Rumunjska 2003.*) Koliko n-znamenkastih brojeva sa znamenkama iz skupa $\{2,3,7,9\}$ je djeljivo s 3?

Rješenje iz [1]. Koristit ćemo karakterizaciju da je broj djeljiv s 3 ako i samo ako je zbroj njegovih znamenaka djeljiv s 3.

Promotrimo funkciju izvodnicu

$$f(x) := (x^2 + x^3 + x^7 + x^9)^n.$$

Njen koeficijent uz x^m nam govori koliko ima n-znamenkastih brojeva sa znamenkama iz skupa $\{2,3,7,9\}$ čiji zbroj znamenaka je upravo m. Uzmimo sada $\omega = e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, tj. ω je primitivni kompleksni treći korijen iz jedinice. Primijetimo da za $m \in \mathbb{Z}$ vrijedi

$$1 + \omega^m + \omega^{2m} = \begin{cases} 3 & \text{ako je } m \text{ djeljiv s } p, \\ \frac{1-\omega^{3m}}{1-\omega^m} = 0 & \text{ako } m \text{ nije djeljiv s 3.} \end{cases}$$

Pogledajmo čemu je jednako

$$\frac{1}{3}\big(f(1) + f(\omega) + f(\omega^2)\big).$$

Ako raspišemo $f(x) = \sum_{m=0}^{9n} a_m x^m$, prema gornjoj formuli to je

$$\sum_{m=0}^{9n} a_m \frac{1}{3}(1 + \omega^m + \omega^{2m}) = \sum_{\substack{0 \le m \le 9n \\ m \text{ je djeljiv s } 3}} a_m,$$

što je upravo traženi broj.

S druge pak strane, direktno uvrštavanje daje

$$\begin{aligned} &\frac{1}{3}\big(f(1) + f(\omega) + f(\omega^2)\big) \\ &= \frac{1}{3}\Big(4^n + (\omega^2 + \omega^3 + \omega^7 + \omega^9)^n + (\omega^4 + \omega^6 + \omega^{14} + \omega^{18})^n\Big) \\ &= \frac{1}{3}\Big(4^n + 2(\underbrace{2 + \omega + \omega^2}_{1+0=1})^n\Big) = \frac{4^n + 2}{3} \end{aligned}$$

i to je željeni rezultat.

Primjer 5. (*Euler*) Dokažite da je broj rastava prirodnog broja na različite pribrojnike jednak broju rastava prirodnog broja na neparne pribrojnike.

Rješenje. Označimo:

$$\begin{aligned} R_n &= \text{broj rastava od } n \text{ na različite pribrojnike}, \\ N_n &= \text{broj rastava od } n \text{ na neparne pribrojnike}. \end{aligned}$$

$$\begin{aligned} \sum_{n=0}^{\infty} R_n x^n &= (1+x)(1+x^2)(1+x^3)\cdots = \prod_{k=1}^{\infty}(1+x^k) = \prod_{k=1}^{\infty} \frac{1-x^{2k}}{1-x^k} \\ &= \frac{\prod_{k=1}^{\infty}(1-x^{2k})}{\prod_{k=1}^{\infty}(1-x^k)} = \frac{1}{\prod_{\substack{k \in \mathbb{N} \\ k \text{ neparan}}}(1-x^k)} = \prod_{\substack{k \in \mathbb{N} \\ k \text{ neparan}}} \frac{1}{1-x^k} \\ &= \prod_{\substack{k \in \mathbb{N} \\ k \text{ neparan}}} (1 + x^k + x^{2k} + x^{3k} + \cdots) = \sum_{n=0}^{\infty} N_n x^n \end{aligned}$$

Izjednačavanjem koeficijenata slijedi $R_n = N_n$.

Primjer 6. (*Zadatak iz knjige [4], poglavlje 2*) Neka je D_n broj permutacija skupa $\{1,2,\ldots,n\}$ bez fiksnih točaka, tj. takvih bijekcija $f\colon \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ da za svaki x vrijedi $f(x) \neq x$. Često se kaže da je D_n broj deranžmana n-članog skupa. Još stavljamo $D_0 := 1$. Najprije izvedite formulu za eksponencijalnu funkciju izvodnicu niza $(D_n)_{n=0}^{\infty}$, a potom dokažite formulu

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Rješenje. Svaka permutacija od $\{1,2,\ldots,n\}$ fiksira nekih k elemenata te potom "deranžira" preostalih $n-k$ elemenata. Kako se k-člani podskup može odabrati na $\binom{n}{k}$ načina, dobili smo formulu

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-k}.$$

Množenjem s $\frac{x^n}{n!}$ i zbrajanjem dobivamo

$$\sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{x^k}{k!} \frac{D_{n-k} x^{n-k}}{(n-k)!}.$$

Na desnoj strani možemo prepoznati produkt redova po principu "svaki sa svakim":

$$\underbrace{\Big(\sum_{k=0}^{\infty} \frac{x^k}{k!} \Big)}_{=e^x} \Big(\sum_{m=0}^{\infty} \frac{D_m x^m}{m!} \Big).$$

Označimo li eksponencijalnu funkciju izvodnicu niza s $D(x)$, dobili smo

$$\frac{1}{1-x} = e^x D(x), \qquad \text{tj. } D(x) = \frac{e^{-x}}{1-x}.$$

Razvijmo sada ponovno $D(x)$ u red.

$$D(x) = \Big(\sum_{k=0}^{\infty} \frac{(-1)^k x^k}{k!} \Big) \big(1 + x + x^2 + x^3 + \cdots \big).$$

Uspoređivanje koeficijenata uz x^n daje

$$\frac{D_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

1.1 Asimptotika nizova

Često je potrebno ustanoviti asimptotsko ponašanje (npr. brzinu rasta) nekog kombinatorno dobivenog niza, a funkcije izvodnice mogu pomoći kod toga.

Kažemo da su nizovi $(a_n)_{n=0}^{\infty}$ i $(b_n)_{n=0}^{\infty}$ asimptotski jednaki i pišemo $a_n \sim b_n$ ako vrijedi

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 1.$$

Naprimjer, poznata Stirlingova formula se može zapisati

$$n! \sim \sqrt{2\pi n} \Big(\frac{n}{e} \Big)^n.$$

Pretpostavke sljedećeg teorema su u praksi zadovoljene za mnoge "kombinatorno dobivene" nizove.

Teorem. (*Iz članka [3]; vidjeti knjigu [2], poglavlje 11*) *Pretpostavimo da je* $(a_n)_{n=0}^{\infty}$ *nenegativni niz čija funkcija izvodnica* $A(x) = \sum_{n=0}^{\infty} a_n x^n$ *ima radijus konvergencije* $r > 0$ *i može se proširiti do holomofne funkcije na području*

$$\{x \in \mathbb{C} \setminus \{r\} : |x| < r + \varepsilon, \ |\operatorname{Arg}(x - r)| > \psi\}$$

za neke $\varepsilon > 0$ *i* $0 < \psi < \pi/2$. *Nadalje pretpostavimo da je ona oblika* $A(x) = f(x)g(x) + h(x)$, *pri čemu vrijedi:*

- $f(x) = \big(-\ln(1 - \frac{x}{r})\big)^b (1 - \frac{x}{r})^c, \quad c \notin \mathbb{N}$ *i nije baš* $b = c = 0$,
- *postoji limes* $L := \lim\limits_{x \uparrow r} g(x) \in \mathbb{R} \setminus \{0\}$,
- *postoji limes* $\lim\limits_{x \uparrow r} h(x) \in \mathbb{R}$.

Ako je $c \neq 0$, *tada vrijedi*

$$a_n \sim \frac{L(\ln n)^b (1/r)^n}{n^{c+1} \Gamma(-c)},$$

a ako je $c = 0$, *tada vrijedi*

$$a_n \sim \frac{bL(\ln n)^{b-1}(1/r)^n}{n}.$$

Ovdje Γ označava gama-funkciju. Obično je dovoljno znati da je $\Gamma(k) = (k-1)!$ za $k \in \mathbb{N}$ te $\Gamma(1/2) = \sqrt{\pi}$, $\Gamma(-1/2) = -2\sqrt{\pi}$, $\Gamma(3/2) = \sqrt{\pi}/2$. Primijetimo još da je $x = r$ prvi "singularitet" funkcije $A(x)$.

Primjer 7. Ako je D_n broj permutacija n-članog skupa bez fiksnih točaka, dokažite

$$D_n \sim \frac{n!}{e}.$$

Rješenje. Funkcija izvodnica od $D_n/n!$ je

$$D(x) = (1 - x)^{-1} e^{-x}$$

pa primjenjujemo teorem za $r = 1$, $b = 0$, $c = -1$, $g(x) = e^{-x}$, $h(x) = 0$,

$$L = \lim_{x \uparrow 1} e^{-x} = e^{-1}.$$

Dobivamo

$$\frac{D_n}{n!} \sim \frac{L \ 1^n}{n^0 \ \Gamma(1)} = L = \frac{1}{e}.$$

Napomenimo da se isti zaključak može izvesti i iz opće formule niza:

$$\lim_{n \to \infty} \frac{D_n}{n!} = \lim_{n \to \infty} \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = e^{-1}.$$

Osim toga, ovdje nije teško dokazati i precizniju tvrdnju: D_n je najbliži cijeli broj broju $n!/e$.

Primjer 8. (*Primjer iz knjige [2], poglavlje 11*) Neka je C_n broj načina na koje se može izračunati izraz

$$a_1 * a_2 * \cdots * a_n$$

(koji ima $n - 1$ znakova $*$) ukoliko je važan poredak vršenja operacije $*$. Naime, zagradama možemo odrediti redoslijed izvšavanja pa je npr. $C_4 = 5$, jer su mogućnosti

$$a_1 * (a_2 * (a_3 * a_4)), \ \ a_1 * ((a_2 * a_3) * a_4), \ \ (a_1 * a_2) * (a_3 * a_4),$$
$$(a_1 * (a_2 * a_3)) * a_4, \ \ ((a_1 * a_2) * a_3) * a_4.$$

To su tzv. Catalanovi brojevi (pomaknuti za 1) i stavljamo $C_0 = 0$. Izvedite izraz za običnu funkciju izvodnicu niza $(C_n)_{n=0}^{\infty}$ pa potom odredite njegovu asimptotiku.

Rješenje. U izrazu $a_1 * a_2 * \cdots * a_n$ promotrimo instancu od $*$ koja se izvršava posljednja. Neka lijevo od nje ima k varijabli i desno od nje $n-k$ varijabli. Dobivamo rekurzivnu relaciju

$$C_n = \sum_{k=1}^{n-1} C_k C_{n-k}.$$

Pomnožimo je s x^n i prosumirajmo po $n \geq 2$.

$$\sum_{n=2}^{\infty} C_n x^n = \sum_{n=2}^{\infty} \sum_{k=1}^{n-1} C_k x^k C_{n-k} x^{n-k} = \sum_{k,m=1}^{\infty} C_k x^k C_m x^m.$$

Označimo li funkciju izvodnicu $C(x) := \sum_{n=0}^{\infty} C_n x^n$, dobivamo (zbog $C_1 = 1$):

$$C(x) - x = C(x)^2,$$

a rješavanje kvadratne jednadžbe po $C(x)$ daje

$$C(x) = \frac{1 - \sqrt{1-4x}}{2}.$$

Kako funkciju izvodnicu možemo zapisati

$$C(x) = \Big(1 - \frac{x}{1/4}\Big)^{1/2} \Big(-\frac{1}{2}\Big) + \frac{1}{2},$$

možemo primijeniti prethodni teorem uz $r = 1/4$, $b = 0$, $c = 1/2$, $g(x) = -1/2$, $L = -1/2$, $h(x) = 1/2$ pa imamo

$$C_n \sim \frac{(-1/2)\ 4^n}{n^{3/2}\ \Gamma(-1/2)} = \frac{4^{n-1}}{\sqrt{\pi}\, n^{3/2}}.$$

To je tražena asimptotika niza.

Napomenimo da se razvojem od $C(x)$ u red može lako izvesti i poznata opća formula

$$C_n = \frac{1}{n}\binom{2n-2}{n-1}, \quad \text{za } n \in \mathbb{N}.$$

2 Fourierova analiza

Fourierova analiza je posebno korisna kod kombinatornih problema koji se bave aritmetičkim strukturama, tj. kada uz same skupove promatramo i operaciju zbrajanja, a ponekad i operaciju množenja. Kako bismo izlaganje održali elementarnim, ovdje ćemo raditi samo na konačnim komutativnim grupama.

Za prirodni broj d označimo sa $\mathbb{Z}_d$ skup ostataka pri dijeljenju s d, tj.

$$\mathbb{Z}_d := \{0, 1, 2, 3, \ldots, d-2, d-1\}.$$

Neka se na skupu $\mathbb{Z}_d$ podrazumijevaju operacije zbrajanja i množenja modulo d, tj. nakon izvršenog zbrajanja ili množenja još podijelimo rezultat s d i uzmemo samo ostatak pri dijeljenju. Tako npr. na $\mathbb{Z}_4$ imamo tablice zbrajanja i množenja:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Fiksirajmo sada $n \in \mathbb{N}$ i $d_1, \ldots, d_n \in \mathbb{N} \setminus \{1\}$. Kada pišemo

$$\mathbb{A} = \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n},$$

tada smatramo da je $\mathbb{A}$ Kartezijev produkt skupova $\mathbb{Z}_{d_1}, \ldots, \mathbb{Z}_{d_n}$ na kojem se promatra zbrajanje po koordinatama. Drugim riječima, elementi od $\mathbb{A}$ su n-torke $x = (x_1, x_2, \ldots, x_n)$ koje se zbrajaju kao:

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) := (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

Često pišemo samo $\mathbf{0}$ umjesto n-torke samih nula, $(0, 0, \ldots, 0)$. Tako npr. operacija zbrajanja na $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ glasi:

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Kažemo da je $(\mathbb{A}, +)$ primjer konačne komutativne grupe i (preciznije) da je $\mathbb{A}$ direktna suma konačno mnogo konačnih cikličkih grupa. Zapravo, svaka konačna komutativna grupa ima strukturu kao gornji primjer za određene parametre n i $d_1, \ldots, d_n$.

Definirajmo preslikavanje

$$E \colon \mathbb{A} \times \mathbb{A} \to \mathbb{C}, \quad E(x, \xi) := \left(e^{2\pi i/d_1}\right)^{x_1 \xi_1} \left(e^{2\pi i/d_2}\right)^{x_2 \xi_2} \cdots \left(e^{2\pi i/d_n}\right)^{x_n \xi_n}$$
$$\text{za } x = (x_1, x_2, \ldots, x_n),\ \xi = (\xi_1, \xi_2, \ldots, \xi_n) \text{ iz } \mathbb{A}.$$

Primijetimo da E poprima vrijednosti u kompleksnim brojevima modula 1. Jedini razlog zašto lijevi argument pišemo latiničnim slovom x, a desni grčkim slovom ξ, je kako bismo naglasili da oni žive u dvije različite "kopije" od $\mathbb{A}$, povezane preslikavanjem E.

To preslikavanje ima sljedeća očigledna svojstva.

$$E(x + y, \xi) = E(x, \xi) E(y, \xi), \quad E(x, \xi + \zeta) = E(x, \xi) E(x, \zeta),$$

$$E(\mathbf{0}, \xi) = 1, \quad E(x, \mathbf{0}) = 1, \quad E(-x, \xi) = \overline{E(x, \xi)}, \quad E(x, -\xi) = \overline{E(x, \xi)},$$

$$\sum_{x \in \mathbb{A}} E(x, \xi) = \begin{cases} |\mathbb{A}| & \text{ako je } \xi = \mathbf{0} \\ 0 & \text{ako je } \xi \neq \mathbf{0} \end{cases} \qquad \sum_{\xi \in \mathbb{A}} E(x, \xi) = \begin{cases} |\mathbb{A}| & \text{ako je } x = \mathbf{0} \\ 0 & \text{ako je } x \neq \mathbf{0} \end{cases}$$

Naprimjer, posljednja formula slijedi za $x = (x_1, x_2, \ldots, x_n)$, $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ iz jednakosti

$$\sum_{\xi \in \mathbb{A}} E(x, \xi) = \left(\sum_{\xi_1 = 0}^{d_1 - 1} \left(e^{2\pi i x_1/d_1}\right)^{\xi_1} \right) \cdots \left(\sum_{\xi_n = 0}^{d_n - 1} \left(e^{2\pi i x_n/d_n}\right)^{\xi_n} \right).$$

Preostaje primijetiti da za $x_j \neq 0$ vrijedi $e^{2\pi i x_j/d_j} \neq 1$ pa formula za parcijalnu sumu geometrijskog reda daje

$$\sum_{\xi_j = 0}^{d_j - 1} \left(e^{2\pi i x_j/d_j}\right)^{\xi_j} = \frac{1 - e^{2\pi i x_j}}{1 - e^{2\pi i x_j/d_j}} = \frac{1 - 1}{1 - e^{2\pi i x_j/d_j}} = 0,$$

dok za $x_j = 0$ imamo

$$\sum_{\xi_j = 0}^{d_j - 1} \left(e^{2\pi i x_j/d_j}\right)^{\xi_j} = \sum_{\xi_j = 0}^{d_j - 1} 1 = d_j.$$

Produkt "preživi" samo kada je $x_1 = \cdots = x_n = 0$ i tada je jednak $d_1 \cdots d_n = |\mathbb{A}|$.

Primjer 9. Koliko se najviše međusobno okomitih "vektora" može odabrati iz skupa $\{-1,1\}^{1024}$?

Napomena: Vektori $u, v \in \mathbb{R}^n$, $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ su okomiti ako i samo ako je njihov skalarni produkt jednak 0, tj. vrijedi $u \cdot v = \sum_{j=1}^{n} u_j v_j = 0$.

Rješenje. U prostoru $\mathbb{R}^n$ može postojati najviše n u parovima okomitih ne-nul vektora. Zato će u našem zadatku odgovor biti 1024 ako još pronađemo primjer koji ima točno 1024 vektora.

Promotrimo grupu $\mathbb{A} = \mathbb{Z}_2^{10} = \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{10}$. Očigledno $\mathbb{A}$ ima $2^{10} = 1024$ elemenata. Za svaki $x \in \mathbb{A}$ promotrimo vektor

$$v^x := \big(E(x,\xi) : \xi \in \mathbb{A}\big)$$

duljine $|\mathbb{A}| = 1024$. Kako se u formuli za E sada pojavljuju samo drugi korijeni iz jedinice (tj. samo potencije od -1), zaključujemo da sve koordinate vektora pripadaju skupu $\{-1,1\}$. Iz svojstava od E se odmah vidi da su vektori v^x međusobno okomiti:

$$v^x \cdot v^y = \sum_{\xi\in\mathbb{A}} E(x,\xi)E(y,\xi) = \sum_{\xi\in\mathbb{A}} E(x,\xi)\overline{E(y,\xi)} = \sum_{\xi\in\mathbb{A}} E(x-y,\xi) = 0$$

ako je $x \neq y$.

Konačno možemo uvesti ključni pojam Fourierove analize. *Fourierova transformacija* funkcije $f\colon \mathbb{A} \to \mathbb{C}$ je nova funkcija $\hat{f}\colon \mathbb{A} \to \mathbb{C}$ definirana formulom

$$\hat{f}(\xi) := \sum_{x\in\mathbb{A}} f(x)E(x,\xi) \quad \text{za svaki } \xi \in \mathbb{A}.$$

Naprimjer:

(a) Ako je $\mathbb{A} = \mathbb{Z}_4$ i ako funkcije na $\mathbb{A}$ pišemo kao uređene četvorke

$$f = (f_0, f_1, f_2, f_3),$$

tada je

$$\hat{f} = \big(f_0 + f_1 + f_2 + f_3,\ f_0 + if_1 - f_2 - if_3,\ f_0 - f_1 + f_2 - f_3,\ f_0 - if_1 - f_2 + if_3\big).$$

(b) Ako je $\mathbb{A} = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ i ako funkcije na $\mathbb{A}$ pišemo kao uređene četvorke

$$f = (f_{00}, f_{01}, f_{10}, f_{11}),$$

tada je

$$\begin{aligned}\hat{f} = \big(&f_{00} + f_{01} + f_{10} + f_{11},\quad f_{00} - f_{01} + f_{10} - f_{11},\\ &f_{00} + f_{01} - f_{10} - f_{11},\quad f_{00} - f_{01} - f_{10} + f_{11}\big).\end{aligned}$$

Neka svojstva Fourierove transformacije su dana u sljedećem teoremu.

Teorem. *(a) Vrijedi sljedeća formula inverzije:*

$$\sum_{\xi\in\mathbb{A}} \hat{f}(\xi)\overline{E(x,\xi)} \;=\; |\mathbb{A}|f(x) \quad \textit{za svaki } x \in \mathbb{A}.$$

Njom se polazna funkcija f može rekonstruirati iz svoje Fourierove transformacije. Posebno, Fourierova transformacija je injektivna, tj. $\hat{f} = \hat{g}$ implicira $f = g$.

(b) Vrijedi Plancherelov identitet:

$$\sum_{\xi\in\mathbb{A}} |\hat{f}(\xi)|^2 \;=\; |\mathbb{A}| \sum_{x\in\mathbb{A}} |f(x)|^2$$

i općenitije:

$$\sum_{\xi\in\mathbb{A}} \hat{f}(\xi)\overline{\hat{g}(\xi)} \;=\; |\mathbb{A}| \sum_{x\in\mathbb{A}} f(x)\overline{g(x)}.$$

(c) Ako je funkcija h definirana kao tzv. konvolucija od f i g,

$$h(x) := \sum_{y\in\mathbb{A}} f(x-y)g(y) \quad \textit{za svaki } x \in \mathbb{A},$$

što pišemo $h = f * g$, tada vrijedi

$$\hat{h}(\xi) = \hat{f}(\xi)\hat{g}(\xi) \quad \textit{za svaki } \xi \in \mathbb{A}.$$

Drugim riječima, Fourierova transformacija prevodi konvoluciju u obični produkt.

(d) Fourierova transformacija je linearna, tj.

$$\widehat{\alpha f + \beta g} = \alpha\hat{f} + \beta\hat{g}.$$

Dokaz. (a)

$$\begin{aligned}\sum_{\xi\in\mathbb{A}} \hat{f}(\xi)\overline{E(x,\xi)} &= \sum_{\xi\in\mathbb{A}}\sum_{y\in\mathbb{A}} f(y)E(y,\xi)\overline{E(x,\xi)} \\ &= \sum_{y\in\mathbb{A}} f(y) \sum_{\xi\in\mathbb{A}} E(y-x,\xi) = |\mathbb{A}|f(x)\end{aligned}$$

(b)

$$\begin{aligned}\sum_{\xi\in\mathbb{A}} \hat{f}(\xi)\overline{\hat{g}(\xi)} &= \sum_{\xi\in\mathbb{A}}\sum_{x,y\in\mathbb{A}} f(x)\overline{g(y)}E(x,\xi)\overline{E(y,\xi)} \\ &= \sum_{x,y\in\mathbb{A}} f(x)\overline{g(y)} \sum_{\xi\in\mathbb{A}} E(x-y,\xi) = |\mathbb{A}| \sum_{x\in\mathbb{A}} f(x)\overline{g(x)}\end{aligned}$$

(c)

$$\begin{aligned}\hat{h}(\xi) &= \sum_{x\in\mathbb{A}} \Big(\sum_{y\in\mathbb{A}} f(x-y)g(y)\Big)E(x,\xi) \\ &= \sum_{x,y\in\mathbb{A}} f(x-y)E(x-y,\xi)\; g(y)E(y,\xi) \\ &= \sum_{z,y\in\mathbb{A}} f(z)E(z,\xi)\; g(y)E(y,\xi) \\ &= \Big(\sum_{z\in\mathbb{A}} f(z)E(z,\xi)\Big)\Big(\sum_{y\in\mathbb{A}} g(y)E(y,\xi)\Big) = \hat{f}(\xi)\hat{g}(\xi)\end{aligned}$$

(d)

$$\begin{aligned}(\widehat{\alpha f + \beta g})(\xi) &= \sum_{x\in\mathbb{A}} \big(\alpha f(x) + \beta g(x)\big)E(x,\xi) \\ &= \alpha\sum_{x\in\mathbb{A}} f(x)E(x,\xi) + \beta\sum_{x\in\mathbb{A}} g(x)E(x,\xi) \\ &= \alpha\hat{f}(\xi) + \beta\hat{g}(\xi)\end{aligned}$$

□

Primjer 10.* (*Bourgain, preuzet iz knjige [6], poglavlje 4*) Neka je p prost broj i $S \subseteq \{1, 2, 3, \ldots, p-1\}$ takav da je $|S| > p^{3/4}$. Dokažite da za svaki cijeli broj m postoje

$$a_1, a_2, b_1, b_2, c_1, c_2 \in S$$

takvi da vrijedi

$$m \equiv a_1 a_2 + b_1 b_2 + c_1 c_2 \pmod{p}.$$

Rješenje. Prisjetimo se da je $\mathbb{Z}_p$ zapravo polje, tj. svaki $s \in \mathbb{Z}_p \setminus \{0\}$ ima inverzni (tj. recipročni) element s^{-1}. U kompaktnijoj skupovnoj notaciji želimo dokazati

$$\mathbb{Z}_p = A \cdot A + A \cdot A + A \cdot A.$$

Promotrimo funkciju $f \colon \mathbb{Z}_p \to \mathbb{C}$, $f := \sum_{s\in S} \chi_{s\cdot S}$, gdje χ označava karakterističnu funkciju skupa. Naprije primijetimo da je

$$\begin{aligned}(f * f * f)(x) &= \sum_{\substack{a,b,c\in\mathbb{Z}_p\\ a+b+c=x}} f(a)f(b)f(c) = \sum_{\substack{a_1,b_1,c_1\in S\\ a,b,c\in\mathbb{Z}_p\\ a+b+c=x}} \chi_{a_1\cdot S}(a)\,\chi_{b_1\cdot S}(b)\,\chi_{c_1\cdot S}(c)\\ &= \sum_{\substack{a_1,b_1,c_1\in S\\ a_2,b_2,c_2\in S\\ a_1a_2+b_1b_2+c_1c_2=x}} 1 \ = \text{broj traženih prikaza od } x\end{aligned}$$

pa zapravo trebamo dokazati da je $(f * f * f)(x) > 0$ za svaki $x \in \mathbb{Z}_p$.

Fourierova transformacija od f je

$$\hat{f}(\xi) = \sum_{s\in S}\sum_{x\in\mathbb{Z}_p} \chi_{sS}(x) e^{2\pi i x\xi/p} = [x = sy] = \sum_{s\in S}\sum_{y\in S} e^{2\pi i s y\xi/p} = \sum_{s\in S} \hat{\chi}_S(s\xi).$$

Imamo $\hat{f}(\xi) = |S|^2$. Za $\xi \neq 0$ su elementi $s\xi$ svi međusobno različiti kako s varira pa aritmetičko-kvadratna nejednakost i Plancherelov identitet daju

$$\begin{aligned}|\hat{f}(\xi)| &\le |S|^{1/2}\Big(\sum_{s\in S} |\hat{\chi}_S(s\xi)|^2\Big)^{1/2} \le |S|^{1/2}\Big(\sum_{\xi\in\mathbb{Z}_p} |\hat{\chi}_S(\xi)|^2\Big)^{1/2}\\ &= |S|^{1/2}\Big(p\sum_{x\in\mathbb{Z}_p} |\chi_S(x)|^2\Big)^{1/2} = |S|^{1/2}p^{1/2}|S|^{1/2} = p^{1/2}|S|.\end{aligned}$$

Zbog nejednakosti Minkowskog imamo

$$\begin{aligned}\Big(\sum_{\xi\in\mathbb{Z}_p} |\hat{f}(\xi)|^2\Big)^{1/2} &\le \sum_{s\in S}\Big(\sum_{\xi\in\mathbb{Z}_p} |\hat{\chi}_{sS}(\xi)|^2\Big)^{1/2}\\ &= \sum_{s\in S} p^{1/2}\Big(\sum_{x\in\mathbb{Z}_p} |\chi_{sS}(x)|^2\Big)^{1/2} = |S|p^{1/2}|S|^{1/2} = p^{1/2}|S|^{3/2}.\end{aligned}$$

Konačno, zbog $(f * f * f)\widehat{\ }(\xi) = \hat{f}(\xi)^3$ i formule inverzije imamo

$$\begin{aligned}(f * f * f)(x) &= \mathrm{Re}(f * f * f)(x) = \frac{1}{p}\mathrm{Re}\sum_{\xi\in\mathbb{Z}_p} \hat{f}(\xi)^3 e^{-2\pi i x\xi/p}\\ &\ge \frac{1}{p}\hat{f}(0)^3 - \frac{1}{p}\sum_{\xi\in\mathbb{Z}_p\setminus\{0\}} |\hat{f}(\xi)|^3\\ &\ge p^{-1}|S|^6 - p^{-1}p^{1/2}|S|\sum_{\xi\in\mathbb{Z}_p} |\hat{f}(\xi)|^2\\ &\ge p^{-1}|S|^6 - p^{-1/2}|S|p|S|^3 = p^{-1}|S|^6 - p^{1/2}|S|^4\\ &= p^{-1}|S|^4\big(|S|^2 - p^{3/2}\big) > 0.\end{aligned}$$

Naime, po pretpostavci zadatka je $|S| > p^{3/4}$, tj. $|S|^2 > p^{3/2}$.

2.1 Princip neodređenosti

Za funkciju $f\colon \mathbb{A} \to \mathbb{C}$ na konačnoj abelovoj grupi $\mathbb{A}$ označimo

$$\begin{aligned} \operatorname{supp}(f) &:= \{x \in \mathbb{A} : f(x) \neq 0\}, \\ \operatorname{supp}(\hat{f}) &:= \{\xi \in \mathbb{A} : \hat{f}(\xi) \neq 0\}. \end{aligned}$$

Kratica “supp” dolazi od engleske riječi “support” koja se na hrvatski prevodi kao “nosač” funkcije.

Teorem. (Princip neodređenosti; *iz članka [5]*)

(a) Za svaku funkciju $f\colon \mathbb{A} \to \mathbb{C}$ koja nije identički jednaka konstanti 0 vrijedi

$$|\operatorname{supp}(f)|\,|\operatorname{supp}(\hat{f})| \geq |\mathbb{A}|.$$

(b) Za svaku funkciju $f\colon \mathbb{Z}_p \to \mathbb{C}$, gdje je p prost broj, koja nije identički jednaka konstanti 0 vrijedi

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \geq p + 1.$$

Obratno, za svake skupove $A, B \subseteq \mathbb{Z}_p$ koji zadovoljavaju $|A|+|B| \geq p+1$ postoji funkcija $f\colon \mathbb{Z}_p \to \mathbb{C}$ takva da je $\operatorname{supp}(f) = A$ i $\operatorname{supp}(\hat{f}) = B$.

Primjer 11. Dokažite (a) dio principa neodređenosti. (Dokaz (b) dijela je puno teži.)

Rješenje. Korištenjem nejednakosti trokuta, Cauchy-Schwarz nejednakosti i Plancherelovog identiteta dobivamo

$$\begin{aligned} \sup_{\xi\in\mathbb{A}} |\hat{f}(\xi)| &= \sup_{\xi\in\mathbb{A}} \Big| \sum_{x\in\mathbb{A}} f(x)E(x,\xi) \Big| \leq \sum_{x\in\mathbb{A}} |f(x)| = \sum_{x\in\operatorname{supp}(f)} |f(x)| \\ &\leq \Big(\sum_{x\in\operatorname{supp}(f)} 1^2 \Big)^{1/2} \Big(\sum_{x\in\operatorname{supp}(f)} |f(x)|^2 \Big)^{1/2} \\ &= |\operatorname{supp}(f)|^{1/2} \Big(\sum_{x\in\mathbb{A}} |f(x)|^2 \Big)^{1/2} \\ &= |\operatorname{supp}(f)|^{1/2} \Big(|\mathbb{A}|^{-1} \sum_{\xi\in\mathbb{A}} |\hat{f}(\xi)|^2 \Big)^{1/2} \\ &= |\mathbb{A}|^{-1/2} |\operatorname{supp}(f)|^{1/2} \Big(\sum_{\xi\in\operatorname{supp}(\hat{f})} |\hat{f}(\xi)|^2 \Big)^{1/2} \\ &\leq |\mathbb{A}|^{-1/2} |\operatorname{supp}(f)|^{1/2} |\operatorname{supp}(\hat{f})|^{1/2} \sup_{\xi\in\mathbb{A}} |\hat{f}(\xi)|. \end{aligned}$$

Ako f nije identički jednaka 0, tada ni $\hat{f}$ nije identički jednaka 0 pa je $\sup_{\xi\in\mathbb{A}} |\hat{f}(\xi)| > 0$. Dijeljenjem s tim faktorom dobivamo traženu nejednakost.

Primjer 12. (*Rezultat iz članka [5].*) Neka je p prost broj i neka je $S := \{z \in \mathbb{C} : z^p = 1\}$ skup p-tih korijena iz jedinice. Nadalje, neka su $c_0, c_1, c_2, \ldots, c_{p-1} \in \mathbb{C}$, među kojima je točno $k \geq 1$ brojeva različito od 0. Dokažite da je moguće odabrati podskup $T \subseteq S$ koji ima $|T| = p-k+1$ elemenata i takav je da za svaki $z \in T$ vrijedi $\sum_{j=0}^{p-1} c_j z^j \neq 0$.

Rješenje. Promotrimo funkciju

$$f\colon \mathbb{Z}_p \to \mathbb{C}, \qquad f(x) := \sum_{j=0}^{p-1} c_j (e^{-2\pi i x/p})^j.$$

Zapravo trebamo dokazati da postoji barem $p-k+1$ različitih $x \in \mathbb{Z}_p$ takvih da je $f(x) \neq 0$, tj. trebamo pokazati $|\operatorname{supp}(f)| \geq p-k+1$.

Primijetimo da je

$$\hat{f}(\xi) = \sum_{x\in\mathbb{Z}_p} \Big(\sum_{j\in\mathbb{Z}_p} c_j e^{-2\pi i x j/p} \Big) e^{2\pi i x\xi/p} = \sum_{j\in\mathbb{Z}_p} c_j \sum_{x\in\mathbb{Z}_p} e^{2\pi i x(\xi-j)/p} = p\, c_\xi.$$

Po pretpostavci zadatka je točno k od brojeva $\hat{f}(0), \hat{f}(1), \ldots, \hat{f}(p-1)$ različito od 0, tj. $|\operatorname{supp}(\hat{f})| = k$. Po (b) dijelu principa neodređenosti imamo

$$|\operatorname{supp}(f)| \geq p+1-|\operatorname{supp}(\hat{f})| = p-k+1.$$

3 Domaća zadaća

Riješite barem 4 zadatka od sljedećih 8 zadataka za vježbu. *Rok predaje*: 1. 4. 2022.

Rješenja mi možete poslati (skenirana ili uslikana) emailom ili ih predati na satu nastavniku koji će tada predavati.

Zadatak 1. Želite podijeliti 20 jednakih čokolada uz sljedeće uvjete.

- Dječaci A, B i C mogu dobiti najviše po jednu čokoladu svaki.
- Djevojčice D i E moraju dobiti neparan broj čokolada.
- Djed F mora dobiti paran broj čokolada, ali ne smije ostati praznih ruku.

Na koliko načina možete podijeliti te čokolade?

Zadatak 2. Neka je $p \geq 3$ prost broj. Nađite broj svih p-članih podskupova od

$$\{1, 2, \ldots, 2p-1, 2p\}$$

čiji zbroj elemenata je djeljiv s p.

Zadatak 3. Pretpostavimo da je skup nenegativnih cijelih brojeva particioniran na k beskonačnih aritmetičkih nizova s razlikama $d_1, d_2, \ldots, d_k$, pri čemu je $k \geq 2$ prirodan broj i $d_1 \geq d_2 \geq \ldots \geq d_k$. Dokažite da mora vrijediti

$$\sum_{j=1}^{k} \frac{1}{d_j} = 1 \quad \text{i} \quad d_1 = d_2.$$

Zadatak 4. Za cijeli broj $n \geq 0$ izračunajte

$$\sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k}.$$

Rezultat zapišite kao zatvorenu formulu, bez suma i produkata.

Zadatak 5. Promotrimo izraz

$$0 \wedge 0 \wedge \cdots \wedge 0,$$

u kojem ima n nula i $n-1$ znakova potenciranja $\wedge$. Otprije znamo da se redoslijed izvršavanja operacija $\wedge$ može izvesti na C_n načina, pri čemu je C_n (pomaknuti) Catalanov broj. Neka je Z_n broj takvih evaluacija koje kao rezultat daju 0. Pritom smatramo da vrijedi:

$$0 \wedge 0 = 1, \quad 0 \wedge 1 = 0, \quad 1 \wedge 0 = 1, \quad 1 \wedge 1 = 1.$$

Dokažite da je

$$\lim_{n\to\infty} \frac{Z_n}{C_n} = \frac{5-\sqrt{5}}{10}.$$

Napomena: Naprimjer, $Z_3 = 1$ jer je $(0 \wedge 0) \wedge 0 = 1 \wedge 0 = 1$ i $0 \wedge (0 \wedge 0) = 0 \wedge 1 = 0$.

Zadatak 6. Neka je B_n broj particija skupa od n elemenata, tzv. *Bellov broj.* Tako je npr.

$$B_0 := 1,\ B_1 = 1,\ B_2 = 2,\ B_3 = 5,\ B_4 = 15,\ B_5 = 52.$$

Najprije izvedite formulu za eksponencijalnu funkciju izvodnicu tog niza, a potom dokažite formulu

$$B_n = \frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}.$$

Zadatak 7. (*Cauchy-Davenportov teorem*) Ako je p prost broj i ako su $A, B \subseteq \mathbb{Z}_p$ neprazni, dokažite da tada vrijedi

$$|A+B| \geq \min\big\{|A| + |B| - 1,\, p\big\}.$$

Pritom, kao i obično, označavamo

$$A + B := \{a + b\,:\, a \in A,\, b \in B\}.$$

Zadatak 8. Neka je n prirodan broj. Označimo s $\mathcal{P}_n$ familiju svih 2^n podskupova skupa $\{1, 2, \ldots, n\}$. Za svaki $S \in \mathcal{P}_n$ dan je realni broj a_S i pretpostavimo da je točno $k \geq 1$ od tih brojeva a_S različito od 0. Dokažite da jednadžba

$$\sum_{S\in\mathcal{P}_n} a_S \prod_{j\in S} x_j = 0$$

ima najviše $\frac{2^n(k-1)}{k}$ rješenja u skupu $\{-1, 1\}^n$, tj. ima najviše toliko n-torki

$$(x_1, x_2, \ldots, x_n)$$

koje zadovoljavaju jednadžbu i za svaki indeks j je ili $x_j = -1$ ili $x_j = 1$.

Napomena: Za $S = \emptyset$ produkt $\prod_{j\in S} x_j$ uvijek interpretiramo kao broj 1. Naprimjer, za $n = 2$ jednadžba glasi

$$a_\emptyset + a_{\{1\}}x_1 + a_{\{2\}}x_2 + a_{\{1,2\}}x_1x_2 = 0.$$

Literatura

[1] Z. R. Abel, *Multivariate Generating Functions and Other Tidbits*, Mathematical reflections **2**, 2006.

[2] E. A. Bender, S. G. Williamson, *Foundations of Combinatorics with Applications*, Dover, 2006.

[3] P. Flajolet, A. Odlyzko, *Singularity Analysis of Generating Functions*, SIAM J. Disc. Math. **3** (1990), 216–240.

[4] H. S. Wilf, *generatingfunctionology*, A K Peters/CRC Press, treće izdanje, 2005.

[5] T. Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett. **12** (2005), 121–127.

[6] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.

Fakultativni kolegij *Studentska natjecanja iz matematike*, ak. god. 2021./2022.

Tema br. 2:

Analitičke metode u kombinatorici

Rješenja zadataka za vježbu

Vjekoslav Kovač

Rješenje zadatka 1. Tražimo koeficijent uz x^{20} nakon što se izmnoži produkt

$$f(x) = (1+x)^3 \Big(\sum_{k=0}^{\infty} x^{2k+1} \Big)^2 \Big(\sum_{k=0}^{\infty} x^{2k+2} \Big).$$

Izračunajmo zatvorenu formulu za $f(x)$.

$$\begin{aligned} f(x) &= (1+x)^3 x^4 \Big(\sum_{k=0}^{\infty} x^{2k} \Big)^3 = (1+x)^3 x^4 \Big(\frac{1}{1-x^2} \Big)^3 \\ &= (1+x)^3 x^4 \frac{1}{(1-x)^3 (1+x)^3} = \frac{x^4}{(1-x)^3}. \end{aligned}$$

Nadalje, razvoj u red potencija koristeći jednu od standardnih formula daje

$$f(x) = x^4 \sum_{n=0}^{\infty} \binom{n+2}{2} x^n = \sum_{n=0}^{\infty} \frac{(n+2)(n+1)}{2} x^{n+4}.$$

Član s potencijom x^{20} odgovara indeksu $n = 16$ pa možemo očitati koeficijent:

$$[x^{20}] f(x) = \frac{18 \cdot 17}{2} = 153.$$

Dakle, možete raspodijeliti čokolade na 153 načina.

Rješenje zadatka 2. Zadatak je sa *IMO 1995. #6.* Rješenje je preuzeto iz knjige [2]. Promotrimo funkciju izvodnicu

$$f(x,y) := \prod_{j=1}^{2p} (xy^j - 1).$$

Za $y = 1$ odmah vidimo da $f(x,1)$ do na predznak prebrojava sve podskupove od $\{1, \ldots, 2p\}$, ali zanimljivo je uvrstiti i druge vrijednosti za y. Označimo $\omega = e^{2\pi i/p}$, tj. ω je primitivni kompleksni p-ti korijen iz jedinice. Primijetimo da za $m \in \mathbb{Z}$ vrijedi

$$\sum_{k=0}^{p-1} \omega^{km} = \begin{cases} p & \text{ako je } m \text{ djeljiv s } p, \\ \frac{1-\omega^{pm}}{1-\omega^{n}} = 0 & \text{ako } m \text{ nije djeljiv s } p. \end{cases}$$

Pogledajmo sada što prebraja funkcija izvodnica

$$\frac{1}{p} \sum_{k=0}^{p-1} f(x, \omega^k).$$

Njezin koeficijent uz x^p je

$$- \sum_{\substack{S \subseteq \{1,\ldots,2p\} \\ |S| = p}} \frac{1}{p} \sum_{k=0}^{p-1} \omega^{k(\text{zbroj elemenata od } S)} = - \sum_{\substack{S \subseteq \{1,\ldots,2p\} \\ |S| = p \\ \text{zbroj elemenata od } S \text{ je djeljiv s } p}} 1$$

pa nakon množenja sa -1 dobivamo upravo broj koji se traži u zadatku.

S druge strane, za $k \in \{1, 2, \ldots, p-1\}$ imamo da su $k, 2k, \ldots, (p-1)k$ modulo p naprosto ispermutirani ostaci $1, 2 \ldots, p-1$, što nam daje

$$\begin{aligned} f(x, \omega^k) &= \prod_{j=1}^{2p} (x\omega^{jk} - 1) = \Big(\prod_{j=0}^{p-1} (x\omega^j - 1) \Big)^2 \\ &= \Big(\omega^{p(p-1)/2} \prod_{j=0}^{p-1} (x - \omega^{-j}) \Big)^2 = \Big(\prod_{j=0}^{p-1} (x - \omega^{-j}) \Big)^2 = (x^p - 1)^2, \end{aligned}$$

pri čemu smo koristili faktorizaciju polinoma pomoću njegovih kompleksnih nultočaka. Dakle,

$$\frac{1}{p} \sum_{k=0}^{p-1} f(x, \omega^k) = \frac{1}{p} (x-1)^{2p} + \frac{p-1}{p} (x^p - 1)^2,$$

a koeficijent posljednje funkcije izvodnice uz x^n iznosi

$$-\frac{1}{p} \binom{2p}{p} + \frac{p-1}{p} \cdot (-2).$$

Slijedi da je traženi broj jednak

$$\frac{\binom{2p}{p} + 2p - 2}{p}.$$

Rješenje zadatka 3. Ovo je rezultat iz knjige [3], poglavlje 4. Neka su aritmetički nizovi na koje je $\mathbb{N}_0$ rastavljen dani sa $(a_j + md_j)_{m=0}^{\infty}$, $j = 1, 2, \ldots, k$. Iz činjenice da oni particioniraju $\mathbb{N}_0$ slijedi

$$\sum_{n=0}^{\infty} x^n = \sum_{j=1}^{k} \sum_{m=0}^{\infty} x^{a_j + md_j},$$

a sumiranje redova daje

$$\frac{1}{1-x} = \sum_{j=1}^{k} \frac{x^{a_j}}{1 - x^{d_j}}.$$

Pomnožimo gornju jednakost s $1 - x$ i pustimo limes kada $x \to 1$. Zbog

$$\lim_{x \to 1} \frac{1-x}{1-x^{d_j}} = \lim_{x \to 1} \frac{1}{1 + x + x^2 + \cdots + x^{d_j - 1}} = \frac{1}{d_j}$$

dobivamo

$$1 = \sum_{j=1}^{k} \frac{1}{d_j}.$$

Zbog $k \geq 2$ mora biti $d_j \geq 2$ za svaki j. Pretpostavimo suprotno tvrdnji $d_1 = d_2$, da vrijedi $d_1 > d_2 \geq \ldots \geq d_k$. Rastavimo desnu stranu gornje jednakosti racionalnih funkcija na parcijalne razlomke nad poljem $\mathbb{C}$. Kod rastava od $\dfrac{x^{a_1}}{1 - x^{d_1}}$ se pojavljuje član $\dfrac{A}{x - e^{2\pi i/d_1}}$, $A \neq 0$, koji se ne pojavljuje na lijevoj strani, a ne može se ni pokratiti s drugim parcijalnim razlomcima na desnoj strani jer $e^{2\pi i/d_1}$ nije nultočka nijednog od polinoma $x^{d_j} - 1$, $j = 2, \ldots, k$. To je kontradikcija.

Rješenje zadatka 4. Ovo je primjer iz knjige [3], poglavlje 4. Označimo $a_n := \sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k}$ i neka je $A(x) = \sum_{n=0} a_n x^n$ funkcija izvodnica tog niza. Korištenjem standardnih formula za sume redova potencija možemo računati

$$A(x) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k} x^n = \sum_{k=0}^{\infty} \sum_{n=k}^{\infty} \binom{n-k+2k}{2k} (2x)^{n-k} x^k$$

$$
\begin{aligned}
&= \sum_{k=0}^{\infty} x^k \sum_{n=0}^{\infty} \binom{n+2k}{2k} (2x)^n = \sum_{k=0}^{\infty} x^k \frac{1}{(1-2x)^{2k+1}} \\
&= \frac{1}{1-2x} \sum_{k=0}^{\infty} \Big(\frac{x}{(1-2x)^2} \Big)^k = \frac{1}{1-2x} \frac{1}{1-\frac{x}{(1-2x)^2}} \\
&= \frac{1-2x}{1-5x+4x^2} = \frac{1-2x}{(1-x)(1-4x)}.
\end{aligned}
$$

Rastav na parcijalne razlomke je

$$A(x) = \frac{1}{3} \cdot \frac{1}{1-x} + \frac{2}{3} \cdot \frac{1}{1-4x},$$

a potom razvijamo u red potencija koristeći standardne formule:

$$A(x) = \frac{1}{3} \sum_{n=0}^{\infty} x^n + \frac{2}{3} \sum_{n=0}^{\infty} (4x)^n = \sum_{n=0}^{\infty} \frac{2^{2n+1}+1}{3} x^n.$$

Uspoređivanje koeficijenata uz x^n daje

$$a_n = [x^n] A(x) = \frac{2^{2n+1}+1}{3}.$$

Rješenje zadatka 5. Ovo je primjer iz knjige [1], poglavlje 11. Praktično nam je staviti $Z_0 = 0$, a očigledno je $Z_1 = 1$. Svaka evaluacija koja daje vrijednost "0" mora biti oblika $A \wedge B$, pri čemu A predstavlja formulu s k nula koja se evaluira u 0, a B predstavlja formulu s $n-k$ nula koja se evaluira u 1. Na taj način dobivamo rekurzivnu relaciju

$$Z_n = \sum_{k=1}^{n-1} Z_k \, (C_{n-k} - Z_{n-k}).$$

Pomnožimo je s x^n i prosumirajmo po $n \geq 2$.

$$
\begin{aligned}
\sum_{n=2}^{\infty} Z_n x^n &= \sum_{n=2}^{\infty} \sum_{k=1}^{n-1} Z_k x^k (C_{n-k} - Z_{n-k}) x^{n-k} \\
&= \Big(\sum_{k=1}^{\infty} Z_k x^k \Big) \Big(\sum_{m=1}^{\infty} (C_m - Z_m) x^m \Big)
\end{aligned}
$$

Označimo sa $Z(x)$ funkciju izvodnicu od $(Z_n)_{n=0}^{\infty}$, a već prije smo s $C(x)$ označili funkciju izvodnicu niza $(C_n)_{n=0}^{\infty}$. Dobili smo kvadratnu jednadžbu po $Z(x)$,

$$Z(x) - x = Z(x) \big(C(x) - Z(x) \big),$$

čije rješavanje daje

$$Z(x) = -\frac{1}{2} \big(1 - C(x) \big) + \frac{1}{2} \sqrt{ \big(1 - C(x) \big)^2 + 4x }.$$

Odabrali smo pozitivni predznak ispred korijena jer mora biti $Z(0) = Z_0 = 0$.

Već smo bili izračunali

$$C(x) = \frac{1}{2} - \frac{1}{2} \sqrt{1-4x}.$$

"Prvi singularitet" funkcije $Z(x)$ je ili $r = \frac{1}{4}$ ili rješenje jednadžbe $\big(1 - C(x)\big)^2 + 4x = 0$. Posljednja jednadžba ima rješenje $x = -\frac{4}{9}$, ali je $\frac{4}{9} > \frac{1}{4}$ pa ostajemo kod $r = \frac{1}{4}$. Slutimo da se $Z(x)$ može prikazati u obliku

$$Z(x) = (1-4x)^{1/2} g(x) + Z(\tfrac{1}{4}).$$

Primijetimo da je

$$C(\tfrac{1}{4}) = \tfrac{1}{2}, \quad Z(\tfrac{1}{4}) = \tfrac{\sqrt{5}-1}{4}.$$

Trebamo izračunati

$$L = \lim_{x\uparrow 1/4} g(x) = \lim_{x\uparrow 1/4} \frac{Z(x) - Z(\frac{1}{4})}{(1-4x)^{1/2}}.$$

Supstitucijom

$$s = \sqrt{1-4x}, \quad x = (1-s^2)/4, \quad C(x) = (1-s)/2$$

taj limes postaje

$$\begin{aligned} L &= \lim_{s\downarrow 0} \frac{-(1+s)/2 + \sqrt{(1+s)^2/4 + (1-s^2)} - 2Z(\frac{1}{4})}{2s} \\ &= \lim_{s\downarrow 0} \frac{-s + \sqrt{5+2s-3s^2} - \sqrt{5}}{4s} = \lim_{s\downarrow 0} \frac{-s + \frac{2s-3s^2}{\sqrt{5+2s-3s^2}+\sqrt{5}}}{4s} \\ &= \lim_{s\downarrow 0} \frac{-1 + \frac{2-3s}{\sqrt{5+2s-3s^2}+\sqrt{5}}}{4} = \frac{-1+\frac{2}{2\sqrt{5}}}{4} = -\frac{5-\sqrt{5}}{20}. \end{aligned}$$

Konačno možemo primijeniti teorem o asimptotici nizova uz parametre

$$r = 1/4, \quad b = 0, \quad c = 1/2, \quad h(x) = Z(\tfrac{1}{4})$$

i dobiti

$$Z_n \sim \frac{L\,4^n}{n^{3/2}\,\Gamma(-1/2)} = \frac{5-\sqrt{5}}{40} \frac{4^n}{n^{3/2}\sqrt{\pi}}.$$

Dijeljenje s formulom izvedenom na satu,

$$C_n \sim \frac{4^{n-1}}{n^{3/2}\sqrt{\pi}},$$

daje

$$\frac{Z_n}{C_n} \sim \frac{5-\sqrt{5}}{10}.$$

Rješenje zadatka 6. Ovo je zadatak iz knjige [3], poglavlje 1. Diskutiranjem u kojem članu particije se nalazi broj $n+1$ i označavajući s k broj preostalih elemenata u tom članu dobivamo rekurzivnu relaciju

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

Množenjem s $\frac{x^n}{n!}$ i zbrajanjem dobivamo

$$\sum_{n=0}^{\infty} B_{n+1} \frac{x^n}{n!} = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{x^{n-k}}{(n-k)!} \frac{B_k x^k}{k!}.$$

Na lijevoj strani prepoznajemo derivaciju:

$$\frac{d}{dx} \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = \sum_{n=1}^{\infty} B_n \frac{x^{n-1}}{(n-1)!},$$

dok na desnoj prepoznajemo produkt redova po principu "svaki sa svakim":

$$\underbrace{\Big(\sum_{m=0}^{\infty} \frac{x^m}{m!}\Big)}_{=e^x} \Big(\sum_{k=0}^{\infty} B_k \frac{x^k}{k!}\Big).$$

Označimo li eksponencijalnu funkciju izvodnicu niza s $B(x)$, dobili smo

$$B'(x) = e^x B(x).$$

Sada rješavamo tu diferencijalmu jednadžbu:

$$\frac{d}{dx}(\ln B(x)) = \frac{B'(x)}{B(x)} = e^x$$

$$\ln B(x) = e^x + C$$

$$B(x) = e^{e^x + C}$$

Konstanta C se odredi iz

$$1 = B_0 = B(0) = e^{1+C}, \qquad \text{tj. } C = -1.$$

Dakle,

$$B(x) = e^{e^x - 1}.$$

Iskoristimo sada dvaput razvoj eksponencijalne funkcije u red:

$$B(x) = \frac{1}{e} e^{e^x} = \frac{1}{e} \sum_{k=0}^{\infty} \frac{e^{kx}}{k!} = \frac{1}{e} \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} \frac{(kx)^n}{k! n!} = \frac{1}{e} \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{\infty} \frac{k^n}{k!} \Big) \frac{x^n}{n!}.$$

Uspoređivanje koeficijenata s $B(x) = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$ daje traženu formulu.

Rješenje zadatka 7. Naredno rješenje je preuzeto iz članka [4]. Najprije tvrdimo da možemo naći skupove $X, Y \subseteq \mathbb{Z}_p$ takve da je

$$|X| = p + 1 - |A|, \quad |Y| = p + 1 - |B|, \quad |X \cap Y| = \max\big\{|X| + |Y| - p,\, 1\big\}.$$

Razlikujemo dva slučaja.

(1°) Ako je $|A| + |B| \le p + 1$, tada možemo uzeti

$$X = \{0, 1, \ldots, p - |A|\}, \quad Y = \{|B| - 1, |B|, \ldots, p - 1\}.$$

(2°) Ako je $|A| + |B| > p + 1$, tada možemo uzeti

$$X = \{0, 1, \ldots, p - |A|\}, \quad Y = \{p - |A|, p - |A| + 1, \ldots, 2p - |A| - |B|\}.$$

Prema (b) dijelu principa neodređenosti postoje funkcije $f, g \colon \mathbb{Z}_p \to \mathbb{C}$ takve da je

$$\operatorname{supp}(f) = A, \quad \operatorname{supp}(\hat{f}) = X, \quad \operatorname{supp}(g) = B, \quad \operatorname{supp}(\hat{g}) = Y.$$

Promotrimo funkciju $f * g$. Iz definicije konvolucije

$$(f * g)(x) := \sum_{y \in \mathbb{Z}_p} f(x - y) g(y)$$

se odmah vidi

$$\operatorname{supp}(f * g) \subseteq \operatorname{supp}(f) + \operatorname{supp}(g) = A + B,$$

dok iz svojstva

$$(\widehat{f * g})(\xi) = \hat{f}(\xi)\hat{g}(\xi)$$

slijedi

$$\operatorname{supp}(\widehat{f * g}) = \operatorname{supp}(\hat{f}) \cap \operatorname{supp}(\hat{g}) = X \cap Y.$$

Konačno, korištenjem (b) dijela principa neodređenosti dobivamo

$$|A + B| + |X \cap Y| = \big|\operatorname{supp}(f * g)\big| + \big|\operatorname{supp}(\widehat{f * g})\big| \ge p + 1,$$

što je upravo

$$|A + B| \ge p + 1 - \max\big\{p + 2 - |A| - |B|,\, 1\big\} = \min\big\{|A| + |B| - 1,\, p\big\}.$$

Rješenje zadatka 8. Promotrimo grupu

$$\mathbb{A} = \mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{n} = \{0,1\}^n$$

i uspostavimo bijektivnu korespondenciju

$$\mathcal{P}_n \to \mathbb{A}, \qquad S \mapsto \text{karakteristična funkcija skupa } S$$

s inverzom

$$\mathbb{A} \to \mathcal{P}_n, \qquad (z_1, \dots, z_n) \mapsto \{j \in \{1,2,\dots,n\} : z_j = 1\}.$$

Dakle, skupu $S \in \mathcal{P}_n$ odgovara n-torka $z = (z_1, \dots, z_n)$ takva da je $z_j = 1$ za $j \in S$ i $z_j = 0$ za $j \in S^c$. Tada umjesto a_S pišemo a_z.

Definiramo funkciju $f\colon \mathbb{A} \to \mathbb{C}$,

$$f(y_1, \dots, y_n) := \sum_{S \in \mathcal{P}_n} a_S \prod_{j \in S} (-1)^{y_j} = \sum_{z=(z_1,\dots,z_n)\in\mathbb{A}} a_z \prod_{j=1}^{n} (-1)^{y_j z_j},$$

tj.

$$f(y) := \sum_{z \in \mathbb{A}} a_z \, E(y,z).$$

Primijetimo da zapravo želimo pobrojati rješenja $(y_1, \dots, y_n) \in \mathbb{A}$ jednadžbe

$$f(y_1, \dots, y_n) = 0.$$

Trebamo dokazati da je $|\operatorname{supp}(f)| \geq \frac{2^n}{k}$, jer će tada broj rješenja biti najviše $2^n - \frac{2^n}{k}$.

Zbog $E(y,z) \in \{-1,1\} \subset \mathbb{R}$ imamo

$$\hat{f}(\xi) = \sum_{y \in \mathbb{A}} \Big(\sum_{z \in \mathbb{A}} a_z \overline{E(y,z)} \Big) E(y,\xi) = \sum_{z \in \mathbb{A}} a_z \sum_{y \in \mathbb{A}} E(y, \xi - z) = 2^n \, a_\xi.$$

Po pretpostavci zadatka je $|\operatorname{supp}(\hat{f})| = k$. Zato (a) dio principa neodređenosti primijenjen na grupu $\mathbb{A}$ daje

$$|\operatorname{supp}(f)| \geq \frac{|\mathbb{A}|}{|\operatorname{supp}(\hat{f})|} = \frac{2^n}{k}.$$

Literatura

[1] E. A. Bender, S. G. Williamson, *Foundations of Combinatorics with Applications*, Dover, 2006.

[2] Ž. Hanjš, *Međunarodne matematičke olimpijade*, treće izdanje, Element, Zagreb, 2000.

[3] H. S. Wilf, *generatingfunctionology*, A K Peters/CRC Press, treće izdanje, 2005.

[4] T. Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett. **12** (2005), 121–127.