Analitičke metode u kombinatorici

Pripreme za IMO 2014

Vjeko Kovač, 25. 6. 2014.
http://web.math.pmf.unizg.hr/~vjekovac/

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.

Definicija 1. *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* $\left(\frac{a_n}{n!}\right)_{n=0}^{\infty}$*, 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 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 2. Obična funkcija izvodnica niza zadanog formulom $a_n = n^2$ je

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

Eksponencijalna funkcija izvodnica tog istog niza je

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

* * *

Primjer 3. 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 4. 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

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

koji se izračuna kao

$$\frac{1}{(1-x)(1-x^2)(1-x^5)(1-x^{10})(1-x^{20})(1-x^{50})(1-x^{100})(1-x^{200})(1-x^{500})}.$$

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

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

* * *

Zadatak 1. Dokažite da je broj rastava prirodnog broja na različite pribrojnike jednak broju rastava prirodnog broja na neparne pribrojnike.

Rješenje. Označimo:

$R_n =$ broj rastava od n na različite pribrojnike, $\quad N_n =$ broj rastava od n na neparne pribrojnike.

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

Izjednačavanjem koeficijenata slijedi $R_n = N_n$.

* * *

Zadatak 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":

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

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

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

* * *

Zadatak 3. 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

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

Rješenje. 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":

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

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.

* * *

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

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

Sljedeći teorem je samo malo neprecizan jer želimo izbjeći previše tehničke pojmove.

Teorem 5. *Neka je $(a_n)_{n=0}^{\infty}$ kombinatorno dobiveni niz i neka njegova obična funkcija izvodnica $A(x) = \sum_{n=0}^{\infty} a_n x^n$ konvergira na nekom intervalu $[-r, r\rangle$, $r > 0$. 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 $A(x)$.

* * *

Zadatak 4. 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 $n!/e$.

* * *

Zadatak 5. 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

$\cdot$	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 $d_1 \cdots d_n = |\mathbb{A}|$.

* * *

Zadatak 6. Koliko se najviše može odabrati međusobno okomitih "vektora" iz $\{-1,1\}^{1024}$?

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:

$$v^x \cdot v^y = \sum_{\xi\in\mathbb{A}} E(x,\xi)E(y,\xi) = \sum_{\xi\in\mathbb{A}} E(x,\xi)\overline{E(y,\xi)} = \sum_{\xi\in\mathbb{A}} E(x-y,\xi) = 0 \quad \text{ako je } x \neq y.$$

* * *

Konačno možemo uvesti ključni pojam Fourierove analize.

Definicija 6. *Fourierova transformacija funkcije $f\colon \mathbb{A} \to \mathbb{C}$ je nova funkcija $\hat{f}\colon \mathbb{A} \to \mathbb{C}$ definirana formulom*

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

Primjer 7. (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

$$\hat{f} = \big(f_{00} + f_{01} + f_{10} + f_{11},\ f_{00} - f_{01} + f_{10} - f_{11},\ f_{00} + f_{01} - f_{10} - f_{11},\ f_{00} - f_{01} - f_{10} + f_{11}\big).$$

Neka svojstva Fourierove transformacije su dana u sljedećem teoremu.

Teorem 8. *(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)

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

□

* * *

Zadatak 7.* 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

$$m\equiv a_1a_2+b_1b_2+c_1c_2 \pmod p.$$

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

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

Imamo $\hat{f}(\xi)=|S|^2$. Za $\xi\neq0$ 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 $(f*f*f)\hat{}(\xi) = \hat{f}(\xi)^3$ i formule inverzije imamo

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

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

* * *

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

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

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

Teorem 9. *(Princip neodređenosti)*

(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 $\operatorname{supp}(\hat{f}) = B$.

* * *

Zadatak 8. Dokažite (a) dio principa neodređenosti. (Dokaz (b) dijela je puno teži i nije sasvim elementaran.)

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.

* * *

Zadatak 9. 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

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

* * *

Zadatak 10. Dokažite Cauchy-Davenportov teorem: Ako je p prost broj i ako su $A, B \subseteq \mathbb{Z}_p$ neprazni, tada vrijedi

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

Pritom, kao i obično, označavamo

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

Uputa: Možete iskoristiti princip neodređenosti, premda nije očigledno kako.

Rješenje. 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 $|A| + |B| \leq p + 1$, 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

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

što je upravo

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