math.e

Hrvatski matematički elektronički časopis

Primjene Fourierove analize na konačnim komutativnim grupama

Fourierova analiza konacne grupe

Vjekoslav Kovač[2] Ljudevit Palle[3]

Sažetak. U ovom članku izlažu se osnove Fourierove analize na konačnim Abelovim grupama. Potom se dobiveni rezultati primjenjuju na raznovrsne zadatke u različitim matematičkim granama: (linearnoj) algebri, geometriji ravnine, elementarnoj teoriji brojeva i (aditivnoj) kombinatorici.

1 Fourierova transformacija

Fourierova analiza je opsežna matematička disciplina koja se razvila iz razmatranja J.-B. J. Fouriera (1768–1830) o razvojima u redove sastavljene od trigonometrijskih funkcija, inicijalno u kontekstu proučavanja jednadžbe provođenja topline. Već oko dvije stotine godina njezina mnogobrojna pitanja intrigiraju poznate matematičare, a i danas se nalaze nove zanimljive primjene teorijskih rezultata. Svrha ovog članka je čitatelju približiti jedan aspekt Fourierove analize na konačnim strukturama, koji ne iziskuje neko posebno predznanje, za razliku od općenite teorije. Tako se već čitatelj sa znanjem srednjoškolske matematike može uvesti u ovo područje, a natjecatelji mogu naučiti poneki trik za rješavanje prilično teških zadataka.

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

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

Na skupu $\mathbb{Z}_d$ se 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 sljedeće 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 brojeve $d_1, \ldots, d_n \in \mathbb{N} \setminus \{1\}$. Kada pišemo

$$\mathbf{A} = \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n}, \tag{1}$$

tada smatramo da je $\mathbf{A}$ Kartezijev produkt skupova $\mathbb{Z}_{d_1}, \ldots, \mathbb{Z}_{d_n}$ na kojem se promatra zbrajanje po koordinatama. Drugim riječima, elementi od $\mathbf{A}$ 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 je npr. operacija zbrajanja na $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ opisana sljedećom tablicom.

$+$	(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)

Čitatelj upoznat s pojmom grupe odmah će prepoznati da je gore opisana struktura $(\mathbf{A}, +)$ primjer *konačne komutativne* (ili *Abelove*) *grupe*. Obratno, poznato je da svaka konačna komutativna grupa ima strukturu (1) za određene parametre n i $d_1, \ldots, d_n$. Zato mi i ne moramo raditi s općenitim grupama, veće upravo s grupama $\mathbf{A}$ danima formulom (1).

Definirajmo preslikavanje $E : \mathbf{A} \times \mathbf{A} \to \mathbb{C}$ formulom

$$E(x, \xi) := \left(e^{2\pi i/d_1}\right)^{x_1 \xi_1} \left(e^{2\pi i/d_2}\right)^{x_2 \xi_2} \cdots \left(e^{2\pi i/d_n}\right)^{x_n \xi_n}$$

za svake n-torke $x = (x_1, x_2, \ldots, x_n)$i $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ iz $\mathbf{A}$. 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 se oni nalaze u dvije različite kopije od $\mathbf{A}$, povezane preslikavanjem E.

Propozicija 1. *Preslikavanje E ima sljedeća svojstva (za svaki izbor od $x, y, \xi, \zeta \in \boldsymbol{A}$):*

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

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

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

Napomenimo da sa $|S|$ označavamo broj elemenata konačnog skupa S.

Proof. Prvih šest formula su direktne posljedice definicije od E, dok su posljednje dvije ekvivalentne radi simetričnosti iste definicije obzirom na x i ξ. Dokažimo zadnju navedenu formulu.

Za fiksirani $x=(x_1,x_2,\ldots,x_n)$ sumiranjem po svim mogućnostima koordinata od $\xi=(\xi_1,\xi_2,\ldots,\xi_n)$ dobivamo

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

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 iz (2) nije jednak 0 samo kada je $x_1=\cdots=x_n=0$ i tada je jednak $d_1\cdots d_n=|\mathbf{A}|$.

Definicija 2. *Fourierova transformacija funkcije $f:\boldsymbol{A}\to\mathbb{C}$ je nova funkcija $\widehat{f}:\boldsymbol{A}\to\mathbb{C}$ definirana formulom*

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

Primjer 3. *(a) Ako je* $\mathbf{A} = \mathbb{Z}_4$ *i ako funkcije na* $\mathbf{A}$ *pišemo kao uređene četvorke*

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

tada je

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

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

$$f = (f_{0,0}, f_{0,1}, f_{1,0}, f_{1,1}),$$

tada je

$$\widehat{f} = \big(f_{0,0} + f_{0,1} + f_{1,0} + f_{1,1},\ f_{0,0} - f_{0,1} + f_{1,0} - f_{1,1},\ f_{0,0} + f_{0,1} - f_{1,0} - f_{1,1},\ f_{0,0} - f_{0,1} - f_{1,0} + f_{1,1}\big).$$

Osnovna svojstva Fourierove transformacije dana su u sljedećem teoremu.

Teorem 4.

- *[(a)] Vrijedi tzv. formula inverzije:*

$$f(x) = \frac{1}{|\mathbf{A}|}\sum_{\xi\in\mathbf{A}}\widehat{f}(\xi)\overline{E(x,\xi)} \quad \text{za svaki} x\in\mathbf{A}.$$

  Njom se polazna funkcija $f:\mathbf{A}\to\mathbb{C}$ može rekonstruirati iz svoje Fourierove transformacije. Posebno, Fourierova transformacija je injektivna, tj. $\widehat{f} = \hat{g}$ implicira $f = g$.
- *[(b)] Vrijedi Plancherelov identitet:*

$$\sum_{\xi\in\mathbf{A}}\left|\widehat{f}(\xi)\right|^2 = \left|\mathbf{A}\right|\sum_{x\in\mathbf{A}}\left|f(x)\right|^2$$

  i općenitije:

$$\sum_{\xi\in\mathbf{A}}\widehat{f}(\xi)\overline{\hat{g}(\xi)} = \left|\mathbf{A}\right|\sum_{x\in\mathbf{A}}f(x)\overline{g(x)}$$

  za proizvoljne funkcije $f,g:\mathbf{A}\to\mathbb{C}$.
- *[(c)] Ako je funkcija $h:\mathbf{A}\to\mathbb{C}$ definirana kao tzv. konvolucija funkcija $f,g:\mathbf{A}\to\mathbb{C}$,*

$$h(x) := \sum_{\substack{y,z\in\mathbf{A}\\ y+z=x}} f(y)g(z) \quad \text{za svaki} x\in\mathbf{A},$$

  što pišemo $h = f * g$, tada vrijedi

$$\widehat{h}(\xi) = \widehat{f}(\xi)\hat{g}(\xi) \quad \text{za svaki} \xi\in\mathbf{A}.$$

  Drugim riječima, Fourierova transformacija prevodi konvoluciju u obični produkt.
- *[(d)] Za funkciju $f:\mathbf{A}\to\mathbb{C}$ te za $y,\zeta\in\mathbf{A}$ definiramo nove funkcije $\mathrm{T}_y f, \mathrm{M}_\zeta f:\mathbf{A}\to\mathbb{C}$ formulama*

$$(\mathrm{T}_y f)(x) := f(x-y), \quad (\mathrm{M}_\zeta f)(x) := E(x,\zeta)f(x) \quad \text{za svaki} x\in\mathbf{A}.$$

  Njihove Fourierove transformacije su dane sa

$$(\widehat{\mathrm{T}_y f})(\xi) = E(y,\xi)\widehat{f}(\xi), \quad (\widehat{\mathrm{M}_\zeta f})(\xi) = \widehat{f}(\xi+\zeta) \quad \text{za svaki} \xi\in\mathbf{A}.$$

  Slova T i M dolaze od riječi translacije i modulacije.
- *[(e)] Fourierova transformacija je linearna, tj.*

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

Proof. (a) Navedena formula je naprosto posljedica zamjene poretka u dvostrukoj sumaciji i svojstava od E iz propozicije 1:

$$\begin{aligned}\sum_{\xi\in\mathbf{A}} \widehat{f}(\xi)\overline{E(x,\xi)} &= \sum_{\xi\in\mathbf{A}}\sum_{y\in\mathbf{A}} f(y)E(y,\xi)\overline{E(x,\xi)}\\ &= \sum_{y\in\mathbf{A}} f(y)\sum_{\xi\in\mathbf{A}} E(y-x,\xi) = \left|\mathbf{A}\right| f(x).\end{aligned}$$

(b) Slično kao i u prethodnom dijelu, zamjena redoslijeda sumiranja daje:

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

(c) Sumiranjem po x i rastavljanjem $E(x,\xi)=E(y,\xi)E(z,\xi)$ dobivamo:

$$\begin{aligned}\widehat{h}(\xi) &= \sum_{x\in\mathbf{A}}\Big(\sum_{\substack{y,z\in\mathbf{A}\\ y+z=x}} f(y)g(z)\Big)E(x,\xi) = \sum_{y,z\in\mathbf{A}} f(y)E(y,\xi)\, g(z)E(z,\xi)\\ &= \Big(\sum_{y\in\mathbf{A}} f(y)E(y,\xi)\Big)\Big(\sum_{z\in\mathbf{A}} g(z)E(z,\xi)\Big) = \widehat{f}(\xi)\hat{g}(\xi).\end{aligned}$$

(d) Ovo su također direktne posljedice definicija i propozicije 1:

$$\begin{aligned}(\widehat{\mathrm{T}_y f})(\xi) &= \sum_{x\in\mathbf{A}} f(x-y)E(x,\xi) = \sum_{x\in\mathbf{A}} f(x)E(x+y,\xi)\\ &= \sum_{x\in\mathbf{A}} f(x)E(x,\xi)E(y,\xi) = E(y,\xi)\widehat{f}(\xi),\\ (\widehat{\mathrm{M}_\zeta f})(\xi) &= \sum_{x\in\mathbf{A}} f(x)E(x,\zeta)E(x,\xi) = \sum_{x\in\mathbf{A}} f(x)E(x,\zeta+\xi) = \widehat{f}(\zeta+\xi).\end{aligned}$$

(e) Ovdje jedino treba rastaviti konačnu sumu na dijelove koji se tiču funkcija f i g redom:

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

2 Primjene u algebri

Već i dosad navedeni koncepti dovoljni su za maštovite primjene na raznolike probleme. Započinjemo s nekoliko jednostavnijih primjera iz linearne algebre ili algebre polinoma.

Zadatak 5. *Koliko se najviše može odabrati međusobno ortogonalnih vektora iz $\mathbb{R}^{1024}$ čije su sve koordinate iz skupa $\{-1,1\}$?*

Napomenimo da su vektori $u,v\in\mathbb{R}^n$, $u=(u_1,\ldots,u_n)$, $v=(v_1,\ldots,v_n)$ *ortogonalni* ili *okomiti* ako i samo ako je njihov skalarni produkt jednak 0, tj. vrijedi $u\cdot v=\sum_{j=1}^n u_jv_j=0$. Za kompleksne vektore $u,v\in\mathbb{C}^n$ definicija ortogonalnosti ostaje ista, osim što skalarni produkt postaje $u\cdot v=\sum_{j=1}^n u_j\overline{v_j}$.

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

Promotrimo grupu $\mathbf{A} = \mathbb{Z}_2^{10} = \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{10}$; ona očigledno ima $2^{10} = 1024$ elemenata.

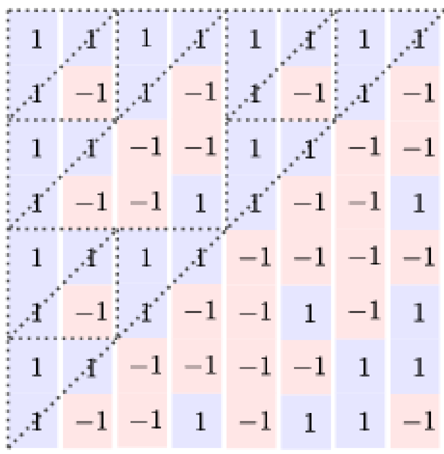
Za svaki $x \in \mathbf{A}$ promotrimo vektor

$$u^x := \big(E(x,\xi) : \xi \in \mathbf{A}\big) \tag{3}$$

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

$$u^x \cdot u^y = \sum_{\xi\in\mathbf{A}} E(x,\xi)\overline{E(y,\xi)} = \sum_{\xi\in\mathbf{A}} E(x-y,\xi) = 0 \tag{4}$$

ako je $x \neq y$.



Slika 1: Međusobno ortogonalni ± 1 vektori iz $\mathbb{R}^8$.

Pogledajte sliku 1 za analogni primjer u 2^3-dimenzionalnom euklidskom prostoru; vektori su ovdje zapisani kao stupci. Naziru se fraktalni uzorci, koji nisu slučajni, već su posljedica rekurzivnih relacija što ih zadovoljava preslikavanje E za grupe $\mathbf{A} = \mathbb{Z}_2^n$.

Zadatak 6. *Neka je $v = (v_0, v_1, \ldots, v_{m-1}) \in \mathbb{C}^m$ vektor kojeg možemo shvatiti kao funkciju na $\mathbb{Z}_m$ i pretpostavimo da vrijedi $\hat{v}(\xi) \neq 0$ za svaki $\xi = 0, 1, \ldots, m-1$. Dokažite da je sistem cikličkih permutacija od v linearno nezavisan.*

Pod *cikličkim permutacijama* od v smatramo vektore

$$(v_j, v_{j+1}, \ldots, v_{m-1}, v_0, v_1, \ldots, v_{j-1})$$

za $j = 0, 1, \ldots, m-1$. Prisjetimo se i da je sistem vektora $w_1, w_2, \ldots, w_n$ *linearno nezavisan* ako činjenica $\sum_{k=1}^n \alpha_k w_k = \mathbf{0}$ za neke skalare $\alpha_1, \alpha_2, \ldots, \alpha_n$ implicira da svi ti skalari moraju biti jednaki 0. Pritom $\mathbf{0}$ označava nul-vektor u odgovarajućem vektorskom prostoru.

Rješenje.. Ovog puta radimo s kompleksnim funkcijama na grupi $\mathbf{A} = \mathbb{Z}_m$. Uočimo da je gornji ciklički permutirani vektor upravo $\mathrm{T}_{-j}v$, pri čemu opet koristimo notaciju iz (d) dijela teorema 4. Prema tome, trebamo pokazati da su funkcije $\mathrm{T}_0 v$, $\mathrm{T}_1 v$, \ldots, $\mathrm{T}_{m-1} v$ linearno nezavisne. Pretpostavimo da su $\alpha_0, \alpha_1, \ldots, \alpha_{m-1} \in \mathbb{C}$ skalari takvi da je $\sum_{j=0}^{m-1} \alpha_j \mathrm{T}_j v = \mathbf{0}$. Zbog linearnosti Fourierove transformacije i (d) dijela teorema 4, za svaki $\xi = 0, 1, \ldots, m-1$ vrijedi

$$0 = \sum_{j=0}^{m-1} \alpha_j (\widehat{\mathrm{T}_j v})(\xi) = \left(\sum_{j=0}^{m-1} \alpha_j E(j, \xi) \right) \hat{v}(\xi)$$

pa po pretpostavci mora biti

$$\sum_{j=0}^{m-1} \alpha_j E(j, \xi) = 0, \quad \text{tj.} \sum_{x \in \mathbf{A}} \alpha_x u^x = \mathbf{0},$$

pri čemu su $u^x : \mathbf{A} \to \mathbb{C}$, $u^x(\xi) := E(x, \xi)$ funkcije koje poistovjećujemo s vektorima danima formulom (3). Istim računom (4) kao u prethodnom zadatku provjeri se da su ti vektori u parovima ortogonalni. Zato su oni pogotovo i linearno nezavisni pa je $\alpha_0 = \alpha_1 = \cdots = \alpha_{m-1} = 0$, čime je dokazana tražena tvrdnja.

Čitatelju ostavljamo dva zadatka za vježbu.

Zadatak 7. *Promotrite sve matrice tipa $2^n \times 2^n$ (gdje je n prirodan broj) s elementima iz skupa $\{-1, 1\}$. Pronađite najveću moguću vrijednost determinante jedne od takvih matrica.*

Uputa.. Potražite *Hadamardovu nejednakost* [5], koja će vam dati gornju ogradu za takve matrice A reda $N = 2^n$:

$$\det A \leqslant N^{N/2} = 2^{n 2^{n-1}}.$$

Sada konstruirajte primjer kada se postiže jednakost koristeći račun iz zadatka 5. Analogni problem je uvelike otvoren za matrice reda N koji nije potencija broja 2 i zove se *Hadamardov problem*.

Zadatak 8. *Faktorizirajte polinom 5 varijabli,*

$$\begin{aligned} P(x_0, x_1, x_2, x_3, x_4) = & \textstyle\sum_{j=0}^4 x_j^5 + 5 \sum_{j=0}^4 x_{j-1} x_j x_{j+1} (x_{j-1} x_{j+1} - x_j^2) \\ & + 5 \textstyle\sum_{j=0}^4 x_{j-2} x_j x_{j+2} (x_{j-2} x_{j+2} - x_j^2) - 5 x_0 x_1 x_2 x_3 x_4, \end{aligned}$$

na faktore s koeficijentima iz prstena

$$\mathbb{Z}[e^{2\pi i/5}] = \left\{ \sum_{j=0}^{4} \alpha_j e^{2\pi i j/5} \;:\; \alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{Z} \right\}.$$

Napomenimo da se zbrajanje i oduzimanje indeksâ u formuli za P shvaćaju modulo 5.

Uputa.. Označite kratko $\varepsilon = e^{2\pi i/5}$ i shvatite vektor varijabli $x = (x_0, x_1, x_2, x_3, x_4)$ kao funkciju na $\mathbb{Z}_5$. Korištenjem formule inverzije nakon duljeg računa dobiva se

$$P(x_0, x_1, x_2, x_3, x_4) = \prod_{j=0}^{4} \widehat{x}(j) = \prod_{j=0}^{4} (x_0 + \varepsilon^j x_1 + \varepsilon^{2j} x_2 + \varepsilon^{3j} x_3 + \varepsilon^{4j} x_4).$$

3 Primjene u geometriji

U ovom odjeljku bavimo se primjenama u planimetriji, tj. geometriji ravnine. Autor sljedećeg zadatka je M. Roseman, a dolje opisano elegantno rješenje korištenjem Fourierove analize predložio je I. J. Schoenberg [8].

Zadatak 9. *Neka je $n \in \mathbb{N}$, $n \geqslant 3$. Definiramo niz n-terokuta $(M^k)_{k=0}^{\infty}$,*

$$M^k = A_0^k A_1^k \ldots A_{n-1}^k,$$

u ravnini na sljedeći način. Neka je M^0 proizvoljan. Za $k \geqslant 1$ vrhovi

$$A_0^k, A_1^k, \ldots, A_{n-2}^k, A_{n-1}^k$$

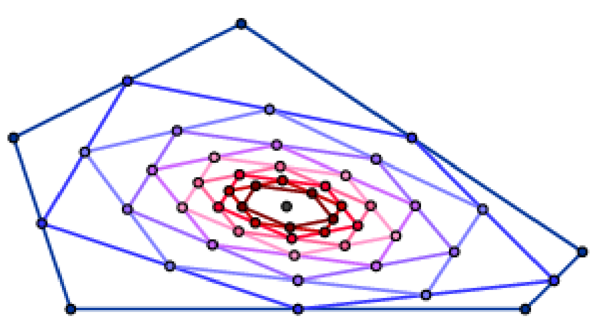
mnogokuta M^k rekurzivno su definirani kao polovišta stranica

$$\overline{A_0^{k-1} A_1^{k-1}},\ \overline{A_1^{k-1} A_2^{k-1}},\ \ldots,\ \overline{A_{n-2}^{k-1} A_{n-1}^{k-1}},\ \overline{A_{n-1}^{k-1} A_0^{k-1}}$$

mnogokuta M^{k-1}. Dokažite da se mnogokuti $(M^k)_{k=0}^{\infty}$ "stišču" prema točki, tj. preciznije, da vrijedi

$$\lim_{k \to \infty} A_j^k = T$$

za $j = 0, 1, \ldots, n-1$, pri čemu je T težište od M^0.



Slika 2: Niz peterokuta koji se stišče prema zajedničkom težištu.

Rješenje.. Pogledajte sliku 2 za ilustraciju nekoliko iteracija u slučaju $n = 5$.

Uvedimo kompleksni koordinatni sustav u ravnini s ishodištem u točki T i neka je $z_j^{(k)} \in \mathbb{C}$ koordinata točke A_j^k. Shvatimo vektor

$$f_k = \left(z_0^{(k)}, z_1^{(k)}, \ldots, z_{n-2}^{(k)}, z_{n-1}^{(k)}\right)$$

kao kompleksnu funkciju na grupi $\mathbf{A} = \mathbb{Z}_n$. Rekurzivnu relaciju možemo zapisati

$$z_j^{(k)} = \frac{1}{2} z_j^{(k-1)} + \frac{1}{2} z_{j+1}^{(k-1)} \quad \text{za } j = 0, 1, \ldots, n-1,$$

pri čemu indekse zbrajamo modulo n, što se još kompaktnije zapisuje

$$f_k = \frac{1}{2} f_{k-1} + \frac{1}{2} \mathrm{T}_{-1} f_{k-1},$$

uz notaciju iz (d) dijela teorema 4. Korištenjem tog istog teorema dobivamo relaciju između Fourierovih transformacija:

$$\begin{aligned} \widehat{f}_k(\xi) &= \tfrac{1}{2} \widehat{f}_{k-1}(\xi) + \tfrac{1}{2} E(-1, \xi) \widehat{f}_{k-1}(\xi) = \tfrac{1}{2}(1 + e^{-2\pi i \xi / n}) \widehat{f}_{k-1}(\xi) \\ &= e^{-\pi i \xi / n} \tfrac{1}{2}(e^{\pi i \xi / n} + e^{-\pi i \xi / n}) \widehat{f}_{k-1}(\xi) = e^{-\pi i \xi / n} \cos \tfrac{\pi \xi}{n} \widehat{f}_{k-1}(\xi), \end{aligned}$$

odakle je

$$\left|\widehat{f}_k(\xi)\right| = \left|\cos \frac{\pi \xi}{\mathrm{n}}\right| \left|\widehat{f}_{k-1}(\xi)\right|$$

pa iteriranjem dobivamo

$$\left|\widehat{f}_k(\xi)\right| = \left|\cos \frac{\pi \xi}{n}\right|^k \left|\widehat{f}_0(\xi)\right|. \tag{5}$$

Po konstrukciji je

$$\widehat{f}_0(0) = z_0^{(0)} + z_1^{(0)} + \cdots + z_{n-2}^{(0)} + z_{n-1}^{(0)} = 0$$

pa prema (5) slijedi $\widehat{f}_k(0) = 0$ za svaki $k \geqslant 0$. S druge strane, za $\xi = 1, 2, \ldots, n-1$ imamo $\left|\cos \frac{\pi \xi}{n}\right| < 1$ te radi (5) postoji limes $\lim_{k \to \infty} \left|\widehat{f}_k(\xi)\right|$ i iznosi 0. Konačno, Plancherelov identitet iz teorema 4 daje

$$\lim_{k \to \infty} \sum_{j \in \mathbb{Z}_n} \left|z_j^{(k)}\right|^2 = \frac{1}{n} \lim_{k \to \infty} \sum_{\xi \in \mathbb{Z}_n} \left|\widehat{f}_k(\xi)\right|^2 = 0,$$

što znači $\lim_{k \to \infty} z_j^{(k)} = 0$ za $j = 0, 1, \ldots, n-1$.

Zadatak kojeg ostavljamo za vježbu čitatelju prilično je težak pa dajemo i detaljnu uputu. Kao problem ga je postavio A. Björner, a riješili su ga D. Svrtan, D. Šterc i I. Urbiha u članku [9], odakle je zadatak i preuzet.

Zadatak 10. *Neka su z_0, z_1, z_2, z_3, z_4 kompleksni brojevi za koje vrijedi*

- *[(i)]* $|z_0| = |z_1| = |z_2| = |z_3| = |z_4| = 1$,
- *[(ii)]* $z_0 + z_1 + z_2 + z_3 + z_4 = 0$,
- *[(iii)]* $z_0 z_1 + z_1 z_2 + z_2 z_3 + z_3 z_4 + z_4 z_0 = 0$.

Dokažite da oni leže u vrhovima pravilnog peterokuta.

Uputa.. Petorku kompleksnih brojeva $\left(z_0, z_1, z_2, z_3, z_4\right)$ shvatite kao funkciju f na grupi $\mathbb{Z}_5$ i neka je njena Fourierova transformacija $\widehat{f} = \left(w_0, w_1, w_2, w_3, w_4\right)$. Iz drugog uvjeta zaključite $w_0 = \widehat{f}(0) = 0$ te potom iz prvog uvjeta i svojstava Fourierove transformacije izvedite

$$w_2 \overline{w_1} + w_3 \overline{w_2} + w_4 \overline{w_3} = 0, \qquad w_3 \overline{w_1} + w_4 \overline{w_2} + w_1 \overline{w_4} = 0.$$

Treći uvjet u zadatku se pak primjenom formule inverzije i $w_0 = 0$ transformira u

$$w_1 w_4 \cos \tfrac{2\pi}{5} + w_2 w_3 \cos \backslash textstyle \tfrac{4\pi}{5} = 0, \quad \text{tj.} \left(\sqrt{5} - 1\right) w_1 w_4 = \left(\sqrt{5} + 1\right) w_2 w_3.$$

Iz dobivenih jednakosti lako slijedi

$$\left|w_2\right| \left(\left(\sqrt{5} - 1\right) \left|w_1\right|^2 + \left(\sqrt{5} + 1\right) \left|w_3\right|^2 \right) = \left(\sqrt{5} - 1\right) \left|w_1\right| \left|w_2\right| \left|w_3\right|.$$

Diskutiranjem slučajeva zaključite da je najviše jedan od brojeva w_1, w_2, w_3, w_4 različit od 0. Preostat će iskoristiti formulu inverzije.

4 Primjene u teoriji brojeva

Autor sljedećeg rezultata je J. Bourgain [1], a njegov dokaz je preuzet iz knjige [11].

Zadatak 11. *Neka je p prost broj i $S \subseteq \{1, 2, 3, \ldots, p-1\}$ skup takav da je $\left|S\right| > p^{3/4}$. 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*

$$m \equiv a_1 a_2 + b_1 b_2 + c_1 c_2 (\mathrm{mod}\ \backslash(\mathrm{p}\backslash)).$$

Rješenje.. Koristeći operacije modulo p vidimo da zapravo treba svaki $x \in \mathbb{Z}_p$ prikazati kao

$$x = a_1 a_2 + b_1 b_2 + c_1 c_2$$

za neke $a_1, a_2, b_1, b_2, c_1, c_2 \in S \subseteq \mathbb{Z}_p$. Zbog činjenice da je p prost, za svake $s, y \in \mathbb{Z}_p$, $s \neq 0$ jednadžba $sx = y$ ima jedinstveno rješenje $x \in \mathbb{Z}_p$. Drugim riječima, za svaki $s \in \mathbb{Z}_p \setminus \{0\}$ funkcija $\mathbb{Z}_p \to \mathbb{Z}_p$, $x \mapsto sx$ je bijekcija. Tu ćemo tvrdnju višestruko koristiti kod zamjene indeksa sumacije.

Promotrimo funkciju $f : \mathbb{Z}_p \to \mathbb{C}$, $f := \sum_{s\in S} \chi_{s\cdot S}$, gdje χ_T označava karakterističnu funkciju skupa T te pišemo $s \cdot S = \{sx : x \in S\}$. Najprije primijetimo da je

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

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

Fourierova transformacija od f je

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

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

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

Zbog nejednakosti Minkowskog (tj. nejednakosti trokuta u euklidskom prostoru $\mathbb{C}^{\mathbb{Z}_p} \cong \mathbb{C}^p \cong \mathbb{R}^{2p}$) imamo

$$\begin{aligned}&\Big(\sum_{\xi\in\mathbb{Z}_p}\left|\widehat{f}\,(\xi)\right|^2\Big)^{1/2} \leqslant \sum_{s\in S}\Big(\sum_{\xi\in\mathbb{Z}_p}\left|\widehat{\chi}_{s\cdot S}(\xi)\right|^2\Big)^{1/2}\\ &= \sum_{s\in S} p^{1/2}\Big(\sum_{x\in\mathbb{Z}_p}\left|\chi_{s\cdot S}(x)\right|^2\Big)^{1/2} = \left|S\right|p^{1/2}\left|S\right|^{1/2} = p^{1/2}\left|S\right|^{3/2}.\end{aligned}$$

Posljednje dvije ocjene se mogu kombinirati u

$$\sum_{\xi\in\mathbb{Z}_p\setminus\{0\}}\left|\widehat{f}\,(\xi)\right|^3 \leqslant p^{1/2}\left|S\right|\sum_{\xi\in\mathbb{Z}_p\setminus\{0\}}\left|\widehat{f}\,(\xi)\right|^2 \leqslant p^{1/2}\left|S\right|\left(p^{1/2}\left|S\right|^{3/2}\right)^2 = p^{3/2}\left|S\right|^4. \quad (6)$$

Konačno, zbog (c) dijela teorema 4 imamo $(\widehat{f*f*f})(\xi) = \widehat{f}\,(\xi)^3$ pa formula inverzije i (6) daju {\allowdisplaybreaks

$$\begin{aligned}(f*f*f)(x) &= p^{-1}\sum_{\xi\in\mathbb{Z}_p}\widehat{f}\,(\xi)^3e^{-2\pi i x\xi/p} \geqslant p^{-1}\widehat{f}\,(0)^3 - p^{-1}\sum_{\xi\in\mathbb{Z}_p\setminus\{0\}}\left|\widehat{f}\,(\xi)\right|^3\\ &\geqslant p^{-1}\left|S\right|^6 - p^{1/2}\left|S\right|^4 = p^{-1}\left|S\right|^4\Big(\left|S\right|^2 - p^{3/2}\Big).\end{aligned}$$

} Preostaje iskoristiti pretpostavku zadatka $\left|S\right| > p^{3/4}$, tj. $\left|S\right|^2 - p^{3/2} > 0$.

Postoje i složenije primjene Fourierove analize na konačnim grupama u teoriji brojeva. Zainteresirani čitatelj može pogledati dokaz tzv. *Gaussovog zakona kvadratnog reciprociteta* izložen u knjizi [2].

5 Primjene u kombinatorici

Fourierova analiza svoje najzanimljivije primjene nalazi u kombinatorici i to posebno u području tzv. *aditivne kombinatorike*, koja se bavi kombinatornim aspektima operacije zbrajanja. O tome svjedoči cijelo jedno poglavlje opsežne knjige [11]. Kako bismo mogli riješiti neke zahtjevnije zadatke, trebamo naučiti još jedan rezultat, koji se popularno naziva *princip neodređenosti*, po uzoru na formalno slične rezultate iz kvantne mehanike.

Za funkciju $f : \mathbf{A} \to \mathbb{C}$ na konačnoj komutativnoj grupi $\mathbf{A}$ označimo

$$\operatorname{supp}(f) := \{x \in \mathbf{A} : f(x) \neq 0\},$$

a promatrat ćemo i

$$\operatorname{supp}(\widehat{f}\,) = \{\xi \in \mathbf{A} : \widehat{f}\,(\xi) \neq 0\}.$$

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

Teorem 12. *[Princip neodređenosti]*

- *[(a)] Neka je $\mathbf{A}$ grupa dana s (1). Za svaku funkciju $f : \mathbf{A} \to \mathbb{C}$ koja nije identički jednaka konstanti $\mathbf{0}$ vrijedi*

$$\left|\operatorname{supp}(f)\right| \left| \operatorname{supp}(\widehat{f}\,)\right| \geqslant \left|\mathbf{A}\right|.$$

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

$$\left|\operatorname{supp}(f)\right| + \left| \operatorname{supp}(\widehat{f}\,)\right| \geqslant p + 1.$$

Obratno, za svaka dva skupa $A, B \subseteq \mathbb{Z}_p$ koji zadovoljavaju $|A| + |B| \geqslant p + 1$ postoji funkcija $f : \mathbb{Z}_p \to \mathbb{C}$ takva da je $\operatorname{supp}(f) = A$ i $\operatorname{supp}(\widehat{f}\,) = B$.

Proof. Dokažimo samo (a) dio teorema. Korištenjem nejednakosti trokuta, aritmetičko-kvadratne nejednakosti i Plancherelovog identiteta redom dobivamo {\allowdisplaybreaks

$$\begin{aligned}\max_{\xi\in\mathbf{A}}\left|\widehat{f}(\xi)\right| &= \max_{\xi\in\mathbf{A}}\left|\sum_{x\in\mathbf{A}} f(x)E(x,\xi)\right| \leqslant \sum_{x\in\mathbf{A}}\left|f(x)\right| = \sum_{x\in\operatorname{supp}(f)}\left|f(x)\right| \\ &\leqslant \left|\operatorname{supp}(f)\right|^{1/2}\Big(\sum_{x\in\operatorname{supp}(f)}\left|f(x)\right|^2\Big)^{1/2} = \left|\operatorname{supp}(f)\right|^{1/2}\Big(\left|\mathbf{A}\right|^{-1}\sum_{\xi\in\mathbf{A}}\left|\widehat{f}(\xi)\right|^2\Big)^{1/2} \\ &= \left|\mathbf{A}\right|^{-1/2}\left|\operatorname{supp}(f)\right|^{1/2}\Big(\sum_{\xi\in\operatorname{supp}(\widehat{f})}\left|\widehat{f}(\xi)\right|^2\Big)^{1/2} \\ &\leqslant \left|\mathbf{A}\right|^{-1/2}\left|\operatorname{supp}(f)\right|^{1/2}\left|\operatorname{supp}(\widehat{f})\right|^{1/2}\max_{\xi\in\mathbf{A}}\left|\widehat{f}(\xi)\right|.\end{aligned}$$

} Ako f nije identički jednaka 0, tada ni $\widehat{f}$ nije identički jednaka 0 pa je $\max_{\xi\in\mathbf{A}}\left|\widehat{f}(\xi)\right| > 0$. Dijeljenjem s tim faktorom dobivamo traženu nejednakost.

Dio (b) je mnogo složeniji i zasniva se na *teoremu Čebotareva* o korijenima iz jedinice, koji govori da za $1 \leqslant m \leqslant p$, za različite $x_1,\ldots,x_m \in \mathbb{Z}_p$ i za različite $\xi_1,\ldots,\xi_m \in \mathbb{Z}_p$ vrijedi

$$\det\left[e^{2\pi i x_j\xi_k/p}\right]_{\substack{j=1,\ldots,m\\k=1,\ldots,m}} \neq 0.$$

Jedan elementaran (ali još uvijek prilično tehnički) dokaz dao je T. Tao [10].

Dio (a) teorema 12 daje ocjenu za proizvoljnu konačnu komutativnu grupu $\mathbf{A}$, dok njegov (b) dio govori o pojačanju te ocjene u slučaju grupe $\mathbb{Z}_p$. R. Meshulam je u članku [6] dao analogno pojačanje i za općenitu grupu $\mathbf{A}$, koje ovdje nećemo diskutirati.

Zadatak 13. *Neka je n prirodan broj. Označimo s $\wp_n$ familiju svih 2^n podskupova skupa $\{1,2,\ldots,n\}$. Za svaki $S\in\wp_n$ dan je realni broj a_S i pretpostavimo da je točno $k\geqslant 1$ od tih brojeva a_S različito od 0. Dokažite da jednadžba*

$$\sum_{S\in\wp_n} a_S \prod_{j\in S} x_j = 0$$

ima najviše $2^n(1-1/k)$ 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 $x_j=1$.

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

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

Rješenje.. Promotrimo grupu

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

i uspostavimo bijektivnu korespondenciju

$$\wp_n \to \mathbf{A}, \quad S \mapsto \text{karakteristična funkcija skupa} S$$

s inverzom

$$\mathbf{A} \to \wp_n, \quad (z_1, \ldots, z_n) \mapsto \{j \in \{1, 2, \ldots, n\} : z_j = 1\}.$$

Dakle, skupu $S \in \wp_n$ odgovara n-torka $z = (z_1, \ldots, z_n)$ 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 $f : \mathbf{A} \to \mathbb{C}$,

$$f(y_1, \ldots, y_n) := \sum_{S \in \wp_n} a_S \prod_{j \in S} (-1)^{y_j} = \sum_{z=(z_1,\ldots,z_n) \in \mathbf{A}} a_z \prod_{j=1}^{n} (-1)^{y_j z_j},$$

tj.

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

Primijetimo da zapravo želimo pobrojati rješenja $(y_1, \ldots, y_n) \in \mathbf{A}$ jednadžbe $f(y_1, \ldots, y_n) = 0$, jer su ona putem $x_j = (-1)^{y_j}$ u korespondenciji s rješenjima $(x_1, \ldots, x_n) \in \{-1, 1\}^n$ polazne jednadžbe. Trebamo dokazati da je $|\mathrm{supp}(f)| \geqslant 2^n/k$, jer će tada broj rješenja biti najviše $2^n - 2^n/k$.

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

$$\widehat{f}\,(\xi) = \sum_{y \in \mathbf{A}} \left(\sum_{z \in \mathbf{A}} a_z \, \overline{E(y, z)} \right) E(y, \xi) = \sum_{z \in \mathbf{A}} a_z \sum_{y \in \mathbf{A}} E(y, \xi - z) = 2^n \, a_\xi.$$

Po pretpostavci zadatka je $\left|\mathrm{supp}(\widehat{f}\,)\right| = k$. Zato (a) dio teorema 12 primijenjen na grupu $\mathbf{A}$ daje

$$\left|\mathrm{supp}(f)\right| \geqslant \frac{|\mathbf{A}|}{\left|\mathrm{supp}(\widehat{f}\,)\right|} = \frac{2^n}{k}.$$

Naredni rezultat zove se *Cauchy-Davenportov teorem*. Elegantni dokaz koji slijedi osmislio je R. Chapman, a mi ga preuzimamo iz članka [10].

Zadatak 14. *Ako je p prost broj i ako su $A, B \subseteq \mathbb{Z}_p$ neprazni, dokažite da tada vrijedi*

$$\Big|A+B\Big| \geqslant \min\Big\{\Big|A\Big| + \Big|B\Big| - 1,\, p\Big\},$$

pri čemu označavamo

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

Rješenje.. Najprije tvrdimo da možemo naći skupove $X, Y \subseteq \mathbb{Z}_p$ takve da je

$$\Big|X\Big| = p+1-\Big|A\Big|, \quad \Big|Y\Big| = p+1-\Big|B\Big|, \quad \Big|X\cap Y\Big| = \max\Big\{p+2-\Big|A\Big|-\Big|B\Big|,\, 1\Big\}.$$

Razlikujemo dva slučaja. Ako je $|A|+|B| \leqslant p+1$, tada možemo uzeti

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

Ako je pak $|A|+|B| \geqslant p+2$, tada možemo uzeti

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

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

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

Promotrimo funkciju $f * g$. Iz definicije konvolucije odmah se vidi

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

dok iz svojstva

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

slijedi

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

Konačno, ponovnim korištenjem (b) dijela teorema 12 dobivamo

$$\Big|A+B\Big| + \Big|X\cap Y\Big| \geqslant \Big|\; \mathrm{supp}(f*g)\Big| + \Big|\; \mathrm{supp}(\widehat{f*g})\Big| \geqslant p+1,$$

što je upravo

$$\left|A+B\right| \geqslant p+1-\max\left\{p+2-\left|A\right|-\left|B\right|,\,1\right\} = \min\left\{\left|A\right|+\left|B\right|-1,\,p\right\}.$$

Za vježbu ostavljamo još jedan zadatak iz članka [10].

Zadatak 15. *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 $k \geqslant 1$ 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 $\sum_{j=0}^{p-1} c_j z^j \neq 0$.*

Uputa.. Promotrite funkciju

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

tako da treba pokazati $|\mathrm{supp}(f)| \geqslant p-k+1$. Primijetite da je $\widehat{f}\,(\xi) = pc_\xi$ i $\left|\mathrm{supp}(\widehat{f}\,)\right| = k$ pa se pozovite na (b) dio teorema 12.

U ovom radu odlučili smo promatrati samo konačne komutativne grupe. Naravno da se bogatija teorija dobiva razmatrajući općenitije komutativne grupe i njih proučava tzv. *harmonijska analiza*, čije osnove zainteresirani čitatelj može naučiti iz knjige [3] ili diplomskog rada [7]. Nekomutativnim grupama bavi se *teorija reprezentacija* i opet je najelementarnije krenuti od konačnih grupa, kao npr. u knjizi [4]. {10}

Bibliografija

[1] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc. **18** (2005), 477–499.

[2] H. Dym, H. P. McKean, *Fourier Series and Integrals*, Probability and Mathematical Statistics **14**, Academic Press, New York-London, 1972.

[3] G. B. Folland, *A Course in Abstract Harmonic Analysis*, drugo izdanje, Textbooks in Mathematics, CRC Press, Boca Raton, 2016.

[4] W. Fulton, J. Harris, *Representation Theory: A First Course*, Graduate Texts in Mathematics **129**, Springer-Verlag, New York, 1991.

[5] S. Kurepa, *Konačno dimenzionalni vektorski prostori i primjene*, Tehnička knjiga, Zagreb, 1967.

[6] R. Meshulam, *An uncertainty inequality for finite abelian groups*, European J. Combin. **27** (2006), 63–67.

[7] Lj. Palle, *Fourierova analiza na lokalno kompaktnim, Abelovim grupama i neke primjene*, diplomski rad, Sveučilište u Zagrebu, 2015.

[8] I. J. Schoenberg, *The finite Fourier series and elementary geometry*, Amer. Math. Monthly **57** (1950), 390–404.

[9] D. Svrtan, D. Šterc, I. Urbiha, *On cyclic characterizations of regular pentagons and heptagons: two approaches*, Math. Commun. **7** (2002), 71–89.

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

[11] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, Cambridge, 2006.

[1]Osnove za gradivo ovog članka čine izlaganja prvog autora na pripremama za *Međunarodnu matematičku olimpijadu* i kolegiju *Studentska natjecanja iz matematike* na Matematičkom odsjeku PMF-a te diplomski rad drugog autora [7].

[2]Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, Bijenička cesta 30, 10000 Zagreb, vjekovac@math.hr
[3]Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, Bijenička cesta 30, 10000 Zagreb, ljpalle@math.hr

ISSN 1334-6083