Naloge iz univerzitetnih matematičnih tekmovanj

Hugo Trebše (hugo.trebse@gmail.com)

16. julij 2025

Kazalo

1 Analiza

Naloga 1.1

Naj bo $A > 1$. Določi vse pare pozitivnih celih števil (m, n), za katere obstaja $x \in \mathbb{R}^+$, da velja

$$(1+x)^m = (1+Ax)^n.$$

Oris dokaza. Z logaritmiranjem pretvorimo enačbo v

$$\frac{m}{n} = \frac{\log(1+Ax)}{\log(1+x)}.$$

Funkcija $f(x) = \frac{\log(1+Ax)}{\log(1+x)}$ je zvezna na $\mathbb{R}^+$, radi pa bi analizirali njeno zalogo vrednosti. Z dvema hitrima uporabama L'Hospitalovega izreka dobimo

$$\lim_{x\to 0} f(x) = A \quad \text{ter} \quad \lim_{x\to\infty} f(x) = 1.$$

Izračunamo tudi, da je

$$\frac{df}{dx} = \frac{\frac{A}{1+Ax}\log(1+x) - \frac{1}{1+x}\log(1+Ax)}{\log(1+x)^2} < 0.$$

Zaloga vrednosti funkcije f je tako interval $(1, A)$, kar pomeni, da vsak par pozitivnih celih števil (m, n), za katerega velja $n < m < An$ reši enačbo. □

Celotna poanta naloge je to, da pretvorimo vprašanje v iskanje zaloge vrednosti določene funkcije, kar je dosegljivo s standardnimi analitičnimi metodami.

Nauk: *Analiza si in v analizo se povrneš.*

Naloga 1.2

Pokaži, da je

$$\lim_{n\to\infty} \frac{1^{(1^p)}2^{2^p}\dots n^{n^p}}{n^{\frac{1}{p+1}}} = e^{\frac{-1}{(p+1)^2}}$$

Oris dokaza. Logaritmiramo ter uporabimo znane lastnosti Riemmanovih integralov:

$$\frac{-1}{(p+1)^2} = \lim_{n\to\infty} \left(\frac{1}{n} \sum_{i=1}^{n} \ln(i) \left(\frac{i}{n}\right)^p - \frac{\ln(n)}{p+1} \right).$$

$$\int_0^1 x^p\,dx = \frac{1}{p+1} \text{ ter } \int_0^1 \ln(x)x^p = \frac{-1}{(p+1^2)}.$$

Treba je pokazati, le še, da Riemmanov integral naslednje funkcije upošteva naslednji decay condition:

$$0 = \lim_{n\to\infty} \ln(n) \left(\frac{1}{n} \sum_{i=1}^{n} \left(\frac{i}{n}\right)^p - \frac{1}{p+1} \right) = \lim_{n\to\infty} \ln(n) \left(\frac{1}{n} \sum_{i=1}^{n} \left(\frac{i}{n}\right)^p - \int_0^1 x^p\,dx \right).$$

Opazujmo graf funkcije x^p na $[0,1]$. Vsota znotraj limite »overapproximira« integral. Vsota precenitev, ki jih povečamo v pravokotnike s širino $\frac{1}{n}$ ter višino enako višini »trikotnika«, ki precenuje ploščino, pa je enaka $\frac{1}{n}$, kar vidimo s projekcijo pravokotnikov na y-os. Sledi, da je izraz znotraj oklepajev v zgornji limiti manjši od $\frac{1}{n}$, kar seveda implicira želeno. □

Nauk: *Analiza* ≅ *geometrija.*

Naloga 1.3: Rešitev spisal Luka Urbanc

Naj bo $p \in \mathbb{C}[z]$ polinom n-te stopnje, katerega ničle imajo vse absolutno vrednost 1. Naj bo $q(z) = \frac{p(z)}{z^{n/2}}$. Dokaži, da imajo ničle $q'(z)$ tudi absolutno vrednost 1.

Oris dokaza. Naj bodo ničle $p(z)$ α_i za $1 \leq i \leq n$. Ker $q(z)$ ni definiran za $z = 0$, so ničle $q'(z)$ ravno ničle $z^{n/2}q'(z) = p'(z) - \frac{n}{2z}p(z)$, torej zanje velja $\frac{p'(z)}{p(z)} = \frac{n}{2z}$. Leva stran je odvod logaritma p, zato dobimo

$$\sum_{i=1}^{n} \frac{1}{z-\alpha_i} = \frac{n}{2z} \iff 0 = \sum_{i=1}^{n} \left(\frac{1}{z-\alpha_i} - \frac{1}{2z} \right) = \sum_{i=1}^{n} \frac{z+\alpha_i}{2z(z-\alpha_i)} \iff \sum_{i=1}^{n} \frac{z+\alpha_i}{z-\alpha_i} = 0.$$

Opazimo, da je $\frac{z+\alpha}{z-\alpha}$ za $|z| = |\alpha| = 1$ imaginaren (to sledi iz npr. Talesovega izreka), kar nam da idejo, da ločimo njegov realen in imaginaren del za splošne z. Dobimo:

$$\frac{z+\alpha}{z-\alpha} = \frac{(z+\alpha)(\bar{z}-\bar{\alpha})}{|z-\alpha|^2} = \frac{|z|^2 - 1 + \alpha\bar{z} - \bar{\alpha}z}{|z-\alpha|^2},$$

Ker mora biti $\Re\left(\sum_{i=1}^{n} \frac{z+\alpha_i}{z-\alpha_i}\right) = 0$, sledi $|z| = 1$. □

Nauk: *Kompleksna števila ≅ geometrija.*

Nauk: *Mobiusove transformacije so vedno lepe.*

Naloga 1.4

Naj bo $f : [0,1] \to \mathbb{R}$ odvedljiva funkcija z integrabilnim odvodom, za katero velja $f(1) = 0$. Pokaži, da je

$$\int_0^1 (xf'(x))^2\,dx \geq 12 \cdot \left(\int_0^1 xf(x)\,dx\right)^2.$$

Oris dokaza. Integracija po delih poda:

$$\int_0^1 xf(x)\,dx = \frac{x^2}{2}f(x)\Big|_{x=0}^{x=1} - \int_0^1 \frac{x^2}{2}f'(x)\,dx = \frac{-1}{2}\int_0^1 x^2 f'(x)\,dx.$$

Cauchy-Schwarz poda:

$$\left(\int_0^1 (xf'(x))^2\,dx\right) \cdot \left(\int_0^1 x^2\,dx\right) \geq \left(\int_0^1 x^2 f'(x)\,dx\right)^2$$
$$\implies \int_0^1 (xf'(x))^2\,dx \geq 3 \cdot 4 \cdot \left(\int_0^1 xf(x)\,dx\right)^2.$$

Nauk: *Integralska neenakost* $\implies$ *Cauchy-Schwarz.*

□

Naloga 1.5

Naj bo $f : [0,1] \to \mathbb{R}$ integrabilna funkcija, za katero velja

$$\int_0^1 f(x)\,dx = \int_0^1 xf(x)\,dx = 1.$$

Pokaži, da velja

$$\int_0^1 f(x)^2\,dx \geq 4.$$

Oris dokaza. Neposredna uporaba Cauchy-Schwarzove neenakosti nam da

$$\left(\int_0^1 f(x)^2\,dx\right)\cdot\left(\int_0^1 x^2\right) \geq \left(\int_0^1 xf(x)\,dx\right)^2 \implies \int_0^1 f(x)^2\,dx \geq 3,$$

kar žal ni dovolj.
Ker še nismo uporabili pogoja glede integrala funkcije f, lahko poskusimo naslednje:

$$\int_0^1 f(x)(x+y)\,dx = 1+y.$$

Cauchy-Schwarzova neenakost nam nato da

$$\begin{aligned}\left(\int_0^1 f(x)^2\,dx\right)\left(\int_0^1 (x+y)^2\,dx\right) &\geq \left(\int_0^1 f(x)(x+y)\,dx\right)^2\\ \left(\int_0^1 f(x)^2\,dx\right)\left(\frac{1}{3}+y+y^2\right) &\geq (1+y)^2\\ \left(\int_0^1 f(x)^2\,dx\right) &\geq \frac{y^2+2y+1}{y^2+y+\frac{1}{3}}\end{aligned}$$

za vse $y \in \mathbb{R}$, saj je izraz na desni vedno definiran. Za $y = \frac{-1}{3}$ dobimo konstanto

$$\frac{\left(\frac{2}{3}\right)^2}{\frac{1}{9}-\frac{1}{3}+\frac{1}{3}} = 9\cdot\left(\frac{2}{3}\right)^2 = 4.$$

Z odvajanjem lahko dejansko pokažemo, da je to najboljša konstanta, ki jo dobimo s tem pristopom (in tudi najboljša možna konstanta, saj funkcija $x \mapsto 6x-2$ doseže enakost). □

Definicija 1.6

Naj bo f integrabilna na D. Tedaj je

$$\|f\|_p = \left(\int_D |f(x)|^p\,dx\right)^{\frac{1}{p}}$$

Izrek 1.7: Hölder

Naj so $p_1, \ldots, p_m$ pozitivna realna števila, za katera velja

$$\sum_{i=1}^{m} \frac{1}{p_i} = 1.$$

Če je družina funkcij $\{f_i\}$ taka, da je družina funkcij $\{f_i^{p_i}\}$ integrabilna na D, potem je funkcija

$$\prod_{i=1}^{m} f_i$$

integrabilna na D ter velja

$$\int_D \left(\prod_{i=1}^{m} |f_i(x)| \right) \, dx \leq \prod_{i=1}^{m} \|f_i\|_{p_i}$$

oziroma

$$\int_D \left(\prod_{i=1}^{m} |f_i(x)| \right) \, dx \leq \prod_{i=1}^{m} \left(\int_D |f_i(x)|^{p_i} \right)^{\frac{1}{p_i}}.$$

Oris dokaza. Izberimo $p = q = r = 3$, očitno je vsota njihovih obratnih vrednosti enaka 1. Sledi, da je

$$\left(\int_0^1 \left(|f(x)|^{\frac{2}{3}} \right)^3 \, dx \right)^{\frac{1}{3}} \cdot \left(\int_0^1 \left(\left| f(x)^{\frac{1}{3}} \right| \right)^3 \, dx \right)^{\frac{1}{3}} \left(\int_0^1 (x)^3 \, dx \right)^{\frac{1}{3}} \geq \int_0^1 |f(x)|^{\frac{2}{3}} \cdot |f(x)|^{\frac{1}{3}} \cdot x \, dx,$$

oziroma ekvivalentno

$$\left(\int_0^1 f(x)^2 \, dx \right) \left(\int_0^1 f(x) \, dx \right) \left(\int_0^1 x^3 \, dx \right) \geq \left(\int_0^1 x f(x) \, dx \right)^3$$
$$\implies \int_0^1 f(x)^2 \, dx \geq 4.$$

□

Nauk: *Integralska neenakost* $\implies$ *Cauchy-Schwarz.*

Nauk: *Equality case (ki je linearna funkcija) skupaj z pogojem za enakost pri Cauchy-Schwarzu za nize poda ta pravi člen za integralskega Cauchy-Schwarza.*

Naloga 1.8: Putnam 2000 B4

Naj bo $f : \mathbb{R} \to \mathbb{R}$ zvezna funkcija, za katero velja

$$f(2x^2 - 1) = 2xf(x)$$

za vse x. Pokaži, da je $f(x) = 0$ za vse $x \in [-1, 1]$.

Rešitev. Argument funkcije na levi strani enakosti spominja na adicijski izrek $2\cos(x)^2 - 1 = \cos(2x)$. Skupaj z dejstvom, da nas zanimajo vrednosti f na sliki funkcije cos to motivira substitucijo $x = \cos(t)$, kar dano enakost preobrazi v naslednjo

$$f(\cos(2t)) = 2\cos(t) \cdot f(\cos(t)).$$

Faktorja $2\cos(t)$ se lahko znebimo z uporabo formule za dvojni kot funkcije sinus, zato za vsak $x \in \mathbb{R}$, ki ni celoštevilski večkratnik π, definiramo

$$g(t) = \frac{f(\cos(t))}{\sin(t)}.$$

Tako sledi

$$g(2t) = \frac{f(\cos(2t))}{\sin(2t)} = \frac{2\cos(t)f(\cos(t))}{\sin(2t)} = \frac{2\cos(t)f(\cos(t))}{2\sin(t)\cos(t)} = \frac{f(\cos(t))}{\sin(t)} = g(t).$$

Če bi bila g zvezna funkcija na intervalu bi lahko s klasičnimi argumenti iz Analize 1 zaključili, da je konstantna. Ker pa je njeno definicijsko območje bolj zapletena množica moramo postopati previdneje. Funkcija g je definirana na množici $D = \mathbb{R} \setminus \{\pi \cdot k \mid k \in \mathbb{Z}\}$, na kateri je tudi zvezna, ter je periodična s periodo π, obenem pa za vsaka $t, 2t \in D$ velja $g(t) = g(2t)$. Te tri dejstva uporabimo ter ugotovimo, da za vsaki celi števili k, m velja

$$g(1 + \frac{\pi m}{2^k}) = g(2^k + \pi m) = g(2^k) = g(1).$$

Zaključili smo, da je g konstantna na množici

$$G = \{1 + \frac{\pi a}{2^b} \mid a, b \in \mathbb{Z}\}.$$

Ta množica je gosta v $\mathbb{R}$, kar lahko utemeljimo s preprostim topološkim argumentom. Preslikava

$$\mathcal{L} : x \mapsto \frac{1}{\pi}(x - 1)$$

preslika množico G v množico $\{\frac{a}{2^b} \mid a, b \in \mathbb{Z}\}$, ki je znano gosta v $\mathbb{R}$. Preslikava $\mathcal{L}$ je linearna, v posebnem primeru je homeomorfizem. Ker homeomorfizmi slikajo goste množice v goste množice sledi da $\mathcal{L}^{-1}$ slika množico, ki je gosta v $\mathbb{R}$, v množico G, ki je posledično tudi gosta v $\mathbb{R}$. Ker je G gosta v $\mathbb{R}$ je gotovo gosta tudi v D. Sklepanje nas je vodilo do zaključka, da je zvezna funkcija g konstantna na gosti podmnožici svojega definicijskega območja, kar pomeni, da je konstantna na celotnem definicijskem območju.

Zaradi lihosti funkcije sin ter sodosti funkcije cos za vse $t \in D$ velja

$$g(-t) = -g(t).$$

Ker je g konstantna na D je $g(t) = g(-t) = -g(t)$, iz česar sledi

$$g(t) = 0 \text{ za vse } t \in D.$$

Sledi, da je $f(\cos(x)) = 0$ za vse $x \in D$. Tako sledi, da je

$$f(x) = 0 \text{ za vse } x \in (-1, 1) \setminus \{0\}.$$

Iz zveznosti f sledi, da je $f(0) = 0$. Vrednosti v krajiščih pa lahko izračunamo iz začetne enakosti, namreč

$$\begin{aligned} f(2 \cdot 0^2 - 1) = f(-1) = 2 \cdot 0 \cdot f(0) &\implies f(-1) = 0 \\ f(2 \cdot 1^2 - 1) = f(1) = 2 \cdot 1 \cdot f(1) = 2 \cdot f(1) &\implies f(1) = 0. \end{aligned}$$

□

Nauk: *Substitucije ter izpeljane funkcije pretvorijo čudne pogoje v manj čudne pogoje.*

Naloga 1.9

Naj bo $f : [a, b] \to \mathbb{R}$ zvezna funkcija in odvedljiva na (a, b). Naj ima f neskončno mnogo ničel, obenem pa naj ne obstaja točka $x \in (a, b)$, za katero velja

$$f(x) = f'(x) = 0.$$

- Pokaži, da je $f(a)f(b) = 0$.
- Podaj primer funkcije f na intervalu $[0, 1]$.

Rešitev. Naj bo c eno izmed stekališč množice ničel f in naj zaporedje ničel f $\{n_i\}$ konvergira proti c. Denimo, da je $c \notin \{a, b\}$. Iz zveznosti f sledi $f(c) = 0$. Sedaj izračunajmo odvod f v c z uporabo definicije limite z zaporedji. Za vsako zaporedje neničelnih točk t_i, ki konvergirajo proti 0, mora biti limita zaporedja

$$\left\{ \frac{f(c + t_i) - f(c)}{t_i} \right\}$$

enaka $f'(c)$. Izberimo zaporedje $\{t_i\} = \{n_i - c\}$. Tako velja

$$f'(c) = \lim_{i\to\infty} \frac{f(c + t_i) - f(c)}{t_i} = \lim_{i\to\infty} \frac{f(c + n_i - c) - f(c)}{n_i - c} = \lim_{i\to\infty} \frac{f(n_i) - f(c)}{n_i - c} = \lim_{i\to\infty} \frac{0 - 0}{n_i - c_i} = 0.$$

To je seveda protislovje, zato sledi $c \in \{a, b\}$.

Primer funkcije z želeno lastnostjo je $g(x) = x \sin\left(\frac{1}{x}\right)$ z zvezno dopolnitvijo $g(0) = 0$. Ničle g na $(0, 1)$ so $\{\frac{1}{k\pi} \mid k \in \mathbb{N}\}$. Odvod g je enak

$$g'(x) = x \cos\left(\frac{1}{x}\right)\left(\frac{-1}{x^2}\right) + \sin\left(\frac{1}{x}\right) = \sin(\frac{1}{x}) - \frac{1}{x}\cos\left(\frac{1}{x}\right),$$

ki očitno nima ničle na omenjeni množici. □

Naloga 1.10

Zvezna funkcija $f : [0,1] \to \mathbb{R}$ je *lepa*, če je

$$f(x) + f(y) \geq |x - y|$$

za vse $x, y \in [0,1]$. Določi minimum $\int_0^1 f$ med vsemi lepimi funkcijami.

Rešitev. Substituiramo $y = x + a$ za nek $a \in [0, 1 - x]$. Sledi, da je

$$f(x) + f(x + a) \geq a,$$

kar je bolj obvladljivo.

Kako bi sedaj človek integriral f po $[0,1]$? Če integriramo levo stran od 0 do a dobimo

$$\int_0^a f(x)\,dx + \int_a^{2a} f(x)\,dx \geq a^2.$$

Sedaj je najpreprostejše nastaviti $a = \frac{1}{2}$ in dobiti $\frac{1}{4}$ kot kandidata za minimum.

Splošnejši pristop integriranja relacije z a po intervalu $[b, c]$ vodi do

$$\int_b^c f(x)\,dx + \int_{b+a}^{c+a} f(x)\,dx \geq (c - b)a.$$

Nastaviti $a = 2^{-k}$ in seštevati integrale se zdi zvito, a vodi do že dokazane spodnje meje $\frac{1}{4}$, kar da sum, da je slednja morda celo optimalna.

Najti je treba še funkcijo, ki doseže enakost. Glede na prisotnost absolutnih vrednosti v pogoju naloge se prej ali slej porodi ideja funkcije $x \mapsto \left|x - \frac{1}{4}\right|$, ki izpolnjuje pogoj in doseže želen minimum. □

Nauk: *Najprej je smiselno poiskusiti najpreprostejše ideje.*

Nauk: *Morebitni linearne meje, ki jih dobimo s substitucijami $y \in \{0, 1, x_m, x_m\}$ (f v x_m in x_M zaporedoma doseže minimum in maksimum m in M) so relativno neuporabni dokler ne iščemo funkcije, ki doseže minimum. Tedaj je iz grafa relativno očitno, da bo smiselen kandidat zamaknjena absolutna vrednost.*

Nauk: *IMC PSC ne ve vedno kaj pomeni težavnost naloge.*

Naloga 1.11

$n \in \mathbb{N}$, $\{a_1, \ldots, a_n\}$ in $\{b_1, \ldots, b_n\}$ sta niza realnih števil, za katera velja $a_i + b_i > 0$. Pokaži, da je

$$\sum_{i=1}^{n} \frac{a_i b_i - b_i^2}{a_i + b_i} \leq \frac{\sum_{i=1}^n a_i \cdot \sum_{i=1}^n b_i - \left(\sum_{i=1}^n b_i\right)^2}{\sum_{i=1}^n a_i + b_i}.$$

Rešitev. Očitno je to Cauchy-Schwarz nekega okusa. Malo kompaktnejše človek želeno neenakost napiše kot:

$$\frac{(\sum b_i) \cdot (\sum a_i - b_i)}{\sum a_i + b_i} \geq \sum \frac{b_i \cdot (a_i - b_i)}{a_i + b_i}.$$

Zelo sumljivo imamo dva izraza tipa

$$\frac{x(x-y)}{x+y},$$

kar se da poenostaviti v

$$\frac{x(y-x)}{y+x} = \frac{xy - x^2}{y+x} = \frac{xy + x^2 - 2x^2}{y+x} = x - \frac{2x^2}{y+x}.$$

Upoštevajoč to enakost se želena neenakost pretvori v

$$\left(\sum b_i\right) - 2\frac{\left(\sum b_i\right)^2}{\sum a_i + b_i} \geq \sum b_i - 2\frac{b_i}{a_i + b_i} = \sum b_i - 2\sum \frac{b_i^2}{a_i + b_i}$$
$$\left(\sum \frac{b_i^2}{a_i + b_i}\right) \geq \frac{\left(\sum b_i\right)^2}{\left(\sum a_i + b_i\right)},$$

kar je seveda Cauchy-Schwarz, oziroma Titujeva lema. □

Nauk: *IMC PSC ne ve kako težka je naloga. (Kako je to P3?)*

Nauk: *Pretvorba neenakosti upoštevajoč zgornjo identiteto je relativno naravna, ko strukturo neenakosti opazujemo malo bolj globalno.*

Naloga 1.12

Naj bo $f : \mathbb{R} \to \mathbb{R}$ dvakrat odvedljiva ter naj bo $f(0) = 0$. Pokaži, da obstaja $\zeta \in (\frac{-\pi}{2}, \frac{\pi}{2})$, da velja

$$f''(\zeta) = f(\zeta)\left(1 + 2\tan(\zeta)^2\right).$$

Rešitev. Definirajmo $g(x) = f(x)\cos(x)$. Na krajiščih intervala $(\frac{-\pi}{2}, \frac{\pi}{2})$ ima g ničli, prav tako v $x = 0$, zato po Rollejevem izreku (oz. Lagrangeevem izreku) obstajata $\zeta_1 \in (\frac{-\pi}{2}, 0)$ in $\zeta_2 \in (0, \frac{\pi}{2})$, ki sta ničli odvoda g.

Definirajmo funkcijo

$$h(x) = \frac{g'(x)}{\cos(x)^2} = \frac{f'(x)\cos(x) - f(x)\sin(x)}{\cos^2(x)}.$$

Z nekaj računanja dobimo želen pogoj po uporabi Rollejvega izreka na intervalu (ζ_1, ζ_2). □

Nauk: *Izpeljane funkcije :). Uporaba neke vrste izpeljane funkcije je relativno naravna, saj je drugače pogoj čisto neumesten.*

Nauk: *Praktično enaka naloga kot Putnam 2000 B4.*

Naloga 1.13

Določi vse zvezne funkcije $f : \mathbb{R} \to \mathbb{R}$, za katere velja

$$x - y \in \mathbb{Q} \implies f(x) - f(y) \in \mathbb{Q}.$$

Rešitev. Očitno delujejo vse funkcije oblike

$$f(x) = q \cdot x + c,$$

kjer je $q \in \mathbb{Q}$ in $c \in \mathbb{R}$. Želimo določiti vse zvezne funkcije, ki zadoščajo določenemu pogoju, obenem pa imamo močen sum, da so take funkcije linearne. Prva ideja je Cauchyjeva funkcijska enačba. Za fiksen $r \in \mathbb{Q}$ je

$$g_r(x) = f(x + r) - f(x)$$

zvezna funkcija, ki zavzame samo racionalne vrednosti. Iz povezanosti sledi, da je g_r konstantna. Ker je $g_r(0) = f(r)$ sledi, da je funkcija

$$h(x, y) = f(x + y) - f(x) - f(y)$$

enaka 0 na množici $\mathbb{R} \times \mathbb{Q}$. Ker je $\mathbb{R} \times \mathbb{Q}$ gosta v $\mathbb{R}^2$ velja, da je

$$h(x, y) = 0$$

za vse $(x, y) \in \mathbb{R}^2$. Tako dobimo, da za vse $(x, y) \in \mathbb{R}^2$ velja

$$f(x) + f(y) = f(x + y).$$

To je Cauchyjeva funkcijska enačba, ki ima v množici zveznih funkcij le linearne rešitve. Izmed vseh linearnih funkcij seveda delujejo le opisane. □

Nauk: *Naloga je pravzaprav funkcijska enačba, obenem vemo, da so rešitve le linearne. Gotovo mora biti Cauchy.*

Nauk: *Iz besedila je že očitno, da je naloga topološka in ne analitična.*

Naloga 1.14

$f : \mathbb{R} \to \mathbb{R}$ je dvakrat odvedljiva funkcija, za katero velja $f(0) = 1$, $f'(0) = 0$ in za vse $x \in [0, \infty)$ velja

$$f''(x) - 5f'(x) + 6f(x) \geq 0.$$

Pokaži, da je za vse $x \in [0, \infty)$

$$f(x) \geq 3e^{2x} - 2e^{3x}.$$

Rešitev. Glede na želeno mejo je najverjetnejši pristop neke sorte faktorizacija, saj je pogoj drugače pregrd, v kombinaciji z integriranjem, saj želimo neko eksplicitno mejo.

Resnično je pogoj ekvivalenten

$$(f''(x) - 2f'(x)) - 3(f'(x) - 2f(x)) \geq 0.$$

Definirajmo $h(x) = f'(x) - 2f(x)$. Enakost se pretvori v

$$h'(x) - 3h(x) \geq 0 \implies \frac{h'(x)}{h(x)} \geq 3 \implies \ln(h(x)) \geq 3x + C \implies h(x) \geq Ce^{3x}.$$

(Čeprav je deljenje z h nedefinirano, saj ima h ničle, lahko to obidemo z opazko, da je desna stran enaka $(g(x)e^{-3x})' \cdot e^{3x}$.)

Iz podanih pogojev o f dobimo, da je $h(0) = -2$, kar pomeni, da je $C \leq -2$. Sledi

$$f'(x) - 2f(x) \geq Ce^{3x} \iff f'(x)e^{-2x} - 2e^{-2x}f(x) \geq Ce^{x} \implies \left(f(x)e^{-2x}\right)' \geq Ce^{x}.$$

Sledi, da je

$$f(x)e^{-2x} \geq Ce^{x} + D \implies f(x) \geq Ce^{3x} + De^{2x}.$$

Vemo, da je $C \leq -2$, kar pomeni, da je $f(x) \geq -2e^{3x} + De^{2x}$. Ker je $f(0) = 0$ je gotovo $f(0) = 1 \geq -2 + D$, kar pomeni, da je $D \leq 3$. Ugotovitve o C in D združimo ter dobimo želeno neenakost. □

Nauk: *Edina metoda s katero naloga sploh zgleda rešljiva je točno ta s faktorizacijo in integriranjem.*
Nauk: *Pri integriranju neenakosti je potrebno nekaj previdnosti.*

Naloga 1.15

Naj bo $f : [0,1) \to (0,1)$ zvezna surjektivna funkcija.

- Pokaži, da je za vse $a \in (0,1)$ zožitev $f|_{(a,1)}$ surjektivna.
- Podaj primer funkcije f, za katero velja pogoj naloge.

Rešitev. Naj bo $A = (a,1)$. Očitno je $[0,1) \setminus A$ kompakt, kar pomeni, da na njem funkcija doseže maksimum $M < 1$ in minimum $m > 0$. Funkcija f more zavzeti tudi vrednosti iz intervalov $(0,m)$ ter $(M,1)$, ker jih ne doseže na $[0,1) \setminus A$ jih doseže na njegovem komplementu A, kar pokaže želeno po izreku o vmesni vrednosti.

Primer funkcije, ki ustreza pogoju je

$$f(x) = \frac{1 + x \sin\left(\frac{1}{1-x}\right)}{2}.$$

Z analiziranjem vrednosti f v točkah oblike

$$x = 1 - \frac{1}{\frac{\pi}{2} + k\pi} \implies \frac{1}{1-x} = \frac{\pi}{2} + k\pi \quad \text{ter} \quad x = 1 - \frac{1}{\frac{3\pi}{2} + k\pi} \implies \frac{1}{1-x} = \frac{3\pi}{2} + k\pi$$

za $k \in \mathbb{Z}$ lahko surjektivnost pokažemo z lahkoto. □

A kako se lahko kdorkoli spomne take funkcije? Naštejmo nekaj lastnosti, ki bi jih želeli od kandidata za funkcijo f

- f ne sme imeti zvezne razširitve na $[0,1]$, saj bi razširitev na kompaktu zavzela minimum in maksimum, kvečjemu enega v $x = 1$. Začetna funkcija f tako ne bi zavzela vseh vrednosti v $(0,1)$.
- S točko $x = 0$ ne moremo storiti »nič posebnega«. Če bi bila $x = 0$ ekstremna točka f ponovno dobili protislovje, zato jo preprosto postavimo na $\frac{1}{2}$.

Kanonični primer »najgrše možne« zvezne funkcije iz Analize 1 je funkcija $x \mapsto x \sin(\frac{1}{x})$ z zvezno dopolnitvijo v točki 0. Ta primer priredimo našim potrebam, izraz $\frac{1}{1-x}$ pa poskrbi, da se patologije omenjene funkcije pojavijo, ko gre x proti 1.

2 Linearna algebra

Trditev 2.1: Matrike, ki komutirajo

- Inverzne matrike komutirajo.
- Diagonalne matrike komutirajo.
- Polinomi v isti matriki komutirajo.

Nasvet

Determinanto si lahko predstavljamo na par načinov:

- kot vsoto produktov, ki vsebuje znak permutacije - tedaj je najuporabnejši razpis po vrstici/stolpcu
- kot količino ki »meri« obrnljivost matrike
- kot n-linearni antisimetrični funkcional, ki trivialno poda trditve o menjavi vrstic, o prištevanju večkratnikov vrstic drugim vrsticam ter o množenju vrstice s skalarjem

Naloga 2.2

Kvadratna matrika A je *skoraj simetrična*, če je $a_{i,j} = -a_{j,i}$. Naj bo A skoraj simetrična matrika sode dimenzije. Pokaži, da je determinanta matrike, ki jo dobimo s prištevanjem danega skalarja vsem vnosom A enaka determinanti A.

Oris dokaza.
Prva rešitev: Zelo preprosto preverimo, da imajo vse skoraj-simetrične matrike lihega reda ničelno determinanto (skoraj simetričnost je namreč ekvivalentna $A+A^T = 0$). Sledi, da je determinanta matrike:

$$\begin{bmatrix} 0 & 1 & 1 & \dots & 1 \\ -1 & a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{bmatrix}$$

ničelna, zato je ničelna tudi determinanta matrike, ki jo dobimo z množenjem prvega stolpca s sklarjem x. Sledi, da je determinanta matrike:

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ -x & a_{1,1} & \dots & a_{n1} \\ \vdots & \vdots & \ddots & \vdots \\ -x & a_{n,1} & \dots & a_{n,n} \end{bmatrix}$$

enaka $\det(A)$. Množenje prvega stolpca matrike nad zgornjo z $-x$ ter prištevanje prvega stolpca vsem ostalim poda želeno trditev.

Druga rešitev: Naj bo $J = \{1\}_{i,j\leq n}$ matrika s samimi enicami. Želeli bi pokazati, da je $\det(A+tJ)$ konstantni polinom. Velja:

$$\det(A+tJ) = \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} (a_{i,\pi(i)} + t).$$

V vsoti se pojavi sumand

$$\operatorname{sgn}(\pi) \cdot a_{i_1,\pi(i_1)} \dots a_{i_k,\pi(i_k)} \cdot t^k,$$

prav tako pa se pojavi sumand

$$\operatorname{sgn}(\pi^{-1}) \cdot a_{i_1,\pi^{-1}(i_1)} \dots a_{i_k,\pi^{-1}(i_k)} \cdot t^k.$$

Ker je

$$\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$$

se ne razlikujeta v znaku permutacije. Velja pa, da je zadnji sumand pravzaprav oblike

$$\operatorname{sgn}(\pi^{-1}) \cdot a_{\pi(i_1),i_1} \dots a_{\pi i_k,i_k} \cdot t^k.$$

Ker je matrika A skoraj simetrična pa je to enako

$$\operatorname{sgn}(\pi^{-1}) \cdot (-1)^k \cdot a_{i_1,\pi(i_1)} \dots a_{i_k,\pi(i_k)} \cdot t^k,$$

posledično je vsota sumandov 0. Sledi, da imajo lihe potence polinoma $\det(A+tJ)$ ničelni koeficient.

Z elementarnimi operacijami na matriki (prištevanje večkratnikov stolpcev stolpcem) lahko determinanto preoblikujemo v obliko, ko se edina spremenljivka t nahaja v zgornjem levem kotu matrike A. Sledi, da je $\det(A+tJ)$ največ linearen, ker pa je koeficient lihih potenc 0 pa je polinom $\det(A+tJ)$ konstanten, kar smo želeli pokazati. □

Nauk: *Obstajajo tri karakterizacije determinante, pogosto je vsota najgrša.*

Nauk: *Ideja z inverzno permutacijo ni nova, uporabil jo je že Šivic v zapiskih...*

Izrek 2.3

Za kvadratni matriki istih dimenzij A in B velja:

$$\operatorname{spec}(AB) = \operatorname{spec}(BA)$$

Naloga 2.4: Putnam 2015 B3

Naj bo S množica vseh realnih 2×2 matrik

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

katerih elementi a, b, c, d v tem vrstnem redu tvorijo aritmetično zaporedje. Določi vse matrike M v S, za katere obstaja neko naravno število $k > 1$, da je M^k prav tako element S.

Rešitev. Naj bosta $a, d \in \mathbb{R}$ ter

$$M = \begin{pmatrix} a & a+d \\ a+2d & a+3d \end{pmatrix}.$$

Sledi, da je

$$\operatorname{char}(M)(t) = \det(M - tI) = t^2 - (2a+3d)t - 2d^2$$

ter

$$\det(M) = -2d^2.$$

Diskriminanta karakterističnega polinoma je $(2a+3d)^2 + 8d^2 \geq 0$, kar pomeni, da ima karakteristični polinom dve realni ničli. Primer $d = 0$ bomo obravnavali kasneje, zato predpostavimo $d \neq 0$. Sledi, da je prosti člen karakterističnega polinoma strogo negativen, kar pomeni, da sta realni lastni vrednosti λ_1 ter λ_2 neničelni in različno predznačeni. Ker obstajata dve različni lastni vrednosti lahko M diagonaliziramo

$$M = \begin{pmatrix} s & -q \\ -r & p \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ps\lambda_1 - qr\lambda_2 & qs(\lambda_1 - \lambda_2) \\ pr(\lambda_2 - \lambda_1) & ps\lambda_2 - sq\lambda_1 \end{pmatrix},$$

kjer so konstante p, s, q, r realna števila, za katera velja

$$ps - qr = 1.$$

Ker je $M \in S$ sledi, da je vsota elementov na diagonali enaka vsoti elementov na antidiagonali, kar implicira

$$(ps - qr)(\lambda_1 + \lambda_2) = (qs - pr)(\lambda_1 - \lambda_2) \implies qs - pr = \frac{\lambda_1 + \lambda_2}{\lambda_1 - \lambda_2}.$$

Če je M^k za neki $k > 1$ prav tako element S analogen izračun pokaže, da je

$$qs - pr = \frac{\lambda_1^k + \lambda_2^k}{\lambda_1^k - \lambda_2^k}.$$

Ker sta obe lastni vrednosti neničelni ter drugače predznačeni lahko definiramo $x = \frac{\lambda_1}{\lambda_2} < 0$. V tem primeru je $x \neq 1$, zato sledi

$$\frac{x+1}{x-1} = qs - pr = \frac{x^k+1}{x^k-1} \implies 1 + \frac{2}{x-1} = 1 + \frac{2}{x^k-1}$$
$$\implies \frac{2}{x-1} = \frac{2}{x^k-1} \implies x = x^k \implies x \in \{-1, 0\}.$$

V primeru $x = 0$ je $\lambda_1 = 0$, kar je v protislovju z ugotovitvijo o neničelnosti lastnih vrednosti. Tako je edina možnost $x = -1$ oziroma $\lambda_1 = -\lambda_2$. Primerjanje lastnih vrednosti z linearnim členom karakterističnega polinoma poda $2a + 3d = 0$. V tem primeru je M oblike

$$\begin{pmatrix} -3t & -t \\ t & 3t \end{pmatrix}, \text{ kjer je } t = \frac{-a}{3} = \frac{d}{2}.$$

Matrike te oblike izpolnjujejo pogoj za $k = 3$, kar lahko preverimo računsko.

$$\begin{pmatrix} -3t & -t \\ t & 3t \end{pmatrix}^3 = t^3 \begin{pmatrix} -3 & -1 \\ 1 & 3 \end{pmatrix}^3 = t^3 \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix} \cdot \begin{pmatrix} -3 & -1 \\ 1 & 3 \end{pmatrix} = (2t)^3 \begin{pmatrix} -3 & -1 \\ 1 & 3 \end{pmatrix}.$$

Če je $d = 0$ je M oblike

$$\begin{pmatrix} t & t \\ t & t \end{pmatrix} \text{ za neki } t \in \mathbb{R}.$$

Ker so vsi elementi M enaki bo enako veljalo za vse potence M, kar pomeni, da ta družina matrik izpolnjuje pogoj za $k = 2$.

Družini matrik nista tako sporadični kot se morda zdi na prvi pogled, prva je specifični primer konstantnega aritmetičnega zaporedja, med tem ko je druga oblika poljubne matrike z želeno lastnostjo ter ničelno sledjo. □

Nauk: *Pri* 2×2 *matrikah računanje karakterističnega polinoma ni težavno.*

3 Algebra

Naloga 3.1

Kolobar A ima lastnost $\star$, če velja

- A ima vsaj 4 elemente
- $2 = 1 + 1$ je obrnljiv element A
- za vse $x \in A$ velja $x + x^4 = x^3 + x^2$

Daj primer kolobarja z lastnostjo $\star$ ter dokaži, da če sta $a, b \in A$ različna elementa, da sta a in $a + b$ enoti, potem je $1 + ab$ enota, b pa ni enota.

Oris dokaza. Primer takega kolobarja je $\mathbb{F}_3 \times \mathbb{F}_3$. Prvi dve točki lastnosti $\star$ sta očitni, tretja sledi iz tega, da je vsak obrnljiv element idempotent (Idejo za ustrezen kolobar morda dobimo z opazko o karakteristiki 3).

Identiteto pretvorimo v naslednjo obliko

$$x^4 + x = x^3 + x^2 \implies x^3(x-1) = x(x-1) \implies x(x-1)^2(x+1) = 0.$$

(vrstni red ni pomemben, saj polinomi v nekomutativnih spremenljivkah komutirajo).

Če vstavimo $x = 2$ dobimo, da je $\mathrm{char}(A) = 3$.

Substitucija $x \mapsto x + 1$ poda identiteto

$$x^2(x+1)(x+2) = 0 \quad \forall x \in A.$$

Če je $a \in A$ enota je tako

$$(a+1)(a+2) = 0 \iff a^2 + 3a + 2 = 0 \iff a^2 = 1.$$

Produkt enot je gotovo enota, zato je

$$a(a+b) = a^2 + ab = 1 + ab$$

enota, prav tako $1 + ba$.

Denimo, da je b enota. Sledi

$$1 = (a+b)^2 = a^2 + ab + ba + b^2 = 2 + ab + ba$$

ter

$$(1+ab)(1+ba) = 1 + ab + ba + abba = 2 + ab + ba$$

Tako je $(1 + ab) = (1 + ab)^{-1} = (1 + ba)$, zato a in b komutirata. Tako velja

$$2 = 2ab \implies 1 = ab,$$

kar pomeni $a = a^{-1} = b$, kar je v protislovju s predpostavljeno različnostjo a in b. Tako b ni enota. □

Nauk: *Čudne identitete se pogosto da pretvoriti na manj čudne identitete (morda z izgubo splošnosti).*

3.1 Polinomi

Definicija 3.2

Naj bo A domena enolične faktorizacije. Tedaj definiramo *rezultanto* polinomov

$$f(x) = \sum_{i=0}^{m} a_i X^i \in A[X] \quad \text{ter} \quad g(x) = \sum_{i=0}^{n} b_i X^i \in A[X]$$

kot determinantno matrike dimenzije $(m+n) \times (m+n)$.

$$\operatorname{Res}(f,g) = \det \begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_0 \end{bmatrix}$$

Izrek 3.3

Polinoma $f, g \in A[X]$ imata skupni faktor natanko tedaj, ko je $\operatorname{Res}(f,g) = 0$.

Dokaz. Linearna odvisnost vrstic je ekvivalentna ničelnosti determinante. Vemo, da to velja nad polji, a če kolobar A vložimo v svoje polje ulomkov nato pa pomnožimo z najmanjšim skupnim večkratnikov imenovalcev dobimo linearno odvisnost vrstic nad A (linearna odvisnost nad A pa trivialno implicira linearno odvisnost nad poljem ulomkov). Zato je ničelnost determinante ekvivalentna linearni odvisnosti vrstic nad A.

Linearna odvisnost vrstic je ekvivalentna linearni odvisnosti množice

$$\{f, Xf, X^2 f, \ldots, X^{n-1} f, g, Xg, \ldots, X^{n-1} g\}$$

nad A. Slednje je ekvivalentno obsoju neničelnih polinomov $\varphi, \psi \in A[X]$, kjer je $\deg \varphi < \deg g$ ter $\deg \psi < \deg f$, da velja

$$\varphi f + \psi g = 0.$$

Slednje je gotovo ekvivalentno obstoju skupnega faktorja f in g, saj bi v primeru tujosti f in g g delil φ, ki je manjše stopnje od g. □

3.1.1 Celoštevilski polinomi

Trditev 3.4

$P \in \mathbb{Z}[X]$. Tedaj $a - b \mid P(a) - P(b)$.

Lema 3.5: Izrek o racionalni ničli

Naj bo

$$P(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$$

ter q racionalna ničla P. Naj bo $q = \frac{a}{b}$, kjer sta a in b tuji si naravni števili. Tedaj $a \mid a_0$ ter $b \mid a_n$.

Naloga 3.6

Polinom $P \in \mathbb{Z}[X]$ zavzame vrednosti ± 1 v treh različnih celoštevilskih točkah. Pokaži, da P nima celoštevilskih ničel.

Rešitev. Denimo, da ima P celoštevilsko ničlo z, ter naj zavzame vrednost ± 1 v točkah $a, b, c \in \mathbb{Z}$. Tedaj velja $z - x \mid \pm 1$ za $x \in \{a, b, c\}$. Sledi, da je $|z - x| = 1$ za tri različne vrednosti x. To ne gre, samo poglej realno premico. □

Izrek 3.7

Naj bo $P \in \mathbb{Z}[X]$. Pokaži, da če je $P(P(\ldots P(X))) = x$ za nek $x \in \mathbb{Z}$, kjer je iteracija k-kratna, potem je $P(P(x)) = x$.

Rešitev. Ponovno uporabimo osnovno dejstvo o deljivosti celoštevilskih polinomov. Vemo, da je $P^{(k)}(x) = x$. Definiramo zaporedje $x_{k+1} = P(x_k)$ ter $x_0 = x$. Vemo, da $x_{i+1} - x_i \mid x_{i+2} - x_{i+1}$. Dodatno definirajmo $d_i = d_{i+1} - d_i$, kar implicira $d_i \mid d_{i+1}$, skupaj z dejstvom $d_k = d_0$ sledi $|d_0| = |d_1| = \ldots = |d_k|$.

Če bi dokazali, da je $d_0 = 0$ ali pa $d_2 = -d_1$ smo pokazali želeno, zato predpostavimo, da je $d_1 = d_0 \neq 0$. Sledi, da je

$$P^{(2)}(x) - P(x) = P(x) - x.$$

Denimo $d_2 = -d_1$, kar pomeni

$$P^{(3)}(x) - P^{(2)}(x) = P(x) - P^{(2)} \implies P^{(3)}(x) = P(x).$$

če sta oba izmed $P(x)$ in $P^{(2)}(x)$ različna od x se tako element x ne pojavi v zaporedju $\{x_i\}$, kar je v nasprotju s pogojem. Tako je vsaj eden izmed nju enak x, in želeno je pokazano.

Tako je $d_2 = d_1 = d_0 = d$. Podobno protislovje se pojavi v primeru $d_3 = -d$, in dobimo $d_3 = \ldots = d_0$. Induktivno dobimo, da so $\{d_i\}$ v artimetičnem zaporedju, kar je seveda protislovje po absolutnih vrednostih. □

Nauk: *Očitno človek hoče zaporedna elementa $\{d_i\}$, ki sta nasprotno predznačena, po možnosti z minimalnim indeksom.*

Polinomi s celoštevilskimi koeficienti zavzamejo celoštevilske vrednosti v celih številih. Obratna trditev ne velja, primer je na primer $\binom{x}{2}$. Velja pa naslednje:

Izrek 3.8

Denimo, da polinom $P \in \mathbb{C}[X]$ stopnje n zavzame celoštevilske vrednosti v celih številih. Potem obstajajo $c_0, \ldots, c_n$, da je

$$P(x) = c_n\binom{x}{n} + c_{n-1}\binom{x}{n-1} + \ldots + c_0\binom{x}{0}.$$

Obrat trditve trivialno velja.

Dokaz. Izvajamo indukcijo na stopnji P. Baza indukcije je očitna. Denimo, da trditev velja za vse polinome stopnje manj od n. Tvorimo polinom

$$Q(x) = P(x+1) - P(x),$$

ki je seveda stopnje manj kot n, in seveda zavzame celoštevilske vrednosti v vseh celih številih. Sledi, da je

$$Q(x) = a_{n-1}\binom{x}{n-1} + \ldots + a_0\binom{x}{0}.$$

Zvita uporaba teleskopske vsote poda, da za vsak naravni x velja

$$P(x) = P(0) + \sum_{i=0}^{x-1} Q(i).$$

Ker to velja za vsak naraven x je enakost tudi identična. Preko uporabe identitete

$$\binom{x}{k+1} = \sum_{i=0}^{x}\binom{i}{k}$$

iz reprezentacije Q kot linearne kombinacije binomskih simbolov dobimo želeno reprezentacijo P z binomskimi simboli

$$P(x) = \sum_{i=1}^{n} a_{i-1}\binom{x}{i} + P(0).$$

□

4 Teorija števil

Naloga 4.1: Putnam 1996 A5

Dokaži, da za vsa praštevila $p > 3$ število p^2 deli

$$\sum_{i=1}^{k} \binom{p}{i}, \text{ kjer je } k = \left\lfloor \frac{2p}{3} \right\rfloor.$$

Rešitev. Opazimo, da je

$$\frac{1}{p}\binom{p}{i} = \frac{p-1}{1} \cdot \frac{p-2}{2} \cdots \frac{p-i+1}{i-1} \cdot \frac{1}{i} \equiv \frac{(-1)^{i-1}}{i},$$

ter prevedemo pogoj na

$$\sum_{i=1}^{k} \frac{(-1)^i}{i} = 0 \pmod{p}.$$

Ločimo sumande vsote na sledeči način

$$\sum_{i=1}^{k} \frac{(-1)^i}{i} = \sum_{i=1}^{k} \frac{1}{i} - 2 \cdot \sum_{i=1}^{\left\lfloor \frac{k}{2} \right\rfloor} \frac{1}{2i} = \sum_{i=1}^{k} \frac{1}{i} + \sum_{i=1}^{\left\lfloor \frac{k}{2} \right\rfloor} \frac{1}{p-i} =$$
$$\sum_{i=1}^{k} \frac{1}{i} + \sum_{i=1}^{p-k-1} \frac{1}{p-i} = \sum_{i=1}^{p-1} \frac{1}{i} \pmod{p}.$$

Prva enakost sledi po ločevanju sumandov glede na predznak (oziroma na sode ter lihe imenovalce), druga sledi po krajšanju faktorjev 2 ter $\frac{1}{2}$ (kar lahko storimo za $p \neq 2$) ter upoštevajoč

$$-i = p - i \pmod{p},$$

tretja enakost pa sledi po enakosti naslednjih množic

$$\left\{ p-1, p-2, \ldots, p - \left\lfloor \frac{k}{2} \right\rfloor \right\} = \left\{ \left\lfloor \frac{2}{3p} \right\rfloor + 1, \left\lfloor \frac{2}{3p} \right\rfloor + 2, \ldots, p-1 \right\}.$$

Dobljeno vsoto moramo še evalvirati. V ta namen definiramo *primitivni koren* multiplikativne grupe ostankov $\mathbb{Z}/n\mathbb{Z}$ kot število katerega potence generirajo celotno grupo.

Lema 4.2

Multiplikativna grupa ostankov $\mathbb{Z}/p\mathbb{Z}$ ima primitivni koren.

Dokaz. Najprej navedemo dve pomožni trditvi.

Trditev 4.3

Če obstaja element reda λ po modulu p, potem je elementov reda λ natanko $\varphi(\lambda)$.

Dokaz. Če je x element reda λ, potem je ničla polinoma

$$f(T) = T^\lambda - 1 \in \mathbb{F}_p[T].$$

Sledi, da so ostale ničle polinoma ravno

$$x^0, x, x^2, \ldots, x^{\lambda-1}.$$

Da so to resnično ničle f je očitno, da več ničel ne obstaja pa je posledica znanega dejstva, da ima polinom stopnje k nad poljem $\mathbb{F}$ kvečjemu k ničel. Obenem vemo, da je red elementa x^k natanko

$$\frac{\lambda}{\gcd(\lambda, k)}.$$

Elementov reda λ je tako natanko $\varphi(\lambda)$, saj ima vsaka potenca x, ki ima eksponent tuj λ red natanko λ, obenem pa so vsi elementi reda λ med naštetimi ničlami f. □

Brez dokaza navedemo še naslednjo kombinatorično lemo, ki jo poznamo iz Diskretne matematike 1.

Trditev 4.4

Velja enakost

$$\sum_{d|n} \varphi(d) = n.$$

Kot posledica zgornjih trditev sledi, da je število elementov reda λ bodisi 0, bodisi $\varphi(\lambda)$. Sledi:

$$p - 1 = \sum_{d|p-1} \text{število elementov reda } d = \sum_{d|p-1} (0 \text{ ali } \varphi(d)).$$

Če bi bil katerikoli izmed sumandov enak nič bi dobili protislovje z zgornjo trditvijo, zato so vsi sumandi neničelni. V posebnem primeru je število elementov reda $p - 1$ neničelno. □

Tako vemo, da po modulu p obstaja tako število $g \neq 0 \pmod{p}$, ki generira celotno grupo ostankov. Velja

$$\sum_{i=1}^{p-1} \frac{1}{i} = \sum_{i=0}^{p-2} g^{-i} = \frac{1 - g^{p-1}}{1 - g} = 0,$$

kjer zadnja enakost sledi po malem Fermatovem izreku. □

Nauk: *Čudne pogoje se da pretvoriti v manj čudne pogoje.*

Naloga 4.5: Putnam 2015 A2

Definiramo $a_0 = 1, a_1 = 2$ ter

$$a_n = 4a_{n-1} - a_{n-2}.$$

Najdi liho praštevilo, ki deli a_{2015}.

Rešitev. Izračunajmo nekaj členov zaporedja

n	a_n	n	a_n
2	$7 = 1 \cdot 7$	6	$1351 = 7 \cdot 193$
3	$26 = 2 \cdot 13$	7	$5042 = 2 \cdot 2521$
4	$97 = 1 \cdot 97$	8	$18817 = 31 \cdot 607$
5	$362 = 2 \cdot 181$	9	$70226 = 2 \cdot 13 \cdot 37 \cdot 73$

Tabela 1: Nekaj členov zaporedja $\{a_n\}$.

Opazimo, da za izračunane elemente velja $a_2 \mid a_6$ ter $a_3 \mid a_9$, ne velja pa $a_2 \mid a_4$ ali $a_3 \mid a_6$. To motivira domnevo, da za vsako liho število ℓ velja

$$a_k \mid a_{\ell k}.$$

Kot smo vajeni iz Diskretne matematike 1 s pomočjo karakterističnega polinoma rekurzivne enačbe ter začetnih vrednosti zaporedja izračunamo eksplicitno formulo

$$a_n = \frac{1}{2}\left((2-\sqrt{3})^n + (2+\sqrt{3})^n\right).$$

Domneva o deljivosti motivira naslednji izračun

$$\frac{a_{\ell k}}{a_k} = \frac{(2-\sqrt{3})^{\ell k} + (2+\sqrt{3})^{\ell k}}{(2-\sqrt{3})^k + (2+\sqrt{3})^k} = \sum_{j=0}^{\ell-1} (-1)^j (2-\sqrt{3})^j (2+\sqrt{3})^{\ell-1-j}$$

Vemo, da algebraična cela števila $\overline{\mathbb{Z}}$ (ničle moničnih celoštevilskih polinomov) tvorijo kolobar. Ker sta $2-\sqrt{3}$ ter $2+\sqrt{3}$ ničli polinoma $X^2 - 4X + 1$ sledi

$$\frac{a_{\ell k}}{a_k} \in \overline{\mathbb{Z}}.$$

Iz rekurzivne zveze je očitno, da so elementi zaporedja cela števila. Tako velja

$$\frac{a_{\ell k}}{a_k} \in \mathbb{Q}.$$

Znana lema (izrek o racionalnih ničlah) pa nam pove, da je

$$\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

Tako sledi, da je za vsako liho naravno število ℓ

$$\frac{a_{\ell k}}{a_k} \in \mathbb{Z}.$$

Ker je $2015 = 5 \cdot 13 \cdot 31$ sledi

$$\frac{a_{2015}}{a_5} \in \mathbb{Z},$$

oziroma ekvivalentno $a_5 \mid a_{2015}$. Izračunali smo $a_5 = 2 \cdot 181$, zato sledi, da 181 deli a_{2015}. □

4.1 Posplošitev

Koeficienti v rekurzivni zvezi v našem dokazu niso igrali pomembne vloge. Ključno je bilo, da so koeficienti celi, kar zagotavlja racionalnost obravnavanega ulomka ter celost koeficientov karakterističnega polinoma, ter da je koeficient a_n enak 1, kar je zagotovilo, da sta ničli karakterističnega polinoma algebraični celi števili. Prav tako je bilo ključnega pomena, da je rekurzivna zveza stopnje 2, saj lahko le v tem primeru zagotovimo, da je eksplicitna rešitev vsota večkratnikov dveh eksponentnih funkcij. To je omogočalo deljenje izrazov za $a_{k\ell}$ ter a_k preko znane formule o vsoti enakih potenc.

Kar pa je bilo pomembno glede specifičnih vrednosti začetnih členov zaporedja ter koeficientov v rekurzivni zvezi je to, da so zagotavljali obstoj dveh različnih ničel karakterističnega polinoma ter enakost koeficientov, ko izrazimo rešitev rekurzivne enačbe kot vsoto eksponentnih rešitev. Prvo je ključno, saj bi v nasprotnem primeru dobili rešitev rekurzivne enačbe kot linearno kombinacijo eksponentne rešitve ter rešitve, ki je produkt linearne funkcije z eksponentno, kar bi onemogočalo deljenje izrazov za $a_{k\ell}$ ter a_k. Do podobne prepreke bi prišli, če absolutni vrednosti koeficientov v linearni kombinaciji eksponentnih rešitev ne bi bili enaki.

Trditev 4.6

Naj bosta a_0 ter a_1 celi števili ter naj bo zaporedje $\{a_n\}_{n\in\mathbb{N}}$ podano z rekurzivno zvezo

$$a_n = a \cdot a_{n-1} + b \cdot a_{n-2}, \text{ za } a, b \in \mathbb{Z}.$$

Naj bo $a^2 \neq -4b$ ter naj bo izpolnjen eden izmed naslednjih pogojev:

- $a_0 = 0$.
- $a_0 \in \mathbb{Z}$ ter $a_1 = \frac{a}{2} \cdot a_0 \in \mathbb{Z}$.

Če je $a_k \neq 0$, potem za vse lihe ℓ velja $a_k \mid a_{k\ell}$.

Dokaz. Naj bosta λ_1 ter λ_2 različni ničli $X^2 - aX - b$, ki obstajata, ker je $a^2 \neq -4b$. Tedaj je

$$a_n = C\lambda_1^n + D\lambda_2^n.$$

C ter D določimo iz začetnih členov zaporedja $a_0 = C + D$ ter $a_1 = C\lambda_1 + D\lambda_2$.

Najprej pokažimo, da je $|C| = |D|$. Enačbo za prva dva člena zaporedja $\{a_n\}_{n\in\mathbb{N}}$ zapišemo v matrični obliki.

$$\begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \begin{pmatrix} C \\ D \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

Determinanta 2×2 matrike na levi je neničelna, saj sta ničli karakterističnega polinoma različni. Če je izpolnjen prvi izmed pogojev v trditvi gotovo velja $C + D = 0$, kar pomeni, da je $|C| = |D|$. Če je izpolnjen drugi izmed pogojev v trditvi sledi

$$\begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} C \\ D \end{pmatrix} = \frac{a_0}{2} \cdot \begin{pmatrix} 2 \\ a \end{pmatrix}.$$

Ker je $-a$ linearni koeficient moničnega polinoma, katerega ničli sta λ_1 ter λ_2, velja $a = \lambda_1 + \lambda_2$. Sledi, da vektor

$$\begin{pmatrix} C \\ D \end{pmatrix} = \frac{a_0}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

reši zgornjo enačbo. Rešitev sistema je enolična, saj je matrika obrnljiva, zato sledi enakost C ter D. Tudi v tem primeru imata konstanti C ter D enako absolutno vrednost.

Tako je

$$a_n = |C| \left(\lambda_1^n \pm \lambda_2^n\right).$$

Za lihe ℓ velja

$$\frac{a_{k\ell}}{a_k} = \frac{|C| \left(\lambda_1^{k\ell} \pm \lambda_2^{k\ell}\right)}{|C| \left(\lambda_1^k \pm \lambda_2^k\right)} = \sum_{i=0}^{\ell-1} (\pm 1)^i \left(\lambda_1^k\right)^i \left(\lambda_2^k\right)^{\ell-1-i} \in \overline{\mathbb{Z}}.$$

Ker so elementi zaporedja cela števila je

$$\frac{a_{k\ell}}{a_k} \in \mathbb{Q}.$$

Sedaj lahko zaključimo kot v rešitvi naloge. Vemo, da so edina racionalna algebraična cela števila natanko običajna cela števila, kar pomeni, da je

$$\frac{a_{k\ell}}{a_k} \in \mathbb{Z},$$

kar smo želeli pokazati. □

Nauk: *Algebraična števila so zelo kul.*

5 Kombinatorika

Naloga 5.1: Putnam 2004, A1

Košarkaška zvezda Duka Lončić[1] spremlja število uspešnih prostih metov, ki jih je zadel med prvimi n prostimi meti igre. V začetku igre je Duka zadel manj kot 80% prostih metov, proti koncu igre pa je kumulativno zadel več kot 80 % prostih metov, ki jih je izvajal. Ali nujno obstaja trenutek v igri, v katerem je Duka zadel natanko 80 % prostih metov?

Rešitev. Morda rahlo nepričakovano je odgovor na vprašanje pritrdilen. Zelo naravna točka, na kateri bi Duka lahko dosegel natančnost 80%, je prva točka na kateri Duka preseže ali ima natančnost 80%. Če bi namreč Duka po tem trenutku zadel vse proste mete bi njegova natančnost ostala večja od 80% tekom celotne igre, kar eliminira vse ostale kandidate. Izziv je sedaj pokazati, da na omenjeni točki Duka ne strogo presega natančnosti 80%.

Definiramo $S(k)$ kot število prostih metov, ki jih je Duka zadel med prvimi k poizkusi. Naj bo i najmanjše tako naravno število, večje od 1, za katerega je $\frac{S(i)}{i} \geq 80\%$. Iz minimalnosti i sledi, da je $S(i-1) = S(i) - 1$. Tedaj je

$$\frac{S(i-1)}{i-1} < \frac{4}{5} \iff 5 \cdot S(i) - 4i < 1.$$

Prav tako velja

$$\frac{S(i)}{i} \geq \frac{4}{5} \iff 5 \cdot S(i) - 4i \geq 0,$$

iz česar sledi

$$0 \leq 5 \cdot S(i) - 4i < 1.$$

Ker je izraz $5 \cdot S(i) - 4 \cdot i$ celo število je leva neenakost pravzaprav enakost, kar implicira želeni zaključek. □

Komentar 5.2: Diskretni izrek o vmesni vrednosti

Definirali smo proces, v katerem dani ulomek (ki je manjši od 1) slikamo v eno izmed dveh različnih vrednosti

$$\frac{k}{n} \mapsto \begin{cases} \frac{k+1}{n+1} \\ \frac{k}{n+1} \end{cases}.$$

Pokazali smo, da če začnemo z ulomkom, manjšim od $\frac{4}{5}$ ter končamo z ulomkom večjim od $\frac{4}{5}$, potem smo gotovo na neki točki dosegli vrednost $\frac{4}{5}$. To spominja na izrek o vmesni vrednosti: zvezna funkcija, definirana na intervalu, ki doseže negativno ter pozitivno vrednost nujno doseže tudi ničelno vrednost.

[1] Originalna oblika naloge v angleščini na tem mestu uporabi ime Shanille O'Keal, ki je besedna igra na ime košarkaša Shaquille O'Neal. Uporaba fiktivnega imena Duka Lončić je tako na mestu.

5.1 Posplošitev

Trditev 5.3

Če ulomek $\frac{4}{5}$ v zgornji nalogi zamenjamo z poljubnim ulomkom oblike $\frac{n-1}{n}$, potem nujno obstaja trenutek v igri, v katerem je Duka zadel $\frac{n-1}{n}$ prostih metov.

Dokaz. Analogno definiramo $S(k)$ in predpostavimo, da je i najmanjše naravno število, večje od 1, za katero velja $\frac{S(i)}{i} \geq \frac{n-1}{n}$. Tedaj velja

$$\frac{S(i-1)}{i-1} = \frac{S(i)-1}{i-1} < \frac{n-1}{n} \iff n \cdot (S(i)-1) < (n-1) \cdot (i-1).$$

Velja tudi

$$\frac{S(i)}{i} \geq \frac{n-1}{n} \iff n \cdot S(i) \geq (n-1) \cdot i.$$

Enakosti preobrazimo

$$n \cdot S(i) - n < (n-1) \cdot i - n + 1 \iff n \cdot S(n) - (n-1) \cdot i < 1$$

ter

$$n \cdot S(i) - (n-1) \cdot i \geq 0.$$

Tako dobimo

$$0 \leq n \cdot S(i) - (n-1) \cdot i < 1.$$

Ker je $n \cdot S(i) - (n-1) \cdot i$ celo število sledi, da je

$$n \cdot S(i) - (n-1) \cdot i = 0 \iff \frac{S(i)}{i} = \frac{n-1}{n},$$

kar smo želeli pokazati. □

Trditev 5.4

Analogna trditev ne velja za vse $p \in (0,1)$, ki niso oblike $\frac{n-1}{n}$.

Dokaz. Denimo, da Duka zgreši prvi met, nato pa zadane vse mete do n-tega, potem pa zapusti igro (morda zaradi poškodbe gležnja). Naj bo n tako naravno število, da je $\frac{n-1}{n} > p$, kar zagotovi, da Duka preseže natančnost p. Po prvem metu ima Duka natančnost 0, po vsakem naslednjem metu pa ima natančnost $\frac{k-1}{k}$, kjer je k število metov, ki jih je do tiste točke izstrelil. Ker p ni število ni oblike $\frac{n-1}{n}$, Duka nikoli ne doseže natančnosti p. □

Nauk: *Minimalnost je kralj kombinatorike.*

Naloga 5.5: Putnam 2012 B3

$2n$ ekip je sodelovalo v turnirju, ki je trajal $2n-1$ dni. Vsak dan je potekalo n tekem, tako da je vsaka ekipa igrala v natanko eni tekmi. Vsako tekmo ena izmed sodelujočih ekip zmaga, druga ekipa pa jo izgubi. Tekom turnirja je vsaka ekipa igrala z vsako drugo ekipo.
Vsak dan turnirja stavimo na neko ekipo, a na nobeno ekipo dvakrat. Stavo dobimo, če izbrana ekipa tisti dan zmaga svojo tekmo. Ali je ne glede na strukturo turnirja (na kateri dan se pomerijo ekipe) ter izide tekem mogoče, da smo zmagali vse svoje stave?

Rešitev. Problem pretvorimo v jezik teorije grafov. Naj bo $G = (E \cup D, E \times D)$ graf, kjer je $|E| = 2n$ množica ekip ter $|D| = 2n-1$ množica dni. Naj bo (e, d) povezava v grafu G natanko tedaj, ko je ekipa e zmagala svojo tekmo na dan d. Problem se sedaj pretvori v iskanje popolnega prirejanja množici D; za vsak dan d namreč želimo najti ekipo e, ki je zmagala na ta dan, hkrati pa nobene ekipe iz E nočemo izbrati dvakrat.

Definicija 5.6

Naj bo (X, Y, P) dvodelni graf z deloma X ter Y ter množico povezav P.

- *Popolno prirejanje* množici X je množica disjunktnih povezav, ki pokrijejo X.
- Za $W \subseteq X$ definiramo *okolico* podmnožice W $N_G(W)$ kot množico vseh vozlišč v Y, ki so povezane z vsaj enim elementom W.

Izrek 5.7: Hallov poročni izrek

Naj bo $G = (X, Y, P)$ dvodelen graf. Potem v grafu G obstaja popolno prirejanje množici X natanko tedaj, ko je

$$|W| \leq |N_G(W)|$$

za vse $W \subseteq G$.

Hallov poročni izrek nam pove, da če za popolno prirejanje množici X ne obstaja nobena lokalna obstrukcija, potem popolno prirejanje gotovo obstaja. Lokalna obstrukcija je v tem primeru neenakost

$$|W| > |N_G(W)|\,,$$

veljavnost katere gotovo onemogoči obstoj popolnega prirejanja.

Denimo, da obstaja taka podmnožica $S \subseteq D$, za katero velja

$$|S| > |N_G(S)|$$

ter naj bo $t \in E \setminus N_G(S)$ ekipa, ki ni zmagala nobene tekme na dan v S. Množica $E \setminus N_G(S)$ je očitno neprazna, saj je

$$|E \setminus N_G(S)| \geq |E| - |N_G(S)| > |E| - |S| = 2n - (2n-1) = 1,$$

zato taka ekipa t resnično obstaja. Ekipa t je na vsak dan iz S igrala z drugo ekipo, obenem pa je ekipa s katero je igrala t vedno zmagala. Po definiciji množice $N_G(S)$ je tako ekipa t vsak dan iz S igrala z neko ekipo iz $N_G(S)$ ter bila poražena. Sledi, da je

$$|N_G(S)| \geq |S|\,,$$

kar je v protislovju z našo predpostavko. Sledi, da taka podmnožica $S \subseteq D$, za katero velja

$$|S| > |N_G(S)|$$

ne obstaja, kar poda želeni zaključek po Hallovem poročnem izreku. □

Nauk: *Turnirje se splača reinterpretirati preko grafov ali pa preko incidenčnih matrik. Incidenčne matrike so dobre pri štetju dvojic, trojic in podobnega. Grafi so vedno dobri, posebej ker imaš več izrekov (matrike tudi zgubijo svojo običajno moč, saj se ponavadi množenja ne da kombinatorično interpretirati). Pri tvorjenju grafov vozlišča niso vedno najbolj očitna.*
Nauk: *Naloga ti pove kako bo rešena, ne ti nalogi (v tem primeru posebej ključno pri izbiri množice vozlišč).*