Kolegij *Studentska natjecanja*, ak. god. 2022./2023.
http://web.math.pmf.unizg.hr/nastava/studnatj/

Tema br. 12:

Geometrija brojeva

Lukas Novak
lukas.novak@math.hr

1 Teorem Minkowskog o konveksnim tijelima

Definicija 1. Za konveksan podskup A od $\mathbb{R}^n$ kažemo da je **konveksno tijelo**, tj. ako za svake dvije točke x i y iz A vrijedi da je segment $\{tx + (1-t)y \mid 0 \leq t \leq 1\}$ sadržan u A.
Za podskup A od $\mathbb{R}^n$ kažemo da je **centralno simetričan** ako je on centralno simetričan s obzirom na ishodište, tj. $-x \in A$, ako je $x \in A$.
Točku $x \in \mathbb{R}^n$ kojoj su sve koordinate cijelobrojne zovemo **čvorom rešetke** (**lattice point**).

Napomena 1. Može se pokazati da omeđena konveksna tijela imaju volumen.

Teorem 1 (Minkowski)**.** *Neka je A omeđeno centralno simetrično tijelo u $\mathbb{R}^n$ volumena strogo većeg od 2^n. Tada u skupu A postoji čvor rešetke različiti od ishodišta.*

Dokaz. Podijelimo prostor $\mathbb{R}^n$ na kocke brida duljine 2 sa središta u točkama kojima su sve koordinate parni brojevi. Jasno je da svake dvije takve kocke imaju disjunktne unutrašnjosti i da pokrivaju cijeli $\mathbb{R}^n$. Budući da je A omeđen skup, on sječe samo konačno mnogo tih kocaka. Volumen od A sada možemo zapisati kao zbroj volumena presjeka skupa A s time kockama. Promotrimo translacije koje šalju te kocke u kocku sa središtem u ishodištu. Kako translacija čuva volumen, u kocki oko ishodišta ćemo nakon tih translacija dobiti skupove čiji je ukupni volumen strogo veći od 2^n. Međutim, volumen kocke brida 2 je 2^n iz čega slijedi da se neka dva skupa u toj kocki moraju sijeći u točki X. Promotrimo sada kocke od kojih dolaze ti skupovi koji se sijeku u X i točke koje se pri tim translacijama slikaju u X. Označimo ih s x i y. Budući da su to translacije za vektore kojima su sve koordinate parne imamo da je $x - y \in 2\mathbb{Z}^n$. Nadalje, kako je A centralno simetričan je $-y \in A$. Iz konveksnosti skupa A konačno imamo da je $\frac{x-y}{2} \in A$, a iz gornjeg vidimo da je to ujedno i čvor rešetke. □

Primjer 1. U prostoru $\mathbb{R}^3$ opišimo oko svakog čvora rešetke kuglu radijusa $r > 0$ (isti za sve kugle). Dokažite da svaki pravac kroz ishodiše siječe barem jednu kuglu.

Rješenje. Uzmimo proizvoljni pravac kroz ishodište. Promotrimo valjak oko tog pravca kojem je radijus baze $\frac{r}{2}$ i koji je centralno simetričan. Uzimajući dovoljno veliku visinu valjka možemo postići da mu volumen bude strogo veći od 8. Primjenom *Minkowskovog teorema* zaključujemo da u tome valjku postoji neki čvor rešetke. Kugla oko tog čvora rešetke će sječi dani pravac. □

Gornji teorem ima bitnu generalizaciju:

Teorem 2 (Minkowski)**.** *Neka je A omeđeno konveksno tijelo u $\mathbb{R}^n$ te $v_1, v_2, \ldots, v_n$ linearno nezavisni vektori u $\mathbb{R}^n$. Promotrimo fundamentalni paralelepiped $P = \{\sum_{i=1}^n x_i v_i \,|\, 0 \leq x_i \leq 1\}$ i označimo s $\mathrm{Vol}(P)$ njegov volumen. Ako A ima volumen strogo veći od $2^n \cdot \mathrm{Vol}(P)$, tada A sadrži točku rešetke $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ različitu od ishodišta.*

Teorem 2 ima lijepu primjenu pri dokazu da se svaki prosti broj oblika $4k+1$ može prikazati kao zbroj dva kvadrata.

Primjer 2 (Fermat)**.** Svaki prosti broj p oblika $4k + 1$ se može prikazati kao zbroj dva kvadrata.

Rješenje. Neka je $p = 4k + 1$ dani prosti broj. Za takav p je -1 kvadratni ostatak modulo p. Zato postoji cijeli broj a takav da $p \mid a^2 + 1$. Promotrimo vektore $v_1 = (p, 0)$ i $v_2 = (a, 1)$. Ti vektori su očito linearno nezavisni. Nadalje, za točku $(x, y) \in L = \mathbb{Z}v_1 + \mathbb{Z}v_2$ imamo da je $x = mp + na$ i $y = n$ za neke cijele brojeve m i n. Uočimo da je tada

$$x^2 + y^2 \equiv n^2(a^2 + 1) \equiv 0 \pmod{p}.$$

Laganim računom dobijemo da površina fundamentalnog paralelograma P razapetog s v_1 i v_2 iznosi p. Promotrimo sada disk D oko ishodišta radijusa $\sqrt{2p}$. Površina diska D je $2\pi p > 4p$ pa prema *Minkowskovom teoremu* znamo da u D postoji točka $(x, y) \in L$ različita od ishodišta. Za tu točku imamo da $p \mid x^2 + y^2$ te kako je u disku vrijedi i $x^2 + y^2 < 2p$. Prema tome, mora biti $p = x^2 + y^2$. □

2 Primjene kod Diofantskih jednadžbi

Dokazati da neka Diofantska jednadžba nema rješenja je klasičan zadatak. Međutim, kako pristupiti problemu u kojem nas traži da pokažemo postojanje rješenja neke Diofantske jednadžbe? Teorem Minkowskog (i općenito geometrija brojeva) daje odgovore na takva pitanja. Glavni problem koji se javlja pri korištenju Minkowskovog teorema je biranje konveksnog tijela i pogodne rešetke, što ćemo vidjeti u sljedećim primjerima.

Primjer 3. Neka su a, b i c prirodni brojevi takvi da vrijedi $ac = b^2 + b + 1$. Dokažite da jednadžba $ax^2 - (2b + 1)xy + cy^2 = 1$ ima cijelobrojna rješenja.

Rješenje. Promotrimo skup $A = \{(x, y) \in \mathbb{R}^2 \,|\, ax^2 - (2b + 1)xy + cy^2 < 2\}$. Nakon malo računa možemo uočiti da je skup $A = \left\{(x, y) \in \mathbb{R}^2 \,|\, (ax - \frac{2b+1}{2}y)^2 + \frac{3}{4}y^2 < 2a\right\}$, ondnosno nakon zamjene varijabli vidimo da je to zapravo "zarotirana" elipsa $\frac{X^2}{2} + \frac{3Y^2}{8} < 1$. Prema tome imamo da je skup A konveksan i centralno simetričan, površine $\frac{4}{\sqrt{3}}\pi > 4$. Prema *Minkowskovom teoremu* imamo da u skupu A postoji točka $(x, y) \in \mathbb{Z}^2$ različita od ishodišta. Uočimo još da je $ax^2-(2b+1)xy+cy^2 > 0$ za sve $(x, y) \neq (0, 0)$ jer je diskriminanta kvadratne forme negativna. Zato imamo da za gornju točku vrijedi $ax^2 - (2b + 1)xy + cy^2 = 1$ i time smo našli cijelobrojno rješenje jednadžbe. □

Primjer 4. Pretpostavimo da je n prirodan broj za koji jednadžba $x^2 + xy + y^2 = n$ ima racionalna rješenja. Dokažite da tada ta jednadžba ima i cijelobrojna rješenja.

Rješenje. Neka je $(\frac{a}{c}, \frac{b}{c})$ racionalno rješenje jednadžbe, pri čemu su a, b i c relativno prosti. Imamo da je tada $a^2 + ab + b^2 = c^2 n$. Nadalje, standardnim argumentima (dijeljenjem s najvećim zajedničkim djeliteljem i do na eventualnu zamjenu broja n s nekim njegovim djeliteljem) bez smanjenja općenitosti možemo pretpostaviti da je $(a, b) = 1$. Uočimo da to također povlači i $(a, n) = (b, n) = 1$. Isto kao i u Primjeru 2 sada promatramo skup $A = \{(x, y) \in \mathbb{R}^2 \mid x^2 + xy + y^2 < 2n\}$. Laganim računom se pokaže da je skup A zarotirana elipsa površine $\frac{4n}{\sqrt{3}}\pi$. Preostaje nam još pronaći odgovarajuću rešetku L dovoljno male površine u kojoj će za čvorove $(x, y) \in L$ vrijediti $n \mid x^2 + xy + y^2$. Promotrimo sljedeće :

$$\begin{aligned} ab(x^2 + xy + y^2) &= (abx^2 - b^2xy) + (aby^2 - a^2xy) + (a^2 + ab + b^2)xy \\ &= c^2nxy + (ax - by)(bx - ay). \end{aligned}$$

Kako su a i b relativno prosti s n iz gornjeg izraza slijedi da ako $n \mid (ax - by)$ onda $n \mid x^2 + xy + y^2$. To nas motivira na promatranje rešetke L koja se sastoji od čvorova $(x, y) \in \mathbb{Z}^2$ za koje $n \mid (ax - by)$. Laganim računom se može pokazati da je površina fundamentalnog paralelograma najviše n pa prema Teoremu 2 imamo da u skupu A postoji točka (x, y) različita od ishodišta koja je također u rešetki L. Dakle, vrijedi da je $0 < x^2 + xy + y^2 < 2n$ i $n \mid x^2 + xy + y^2$ iz čega zaključujemo da je $x^2 + xy + y^2 = n$. □

Za računanje volumena nekih tijela određenog oblika će nam biti koristan sljedeći rezultat:

Propozicija 3. *Neka je $A \in M_n(\mathbb{R})$ simetrična i pozitivno definitna matrica. Neka je $S = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \sum_{1 \le i,j \le 1} a_{ij} x_i x_j \le 1\}$. Tada je*

$$\mathrm{Vol}(S) = \frac{\mathrm{Vol}(B^n)}{\sqrt{\det A}} \text{ pri čemu je } \mathrm{Vol}(B^n) = \frac{\pi^{\frac{n}{2}}}{\Gamma(1 + \frac{n}{2})} \text{ volumen jedinične kugle,}$$

$$\Gamma\left(1 + \frac{n}{2}\right) = (n/2)! \text{ za } n \text{ paran i } \Gamma\left(1 + \frac{n}{2}\right) = \frac{n!\sqrt{\pi}}{2^{\frac{3n+1}{2}}(\frac{n-1}{2})!} \text{za } n \text{ neparan.}$$

Primjer 5 (Lagrange)**.** Svaki prirodan broj možemo zapisati kao sumu četiri kvadrata.

Rješenje. Dokažimo prvo da je svaki prost broj suma četiri kvadrata. Neka je p prost broj. Za $p = 2$ tvrdnja očito vrijedi. Pretpostavimo da je $p > 2$. Neka je $K = \{(t, u, v, w) \in \mathbb{R}^4 \mid t^2 + u^2 + v^2 + w^2 < 2p\}$ kugla u $\mathbb{R}^4$ oko ishodišta radijusa $\sqrt{2p}$. Primjenom gornje formule imamo da je $\mathrm{Vol}(K) = 2p^2\pi^2$. Promotrimo skupove $A = \{a^2 \mid a \in \mathbb{Z}/p\mathbb{Z}\}$ i $B = \{-b^2 - 1 \mid b \in \mathbb{Z}/p\mathbb{Z}\}$. Broj kvadratnih ostataka modulo p je $\frac{p+1}{2}$ pa je zato $|A| = |B| = \frac{p+1}{2}$. Uočimo da je $|A| + |B| = p + 1 > |\mathbb{Z}/p\mathbb{Z}|$ iz čega slijedi da postoje cijeli brojevi $x \in A$ i $y \in B$ takvi da je $x^2 \equiv -y^2 - 1 \pmod{p}$, tj. $p \mid x^2 + y^2 + 1$. Brojevi x i y će nam pomoći pri konstrukciji željene rešetke. Promotrimo rešetku L razapetu s vektorima $v_1 = (p, 0, 0, 0)$, $v_2 = (0, p, 0, 0)$, $v_3 = (x_1, y_1, 1, 0)$ i $v_4 = (x_2, y_2, 0, 1)$ gdje su x_1, y_1, x_2 i y_2 cijeli brojevi.

Želimo odabrati te brojeve tako da za sve čvorove rešetke $(t,\, u,\, v,\, w)$ vrijedi $p \mid t^2+u^2+v^2+w^2$. Za $(t,\, u,\, v,\, w) \in L$ je $t = ap + cx_1 + dx_2$, $u = bp + cy_1 + dy_2$, $v = c$ i $w = d$ za neke cijele brojeve a, b, c i d.

$$t^2 + u^2 + v^2 + w^2 \equiv c^2(x_1^2 + y_1^2 + 1) + d^2(x_2^2 + y_2^2 + 1) + 2cd(x_1x_2 + y_1y_2) \pmod{p}.$$

Stavljanjem $x_1 = x$, $y_1 = y$, $x_2 = y$ i $y_2 = -x$ iz gornjeg dobivamo da će tada $p \mid t^2+u^2+v^2+w^2$. Nadalje, volumen fundamentalnog paralelepipeda P rešetke L je $\mathrm{Vol}(P) = p^2$. Time je $\mathrm{Vol}(K) > 2^4 \cdot \mathrm{Vol}(P)$ iz čega slijedi da postoji $(t,\, u,\, v,\, w) \in L \cap K$. Tada je $p = t^2+u^2+v^2+w^2$. Preostaje nam još pokazati da je produkt dvije sume četiri kvadrata ponovo suma četiri kvadrata (vidi Zadatak 2 za DZ) iz čega nam konačno slijedi tvrdnja. □

3 Primjene u aproksimacijama realnih brojeva

Primjer 6 (Teorem Minkowskog o linearnim formama)**.** Neka je $A = (a_{ij})_{i,j} \in GL_n(\mathbb{R})$. Neka su $c_1,\, c_2,\, \ldots,\, c_n$ pozitivni realni brojevi takvi da je $c_1c_2 \cdots c_n > |\det A|$. Tada postoje cijeli brojevi $x_1,\, x_2,\, \ldots,\, x_n$ koji nisu svi jednaki 0 za koje vrijedi $|\sum_{j=1}^{n} a_{ij}x_j| < c_i$ za sve $i = 1,\, 2, \ldots, n$.

Rješenje. Promotrimo skup $S = \{y \in \mathbb{R}^n : |(Ay)_i| < c_i,\, i = 1,\, \ldots,\, n\}$. Uočimo da je skup S slika skupa $\{z \in \mathbb{R}^n : |z_i| < c_i,\, i = 1,\, \ldots,\, n\}$ pri preslikavanju A^{-1}. Prema tome, imamo da je skup S centralno simetričan i konveksan, volumena $\frac{1}{|\det A|}(2c_1) \cdots (2c_n) > 2^n$. Primjenom *Minkovskovog teorema* slijedi da postoji nenul vektor $x \in \mathbb{Z}^n$ koji je također i u skupu S. Komponente tog vektora x su traženi cijeli brojevi. □

Primjer 7. Neka je $A = (a_{ij})_{i,j} \in GL_n(\mathbb{R})$ $(n \geq 2)$. Dokažite da postoje cijeli brojevi $x_1,\, x_2,\, \ldots,\, x_n$ koji nisu svi jednaki 0 za koje vrijedi

$$\sum_{i=1}^{n} |a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n| \leq \sqrt[n]{n! \cdot |\det A|}.$$

Rješenje. Za realan broj $M > 0$ i prirodni broj n definiramo skup

$$O(M, n) := \{(x_1,\, \ldots,\, x_n) \in \mathbb{R}^n \,|\, |x_1| + \ldots + |x_n| \leq M\}.$$

Volumen tog skupa je

$$\begin{aligned}
\mathrm{Vol}(O(M,n)) &= \int_{|x_1|+\ldots+|x_n| \leq M} dx_1\, dx_2 \ldots\, dx_n = \\
&= \int_{-M}^{M} \left(\int_{|x_1|+\ldots+|x_{n-1}| \leq M-|x_n|} dx_1\, dx_2 \ldots\, dx_{n-1} \right) dx_n = \\
&= \int_{-M}^{M} \mathrm{Vol}(O(1, n-1)) \cdot (M - |x_n|)^{n-1}\, dx_n = \frac{2M^n}{n} \cdot \mathrm{Vol}(O(1, n-1)).
\end{aligned}$$

Indukcijom se dobije da je $\mathrm{Vol}(O(M,n)) = \frac{(2M)^n}{n!}$. Promotrimo skup

$$S = \{x \in \mathbb{R}^n \mid \sum_{i=1}^{n} |(Ax)_i| \leq \sqrt[n]{n!|\det A|}\} = A^{-1}\left(O(\sqrt[n]{n!|\det A|}, n)\right).$$

Iz gornjeg imamo da je $\mathrm{Vol}(S) = 2^n$ pa ne možemo primijeniti direktno *teorem Minkowskog*. Promotrimo stoga malo veće skupove. Za prirodan broj k imamo da je volumen skupa $S_k = A^{-1}\left(O(\sqrt[n]{n!|\det A|} + \frac{1}{k}, n)\right)$ veći od 2^n iz čega zaključujemo da postoji nenul vektor $v_k \in \mathbb{Z}^n$ takav da je $Av_k \in O(\sqrt[n]{n!|\det A|} + \frac{1}{k}, n)$. Iz gornjeg se lako vidi da je svaka komponenta vektora Av_k ograničena pa primjenom preslikavanja A^{-1} dobijemo da je i svaka komponenta vektotora v_k ograničena. Nadalje, sve komponente od v_k su cijeli brojevi i kako su one ograničene slijedi da takvih vektora v_k ima samo konačno mnogo. To nam sada omogućuje da konstruiramo niz vektora v_k koji ne ovise o k takvi da je $Av_k \in O(\sqrt[n]{n!|\det A|} + \frac{1}{k}, n)$ za sve prirodne brojeve k. Puštanjem $k \to \infty$ time dobivamo nenul vektor x s cijelobrojnim koordinatama takav da je $Ax \in O(\sqrt[n]{n!|\det A|}, n)$. □

Primjer 8 (IMO 1997., P6)**.** Za prirodan broj n, označimo s $f(n)$ broj načina na koji broj n možemo prikazati kao zbroj (ne nužno različitih) potencija od 2. Prikazi koji se razlikuju samo u poretku sumanada smatramo istim. Na primjer $f(4) = 4$ jer 4 možemo prikazati kao 2^2, $2+2$, $1+1+2$ i $1+1+1+1$. Dokažite da postoje konstante a, b takve da

$$2^{\frac{n^2}{2} - n\log_2(n) - an} < f(2^n) < 2^{\frac{n^2}{2} - n\log_2(n) - bn}$$

vrijedi za sve dovoljno velike n.

Rješenje. Uočimo da je $f(2^n)$ broj rješenja $(a_0, \ldots, a_n) \in \mathbb{N}_0^{n+1}$ jednadžbe $a_0 + a_1 \cdot 2 + \ldots + a_n \cdot 2^n = 2^n$. Nadalje, a_0 je jedinstveno određen s $a_1, \ldots, a_n$ pa je $f(2^n)$ upravo broj rješenja $(a_1, \ldots, a_n) \in \mathbb{N}_0^n$ nejednadžbe $a_1 \cdot 2 + \ldots + a_n \cdot 2^n \leq 2^n$. Jedno rješenje je očito $(0, 0, \ldots, 1)$, a za sva ostala rješenja je $a_n = 0$. Za rješenje oblika $(a_{n-1}, \ldots, a_{n-1}, 0)$ promotrimo kocku $H(a_1, \ldots, a_{n-1}) = [a_1, a_1 + 1\rangle \times \ldots \times [a_{n-1}, a_{n-1} + 1\rangle$. Za različita rješenja su te kocke disjunktne. Volumen svake takve kocke je 1 pa je zato broj takvih rješenja ukupan volumen tih kocaka. Ideja je sada pronaći dovoljno dobar manji i veći skup od skupa danih kocaka kojima možemo odrediti volumen, na taj način ćemo onda dobiti gornju i donju ogradu za $f(2^n)$. Uočimo da je svaka kocka sadržana u skupu $\{(x_1, \ldots, x_{n-1}) \in \mathbb{R}_{\geq 0}^{n-1} \mid \sum_{i=1}^{n-1} 2^i(x_i - 1) < 2^n\}$. Nadalje, unija svih kocaka prekriva skup $\{(x_1, \ldots, x_{n-1}) \in \mathbb{R}_{\geq 0}^{n-1} \mid \sum_{i=1}^{n-1} 2^i x_i \leq 2^n\}$ jer je točka $(x_1, \ldots, x_{n-1})$ tog skupa sadržana u kocki $H(\lfloor x_1 \rfloor, \ldots, \lfloor x_{n-1} \rfloor)$. Izračunajmo općenito volumen skupova tog oblika. Označimo s $R(a_1, \ldots, a_n; A) = \{(x_1, \ldots, x_n) \in \mathbb{R}_{\geq 0}^n \mid \sum_{i=1}^n a_i x_i \leq A\}$.

Volumen tog skupa je

$$\mathrm{Vol}\,(R(a_1,\,\ldots\,,\,a_n;\,A)) = \int_{\substack{a_1x_1+\ldots+a_nx_n\le A\\ x_i\ge 0}} dx_1\ldots\,dx_n =$$

$$= \int_0^{\frac{A}{a_n}} \left(\int_{\substack{a_1x_1+\ldots+a_{n-1}x_{n-1}\le A-a_nx_n\\ x_i\ge 0}} dx_1\ldots\,dx_{n-1} \right) dx_n = \int_0^{\frac{A}{a_n}} \mathrm{Vol}\,(R(a_1,\,\ldots\,,\,a_{n-1};\,A-a_nx_n))\,dx_n =$$

$$= \mathrm{Vol}\,(R(a_1,\,\ldots\,,\,a_{n-1};\,1)) \int_0^{\frac{A}{a_n}} (A-a_nx_n)^{n-1}\,dx_n = \frac{A^n}{na_n}\,\mathrm{Vol}\,(R(a_1,\,\ldots\,,\,a_{n-1};\,1))$$

Indukcijom dobijemo da je $\mathrm{Vol}\,(R(a_1,\,\ldots\,,\,a_n;\,A)) = \frac{A^n}{n!a_1\cdots a_n}$. Iz gornjeg sada konačno imamo da je $1+\mathrm{Vol}\,(R(2,\,\ldots\,,\,2^{n-1};\,2^n)) \le f(2^n) \le \mathrm{Vol}\,(R(2,\,\ldots\,,\,2^{n-1};\,2+2^2+\ldots+2^n))$, odnosno

$$1+\frac{2^{\frac{n^2-n}{2}}}{(n-1)!} \le f(2^n) \le 1+\frac{(2^{n+1}-2)^{n-1}}{2^{\frac{n^2-n}{2}}(n-1)!}.$$

Korištenjem *Stirlingove formule* za $(n-1)!$ i sređivanjem gornjeg izraza dobijemo da postoje tražene konstante a i b. □

4 Prikazi rješenja nekih Diofantskih jednadžbi

Glavni rezultat u ovome poglavlju je sljedeći teorem:

Teorem 4. *Neka je $A \in SL_n(\mathbb{Z})$ simetrična pozitivno definitna matrica i $n \le 4$. Tada postoji matrica $B \in M_n(\mathbb{Z})$ takva da je $A = B^\top B$.*

Napomena 2. Tvrdnja zapravo vrijedi za sve $n \le 7$ dok za $n = 8$ postoji protuprimjer.

Prije nego što krenemo s dokazom teorema uvesti ćemo par pojmova i dvije tehničke leme. **Baza za** $\mathbb{Z}^n$ je familija vektora $(v_1, v_2, \ldots, v_p)$ od $\mathbb{Z}^n$ takva da za svaki vektor $x \in \mathbb{Z}^n$ postoji jedinstveni prikaz $x = k_1v_1+\ldots+k_pv_p$, pri čemu su k_1, k_2, …, k_p cijeli brojevi. Jedan primjer baze za $\mathbb{Z}^n$ je standardna kanonska baza $(e_1, e_2, \ldots, e_n)$. Slično kao i za vektorske prostore, može se pokazati da sve baze od $\mathbb{Z}^n$ imaju n vektora.

Za matricu $A = (a_{ij})_{i,j} \in M_n(\mathbb{Z})$ neka je $g_A(x,y) = x^\top Ay = \sum_{1\le i,j\le n} a_{ij}x_iy_j$ njena pridružena bilinearna forma, pri čemu su $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$ zapisi vektora x i y u kanonskoj bazi. Neka je $f_A(x) = g_A(x,x)$ kvadratna forma asocirana s $g_A(x,x)$.

Promotrimo neku drugu bazu $(v_1, v_2, \ldots, v_n)$ za $\mathbb{Z}^n$. Neka je $v_i = \sum_{j=1}^n v_{ji}e_j$ zapis vektora v_i u kanonskoj bazi za svaki $1 \le i \le n$. Promotrimo matricu prijelaza $V = (v_{ij})_{i,j}$. Slično kao i za matrice prijelaza između dviju baza vektorskog prostora vrijedi da je matrica V invertibilna u $M_n(\mathbb{Z})$. Nadalje, ako je $x' = (x'_1, \ldots, x'_n)$ zapis vektora x u bazi $(v_1, v_2, \ldots, v_n)$ tada vrijedi $x = Vx'$. Uvrštavanjem te relacije u definiciju bilinearne forme matrice A dobijemo

$g_A(x,y) = x'^{\top}\left(V^{\top}AV\right)y'$. S druge strane, stavimo da je $g_A(x,y) = x'^{\top}Gy'$ za neku matricu $G = (g_{ij})_{i,j} \in M_n(\mathbb{Z})$. Uvrštavanjem $x = v_i$ i $y = v_j$ dobijemo da su $x' = e_i$ i $y' = e_j$ te $g_{ij} = g_A(v_i, v_j)$. Dakle, $G = V^{\top}AV = (g_A(v_i,v_j))_{i,j}$.

Lema 5. *Neka je $A \in SL_n(\mathbb{Z})$ i $n \leq 4$. Tada postoji vektor $v_1 \in \mathbb{Z}^n$ takav da je $f_A(v_1) = 1$.*

Lema 5 direktno slijedi primjenom *Minkowskovog teorema* i ostavljena je za zadaću.

Lema 6. *Neka je $A \in SL_n(\mathbb{Z})$, $n \leq 4$ i v_1 vektor iz Leme 5. Tada postoje vektori $v_2, \ldots, v_n \in \mathbb{Z}^n$ takvi da je $(v_1, v_2, \ldots, v_n)$ baza za $\mathbb{Z}^n$ i $g_A(v_1, v_i) = 0$ za sve $i \geq 2$.*

Dokaz. Promotrimo skup $H = \{x \in \mathbb{Z}^n \mid g_A(v_1, x) = 0\}$. H je podmodul slobodnom modula $\mathbb{Z}^n$ pa je oblika $\mathbb{Z}v_2 + \mathbb{Z}v_3 + \ldots + \mathbb{Z}v_r$ za neke linearno nezavisne vektore $v_2, v_3, \ldots, v_r \in \mathbb{Z}^n$. Pokažimo da je $(v_1, v_2, \ldots, v_r)$ baza za $\mathbb{Z}^n$. Uzmimo $x \in \mathbb{Z}^n$ i promotrimo jednadžbu $x = k_1v_1 + v$ gdje je k_1 cijeli broj, a $v \in H$. Tada je $g_A(v_1, x - k_1v_1) = g_A(v_1, v) = 0$. Korištenjem linearnosti od g_A i $f_A(v_1) = 1$ slijedi da je $k_1 = g_A(v_1, x)$. Dakle, koeficijent k_1 postoji i jedinstveno je određen s x. Nadalje, kako je $(v_2, v_3, \ldots, v_r)$ baza za H imamo da postoje jedinstveni cijeli brojevi $k_2, k_3, \ldots, k_r$ takvi da je $v = k_2v_2 + \ldots + k_rv_r$. Konačno imamo da je $x = k_1v_1 + k_2v_2 + \ldots + k_rv_r$. Prema tome, $(v_1, v_2, \ldots, v_r)$ je tražena baza za $\mathbb{Z}^n$ i posebno je $r = n$. □

Dokaz Teorema 4. Dokaz provodimo indukcijom po n. Za $n = 1$ tvrdnja očito vrijedi. Pretpostavimo da tvrdnja vrijedi za $n-1$ i dokažimo da vrijedi za n. Prema Lemi 6 znamo da postoji baza $(v_1, v_2, \ldots, v_n)$ za $\mathbb{Z}^n$ takva da je $g_A(v_1, v_1) = 1$ i $g_A(v_1, v_i) = 0$ za sve $i \geq 2$. Neka je V matrica prijelaza iz kanonske baze u bazu $(v_1, v_2, \ldots, v_n)$. Iz obzervacija prije dokaza smo zaključili da je tada $G = V^{\top}AV$ gdje je $G = (g_A(v_i,v_j)) = \begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix}$. Matrica V je invertibilna u $M_n(\mathbb{Z})$ pa slijedi da postoji matrica $S = V^{-1} \in M_n(\mathbb{Z})$ takva da je $A = S^{\top}\begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix}S$. Računanjem determinanti gornjeg izraza lagano dobijemo da je $A' \in SL_{n-1}(\mathbb{Z})$. Iz pretpostavke indukcije je $A' = B'^{\top}B'$ za neku matricu $B' \in M_n(\mathbb{Z})$. Uvrštavanjem u izraza za matricu A konačno dobijemo da je $A = B^{\top}B$ gdje je $B = \begin{pmatrix} 1 & 0 \\ 0 & B' \end{pmatrix}S$. □

Primjer 9. Neka su x, y i z prirodni brojevi takvi da je $xy = z^2 + 1$. Dokažite da postoje cijeli brojevi a, b, c i d takvi da je $x = a^2 + b^2$, $y = c^2 + d^2$ i $z = ac + bd$.

Rješenje. Promotrimo matricu $A = \begin{pmatrix} x & z \\ z & y \end{pmatrix}$. Matrica A je očito simetrična i sadržana u $SL_2(\mathbb{Z})$ jer je $xy - z^2 = 1$. Nadalje, $\mathrm{tr}(A) = x + y > 0$, iz čega slijedi da A ima pozitivne svojstvene vrijednosti (determinanta joj je 1 pa ima ili dvije negativne ili dvije pozitivne svojstvene vrijednosti). Prema prijašnjem primjeru znamo da postoji matrica $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ s cijeobrojnim elementima takva da je $A = B^{\top}B$. Izjednačavanjem odgovarajućih elemenata matrica na lijevoj i desnoj strani dobijemo da je $x = a^2 + b^2$, $y = c^2 + d^2$ i $z = ac + bd$. □

Primjer 10 (Davenport-Casseles)**.** Dokažite da svaki cijeli broj koji se može prikazati kao suma tri kvadrata racionalnih brojeva se može zapisati i kao suma kvadrata tri cijela broja.

Rješenje. Pretpostavimo suprotno, tj. da ne postoje cijeli brojevi a, b i c takvi da je $n = a^2 + b^2 + c^2$. Koristit ćemo geometrijske argumente zajedno s metodom spusta da dođemo do kontradikcije. Neka je S sfera oko ishodišta radijusa $\sqrt{n}$ u $\mathbb{R}^3$. Iz uvjeta zadatka imamo da postoji točka $x \in S$ kojoj su sve koordinate racionalne. Svođenjem koordinata na najmanji zajednički nazivnik dobivamo da postoji vektor $v \in \mathbb{Z}^3$ takav da je $x = \frac{v}{d}$ za neki prirodan broj d. Izaberimo takav par (x, v) za koji je nazivnik d iz zapisa $x = \frac{v}{d}$ najmanji mogući. Neka je $x = (x_1, x_2, x_3)$. Uzmimo cijele brojeve y_1, y_2 i y_3 takve da je $|x_1 - y_1| \leq \frac{1}{2}$, $|x_2 - y_2| \leq \frac{1}{2}$ i $|x_3 - y_3| \leq \frac{1}{2}$ i promotrimo vektor $y = (y_1, y_2, y_3)$. Uočimo da iz gornjih uvjeta imamo da je $\|x - y\| \leq \frac{\sqrt{3}}{2} < 1$. Nadalje, iz početne pretpostavke znamo da x ima barem jednu koordinatu koja nije cijeli broj što znači da je sigurno $x \neq y$. Neka je presjek pravca xy i sfere S točka z. Kako je z na pravcu određenom s x i y imamo da postoji realan broj λ takav da je $z = y + \lambda(x - y)$. Također z se nalazi na sferi pa je $\|z\|^2 = n$. Uvrštavanjem izraza za z i raspisivanjem norme dobijemo kvadratnu jednadžbu u λ

$$\|x - y\|^2\lambda^2 + 2\langle x - y, y\rangle \lambda + \|y\|^2 - n = 0.$$

Znamo da je jedno rješenje gornje jednadžbe 1 i ono odgovara točki x. Iz Viètеovih formula dobijemo da je drugo rješenje $\lambda = \frac{\|y\|^2 - n}{\|x-y\|^2}$, odnosno $z = y + \frac{\|y\|^2 - n}{\|x-y\|^2}(x - y)$. Uvrštavanjem $x = \frac{v}{d}$ imamo da je $\|x - y\|^2 = n + \|y\|^2 - \frac{2}{d}\langle v, y\rangle = \frac{l}{d}$ za neki nenegativan cijeli broj l. Kako je $0 < \|x - y\| < 1$ slijedi da je l prirodan broj i vrijedi $l < d$. Prema tome, imamo da je $z = \frac{w}{l}$ za neki vektor $w \in \mathbb{Z}^3$. Ovime smo konstruirali novi par (z, w) u kojem je nazivnik $l < d$ što je u kontradikciji s odabirom para (x, v). Dakle, početna pretpostavka je bila pogrešna, odnosno postoje cijeli brojevi a, b i c takvi da je $n = a^2 + b^2 + c^2$. □

5 Zadaci za domaću zadaću

Za uspješno polaganje zadaće potrebno je riješiti barem 5 od sljedećih 9 zadataka. Rok predaje je 14. 7. 2023.

Zadatak 1. Dokažite teorem 2 koristeći prvu verziju *Minkowskovog teorema* (1).

Uputa: Koristite odgovarajuću "zamjenu" baza za $\mathbb{R}^n$.

Zadatak 2. Dokažite Lemu 5.

Zadatak 3. Koristeći kvaternione pokažite da je produkt dvije sume četiri kvadrata cijelih brojeva ponovo suma četiri kvadrata cijelih brojeva.

Zadatak 4. Neka su a, b i c prirodni brojevi za koje vrijedi $ac = b^2+1$. Dokažite da jednadžba $ax^2 + 2bxy + cy^2 = 1$ ima cijelobrojna rješenja.

Zadatak 5. Neka su a i b racionalni brojevi takvi da jednadžba $ax^2 + by^2 = 1$ ima barem jedno racionalno rješenje. Dokažite da jednadžba ima beskonačno mnogo racionalnih rješenja.

Zadatak 6. Zadani su realni brojevi α_1, α_2, $\ldots$, α_n i $N > 0$. Dokažite da postoje cijeli brojevi p_1, p_2, $\ldots$, p_n i q takvi da je $1 \leq q \leq N$ i $|\alpha_i - \frac{p_1}{q}| < \frac{1}{qN^{\frac{1}{n}}}$ za sve $i = 1, \ldots, n$.

Uputa: Koristite rezultat iz Primjera 6.

Zadatak 7. Odredite sve cijele brojeve a, b, c, x, y i z tako da vrijedi $ax^2 + by^2 + cz^2 = abc + 2xyz - 1$, $ab + bc + ca \geq x^2 + y^2 + z^2$ i $a, b, c > 0$.

Zadatak 8. Dokažite da za $A = (a_{ij}) \in GL_n(\mathbb{R})$ $(n \geq 2)$ postoje cijeli brojevi x_1, x_2, $\ldots$, x_n, ne svi jednaki nula, takvi da vrijedi

$$\prod_{i=1}^{n} \left| \sum_{j=1}^{n} a_{ij} x_j \right| \leq \frac{n!}{n^n} \cdot |\det A|.$$

Zadatak 9. Za prirodan broj n označimo s $f(n)$ broj načina za dobiti $n!$ centa koristeći neuređenu kolekciju kovanica od po $k!$ centa $(1 \leq k \leq n)$. Dokažite da postoji konstanta C, koja ne ovisi o n, takva da je za sve prirodne brojeve n vrijedi

$$n^{\frac{n^2}{2} - Cn} e^{-\frac{n^2}{4}} \leq f(n) \leq n^{\frac{n^2}{2} + Cn} e^{-\frac{n^2}{4}}.$$