

# Rotacije opisane s kvaternioni

## Seminar

Timotej Mlakar  
Fakulteta za matematiko in fiziko  
Oddelek za matematiko

21. marec 2023

## 1 Uvod

Rotacije  $\mathbb{R}^3$  navadno opisujemo z linearnimi preslikavami oziroma njim pripadajočimi matrikami. Zaradi narave matričnega množenja so lahko take operacije precej računsko časovno in prostorsko zahtevne. Tako lahko rotacije  $\mathbb{R}^3$  predstavimo kot stranske učinke transformacij  $\mathbb{E}^4 \simeq \mathbb{H}$ .

Najprej se spomnimo rotacij na  $\mathbb{R}^2 \simeq \mathbb{C}$ . Naj bo  $w = \frac{v}{|v|}$  za poljuben  $v \in \mathbb{C}$ . Preslikava  $\varphi : \mathbb{C} \rightarrow \mathbb{C} : \varphi(z) = wz$  je bijektivna preslikava, ki zavrti celotno kompleksno ravnino za kot  $\arg(z)$  okoli izhodišča.

Če  $v$  zapišemo v polarnem zapisu kot  $|z|e^{i\theta}$ , je tedaj preslikava

$$\begin{aligned}\varphi : [0, 2\pi] \times \mathbb{C} &\rightarrow \mathbb{C} : \\ \varphi(\theta, z) &= ze^{i\theta}\end{aligned}$$

zvezno odvedljiva na  $[0, 2\pi] \times \mathbb{C}$ . Za fiksen  $z \in \mathbb{C}$  preslikava  $\varphi$  opiše krožnico z radijem  $|z|$ , za fiksen  $\theta$  pa preslikava opiše rotacijo ravnine za kot  $\theta$ .

Vemo torej, da se vsak  $z \in \mathbb{C}$  da zapisati v polarnih koordinatah. Spomnemo se zapisa

$$z = |z|e^{i\theta} = |z|\cos\theta + |z|i\sin\theta,$$

kjer je  $\theta \in \mathbb{R}$ . Zapis ni enoličen, saj nam vsaka  $\theta' = \theta + 2k\pi$ ;  $k \in \mathbb{Z}$  opiše isto kompleksno število. Tak zapis bomo v podobnem smislu uporabili kasneje.

Definiramo  $\Phi : \mathbb{R}^2 \rightarrow \mathbb{C} : (x, y) \mapsto x + iy$ . S preprostim računom pokažemo, da je  $\Phi$  izomorfizem.

Vidimo, da namesto množenja vektorja z matriko lahko rotacijo realne ravnine predstavimo s preprostim množenjem dveh kompleksnih števil. To motivira podobni razmislek za rotacije v  $\mathbb{R}^3$ .

## 2 Kvaternionska algebra

### 2.1 Definicije in oznake

**Definicija 1** Naj bo  $V$  4-razsežen vektorski prostor nad  $\mathbb{R}$ . Izberemo bazo  $\{\mathbf{1}, i, j, k\}$ . Elementi  $V$  so oblike  $\mathbf{q} = q_0\mathbf{1} + q_1i + q_2j + q_3k = q_0 + \vec{q}$ . Vektorski prostor  $V$  opremimo z operacijo množenja tako, da definiramo množenje njegovih baznih elementov, in sicer

$$\begin{aligned}\mathbf{1}\mathbf{1} &= \mathbf{1}, & \mathbf{1}i &= i, & \mathbf{1}j &= j, & \mathbf{1}k &= k, \\ ij &= k, & jk &= i, & ki &= j, \\ i^2 &= j^2 = k^2 = ijk = -\mathbf{1}.\end{aligned}$$

Naj bosta  $p, q \in \mathbb{H}$ . Definiramo seštevanje in množenje s skalarjem kot običajno

$$\begin{aligned}p + q &= (p_0 + q_0) + (\vec{p} + \vec{q}), \\ \lambda q &= \lambda(q_0 + \vec{q}) = \lambda q_0 + (\lambda \vec{q}).\end{aligned}$$

Prav tako definiramo običajno množenje v skladu z definicijo množenja baznih elementov. Tedaj lahko produkt  $pq$  napišemo kot

$$pq = (p_0 + q_0 - \vec{p}\vec{q}) + (p_0\vec{q} + q_0\vec{p} + \vec{p} \times \vec{q}),$$

kjer je  $\vec{p}\vec{q}$  običajni skalarni produkt v  $\mathbb{R}^3$ . Tedaj  $V$  postane 4-razsežna algebra nad  $\mathbb{R}$ . Označimo  $\mathbb{H}$  in jo imenujemo Kvaternionska algebra.

**Opomba 1** Za  $p, q \in \mathbb{H}, \lambda \in \mathbb{R}$  velja

$$(\lambda p)q = p(\lambda q) = \lambda(pq).$$

**Definicija 2** Naj bo  $q = q_0 + \vec{q} \in \mathbb{H}$ . S  $\bar{q} = q_0 - \vec{q}$  označimo konjugirani kvaternion  $q$ .

Velja, da je  $q\bar{q} \in \mathbb{R}$ . Tako lahko definiramo še

$$q^{-1} = \frac{1}{q\bar{q}}\bar{q}.$$

Prav tako lahko vidimo da je  $\overline{p \cdot q} = \bar{q} \cdot \bar{p}$ . Ker množenje kvaternionov ni komutativno, v splošnem  $\overline{pq} \neq \bar{q}\bar{p}$ . Ker je  $\mathbb{H}$  algebra, je na njej smiselno definirati skalarni produkt.

**Definicija 3** Naj bosta  $p, q \in \mathbb{H}$ . Definiramo skalarni produkt kvaternionov

$$\langle p, q \rangle = \frac{1}{2}(\bar{p}q + \bar{q}p).$$

Norma porojena s skalarnim produktom je tedaj

$$|q| = ||q|| = \sqrt{\langle q, q \rangle}.$$

**Opomba 2** Iz definicije skalarnega produkta takoj sledi  $\langle q, q \rangle = q\bar{q} = \bar{q}q$ . Podobno kot absolutna vrednost na  $\mathbb{R}$  in  $\mathbb{C}$  je norma na kvaternionih multiplikativna.

Za poljubna  $p, q \in \mathbb{H}$  torej velja  $|pq| = |p||q|$ . Oglejmo si  $|pq|^2$

$$|pq|^2 = \langle pq, pq \rangle = pq\bar{p}\bar{q}.$$

Spomnimo se, da  $\overline{p \cdot q} = \bar{q} \cdot \bar{p}$ . Torej je

$$pq\bar{p}\bar{q} = p \cdot q \cdot \bar{q} \cdot \bar{p} = p|q|^2\bar{p}.$$

Ker je  $|q|^2$  skalar, pri množenju komutira s kvaternioni. Torej

$$p|q|^2\bar{p} = |q|^2p\bar{p} = |q|^2|p|^2 = |p|^2|q|^2.$$

Sledi torej  $|pq| = |p||q|$ .

Podobno kot pri rotaciji kompleksne ravnine, kjer množimo s števili iz enotske krožnice, tukaj potrebujemo enotske kvaternione.

**Definicija 4** Naj bo  $q \in \mathbb{H}$ . Kvaternion  $q$  imenujemo versor oziroma enotski kvaternion, če velja  $|q| = 1$ . Če je  $q \in \mathbb{H}$  poljuben  $|q| \neq 1$  versor kvaterniona  $q$  dobimo z normiranjem. Označimo ga z  $U_q = \frac{q}{|q|}$ . Množico versorjev označimo s  $\mathbf{Q}_e$

Če velja  $u \in \mathbb{H}, u = \vec{u}$  in  $|u| = 1$ , kvaternion  $u$  imenujemo čisti oziroma pravi versor. Množico pravih versorjev označimo z  $\mathbf{U}_e$ .

Kvaternione oblike  $q = q_0\mathbf{1}, q_0 \in \mathbb{R}$  imenujemo skalarni kvaternioni.

**Opomba 3** Za čista versorja  $u, v \in \mathbf{U}_e$  velja da  $\langle u, v \rangle = 0 \iff uv + vu = 0$ .

Naj bosta  $u, v \in \mathbf{U}_e$ . Za poljuben versor iz  $\mathbf{U}_e$  velja  $\bar{u} = -u$ . Pogledamo  $\langle u, v \rangle$ :

$$\langle u, v \rangle = \frac{1}{2}(\bar{u}v + \bar{v}u) = \frac{1}{2}(-uv - vu) = -\frac{1}{2}(uv + vu).$$

Od tu sledi da  $\langle u, v \rangle = 0 \iff uv + vu = 0$ .

Pomembna opazka tu je še naslednja: naj bo  $u \in \mathbf{U}_e$ . Ker  $|u| = 1$  sledi, da je  $u$  neničeln kvaternion. Ker je  $\mathbf{U}_e \subset \mathbb{H}$  in je  $\mathbb{H}$  algebra, je vsak neničeln kvaternion obrnljiv. Vemo torej, da obstaja tak  $u^{-1}$  da je

$$uu^{-1} = 1.$$

Ker je za poljuben  $q \in \mathbb{H}$ ,  $q^{-1} = \frac{1}{\bar{q}q}$ , za  $u \in \mathbf{U}_e$  pa velja  $u\bar{u} = |u|^2$ , je

$$u^{-1} = \frac{\bar{u}}{|u|^2} = \frac{-u}{1} = -u.$$

Če združimo te dve dejstvi sledi, da

$$uu^{-1} = -uu = -u^2 = 1 \Rightarrow u^2 = -1.$$

## 2.2 Zapis kvaternionov v polarni obliki

Podobno kot kompleksna števila lahko kvaternione zapišemo v polarni obliki. T.j. kompleksno število  $z = x + iy$  lahko zapišemo kot  $|z|(\cos \theta + i \sin \theta)$ . Z *eulerjevo formulo* lahko to kompleksno število zapišemo kot  $z = e^{i\theta}$ .

V kompleksni ravnini je ta zapis dobro definiran, saj imamo le eno kompleksno enoto  $i$ . V kvaternionih pa imamo celo množico čistih enotskih kvaternionov  $\mathbf{U}_e$ , s katerimi lahko zapišemo kvaternion.

**Trditev 1** Naj bo  $q \in \mathbb{H}$ . Tedaj obstajajo  $r, \theta \in \mathbb{R}$  in  $u \in \mathbf{U}_e$ , da

$$q = r(\mathbf{1} \cos \theta + u \sin \theta).$$

**Opomba 4** Preden dokažemo trditev opazimo, da tukaj zagotavljamo le obstoj in ne enoličnosti.

Preprost protiprimer za enoličnost je  $q \in \mathbf{Q}_e$ ,  $q = \mathbf{1} \cos \theta + u \sin \theta$ . Pogledamo  $\theta' = -\theta$  in  $u' = \bar{u} = -u$ . Tedaj je

$$\mathbf{1} \cos \theta' + u' \sin \theta' = \mathbf{1} \cos(-\theta) - u \sin(-\theta) = \mathbf{1} \cos \theta + u \sin \theta = q.$$

Vidimo, da ima  $q$  torej 2 zapisa.

**Opomba 5** Če v trditvi za  $r$  vzamemo 1, dobimo vse kvaternione oblike  $\mathbf{1} \cos \theta + u \sin \theta$ . Torej je množica  $\{\mathbf{1} \cos \theta + u \sin \theta; \theta \in \mathbb{R}, u \in \mathbf{U}_e\}$  enaka  $\mathbf{Q}_e$ .

*Dokaz:* Naj bo  $q \in \mathbb{H}$ . Razpišemo  $q = q_0 + \vec{q}$ . Definiramo  $q' = \frac{1}{|q|}(q_0 + \vec{q}) = q'_0 + \vec{q}'$ . Velja  $|q'| = \frac{1}{|q|}|q| = 1$ .

Ker je  $q'_0 \mathbf{1}$  pravokoten na  $\vec{q}'$ , velja pitagorov izrek:

$$|q'_0|^2 + |\vec{q}'|^2 = |q'|^2 = 1.$$

Naj bo  $\theta \in \mathbb{R}$ . Za  $q'_0$  vzamemo  $\mathbf{1} \cos \theta$ . Podobno želimo narediti še s  $\vec{q}'$ . Ker je  $\vec{q}'$  čisti kvaternion (t.j.  $\vec{q}' \in \mathbb{H} - \mathbb{R}$ ), želimo k drugemu delu zapisa dati čisti enotski kvaternion. Naj bo torej  $u \in \mathbf{U}_e$ . Pogledamo  $\mathbf{1} \cos \theta + u \sin \theta$ .

$$|\mathbf{1} \cos \theta + u \sin \theta|^2 = \cos^2 \theta + |u|^2 \sin^2 \theta.$$

Ker je  $u \in \mathbf{U}_e$ , je  $|u| = 1$ .

$$\Rightarrow \cos^2 \theta + \sin^2 \theta = 1.$$

Imamo torej  $q' = q'_0 + \vec{q}' = \mathbf{1} \cos \theta + u \sin \theta$ . Sledi

$$q = |q| \cdot q' = |q|(\mathbf{1} \cos \theta + u \sin \theta).$$

□

Zaradi lažjega računanja bomo polarni zapis kvaternionov spremeniti v eksponentni zapis, saj nam to olajša delo pri računanju. Spet se najprej spomnimo kompleksne ravnine, kjer lahko vsak  $z \in \mathbb{C}$  zapišemo kot  $|z|e^{i\varphi}$  za nek  $\varphi \in \mathbb{R}$ . To naredimo, saj je tako algebraična manipulacija kompleksnih izrazov lažja.

Vzamemo Taylorjev razvoj  $e^t$ . Velja

$$e^t = 1 + t + \frac{t^2}{2} + \frac{t^3}{6} + \frac{t^4}{24} + \dots$$

V Taylorjev razvoj vstavimo  $t = u\theta$ ,  $u \in \mathbf{U}_e$ ,  $\theta \in \mathbb{R}$ . Dobimo

$$e^{u\theta} = 1 + u\theta + \frac{(u\theta)^2}{2} + \frac{(u\theta)^3}{6} + \frac{(u\theta)^4}{24} + \dots$$

Spomnimo se, da ker je  $u \in \mathbf{U}_e$ , velja  $u^2 = -1$ . Ker  $e^t$  konvergira enakomerno povsod, lahko vrsto preuredimo, in sicer:

$$\begin{aligned} & 1 + u\theta + \frac{(u\theta)^2}{2} + \frac{(u\theta)^3}{6} + \frac{(u\theta)^4}{24} + \dots = \\ & (1 + \frac{(u\theta)^2}{2} + \frac{(u\theta)^4}{24} + \dots) + (u\theta + \frac{(u\theta)^3}{6} + \dots) = \\ & (1 - \frac{\theta^2}{2} + \frac{\theta^4}{24} - \dots) + u(\theta - \frac{\theta^3}{6} + \frac{\theta^5}{120} - \dots) \end{aligned}$$

V levem in desnem oklepaju vidimo Taylorjev razvoj funkcij  $\cos$  in  $\sin$ . Sledi torej

$$e^{u\theta} = \cos \theta + u \sin \theta.$$

Zgornjo trditev lahko sedaj spremenimo v lepšo obliko, t.j. za vsak  $q \in \mathbf{Q}_e$  obstajata  $\theta \in \mathbb{R}$  in  $u \in \mathbf{U}_e$ , da velja  $q = e^{u\theta}$ .

### 3 Eulerjeva funkcija

**Definicija 5** Za vse  $n \in \mathbb{N}$  s  $\varphi(n)$  označimo število celih števil iz množice  $\{1, 2, \dots, n\}$ , ki so tuja številu  $n$ . Preslikavo  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  imenujemo Eulerjeva funkcija.

**Zgled 1** Tabela 1 prikazuje izračun prvih šest vrednosti funkcije  $\varphi(n)$ . V  $n$ -ti vrstici so krepko natisnjena števila med 1 in  $n$ , ki so tuja številu  $n$ . Slika 1 pa grafično prikazuje prvih 100 vrednosti funkcije  $\varphi(n)$ .

$n$	$\{1, 2, \dots, n\}$	$\varphi(n)$
1	<b>{1}</b>	1
2	<b>{1, 2}</b>	1
3	<b>{1, 2, 3}</b>	2
4	<b>{1, 2, 3, 4}</b>	2
5	<b>{1, 2, 3, 4, 5}</b>	4
6	<b>{1, 2, 3, 4, 5, 6}</b>	2

Tabela 1: Vrednosti funkcije  $\varphi(n)$  za  $n = 1, 2, \dots, 6$

Slika 1: Vrednosti funkcije  $\varphi(n)$  za  $n = 1, 2, \dots, 100$

Računanje  $\varphi(n)$  po definiciji je pri velikem  $n$  zelo zamudno. Vendar ima Eulerjeva funkcija lepe lastnosti, zaradi katerih lahko njeno vrednost izračunamo tudi pri velikem argumentu, če ga le znamo razcepiti na prafaktorje.

Če je  $p$  praštevilo, med števili  $1, 2, \dots, p$  edinole število  $p$  ni tuje številu  $p$ , torej je  $\varphi(p) = p - 1$ . Skoraj prav tako preprosto lahko poiščemo vrednost  $\varphi(n)$ , če je  $n$  potenca nekega praštevila.

**Trditev 2** Naj bo  $p$  praštevilo in  $k \in \mathbb{N}$ . Potem je  $\varphi(p^k) = p^k - p^{k-1}$ .

*Dokaz:* Število  $a$  je tuje številu  $p^k$  natanko tedaj, ko ni večkratnik praštevila  $p$ . Med števili  $1, 2, \dots, p^k$  je natanko  $p^k/p = p^{k-1}$  večkratnikov števila  $p$ , torej je  $\varphi(p^k) = p^k - p^{k-1}$ .  $\square$

**Izrek 1** Eulerjeva funkcija je multiplikativna.

*Dokaz:* Vzemimo tuji naravni števili  $a$  in  $b$ . Zapišimo vsa števila med 1 in  $ab$  v obliki tabele z  $a$  vrsticami in  $b$  stolpci:

1	2	...	$b$
$b + 1$	$b + 2$	...	$2b$
$2b + 1$	$2b + 2$	...	$3b$
$\vdots$	$\vdots$	...	$\vdots$
$(a - 1)b + 1$	$(a - 1)b + 2$	...	$ab$

Za vsako število velja, da je tuje številu  $ab$  natanko tedaj, ko je tuje številu  $a$  in tuje številu  $b$ . Vrednost  $\varphi(ab)$  lahko torej dobimo tako, da preštejemo, koliko je v gornji tabeli števil, ki so tuja tako številu  $a$  kot tudi številu  $b$ .

Števila v posameznem stolpcu dajejo vsa isti ostanek pri deljenju z  $b$ . Torej so bodisi vsa tuja številu  $b$  bodisi mu ni tuje nobeno od njih. Stolpcev, katerih elementi so tuji številu  $b$ , je toliko, kot je takih števil v prvi vrstici tabele, teh pa je ravno  $\varphi(b)$ .

Različna števila v posameznem stolpcu dajo različne ostanke pri deljenju z  $a$ . Če namreč števili  $k_1b + r$  in  $k_2b + r$ , kjer je  $0 \leq k_1, k_2 \leq a - 1$ , dasta isti ostanek pri deljenju z  $a$ , je njuna razlika  $(k_1 - k_2)b$  deljiva z  $a$ . Ker sta števili  $a$  in  $b$  tuji, sledi, da je z  $a$  deljiva razlika  $k_1 - k_2$ . To pa je možno le, če je  $k_1 = k_2$ , saj je  $-(a - 1) \leq k_1 - k_2 \leq a - 1$ . Ker je dolžina stolpca enaka  $a$ , dobimo pri deljenju elementov stolpca z  $a$  ravno vse možne ostanke  $0, 1, \dots, a - 1$ . Torej je v vsakem stolpcu  $\varphi(a)$  števil tujih  $a$ .

To velja tudi za  $\varphi(b)$  stolpcev, katerih elementi so tuji številu  $b$ . Potemtakem je v gornji tabeli  $\varphi(b)\varphi(a)$  števil, ki so tuja tako številu  $b$  kot tudi številu  $a$ . Torej je  $\varphi(ab) = \varphi(a)\varphi(b)$ , kar pomeni, da je Eulerjeva funkcija multiplikativna.  $\square$

**Zgled 2** Izračunajmo  $\varphi(10^k)$ . Ker je  $10^k = 2^k 5^k$ , je po izreku 1 in trditvi 2

$$\varphi(10^k) = \varphi(2^k)\varphi(5^k) = (2^k - 2^{k-1})(5^k - 5^{k-1}) = 4 \times 10^{k-1}.$$

**Posledica 1**

$$\varphi(n) = n \times \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

kjer  $p$  preteče vse različne prafaktorje števila  $n$ .

*Dokaz:* Naj bo  $n = \prod_{i=1}^r p_i^{k_i}$ , kjer so  $p_1, p_2, \dots, p_r$  različna praštevila in  $k_1, k_2, \dots, k_r \in \mathbb{N}$ . Po izreku 1 in trditvi 2 je potem

$$\begin{aligned} \varphi(n) &= \prod_{i=1}^r \varphi(p_i^{k_i}) = \prod_{i=1}^r (p_i^{k_i} - p_i^{k_i-1}) \\ &= \left(\prod_{i=1}^r p_i^{k_i}\right) \times \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) = n \times \prod_{p|n} \left(1 - \frac{1}{p}\right). \quad \square \end{aligned}$$

**Trditev 3** Za vse  $n \in \mathbb{N}$  velja enačba

$$\sum_{d|n} \varphi(d) = n, \quad (1)$$

kjer  $d$  preteče vse pozitivne delitelje števila  $n$ .

*Dokaz:* Za vse delitelje  $d$  števila  $n$  označimo

$$A_d = \left\{ \frac{kn}{d}; k \in \mathbb{Z}, 0 \leq k < d, D(k, d) = 1 \right\}.$$

Recimo, da je  $k_1n/d_1 = k_2n/d_2$ , kjer je  $D(k_1, d_1) = D(k_2, d_2) = 1$ . Potem je  $k_1d_2 = k_2d_1$ , od koder sledi, da  $d_1$  deli  $d_2$  in obratno, kar pomeni, da je  $d_1 = d_2$ . Od tod zaključimo, da so si množice  $A_d$  paroma tuje, torej je

$$\left| \bigcup_{d|n} A_d \right| = \sum_{d|n} |A_d| = \sum_{d|n} \varphi(d).$$

Po drugi strani pa je

$$\bigcup_{d|n} A_d = \{0, 1, \dots, n-1\}.$$

Res, naj bo  $kn/d \in A_d$ . Ker  $d$  deli  $n$ , je število  $kn/d$  celo, iz  $0 \leq k < d$  pa sledi  $0 \leq kn/d < n$ , torej  $kn/d \in \{0, 1, \dots, n-1\}$ . Vzemimo zdaj še poljuben  $j \in \{0, 1, \dots, n-1\}$  in označimo:  $k = j/D(n, j)$ ,  $d = n/D(n, j)$ . Potem je  $j = kD(n, j) = kn/d \in A_d$ .

To pa pomeni, da je  $\left| \bigcup_{d|n} A_d \right| = n$  in izrek je dokazan.  $\square$

**Izrek 2 (Eulerjev izrek)** Naj bosta  $n \in \mathbb{N}$  in  $a \in \mathbb{Z}$  tuji števili. Potem je

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

*Dokaz:* Naj bodo  $k_1, k_2, \dots, k_{\varphi(n)}$  vsa števila med 1 in  $n$ , ki so tuja  $n$ . Če za indeksa  $i, j \in \{1, 2, \dots, \varphi(n)\}$  velja  $k_i a \equiv k_j a \pmod{n}$ , sledi  $n | (k_i a - k_j a)$  in zato  $n | (k_i - k_j)$ , saj sta števili  $n$  in  $a$  tuji. To pa je mogoče le, če je  $i = j$ . Števila  $k_1 a, k_2 a, \dots, k_{\varphi(n)} a$  so torej med seboj paroma nekongruentna po modulu  $n$ . Ker so tuja številu  $n$ , je množica njihovih ostankov pri deljenju z  $n$  enaka množici  $\{k_1, k_2, \dots, k_{\varphi(n)}\}$ . Zato je  $k_1 a \cdot k_2 a \cdots k_{\varphi(n)} a \equiv k_1 \cdot k_2 \cdots k_{\varphi(n)} \pmod{n}$ , od tod pa po krajšanju s produktom  $k_1 \cdot k_2 \cdots k_{\varphi(n)}$ , ki je tuj številu  $n$ , dobimo  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .  $\square$

**Posledica 2 (mali Fermatov izrek)** Naj bo  $p$  praštevilo in  $a \in \mathbb{Z}$  celo število, ki ni deljivo s  $p$ . Potem je

$$a^{p-1} \equiv 1 \pmod{p}.$$



## 4 Möbiusova funkcija

**Definicija 6** Za vse  $n \in \mathbb{N}$  naj bo

$$\mu(n) = \begin{cases} 0, & \text{če } n \text{ deljiv s kvadratom praštevíla,} \\ (-1)^r, & \text{sicer,} \end{cases}$$

kjer je  $r$  število različnih prafaktorjev števila  $n$ . Preslikavo  $\mu : \mathbb{N} \rightarrow \mathbb{Z}$  imenujemo Möbiusova funkcija.

**Zgled 3** Tabela 2 prikazuje prvih nekaj vrednosti funkcije  $\mu(n)$ .

$n$	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

Tabela 2: Vrednosti funkcije  $\mu(n)$

**Izrek 3** Möbiusova funkcija je multiplikativna.

*Dokaz:* Vzemimo tuji naravni števili  $a$  in  $b$ . Če je število  $ab$  deljivo s kvadratom praštevíla, velja to tudi za  $a$  ali za  $b$ . V tem primeru je torej  $\mu(ab) = 0 = \mu(a)\mu(b)$ . Če pa število  $ab$  ni deljivo s kvadratom praštevíla, velja to tudi za  $a$  in za  $b$ . Naj bo  $r$  število različnih prafaktorjev števila  $a$ ,  $s$  pa število različnih prafaktorjev števila  $b$ . Potem je število različnih prafaktorjev števila  $ab$  enako  $r + s$ , torej je v tem primeru  $\mu(ab) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(a)\mu(b)$ .  $\square$

**Trditev 4** Za vse  $n \in \mathbb{N}$  velja enačba

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1, \end{cases} \quad (2)$$

kjer  $d$  preteče vse pozitivne delitelje števila  $n$ .

*Dokaz:* Zadošča seštevati po tistih deliteljih  $d$  števila  $n$ , ki imajo same različne prafaktorje (sicer je  $\mu(d) = 0$ ). Imenujmo takšne delitelje *enostavni*. Naj bo  $r$  število različnih prafaktorjev števila  $n$ . Število enostavnih deliteljev števila  $n$ , ki imajo natanko  $k$  prafaktorjev, je potem  $\binom{r}{k}$ , prispevek takega delitelja h gornji vsoti pa znaša  $\mu(d) = (-1)^k$ . Torej je

$$\sum_{d|n} \mu(d) = \sum_{k=0}^r (-1)^k \binom{r}{k} = \begin{cases} 1, & r = 0, \\ 0, & r > 0 \end{cases} = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases} \quad \square$$

**Opomba 6** Enačbo (2) bi lahko uporabili tudi za (rekurzivno) definicijo funkcije  $\mu(n)$ :

$$\mu(n) = \begin{cases} 1, & n = 1, \\ - \sum_{d|n, d < n} \mu(d), & n > 1. \end{cases}$$

Möbiusova funkcija igra pomembno vlogo pri Möbiusovem obratu, ki nam omogoča izraziti aritmetično funkcijo  $f(n)$ , če poznamo funkcijo  $g(n) = \sum_{d|n} f(d)$ , kjer  $d$  preteče vse pozitivne delitelje števila  $n$ .

**Izrek 4** (Möbiusov obrat) Za aritmetični funkciji  $f, g$  velja:

$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

*Dokaz:* Najprej vzemimo, da je  $g(n) = \sum_{d|n} f(d)$  za vse  $n \in \mathbb{N}$ . Potem je

$$\begin{aligned} \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{k|d} f(k) = \sum_{k|n} f(k) \sum_{k|d|n} \mu\left(\frac{n}{d}\right) \\ &= \sum_{k|n} f(k) \sum_{a|(n/k)} \mu(a) = f(n). \end{aligned}$$

Drugo enakost smo dobili z zamenjavo vrstnega reda seštevanja, tretjo z uvedbo nove spremenljivke  $a = n/d$ , četrta pa sledi iz (2).

Vzemimo zdaj, da je  $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$  za vse  $n \in \mathbb{N}$ . Potem je

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} \sum_{k|d} \mu\left(\frac{d}{k}\right) g(k) = \sum_{k|n} g(k) \sum_{k|d|n} \mu\left(\frac{d}{k}\right) \\ &= \sum_{k|n} g(k) \sum_{b|(n/k)} \mu(b) = g(n). \end{aligned}$$

Drugo enakost smo dobili z zamenjavo vrstnega reda seštevanja, tretjo z uvedbo nove spremenljivke  $b = d/k$ , četrta pa sledi iz (2).  $\square$

**Zgled 4** • Iz enačbe (1) sledi z Möbiusovim obratom, da je

$$\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d.$$

- Za vse  $n \in \mathbb{N}$  s  $\tau(n)$  označimo število vseh pozitivnih deliteljev števila  $n$ . Torej je  $\tau(n) = \sum_{d|n} 1$ , od koder sledi z Möbiusovim obratom, da je

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d) = 1.$$

- Za vse  $n \in \mathbb{N}$  s  $\sigma(n)$  označimo vsoto vseh pozitivnih deliteljev števila  $n$ . Torej je  $\sigma(n) = \sum_{d|n} d$ , od koder sledi z Möbiusovim obratom, da je

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d) = n.$$

## 5 Kolobar aritmetičnih funkcij

**Definicija 7** Za aritmetični funkciji  $f, g : \mathbb{N} \rightarrow \mathbb{C}$  in za vse  $n \in \mathbb{N}$  naj bo

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Aritmetična funkcija  $f * g$  je Dirichletova konvolucija funkcij  $f$  in  $g$ .

**Trditev 5** Naj bodo  $f, g, h$  aritmetične funkcije. Potem velja:

- (i)  $f * g = g * f$ ,
- (ii)  $(f * g) * h = f * (g * h)$ ,
- (iii)  $f * (g + h) = f * g + f * h$ .

*Dokaz:*

- (i) Trditev sledi iz zapisa Dirichletove konvolucije v simetrični obliki

$$(f * g)(n) = \sum_{de=n} f(d)g(e), \quad (3)$$

kjer seštevamo po vseh urejenih parih naravnih števil  $(d, e)$ , katerih produkt je enak  $n$ .

- (ii) Z uporabo enačbe (3) izračunamo

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{de=n} (f * g)(d)h(e) = \sum_{de=n} \left( \sum_{ab=d} f(a)g(b) \right) h(e) \\ &= \sum_{abe=n} f(a)g(b)h(e) = \sum_{ac=n} f(a) \sum_{be=c} g(b)h(e) \\ &= \sum_{ac=n} f(a)(g * h)(c) = (f * (g * h))(n). \end{aligned}$$

Četrto enakost smo dobili z uvedbo nove spremenljivke  $c = be$ .

(iii) Z uporabo enačbe (3) izračunamo

$$\begin{aligned}
(f * (g + h))(n) &= \sum_{de=n} f(d)(g + h)(e) = \sum_{de=n} f(d)(g(e) + h(e)) \\
&= \sum_{de=n} f(d)g(e) + \sum_{de=n} f(d)h(e) \\
&= (f * g + f * h)(n). \quad \square
\end{aligned}$$

Iz trditve 5 sledi, da je množica vseh aritmetičnih funkcij  $f : \mathbb{N} \rightarrow \mathbb{C}$  z operacijama  $+$  in  $*$  komutativen kolobar. Imenujemo ga *Dirichletov kolobar* in označimo z  $\mathcal{D}$ .

Funkcija  $\varepsilon \in \mathcal{D}$ , ki za vse  $n \in \mathbb{N}$  zadošča enačbi

$$\varepsilon(n) = \begin{cases} 1, & n = 1, \\ 0, & n > 1, \end{cases}$$

je enica kolobarja  $\mathcal{D}$ , saj za vse  $f \in \mathcal{D}$  in  $n \in \mathbb{N}$  velja

$$(f * \varepsilon)(n) = \sum_{de=n} f(d)\varepsilon(e) = f(n)\varepsilon(1) = f(n).$$

Brez težav se lahko prepričamo tudi, da je  $\mathcal{D}$  cel kolobar in da je funkcija  $f \in \mathcal{D}$  obrnljiva natanko tedaj, ko  $f(1) \neq 0$ .

Zdaj lahko enačbo (2) prepišemo v obliki

$$\mu * \mathbf{1} = \varepsilon,$$

kjer  $\mathbf{1}$  označuje konstantno funkcijo z vrednostjo 1. Z drugimi besedami, Möbiusova funkcija je inverz konstantne funkcije  $\mathbf{1}$  glede na Dirichletovo konvolucijo:

$$\mu = \mathbf{1}^{-1}.$$

Möbiusov obrat lahko torej zapišemo v obliki

$$g = f * \mathbf{1} \iff f = g * \mu,$$

kjer njegova veljavnost postane očitna. Zgled 4 pa lahko prepišemo v obliki

$$\begin{aligned}
\varphi * \mathbf{1} = \text{id}_{\mathbb{N}} &\implies \varphi = \mu * \text{id}_{\mathbb{N}}, \\
\tau = \mathbf{1} * \mathbf{1} &\implies \mu * \tau = \mathbf{1}, \\
\sigma = \text{id}_{\mathbb{N}} * \mathbf{1} &\implies \mu * \sigma = \text{id}_{\mathbb{N}}.
\end{aligned}$$

## Angleško-slovenski slovar strokovnih izrazov

**proper** pravi

**pure** pravi, čisti

**versor** versor, enotski kvaternion

**dot product** skalarni produkt

**by-product** stranski učinek

## Literatura

- [1] M. Aigner in G. M. Ziegler, *Proofs from THE BOOK*, 2. izdaja, Springer, Berlin–Heidelberg–New York, 2001.
- [2] N. Calkin in H. S. Wilf, Recounting the rationals, *Amer. Math. Monthly* **107** (2000), 360–363.
- [3] J. Grasselli, *Elementarna teorija števil*, DMFA – založništvo, Ljubljana, 2009.