Univerzitet u Beogradu
Matematički fakultet

ARITMETIKA CELOBROJNIH KVATERNIONA

Master rad

Smer: Profesor matematike i računarsta
Student: Jovana Simić, 1082/2019
Mentor: prof. dr Goran Đanković
Članovi komisije: prof. dr Aleksandar Lipkovski
prof. dr Zoran Petrović

Beograd, 2024.

Sadržaj

Uvod

Kvaternioni predstavljaju zanimljivu i duboku algebarsku strukturu koja se istovremeno izdvaja i po bogatstvu svojstava i po svojoj složenosti. Ova matematička konstrukcija proširuje poznate oblasti realnih i kompleksnih brojeva, uvodeći novi nivo apstrakcije i izazova.

U osnovi, kvaternioni su proširenje kompleksnih brojeva na četiti dimenzije, što je ujedno i značenje latinske reči quaternion po kojoj su dobili ime, a koja se prevodi kao četvorka ili celina od četiri dela. Dok su kompleksni brojevi definisani kao linearna kombinacija realnog i imaginarnog dela, kvaternioni idu korak dalje dodajući još dve imaginarnosti. Ova proširenja omogućavaju bogatije opisivanje rotacija, transformacija i rešavanje problema iz različitih matematičkih oblasti.

Kvaternione je prvi opisao irski matematičar i fizičar William Rowan Hamilton. On je, fasciniran ulogom skupa $\mathbb{C}$ u geometriji dvodimenzionalnog prostora, pokušavao dobiti algebarsku strukturu koja bi bila proširenje skupa kompleksnih brojeva i imala sličnu ulogu u $\mathbb{R}^3$. Međutim, godinama mu je problem predstavljala definicija množenja u $\mathbb{R}^3$, i to na sledeći način.

Ukoliko bismo mogli da definišemo množenje u $\mathbb{R}^3$, onda bismo sem i koja je imaginarna jedinica, dodali još jedan generator j. Dakle, svaki element bi bio napisan u obliku $x + iy + zj$, gde su $x, y, z \in \mathbb{R}$ na tačno jedan način. Dakle, $\mathbb{R}^3$ postaje algebra nad $\mathbb{R}$. I tada nam je važno koliko je $i \cdot j$. Neka je

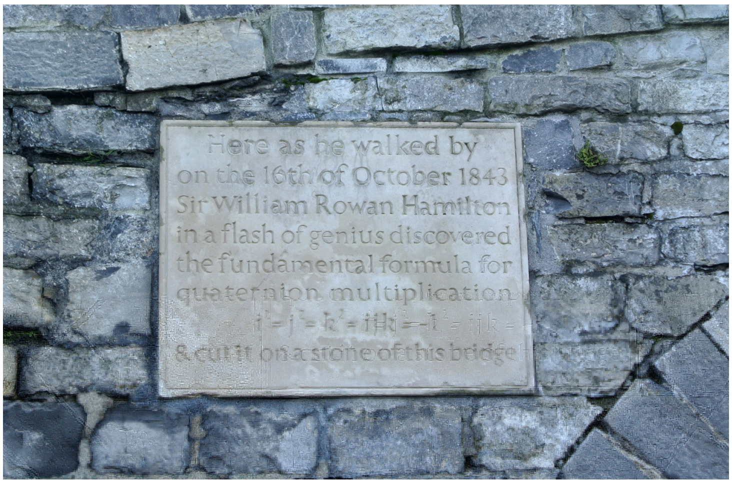
$$i \cdot j = a + bi + cj.$$

Ako ovu jednakost pomnožimo sleva sa i i pretpostavimo da je algebra asocijativna, onda dobijamo

$$\begin{aligned} -j = i \cdot (i \cdot j) &= i \cdot (a + bi + cj) = ai + b(-1) + c(i \cdot j) = ai - b + c(a + bi + cj) \\ &= ai - b + ca + cbi + c^2 j = (ac - b) + (a + bc)i + c^2 j. \end{aligned}$$

No, odavde sledi da je $-1 = c^2$, te dobijamo kontradikciju.

Nakon višegodišnjih neuspelih pokušaja, Hamilton je 16. oktobra 1843. god. u Dablinu na putu do Irske kraljevske akademije shvatio da to ne može postići u dimenziji 3, već u dimenziji 4, sa tri imaginarne jedinice i, j, k koje moraju zadovoljavati jednakost $i^2 = j^2 = k^2 = ijk = -1$. Tu formulu je odmah urezao u kamen mosta kojim je prolazio. Ova formula je obeležila celokupan Hamiltonov budući rad, stoga je ostatak života posvetio proučavanju kvaterniona.



Slika 1: Ploča o kvaternionima na mostu u Dablinu

Kvaternion je broj q oblika $q = a + bi + cj + dk$, gde su $a, b, c, d \in \mathbb{R}$, dok $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ označava prostor kvaterniona. Sa operacijama sabiranja, množenja i množenja skalarom $\mathbb{H}$ čini nekomutativnu asocijativnu algebru s deljenjem nad poljem realnih brojeva i upravo zbog svojstva množenja kvaterniona koje nije komutativno, kvaternioni su posebni i izazovni za proučavanje. To znači da redosled množenja kvaterniona igra ulogu, što se razlikuje od realnih i kompleksnih brojeva. Ova osobina čini kvaternione dubokim i fascinatnim istraživačkim poljem, ali istovremeno i zahtevnim za razumevanje.

U prvom delu istražujemo osnovne definicije, svojstva, operacije i pravila koja upravljaju ovom strukturom, dok ćemo u drugom delu koji se odnosi na aritmetiku celobrojnih kvaterniona istraživati pitanja kao što su deljenje, deljenje sa ostatkom, faktorizacija i pronalaženje najvećeg zajedničkog delioca. Ovi koncepti postaju još izazovniji u kontekstu kvaterniona zbog njihove nelinearne prirode. Faktorizacija kvaterniona, na primer, zahteva posebne pristupe kako bi se identifikovali faktori i pravilno analizirala jedinstvena faktorizacija.

Algebarska svojstva kvaterniona

U ovom delu rada definisaćemo skup kvaterniona i osnovne operacije na tom skupu, definisaćemo moduo i inverz kvaterniona i zaključićemo da je norma kvaterniona multiplikativna. Zatim ćemo pokazati da skup kvaterniona čini jednu $\mathbb{R}$-algebru sa deljenjem. Identifikovaćemo kvaternione sa matricama dimenzije 2x2 i definisaćemo celobrojne kvaternione kao uvod u sledeći deo koji se odnosi na aritmetiku celobrojnih kvaterniona.

1.1 Osnovne operacije i svojstva

Definicija 1.1. *Skup kvaterniona je skup*

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

gde su i, j, k međusobno različiti imaginarni elementi za koje važi

$$i^2 = j^2 = k^2 = ijk = -1.$$

Definicija 1.2. *Neka je $q = a + bi + cj + dk \in \mathbb{H}$.*
Realni deo a naziva se realni deo kvaterniona q i označava se $\Re(q)$.
Kvaternion $bi + cj + dk$ naziva se imaginarni deo kvaterniona q i označava se $\Im(q)$.

Najpre ćemo se podsetiti definicije grupe, a zatim ćemo definisati osnovne operacije na skupu $\mathbb{H}$.

Definicija 1.3. *Grupa je skup G sa jednom binarnom operacijom $G \times G \to G$, koja svakom uređenom paru (a, b) elemenata iz G dodeljuje novi element $a * b$ iz G i koja ima sledeće osobine:*

(i) *za svaka tri elementa $a, b, c \in G$ važi $(a * b) * c = a * (b * c)$ (zakon asocijativnosti);*

(ii) *postoji element $e \in G$, koji nazivamo neutralni ili jedinični element, takav da za sve elemente $a \in G$ važi $a * e = e * a = a$;*

(iii) *za svaki element $a \in G$ posotoji element $b \in G$, koji nazivamo inverzni element, takav da je $a * b = b * a = e$.*

Grupa G je Abelova ili komutativna ako u njoj važi

(iv) *$a * b = b * a$, $(\forall a, b \in G)$ (zakon komutativnosti).*

Definicija 1.4. *Neka su $q_1, q_2 \in \mathbb{H}$, pri čemu su $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$.*
Binarnu operaciju sabiranja $+$ na skupu $\mathbb{H}$ definišemo na sledeći način:

$$\begin{aligned} q_1 + q_2 &= (a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) \\ &= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k. \end{aligned}$$

Sabiranje kvaterniona ima svojstvo asocijativnosti i komutativnosti. Naime, iz definicije operacije $+$ sledi

$$\begin{aligned} & (q_1 + q_2) + q_3 \\ = \; & ((a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k) + (a_3 + b_3 i + c_3 j + d_3 k) \\ = \; & ((a_1 + a_2) + a_3) + ((b_1 + b_2) + b_3)i + ((c_1 + c_2) + c_3)j + ((d_1 + d_2) + d_3)k \\ = \; & (a_1 + (a_2 + a_3)) + (b_1 + (b_2 + b_3))i + (c_1 + (c_2 + c_3))j + (d_1 + (d_2 + d_3))k \\ = \; & (a_1 + b_1 i + c_1 j + d_1 k) + ((a_2 + b_2 i + c_2 j + d_2 k) + (a_3 + b_3 i + c_3 j + d_3 k)) \\ = \; & q_1 + (q_2 + q_3), \end{aligned}$$

a kako se komutativnost operacije sabiranja kvaterniona svodi na komutativnost sabiranja u skupu $\mathbb{R}$ imamo da važi

$$\begin{aligned} q_1 + q_2 &= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k \\ &= (a_2 + a_1) + (b_2 + b_1)i + (c_2 + c_1)j + (d_2 + d_1) \\ &= q_2 + q_1. \end{aligned}$$

Neutralni element za sabiranje kvaterniona je $0 = 0 + 0i + 0j + 0k$, a inverzni element kvaterniona $q = a + bi + cj + dk$ je kvaternion $-q = -a - bi - cj - dk$. Sada, kada smo videli da za sabiranje kvaterniona važi zakon asocijativnosti i komutativnosti, da postoji neutralni i inverzni element, važi sledeća lema:

Lema 1.1. *Algebarska struktura $(\mathbb{H}, +)$ gde je $+$ sabiranje u skupu $\mathbb{H}$ jeste jedna Abelova grupa.*

Definicija 1.5. *Za svako $\alpha \in \mathbb{R}$ i svako $q \in \mathbb{H}$, $q = a+bi+cj+dk$ definišemo*

$$\alpha * q = (\alpha a) + (\alpha b)i + (\alpha c)j + (\alpha d)k.$$

Spoljnu operaciju $* : \mathbb{R} \times \mathbb{H} \to \mathbb{H}$ nazivamo množenje kvaterniona skalarom.

Teorema 1.1. *Skup kvaterniona $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ sa operacijom sabiranja $+$ i operacijom množenja kvaterniona skalarom $*$ definisanim sa:*

$$\begin{aligned} q_1 + q_2 &= (a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) \\ &= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k, \\ \alpha * q &= (\alpha a) + (\alpha b)i + (\alpha c)j + (\alpha d)k \end{aligned}$$

čini vektorski prostor nad poljem $\mathbb{R}$.

Dokaz. U prethodnoj lemi smo videli da je skup $\mathbb{H}$ Abelova grupa, pa uz operaciju sabiranja važi zakon asocijativnosti, komutativnosti, postojanje neutralnog i inverznog elementa. Ostale aksiome vektorskog prostora: $\alpha * (q_1 + q_2) = \alpha q_1 + \alpha q_2$; $(\alpha + \beta) * q = \alpha q + \beta q$; $(\alpha * \beta) * q = \alpha * (\beta q)$; $1 * q = q$ za $\forall q, q_1, q_2 \in \mathbb{H}$ i $\forall \alpha, \beta \in \mathbb{R}$ slede direktno iz definicije navedenih operacija. $\square$

Vektorski prostor nad poljem $\mathbb{R}$ označavamo sa $(\mathbb{H}, +, *)$. Kako je prema definiciji svaki element skupa $\mathbb{H}$ oblika $a + bi + cj + dk$ za $a, b, c, d \in \mathbb{R}$, moguće ga je prikazati kao linearnu kombinaciju elemenata $1, i, j, k$, što znači da je skup $[1, i, j, k]$ jedna baza vektorskog prostora $\mathbb{H}$, pa je dimenzija ovog vektorskog prostora $\dim(\mathbb{H}) = 4$.

Da bismo definisali množenje kvaterniona potrebne su nam sledeće relacije iz definicije

$$i^2 = j^2 = k^2 = ijk = -1,$$

uz pretpostavku da je množenje asocijativno i jednice 1 kao neutralnog elementa za množenje. Primetimo da ove relacije određuju sve moguće proizvode i, j i k. Na primer, ako pođemo od relacije

$$ijk = -1$$

i pomnožimo zdesna obe strane ove jednakosti elementom k , dobićemo

$$(ijk)k = -k$$

$$ij(kk) = -k$$

$$-ij = -k$$

$$ij = k.$$

Na sličan način možemo dobiti i ostale mogućnosti proizvoda, pa tako dolazimo do toga da važi:

$$ij = k,\ ji = -k$$

$$jk = i,\ kj = -i$$

$$ki = j,\ ik = -j.$$

Sada množenje elemenata baze vektorskog prostora $\mathbb{H}$ možemo predstaviti Kejlijevom tablicom

$\cdot$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

Tabela 1.1: Kejlijeva tablica

Uz pomoć Kejlijeve tablice i aksiome vektorsko prostora $(\mathbb{H}, +, *)$ možemo pomnožiti dva kvaterniona

$$\begin{aligned}
q_1 \cdot q_2 &= (a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k) \\
&= a_1 \cdot (a_2 + b_2 i + c_2 j + d_2 k) + b_1 i \cdot (a_2 + b_2 i + c_2 j + d_2 k) \\
&+ c_1 j \cdot (a_2 + b_2 i + c_2 j + d_2 k) + d_1 k \cdot (a_2 + b_2 i + c_2 j + d_2 k) \\
&= a_1 a_2 + a_1 b_2 i + a_1 c_2 j + a_1 d_2 k + b_1 a_2 i + b_1 b_2 ii + b_1 c_2 ij + b_1 d_2 ik \\
&+ c_1 a_2 j + c_1 b_2 ji + c_1 c_2 jj + c_1 d_2 jk + d_1 a_2 k + d_1 b_2 ki + d_1 c_2 kj + d_1 d_2 kk \\
&= a_1 a_2 + a_1 b_2 i + a_1 c_2 j + a_1 d_2 k + b_1 a_2 i - b_1 b_2 + b_1 c_2 k - b_1 d_2 j \\
&+ c_1 a_2 j - c_1 b_2 k - c_1 c_2 + c_1 d_2 i + d_1 a_2 k + d_1 b_2 j - d_1 c_2 i - d_1 d_2 \\
&= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i \\
&+ (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) k.
\end{aligned}$$

Stoga imamo sledeću definiciju.

Definicija 1.6. *Neka su* $q_1, q_2 \in \mathbb{H}$, *pri čemu su* $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ *i* $q_2 = a_2 + b_2 i + c_2 j + d_2 k$.
Množenje kvaterniona q_1 *i* q_2 *se definiše na sledeći način*

$$
\begin{aligned}
q_1 \cdot q_2 &= (a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k) \\
&= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i \\
&+ (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) k.
\end{aligned}
$$

Množenje kvaterniona je asocijativno ako i samo ako je množenje elemenata i, j, k asocijativno. Isto važi i za svojstvo komutativnosti. Ali ako pogledamo Kejlijevu tablicu množenja baznih elemenata, primetićemo da ona nije simetrična s obzirom na glavnu dijagonalu pa množenje tih elemenata nije komutativno. Prema tome, množenje kvaterniona je asocijativna operacija koja nije komutativna.

Definicija 1.7. *Konjugovani kvaternion kvaterniona* $q = a + bi + cj + dk$ *je kvaternion*

$$\overline{q} = a - bi - cj - dk.$$

Po definiciji će očigledno važiti $\overline{\overline{q}} = q$, pa možemo reći da je preslikavanje $q \to \overline{q}$ jedno involutivno preslikavanje. Dokažimo sledeću lemu.

Lema 1.2. *Neka su* $q_1, q_2 \in \mathbb{H}$ *dva proizvoljna kvaterniona, tako da je* $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ *i* $q_2 = a_2 + b_2 i + c_2 j + d_2 k$. *Tada važi:*

$$\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$$

$$\overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}$$

Dokaz. Na osnovu definicije sabiranja kvaterniona imamo

$$
\begin{aligned}
\overline{q_1 + q_2} &= \overline{(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k)} \\
&= \overline{(a_1 + a_2) + (b_1 + b_2) i + (c_1 + c_2) j + (d_1 + d_2)} \\
&= (a_1 + a_2) - (b_1 + b_2) i - (c_1 + c_2) j - (d_1 + d_2) \\
&= (a_1 - b_1 i - c_1 j - d_1 k) + (a_2 - b_2 i - c_2 j - d_2 k) \\
&= \overline{q_1} + \overline{q_2}.
\end{aligned}
$$

Na slačan način dokazujemo i drugu jednakost

$$\begin{aligned}
\overline{q_1 \cdot q_2} &= \overline{(a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k)} \\
&= \overline{(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i} \\
&+ \overline{(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k} \\
&= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) - (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i \\
&- (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j - (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k
\end{aligned}$$

S druge strane imamo

$$\begin{aligned}
\overline{q_2} \cdot \overline{q_1} &= (a_2 - b_2 i - c_2 j - d_2 k) \cdot (a_1 - b_1 i - c_1 j - d_1 k) \\
&= (a_2a_1 - b_2b_1 - c_2c_1 - d_2d_1) - (b_2a_1 + b_2a_1 + c_2d_1 - d_2c_1)i \\
&- (a_2c_1 + b_2d_1 + c_2a_1 - d_2b_1)j - (a_2d_1 - b_2c_1 + c_2b_1 + d_2a_1)k.
\end{aligned}$$

Neposrednim upoređivanjem prethodne dve relacije imamo jednakost desnih strana pa i leve strane moraju biti jednake čime smo dokazali tvrđenje. □

Definišimo moduo i normu kvaterniona.

Definicija 1.8. *Moduo kvaterniona $q = a+bi+cj+dk$ je nenegativan realan broj $|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$.*

Tvrđenje 1.1. *Neka je $q = a + bi + cj + dk \in \mathbb{H}$ i $\overline{q} = a - bi - cj - dk \in \mathbb{H}$ njemu konjugovani kvaternion. Tada važi:*

$$q\overline{q} = |q|^2.$$

Dokaz. Primenjujući svojstvo množenja kvaterniona, desna strana jednaka je:

$$\begin{aligned}
q\overline{q} &= (a + bi + cj + dk)(a - bi - cj - dk) \\
&= a^2 - abi - acj - adk + abi + b^2 - bck + bdj \\
&+ acj + bck + c^2 - cdi + adk - bdj + cdi + d^2 \\
&= a^2 + b^2 + c^2 + d^2.
\end{aligned}$$

Kako je po definiciji $|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$, onda je $|q|^2 = a^2 + b^2 + c^2 + d^2$ čime je jednakost dokazana. □

Na osnovu ovoga možemo definisati normu kvaterniona.

Definicija 1.9. *Norma kvaterniona* $q = a+bi+cj+dk$ *je nenegativan realan broj*
$$N(q) = q \cdot \overline{q} = |q|^2 = a^2 + b^2 + c^2 + d^2.$$

Iz definicije modula sledi da važi:
$$|\overline{q}| = \sqrt{\overline{q} \cdot \overline{\overline{q}}} = \sqrt{\overline{q} \cdot q} = \sqrt{a^2 + b^2 + c^2 + d^2} = |q|,$$
jer je
$$\overline{q} \cdot q = (a - bi - cj - dk)(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2.$$
Ovde vidimo da je svaki kvaternion komutativan sa svojim konjugovanim kvaternionom: $\overline{q}q = q\overline{q}$, a takođe imamo da važi:
$$|q\overline{q}| = \sqrt{(q\overline{q} \cdot \overline{q\overline{q}})} = \sqrt{q\overline{q}}\sqrt{\overline{q}q} = |q||q| = |q|^2 = |q||\overline{q}|,$$

Sada možemo definisati inverz kvaterniona koristeći konjugaciju i normu kvaterniona. Proizvod nenula kvaterniona i njegovog inverza treba da bude jednak 1, pa je inverz kvaterniona q kvaternion
$$q^{-1} = \frac{\overline{q}}{N(q)} = \frac{\overline{q}}{|q|^2}.$$

Kako je $q = 1+0i+0j+0k = 1$ neutralni element za množenje kvaterniona, time smo dokazali sledeću lemu.

Lema 1.3. *Algebarska struktura* $(\mathbb{H} \setminus \{0\}, \cdot)$ *gde je* $\mathbb{H}$ *skup svih kvaterniona, a* $\cdot$ *binarna operacija množenja kvaterniona u tom skupu, jeste jedna grupa. Pritom, kako operacija* $\cdot$ *nije komutativna u skupu* $\mathbb{H}$ *ova grupa nije Abelova.*

Sada ćemo se podsetiti definicije prstena.
Neka je A skup s dve binarne operacije $(a, b) \to a + b$ i $(a, b) \to ab$. Moguće osobine tih operacija su sledeće:

(A1) za svaka tri elementa $a, b, c \in A$ je $a + (b + c) = (a + b) + c$;

(A2) postoji element $0 \in A$ tako da za svako $a \in A$, $a + 0 = 0 + a = a$;

(A3) za svako $a \in A$ postoji $b \in A$ takav da je $a + b = b + a = 0$;

(A4) za svaka dva elementa $a, b \in A$ je $a + b = b + a$;

(M1) za svaka tri elementa $a, b, c \in A$ je $a(bc) = (ab)c$;

(M2) postoji element $1 \in A$ takav da za svako $a \in A$, $a1 = 1a = a$;

(M3) za svako $a \in A \setminus \{0\}$ postoji $b \in A$ takav da je $ab = ba = 1$;

(M4) za svaka dva elementa $a, b \in A$ je $ab = ba$;

(D) za svaka tri elementa $a, b, c \in A$ je $(a+b)c = ac+bc$ i $a(b+c) = ab+ac$.

Definicija 1.10. *Neka je A skup sa dve binarne operacije - sabiranjem i množenjem, u kome sabiranje zadovoljava aksiome A1-A4 (tj.* $(A, +)$ *je Abelova grupa) i važi aksioma D (distributivnost). Skup A je prsten ako zadovoljava aksiomu M1; prsten A ima jedinicu ako zadovoljava i aksiomu M2; prsten A je komutativan ako zadovoljava i aksiomu M4. Skup A je telo ako važe aksiome M1, M2, M3; telo A je polje ako, pored M1, M2, M3, važi i aksioma M4.*

Iz definicije sabiranja i množenja kvaterniona možemo dokazati distributivnost množenja prema sabiranju, to jest da važi

$$\begin{aligned} q_1 \cdot (q_2 + q_3) &= q_1q_2 + q_1q_2, \\ (q_1 + q_2) \cdot q_3 &= q_1q_2 + q_1q_3. \end{aligned}$$

$$\begin{aligned}
& q_1 \cdot (q_2 + q_3) \\
= \; & (a_1 + b_1i + c_1j + d_1k)((a_2 + a_3) + (b_2 + b_3)i + (c_2 + c_3)j + (d_2 + d_3)k) \\
= \; & (a_1 + b_1i + c_1j + d_1k)(a_2 + a_3 + b_2i + b_3i + c_2j + c_3j + d_2k + d_3k) \\
= \; & a_1a_2 + a_1a_3 + a_1b_2i + a_1b_3i + a_1c_2j + a_1c_3j + a_1d_2k + a_1d_3k \\
+ \; & b_1a_2i + b_1a_3i - b_1b_2 - b_1b_3 + b_1c_2k + b_1c_3k - b_1d_2j - b_1d_3j \\
+ \; & c_1a_2j + c_1a_3j - c_1b_2k - c_1b_3k - c_1c_2 - c_1c_3 + c_1d_2i + c_1d_3i \\
+ \; & d_1a_2k + d_1a_3k + d_1b_2j + d_1b_3j - d_1c_2i - d_1c_3i - d_1d_2 - d_1d_3 \\
= \; & (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i \\
+ \; & (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k \\
+ \; & (a_1a_3 - b_1b_3 - c_1c_3 - d_1d_3) + (a_1b_3 + b_1a_3 + c_1d_3 - d_1c_3)i \\
+ \; & (a_1c_3 - b_1d_3 + c_1a_3 + d_1b_3)j + (a_1d_3 + b_1c_3 - c_1b_3 + d_1a_3)k \\
= \; & q_1q_2 + q_1q_3.
\end{aligned}$$

$$
\begin{aligned}
& (q_1 + q_2) \cdot q_3 \\
= \; & ((a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k)(a_3 + b_3 i + c_3 j + d_3 k) \\
= \; & (a_1 + a_2 + b_1 i + b_2 i + c_1 j + c_2 j + d_1 k + d_2 k)(a_3 + b_3 i + c_3 j + d_3 k) \\
= \; & a_1a_3 + a_1b_3i + a_1c_3j + a_1d_3k + a_2a_3 + a_2b_3i + a_2c_3j + a_2d_3k \\
+ \; & b_1a_3i - b_1b_3 + b_1c_3k - b_1d_3j + b_2a_3i - b_2b_3 + b_2c_3k - b_2d_3j \\
+ \; & c_1a_3j - c_1b_3k - c_1c_3 + c_1d_3i + c_2a_3j - c_2b_3k - c_2c_3 + c_2d_3i \\
+ \; & d_1a_3k + d_1b_3j - d_1c_3i - d_1d_3 + d_2a_3k + d_2b_3j - d_2c_3i - d_2d_3 \\
= \; & (a_1a_3 - b_1b_3 - c_1c_3 - d_1d_3) + (a_1b_3 + b_1a_3 + c_1d_3 - d_1c_3)i \\
+ \; & (a_1c_3 - b_1d_3 + c_1a_3 + d_1b_3)j + (a_1d_3 + b_1c_3 - c_1b_3 + d_1a_3)k \\
+ \; & (a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3) + (a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)i \\
+ \; & (a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)j + (a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)k \\
= \; & q_1q_3 + q_2q_3.
\end{aligned}
$$

Sada, kada smo dokazali da važi distributivnost množenja prema sabiranju, a na osnovu leme 1.1. i leme 1.3. sledi da važi i sledeća teorema.

Tvrđenje 1.2. *Algebarska struktura* $(\mathbb{H}, +, \cdot)$ *gde je* $+$ *binarna operacija sabiranja kvaterniona i* $\cdot$ *binarna operacija množenja kvaterniona jeste jedan nekomutativni prsten sa jedinicom. Tačnije, na osnovu leme 1.3. važi da je prsten kvaterniona* $(\mathbb{H}, +, \cdot)$ *jedno telo (polje bez komutativnosti).*

Posledica 1.1. *(Multiplikativnost norme) Neka su* $q_1, q_2 \in \mathbb{H}$ *proizvoljni. Tada važi:*

$$N(q_1q_2) = N(q_1)N(q_2).$$

Dokaz. Prema definiciji norme leva strana jednakosti je jednaka:

$$N(q_1q_2) = |q_1q_2|^2 = (q_1q_2)\overline{(q_1q_2)}.$$

Koristeći $\overline{q_1q_2} = \overline{q_2}\;\overline{q_1}$ i asocijativnost množenja u $\mathbb{H}$ dobijamo:

$$N(q_1q_2) = (q_1q_2)(\overline{q_1q_2}) = q_1(q_2\overline{q_2})\overline{q_1} = q_1|q_2|^2\overline{q_1}$$

Kako je norma kvaterniona realan broj, možemo pisati:

$$N(q_1q_2) = q_1\overline{q_1}|q_2|^2 = |q_1|^2|q_2|^2 = N(q_1)N(q_2).$$

□

1.2 Algebra sa deljenjem

Definicija 1.11. *Asocijativna algebra nad poljem $\mathbb{F}$ je vektorski prostor nad $\mathbb{F}$ na kojem je definisano bilinearno preslikavanje $m : A \times A \to A, m(a,b) = ab$, koje zadovoljava $a(bc) = (ab)c$ za sve $a, b, c \in A$.*

Preslikavanje $m : A \times A \to A$ nazivamo množenje u algebri A. Bilinearnost množenja povlači da za sve $a, b, c \in A$ i $\lambda \in \mathbb{F}$ važi:

(i) (a+b)c=ac+bc,

(ii) a(b+c)=ab+ac,

(iii) a(λb)=a(λb)=λ(ab).

Asocijativnost i distributivnost množenja povlači da je A prsten u kome su sabiranje i množenje isti kao u algebri A.

Definicija 1.12. *Kažemo da je A unitalna algebra ili algebra sa jedinicom ako postoji element $1 \in A$ takav da je $1a = a1 = a$ za svaki $a \in A$.*

Algebra A je komutativna ako je $ab = ba$ za svaki $a, b \in A$. Dimenzija algebre A je dimenzija vektorskog prostora A nad poljem $\mathbb{F}$. Element $a \in A$ je invertibilan ako postoji $b \in A$ za koji je $ab = ba = 1$.

Definicija 1.13. *Asocijativna algebra A nad poljem $\mathbb{F}$ je algebra sa deljenjem ako je svaki element različit od nule invertibilan.*

Prema teoremi 1.1. važi da je $(\mathbb{H}, +, *)$ realan vektorski prostor, gde $+$ predstavlja operaciju sabiranja kvaterniona, a $*$ predstavlja množenje skalarom. Takođe, prema tvrđenju 1.2. važi da je $(\mathbb{H}, +, \cdot)$ nekomutativan prsten sa jedinicom, pri čemu operacija $\cdot$ predstavlja množenje kvaterniona. Algebarska struktura $(\mathbb{H}, +, \cdot, *)$ predstavlja asocijativnu algebru. Kako smo takođe utvrdili da svaki element skupa $\mathbb{H}$ različit od nule ima inverz, ona predstvalja i algebru sa deljenjem. Dimenzija vektorskog prostora je 4, pa je ova algebra sa deljenjem konačnodimenzionalna.
Algebre sa deljenjem nad poljem realnih brojeva nazivamo $\mathbb{R}$-algebrama. Frobenijusova teorema tvrdi da na izomorfizam postoje tri konačnodimenzionalne algebre sa deljenjem nad poljem $\mathbb{R}$.

Teorema 1.2. *Ako je A konačnodimenzionalna algebra sa deljenjem nad poljem $\mathbb{R}$, onda*

$$A \cong \mathbb{R},\ A \cong \mathbb{C} \text{ ili } A \cong \mathbb{H}.$$

Dimenzije ovih $\mathbb{R}$-algebri sa deljenjem su $\dim(\mathbb{R}) = 1$, $\dim(\mathbb{C}) = 2$ i $\dim(\mathbb{H}) = 4$. Među ovim algebrama jedino $\mathbb{H}$ nije komutativna.

Definicija 1.14. *Algebra nad poljem $\mathbb{R}$ za čija svaka dva elementa a_1 i a_2 važi $|a_1 a_2|^2 = |a_1|^2 |a_2|^2$ naziva se normirana algebra.*

Dokazom posledice 1.1. ujedno smo pokazali i da je algebra kvaterniona jedna normirana algebra.

1.3 Identifikacija kvaterniona sa matricama dimenzije 2x2

Identifikovaćemo određene kvaternionske algebre sa algebrama matrica dimenzije 2x2 nad poljem. Iako će nas posebno zanimati konačno polje F_q, ovu identifikaciju možemo definisati nad opštijim poljima.

Najpre ćemo se podsetiti karakteristike prstena.

Definicija 1.15. *Neka je R prsten. Pretpostavimo da postoji prirodan broj m takav da je $ma = 0$ za svaki element $a \in R$. Najmanji takav prirodni broj naziva se karakteristikom prstena R. Ako takav broj ne postoji, onda kažemo da R ima karateristiku nula.*

Dakle, karakteristika prstena je ili nula ili najmanji pozitivan ceo broj m, takav da važi

$$0 = m \cdot 1 = 1 + 1 + ... + 1 \text{ } (m \text{ puta}).$$

Teorema 1.3. *Neka je F polje. Tada je karakteristika polja F nula ili prost broj.*

Polja $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su polja sa karakteristikom nula, dok za bilo koje $q = p^l$, konačno polje $\mathbb{F}_q$ ima karakteristiku p. Na osnovu ovoga imamo tvrđenje.

Tvrđenje 1.3. *Neka je K polje sa karakteristikom različitom od 2. Pretpostavimo da postoje $x, y \in K$, takvi da važi $x^2 + y^2 + 1 = 0$. Tada je $\mathbb{H}(K)$ izomorfan algebri $M_2(K)$ (2x2 matrica) nad poljem K.*

Dokaz. Neka je funkcija: $\psi : \mathbb{H}(K) \to M_2(K)$ definisana sa

$$\psi(a + bi + cj + dk) = \begin{pmatrix} a + bx + dy & -by + c + dx \\ -by - c + dx & a - bx - dy \end{pmatrix},$$

gde su $x, y \in K$, takvi da važi $x^2 + y^2 + 1 = 0$.
Proveravamo da važi $\psi(q_1 q_2) = \psi(q_1)\psi(q_2)$ za $q_1, q_2 \in \mathbb{H}\,(K)$.
Prvo ćemo izračunati obe strane jednkosti. Za $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$, gde su $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2 \in K$ imamo:

$$\begin{aligned} \psi(q_1 q_2) &= \psi((a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k)) \\ &= \psi((a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i \\ &+ (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) k) \end{aligned}$$

Radi lakšeg računanja, uvedimo sledeće oznake:

$$\begin{aligned} A &= a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2, \\ B &= a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2, \\ C &= a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2, \\ D &= a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2. \end{aligned}$$

Tada je funkcija $\psi(q_1 q_2)$ jednaka

$$\psi(A + Bi + Cj + Dk) = \begin{pmatrix} A + Bx + Cy & -By + C + Dx \\ -By - C + Dx & A - Bx - Dy \end{pmatrix}$$

Sada računamo desnu stranu jednakosti $\psi(q_1 q_2) = \psi(q_1)\psi(q_2)$.

$$\psi(q_1)\psi(q_2) = \psi(a_1 + b_1 i + c_1 j + d_1 k)\psi(a_2 + b_2 i + c_2 j + d_2 k)$$

$$= \begin{pmatrix} a_1 + b_1 x + d_1 y & -b_1 y + c_1 + d_1 x \\ -b_1 y - c_1 + d_1 x & a_1 - b_1 x - d_1 y \end{pmatrix} \begin{pmatrix} a_2 + b_2 x + d_2 y & -b_2 y + c_2 + d_2 x \\ -b_2 y - c_2 + d_2 x & a_2 - b_2 x - d_2 y \end{pmatrix}.$$

Ako pomnožimo prvi red prve matrice i drugu kolonu druge matrice dobićemo da važi

$$\begin{aligned} & (a_1 + b_1 x + d_1 y)(-b_2 y + c_2 + d_2 x) + (-b_1 y + c_1 + d_1 x)(a_2 - b_2 x - d_2 y) \\ = & -(a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) y + (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) \\ + & (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) x \\ = & -By + C + Dx. \end{aligned}$$

Pažljivim računanjem možemo pokazati da su ovi izrazi za odgovarajuće elemente na obe strane zaista jednaki, što znači da važi $\psi(q_1 q_2) = \psi(q_1)\psi(q_2)$ za sve kvaternione $q_1, q_2 \in \mathbb{H}(K)$.

Sada hoćemo da pokažemo da je ψ K-linearno preslikavanje između dva K-vektorska prostora, tj. da za svako $\alpha \in K$ i svaki kvaternion $q, q_1, q_2 \in \mathbb{H}(K)$ važi:

(i) $\psi(q_1+q_2) = \psi(q_1) + \psi(q_2)$ (aditivnost);

(ii) $\psi(\alpha q_1) = \alpha\psi(q_1)$ (homogenost).

Prvo ćemo pokazati da važi aditivnost. Za $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$, imamo:

$$\begin{aligned}
\psi(q_1+q_2) &= \psi((a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k) \\
&= \psi((a_1+b_1 i+c_1 j+d_1 k)+(a_2+b_2 i+c_2 j+d_2 k)) \\
&= \psi(a_1+b_1 i+c_1 j+d_1 k)+\psi(a_2+b_2 i+c_2 j+d_2 k) \\
&= \psi(q_1)+\psi(q_2).
\end{aligned}$$

Zatim, pokažimo da važi homogenost. Za $q = a + bi + cj + dk$, imamo:

$$\begin{aligned}
\psi(\alpha q) &= \psi(\alpha a + \alpha b i + \alpha c j + \alpha d k) \\
&= \psi(\alpha(a+bi+cj+dk)) \\
&= \alpha\psi(a+bi+cj+dk) \\
&= \alpha\psi(q).
\end{aligned}$$

Odavde možemo zaključiti da je ψ K-linearno preslikavanje između dva K-vektorska prostora iste dimenzije 4. Kako bismo dokazali da je ψ izomorfizam, dovoljno je pokazati da je ψ injektivno preslikavanje. Kako uslov $\psi(a+bi+cj+dk) = 0$ dovodi do sistema od 4 homogene linearne jednačine sa promenljivima a, b, c, d, čija je determinanta

$$\begin{vmatrix}
1 & x & 0 & y \\
0 & -y & 1 & x \\
0 & -y & -1 & x \\
1 & -x & 0 & -y
\end{vmatrix}$$

jednaka $-4(x^2+y^2) = 4 \neq 0$ (jer je karakteristika polja K različita od 2), na osnovu čega zaključujemo da je matrica regularna (ima svoju inverznu matricu), što znači da postoji jednoznačno rešenje sistema, pa je ψ injektivno preslikavanje. Ovim smo pokazali da je ψ izomorfizam između $\mathbb{H}(K)$ i $M_2(K)$, čime je tvrđenje dokazano. $\square$

Za prelikavanje $\psi : \mathbb{H}(K) \to M_2(K)$ definisano u dokazu tvrđenja 1.3. i $q \in \mathbb{H}(K)$ možemo pokazati da važi:

(a) $\det \psi(q) = N(q)$ i $\mathrm{Tr}\psi(q) = q + \overline{q}$;

(b) ψ preslikava realne kvaternione (one za koje važi $q = \overline{q}$) u skalarnu matricu.

(a) Neka je $q = a + bi + cj + dk$. Tada je $N(q) = a^2 + b^2 + c^2 + d^2$, a kako je determinanta jednaka

$$\begin{aligned}
\det \psi(q) &= \det \begin{vmatrix} a + bx + dy & -by + c + dx \\ -by - c + dx & a - bx - dy \end{vmatrix} \\
&= (a + bx + dy)(a - bx - dy) - (-bx + c + dx)(-by - c + dx) \\
&= a^2 - b^2x^2 - d^2y^2 - b^2y^2 + c^2 - d^2x^2 \\
&= a^2 + c^2 - d^2(x^2 + y^2) - b^2(x^2 + y^2) \\
&= a^2 + b^2 + c^2 + d^2,
\end{aligned}$$

možemo zaključiti da važi jednakost $\det \psi(q) = N(q)$.

Sada pokažimo da važi $\mathrm{Tr}\psi(q) = q + \overline{q}$. Po definiciji traga matrice imamo da je $\mathrm{Tr}\psi(q) = a + bx + dy + a - bx - dy = 2a = q + \overline{q}$.

(b) Potrebno je da pokažemo da za kvaternion $q = a$, tj. čisti realni kvaternion, $\psi(q)$ je skalarna matrica.
Računamo $\psi(q)$ za $q = a$

$$\psi(q) = \psi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

Ovo je očigledno skalarna matrica. Dakle ψ preslikava realne kvaternione u skalarnu matricu.

Tvrđenje 1.3. važi ne samo za algebarski zatvorena polja, već i za bilo koje konačno polje $\mathbb{F}_q$, gde je q stepen neparnog prostog broja.

Tvrđenje 1.4. *Neka je q stepen neparnog prostog broja. Postoje $x, y \in \mathbb{F}_q$, takvi da važi $x^2 + y^2 + 1 = 0$.*

Prvi dokaz (Nekonstruktivan). Definišimo

$$A_+ = \left\{1 + x^2 : x \in \mathbb{F}_q\right\}; \;\; A_- = \left\{-y^2 : y \in \mathbb{F}_q\right\}.$$

Ako posmatramo brojeve iz skupa A_+

$$1 + 0^2, 1 + 1^2, 1 + 2^2, ..., 1 + (\frac{q-1}{2})^2,$$

videćemo da među njima ne postoje dva broja koja su kongruentna modulo q. Isto važi i za brojeve iz skupa A_-

$$-0^2, -1^2, -2^2, ..., -(\frac{q-1}{2})^2.$$

Odavde imamo da je $|A_+| = |A_-| = \dfrac{q+1}{2}$, što je ukupno $\dfrac{q+1}{2} + \dfrac{q+1}{2} = q+1$ brojeva, pa prema Dirihleovom principu, dva među njima daju isti ostatak pri deljenju sa q.
Prema tome, imamo $A_+ \cap A_- \neq \emptyset$, što znači da postoje $x, y \in \{0, 1, 2, ...(\dfrac{q-1}{2})\}$ takvi da je $1 + x^2 \equiv -y^2 \pmod q$. $\square$

Drugi dokaz (Konstruktivan). Dovoljno je dokazati tvrđenje za polje $\mathbb{F}_p$ (p neparan prost broj). Ako je -1 kvadrat modulo p, uzmemo najmanji x iz skupa $\{2, ..., p-2\}$, takav da $x^2 + 1 = 0$, i $y = 0$.
Ako -1 nije kvadrat modulo p, neka a bude najveći kvadratni ostatak iz skupa $\{1, ..., p-2\}$. Koristeći Ležandrov simbol, pokažimo da je tada i $-a-1$ kvadrat modulo p. Kako -1 i $a+1$ nisu kvadrati modulo p važi $(\dfrac{-1}{p}) = -1$ i $(\dfrac{a+1}{p}) = -1$, pa je

$$(\frac{-a-1}{p}) = (\frac{-1}{p})(\frac{a+1}{p}) = 1,$$

što pokazuje da je $-a-1$ kvadrat modulo p. Neka x (odnosno y) bude najmanji element iz skupa $\{1, ..., p-2\}$ takav da $x^2 \equiv a \pmod p$ (odnosno $y^2 \equiv -a-1 \pmod p$). Tada $x^2 + y^2 + 1 \equiv 0 \pmod p$. $\square$

1.4 Kvaternioni sa celobrojnim koeficijentima

Hurvicovi kvaternioni su podskup kvaterniona čiji su koeficijenti ili svi celi brojevi ili sve polovine neparnih celih brojeva. Skup svih Hurvicovih kvaterniona je

$$\mathcal{H} = \{a + bi + cj + dk \in \mathbb{H} : a, b, c, d \in \mathbb{Z} \text{ ili } a, b, c, d \in \mathbb{Z} + \frac{1}{2}\}.$$

Kako bismo pokazali da je $\mathcal{H}$ zatvoren u odnosu na množenje kvaterniona, razmotrićemo tri slučaja:

(i) Množenje dva kvaterniona čiji su koeficijenti celi brojevi;

(ii) Množenje dva kvaterniona od kojih je jedan kvaternion sa celobrojnim koeficijentima, a drugi sa polovinama neparnih celih brojeva;

(iii) Množenje dva kvaterniona čiji su svi koeficijenti polovine neparnih celih brojeva.

Razmotrimo prvo prvi slučaj. Neka su $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$ kvaternioni, gde su $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2$ celi brojevi. Njihov proizvod je:

$$\begin{aligned} q_1 \cdot q_2 &= (a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k) \\ &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i \\ &+ (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) k. \end{aligned}$$

Kako su $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2$ celi brojevi, svi izrazi $a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2, a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2, a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2, a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2$ su takođe celi brojevi, pa je proizvod ova dva kvaterniona kvaternion sa celobrojnim koeficijentima.

Neka su $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = \frac{1}{2}a_2 + \frac{1}{2}b_2 i + \frac{1}{2}c_2 j + \frac{1}{2}d_2 k$ kvaternioni, gde su a_1, b_1, c_1, d_1 celi brojevi, a a_2, b_2, c_2, d_2 neparni celi brojevi. Pa je proizvod ova dva kvaterniona:

$$\begin{aligned} q_1 \cdot q_2 &= (a_1 + b_1 i + c_1 j + d_1 k) \cdot (\frac{1}{2}a_2 + \frac{1}{2}b_2 i + \frac{1}{2}c_2 j + \frac{1}{2}d_2 k) \\ &= \frac{1}{2}(a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + \frac{1}{2}(a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i \\ &+ \frac{1}{2}(a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) j + \frac{1}{2}(a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) k. \end{aligned}$$

Da bismo pokazali da su sve komponente proizvoda istog oblika, dakle da su sve celi brojevi ili sve polovine neparnih celih brojeva, treba proveriti da li su brojevi $a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2$, $a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2$, $a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2$, $a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2$ iste parnosti. Pošto su a_2, b_2, c_2, d_2 neparni to je parnost broja $a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2$ ista kao i parnost broja $a_1 - b_1 - c_1 - d_1$, a ova je pak ista kao i parnost broja $a_1 + b_1 + c_1 + d_1$. A zapravo su takve parnosti i ostali zbirovi u zagradama, te su svi ili parni ili neparni, pa su sve komponente proizvoda ili celi brojevi ili polovine neparnih celih brojeva.

Neka su $q_1 = \frac{1}{2}a_1 + \frac{1}{2}b_1i + \frac{1}{2}c_1j + \frac{1}{2}d_1k$ i $q_2 = \frac{1}{2}a_2 + \frac{1}{2}b_2i + \frac{1}{2}c_2j + \frac{1}{2}d_2k$ kvaternioni, gde su $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2$ neparni celi brojevi. Proizvod ova dva kvaterniona je:

$$
\begin{aligned}
q_1 \cdot q_2 &= (\frac{1}{2}a_1 + \frac{1}{2}b_1i + \frac{1}{2}c_1j + \frac{1}{2}d_1k) \cdot (\frac{1}{2}a_2 + \frac{1}{2}b_2i + \frac{1}{2}c_2j + \frac{1}{2}d_2k) \\
&= \frac{1}{4}(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + \frac{1}{4}(a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i \\
&+ \frac{1}{4}(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j + \frac{1}{4}(a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k.
\end{aligned}
$$

Slično kao u prethodnom slučaju, i ovde proveravamo da li su brojevi $a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2$, $a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2$, $a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2$, $a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2$ istog oblika. Parnost brojeva $a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2$, $a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2$, $a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2$, $a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2$ je ista kao i parnost brojeva $a_1 - b_1 - c_1 - d_1$, $a_2 - b_2 - c_2 - d_2$, a kako su $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2$ neparni celi brojevi, svi ovi zbirovi i razlike su parni brojevi, pa su svi koeficijenti proizvoda celi brojevi ili polovine neparnih celih brojeva. Ostaje još da proverimo kada su koeficijenti proizvoda celi brojevi a kada polovine neparnih celih brojeva.
Pošto su $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2$ neparni celi brojevi, svi oni se mogu zapisati u obliku $2n + 1, n \in \mathbb{Z}$. Ako se neparan broj ovih brojeva može zapisati u obliku $4n + 1, n \in \mathbb{Z}$, onda su svi koeficijenti proizvoda celi brojevi, a u suprotnom koeficijenti proizvoda su polovine neparnih celih brojeva.

Ovim smo pokazali da su sva tri slučaja zadovoljena što znači da je skup $\mathcal{H}$ zatvoren za množenje. Kako je skup $\mathcal{H}$ zatvoren i u odnosu na sabiranje kvaterniona, skup $\mathcal{H}$ predstavlja potprsten svih kvaterniona $\mathbb{H}$.

Skup svih kvaterniona sa celobrojnim koeficijentima

$$\mathbb{H}(\mathbb{Z}) = \{a + bi + cj + dk \in \mathbb{H} : a, b, c, d \in \mathbb{Z}\}$$

predstavlja podprsten Hurvicovih kvaterniona $\mathcal{H}$.

Posledica 1.2. *Za proizvoljne cele brojeve a_1, b_1, c_1, d_1 i a_2, b_2, c_2, d_2 postoje celi brojevi A, B, C, D takvi da važi*

$$(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = (A^2 + B^2 + C^2 + D^2).$$

Dokaz. Neka su a_1, b_1, c_1, d_1 i a_2, b_2, c_2, d_2 proizvoljni celi brojevi. Tada oni određuju i dva kvaterniona $q_1, q_2 \in \mathbb{H}(\mathbb{Z}), q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$. Proizvod ova dva kvaterniona je jednak

$$q_1 q_2 = A + Bi + Cj + Dk,$$

gde su $A, B, C, D \in \mathbb{Z}$. Prema poseledici 1.1. imamo

$$N(q_1 q_2) = N(q_1) N(q_2),$$

tj.

$$(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = (A^2 + B^2 + C^2 + D^2),$$

što dokazuje tvrđenje. $\square$

Za $q \in \mathbb{H}(\mathbb{Z})$ dokažimo da su sledeća svojstva ekvivalentna:

(a) q je invertibilan u $\mathbb{H}(\mathbb{Z})$

(b) $N(q) = 1$

(c) $q \in \{\pm 1, \pm i, \pm j, \pm k\}$.

Dokazujemo implikacije u obe strane redom.

$((a) \Rightarrow (b))$ Pretpostavimo da je q inverbibilan u $\mathbb{H}(\mathbb{Z})$, tj. postoji $r \in \mathbb{H}(\mathbb{Z})$ tako da je $qr = rq = 1$. Ovo implicira da je $N(q)N(r) = N(qr) = N(1) = 1$, što znači da je $N(q) = 1$.

$((b) \Rightarrow (c))$ Pretpostavimo da je $N(q) = 1$, a kako je $N(q) = a^2 + b^2 + c^2 + d^2$, imamo $a^2 + b^2 + c^2 + d^2 = 1$. S obzirom na to da su sva četiri kvadrata pozitivna ili nula, to znači da samo jedan koeficijent može biti različit od nule, a svi ostali su nule. To znači da je q jedan od kvaterniona iz skupa $\{\pm 1, \pm i, \pm j, \pm k\}$.

$((c) \Rightarrow (a))$ Pretpostavimo da je q jedan od kvaterniona iz skupa $\{\pm 1, \pm i, \pm j, \pm k\}$. Inverz od svakog od navedenih q je jednak $-q$, sem u slučaju kada je $q \in \{\pm 1\}$ kada je inverz jednak samom q.

Aritmetika celobrojnih kvaterniona

Sada ćemo se ograničiti na prsten $\mathbb{H}(\mathbb{Z})$ i istražiti neka aritmetička svojstva ovog konkretnog prstena. Njegova važnost proizlazi iz činjenice da je ceo broj zbir četiri kvadrata ako i samo ako je taj broj norma nekog kvaterniona u $\mathbb{H}(\mathbb{Z})$. U prethodnom podglavlju videli smo da su ± 1, $\pm i$, $\pm j$, $\pm k$ invertibilni elementi ili jedinice. Kao i u $\mathbb{Z}$ i $\mathbb{Z}[i]$, postoji faktorizacija na proste brojeve za svaki celobrojni kvaternion, mada u $\mathbb{H}(\mathbb{Z})$ ova faktorizacija više nije jedinstvena. Pokazaćemo da kao nekomutativan prsten, $\mathbb{H}(\mathbb{Z})$ poseduje modifikovani Euklidov algoritam i odgovarajuće najveće zajedničke delioce sa desne i leve strane koji su jedinstveni do na asocijativnost. Tada ćemo videti da nijedan prost broj ne ostaje prost u $\mathbb{H}(\mathbb{Z})$, već se može razložiti u proizvod dva konjugovana prosta kvaterniona. U stvari, određivanjem da li je celobrojni kvaternion prost broj je krajnje jednostavno: $\alpha \in \mathbb{H}(\mathbb{Z})$ je prost ako i samo ako je $N(\alpha)$ prost u $\mathbb{Z}$. Ovo predstavlja suprotnost u odnosu na situaciju u $\mathbb{Z}[i]$, gde bilo koji prost broj $q \equiv 3 \pmod 4$ ostaje prost, i ako ima Gausovu normu $N(q) = q^2$. Započnimo sa sledećom definicijom.

Definicija 2.16. **(a)** *Kvaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ je neparan (odnostno paran) ako je $N(\alpha)$ neparan (odnosno paran) ceo broj.*

(b) *Kvatarnion $\alpha \in \mathbb{H}(\mathbb{Z})$ je prost ako α nije jedinica u $\mathbb{H}(\mathbb{Z})$, i ako, kad je $\alpha = \beta\gamma$ u $\mathbb{H}(\mathbb{Z})$, tada je ili β ili γ jedinica.*

(c) *Dva kvatarniona α, $\alpha^{'} \in \mathbb{H}(\mathbb{Z})$ su asocirani ako postoje jedinični kvaternioni ϵ, $\epsilon^{'} \in \mathbb{H}(\mathbb{Z})$ takvi da je $\alpha^{'} = \epsilon\alpha\epsilon^{'}$.*

(d) *$\delta \in \mathbb{H}(\mathbb{Z})$ je desni delilac broja $\alpha \in \mathbb{H}(\mathbb{Z})$ ako postoji $\gamma \in \mathbb{H}(\mathbb{Z})$, tako da je $\alpha = \gamma\delta$.*

Budući da je za svaku jedinicu ϵ vrednost $N(\epsilon)$ jednaka 1, asocijativnost predstavlja relaciju ekvivalencije među elementima u $\mathbb{H}(\mathbb{Z})$ koja čuva aritmetička svojstva kao što su parnost, neparnost, biti prost broj i svojstvo jedinice.

Podsetimo se da smo za prstene $\mathbb{Z}$ i $\mathbb{Z}[i]$ mogli koristiti Bezuovu relaciju kako bismo od definicije prostog broja kao ireducibilnog elementa prešli na sledeće: π je prost broj ako i samo ako svaki put kad π deli proizvod xy, tada π deli x ili π deli y. Međutim, to ne možemo da primenimo na prsten $\mathbb{H}(\mathbb{Z})$, jer desni delilac proizvoda xy ne mora nužno biti mogući desni delilac broja x. Na primer, broj $2+5i \in \mathbb{H}(\mathbb{Z})$ deli proizvod $(4+3i+2j)(4-3i-2j) = 29 = (2+5i)(2-5i)$, ali ne deli činioce $4+3i+2j$ i $4-3i-2j$. Stoga, moraćemo da nastavimo bez te osobine za proste brojeve u $\mathbb{H}(\mathbb{Z})$. Ipak, definicija prostih brojeva 2.16. nam pruža mogućnost faktorizacije u proste kvaternione.

Tvrđenje 2.5. *Svaki nenula i neinvertibilan kvaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ je proizvod prostih kvaterniona.*

Dokaz. Indukcijom po $N(\alpha)$, slučaj $N(\alpha) = 1$ (tj. α je invertibilan) je trivijalan. Pretpostavimo sada $N(\alpha) > 1$. Ako je α prost, nema ništa za dokazivanje. Inače, nađemo razlaganje $\alpha = \beta\gamma$, gde ni β, ni γ nisu invertibilni u $\mathbb{H}(\mathbb{Z})$. Dakle, β i γ zadovoljavaju $N(\beta) < N(\alpha)$, $N(\gamma) < N(\alpha)$. Prema indukcijskoj hipotezi, β i γ su proizvodi prostih kvaterniona, isto važi i za α. $\square$

Razlaganje u tvrđenju nije nužno jedinstveno (čak ni do na asocijativnost). Na primer:

$$13 = (1+2i+2j+2k)(1-2i-2j-2k) = (3+2i)(3-2i)$$

su dva zaista različita razlaganja broja 13 na proste kvaternione. To znači da odgovarajući faktori nisu asocirani, tj. ne postoje jedinični kvaternioni $\epsilon, \epsilon' \in \mathbb{H}(\mathbb{Z})$ takvi da je jedan faktor jednak proizvodu drugog faktora i jediničnog kvaterniona. Ako postoji takav jedinični kvaternion, onda bi trebalo da možemo dobiti jedan faktor iz drugog faktora pomnoženog s jediničnim kvaternionom. Međutim, to nije moguće jer se izrazi $(1+2i+2j+2k)$ i $(3+2i)$ ne mogu pomnožiti s jedničnim kvaternionom kako bi se dobila drugačija forma. Stoga, na osnovu ovoga možemo zaključiti da odgovarajući faktori broja 13 nisu asocirani u prstenu $\mathbb{H}(\mathbb{Z})$ i zbog toga su ova dva razlaganja broja 13 različita.

Nastavljamo s delimičnim Euklidovim algoritmom, tj onim koji se ograničava na neparne kvaternione i množenje s desne strane. Analogan rezultat važi i za množenje s leve strane, ali pripadajući γ_1 i δ_1 nisu nužno isti. Koristićemo ovaj desni Euklidov algoritam za konstrukciju najvećeg zajedničkog desnog delioca, ali očigledne modifikacije u dokazima vode do ekvivalentnih rezultata za levi delilac.

Lema 2.4. *Neka su α i $\beta \in \mathbb{H}(\mathbb{Z})$, pri čemu je β neparan broj. Postoje γ, $\delta \in \mathbb{H}(\mathbb{Z})$ takvi da važi*

$$\alpha = \gamma\beta + \delta \ i \ N(\delta) < N(\beta).$$

Dokaz.
Počinjemo sa tvrđenjem:
Dato je $\sigma = s_0 + s_1 i + s_2 j + s_3 k \in \mathbb{H}(\mathbb{Z})$, a m je neparan pozitivan ceo broj. Tada postoji $\gamma \in \mathbb{H}(\mathbb{Z})$, takav da važi $N(\sigma - \gamma m) < m^2$. Za svaki s_i možemo naći $r_i \in \mathbb{Z}$, tako da

$$mr_i - \frac{m}{2} < s_i < mr_i + \frac{m}{2}$$

(važi stroga nejednakost jer je m neparan). Pišemo $s_i = mr_i + t_i$, gde je $|t_i| < \frac{m}{2}$. Postavljamo $\gamma = r_0 + r_1 i + r_2 j + r_3 k$; tada je $N(\sigma - \gamma m) = t_0^2 + t_1^2 + t_3^2 < 4(\frac{m}{2})^2 = m^2$, što dokazuje tvrđenje.
Da bismo dokazali lemu, postavimo $m = N(\beta) = \beta\overline{\beta}$ i $\sigma = \alpha\overline{\beta}$. Prema tvrđenju, možemo naći $\gamma \in \mathbb{H}(\mathbb{Z})$, takav da važi

$$N(\beta)N(\overline{\beta}) = N(\beta)^2 = m^2 > N(\sigma - \gamma m) = N(\alpha\overline{\beta} - \gamma\beta\overline{\beta}) = N(\alpha - \gamma\beta)N(\overline{\beta}).$$

Postavljamo $\delta = \alpha - \gamma\beta$ i deljenjem sa $N(\overline{\beta})$, dobijamo $N(\delta) < N(\beta)$, kao što je i traženo. □

Primer 2.1. *Neka su dati kvaternioni $\alpha = 2+i+3j+k$ i $\beta = 2i-j$. Prateći dokaz leme pokazaćemo da za njih važi lema o deljenju sa ostatkom. Vidimo da je β neparan kvaternion jer je $N(\beta) = 5$, pa je uslov iz leme ispunjen i važi $m = N(\beta) = 5$.*
Najpre računamo:

$$\sigma = \alpha\overline{\beta} = (2+i+3j+k)(-2i+j) = (-1-5i+7k).$$

Tražimo kvaternion $\gamma = r_0+r_1i+r_2j+r_3k$, takav da su koeficijenti $r_0, r_1, r_2, r_3 \in \mathbb{Z}$ i da važe nejednakosti:

$$\begin{aligned}
|-1-5r_0| &< \frac{5}{2} \Rightarrow -\frac{5}{2} < -1-5r_0 < \frac{5}{2} \Rightarrow -\frac{7}{10} < r_0 < \frac{3}{10} \Rightarrow r_0 = 0,\\
|-5-5r_1| &< \frac{5}{2} \Rightarrow -\frac{5}{2} < --5-5r_1 < \frac{5}{2} \Rightarrow -\frac{3}{2} < r_1 < -\frac{1}{2} \Rightarrow r_1 = -1,\\
|-5r_2| &< \frac{5}{2} \Rightarrow -\frac{5}{2} < -5r_2 < \frac{5}{2} \Rightarrow -\frac{1}{2} < r_2 < \frac{1}{2} \Rightarrow r_2 = 0,\\
|7-5r_3| &< \frac{5}{2} \Rightarrow -\frac{5}{2} < 7-5r_3 < \frac{5}{2} \Rightarrow \frac{9}{10} < r_3 < \frac{19}{10} \Rightarrow r_3 = 1,\\
\Rightarrow \quad & \gamma = -i+k.
\end{aligned}$$

Možemo proveriti da je $N(\sigma - \gamma m) = N(-1+2k) = 5 < m^2$.

$\delta = \alpha - \gamma\beta = (2+i+3j+5) - (-i+k)(2i-j) = 2+i+3j+k-(2+k+2j+i) = j,$

pa je norma $N(\delta) = 1 < m$.
Tada je $\alpha = (-i+k)(2i-j) + j$.

Napomena 2.1. *Levi Euklidov algoritam obezbeđuje postojanje $\gamma_1, \delta_1 \in \mathbb{H}(\mathbb{Z})$, takvih da važi $\alpha = \beta\gamma_1 + \delta_1$, pri čemu je $N(\delta_1) < N(\beta)$.*

Definicija 2.17. *Neka su α i β celobrojni kvaternioni. Kažemo da je $\delta \in \mathbb{H}(\mathbb{Z})$ desni najveći zajednički delilac od α i β ako*

(a) *δ je desni delilac od α i β;*

(b) *ako je $\delta_0 \in \mathbb{H}(\mathbb{Z})$ desni delilac i α i β, tada je δ_0 i desni delilac od δ.*

Takvo δ označavamo sa $(\alpha, \beta)_D$.

Primer 2.2. *Odredimo pomoću Euklidovog algoritma desni najveći zajednički delilac za kvaternione $\alpha = 3+2i+j-k$ i $\beta = 1+2i$. Najpre podelimo ove kvaternione. Prilikom deljenja ovih kvaterniona imaćemo i ostatak.*

$$\alpha\beta^{-1} = \alpha\frac{\overline{\beta}}{N(\beta)} = (3+2i+j-k)\frac{1-2i}{5} = \frac{7}{5} - \frac{4}{5}i + \frac{3}{5}j + \frac{1}{5}k$$

Budući da koeficijenti kvaterniona $\alpha\beta^{-1}$ nisu svi u $\mathbb{Z}$, za količnik γ_1 možemo uzeti kvaternion sa celobrojnim koeficijentima koji su najbliži odgovarajućim koeficijentima kvaterniona $\alpha\beta^{-1}$, dakle stavimo

$$\gamma_1 = 1 - i + j$$

pa je ostatak δ_1 *dat sa*

$$\delta_1 = \alpha - \gamma_1\beta = (3 + 2i + j - k) - (1 - i + j)(1 + 2i) = i + k,\ N(\delta_1) = 2.$$

Imamo da važi jednakost

$$3 + 2i + j - k = (1 - i + j)(1 + 2i) + (i + k).$$

Podelimo β *sa* δ_1 *sa ostatkom. Imamo*

$$\beta\delta_1^{-1} = (1 + 2i)\frac{-i - k}{2} = 1 - \frac{1}{2}i + j - \frac{1}{2}k$$

Kao i u prethodnom koraku, za kvaternion γ_2 *možemo uzeti kvaternion sa celobrojnim koeficijentima, pa je*

$$\gamma_2 = 1 + j.$$

Ostatak je dat sa

$$\delta_2 = \beta - \gamma_2\delta_1 = (1 + 2i) - (1 + j)(i + k) = 1,\ N(\delta_2) = 1.$$

Prema tome imamo jednakost

$$1 + 2i = (1 + j)(i + k) + 1.$$

Sada delimo δ_1 *sa* δ_2.

$$\delta_1\delta_2^{-1} = i + k$$

Imamo

$$\gamma_3 = i + k.$$

$$\delta_3 = \delta_1 - \gamma_3\delta_2 = i + k - (i + k) = 0.$$

Jednakost glasi

$$i + k = (i + k) \cdot 1 + 0.$$

Kako je $\gamma_3 = 0$*, ovim je Euklidov algoritam završen. Desni najveći zajednički delilac za kvaternione* $\alpha = 3 + 2i + j - k$ *i* $\beta = 1 + 2i$ *je* $\delta_2 = 1$.

Jasno je da je $(\alpha, \beta)_D$ jedinstven, ukoliko postoji. Hoćemo da pokažemo da, pod pogodnim uslovima, $(\alpha, \beta)_D$ zaista postoji.

Lema 2.5. *Neka je* $\alpha \in \mathbb{H}(\mathbb{Z})$*. Tada* α *ima jedinstvenu faktorizaciju:*

$$\alpha = 2^l \pi \alpha_0,$$

gde je $l \in \mathbb{N}_0, \pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ *i* $\alpha_0 \in \mathbb{H}(\mathbb{Z})$ *neparan.*

Dokaz. Prvo ćemo dokazati da takva faktorizacija postoji, a zatim i njenu jedinstvenost.
Neka je $\alpha \in \mathbb{H}(\mathbb{Z})$ i 2^l najveći stepen broja 2 koji deli α i neka je $\alpha^{'} = \frac{\alpha}{2^l}$.
Tada pišemo

$$\alpha^{'} = a_0 + a_1 i + a_2 j + a_3 k,$$

gde je bar jedan od $a_i, i = 0, ..., 3$ neparan. Pošto množenje jedinicom menja poziciju $a_i, i = 0, ..., 3$, možemo pretpostaviti, bez gubitka opštosti, da je a_0 neparan broj. Sada, ako je $\alpha^{'}$ neparan, onda je $\alpha = 2^l \alpha^{'}$, pa smo lemu dokazali.
Stoga možemo pretpostaviti da je α' paran i tada postoje dva slučaja:

(a) $N(\alpha^{'}) \equiv 2 \pmod 4$.
Tada tačno dva a_i-a su neparna, pri čemu je a_0 među njima. Ako su recimo a_0 i a_1 neparni, tada

$$\alpha_0 = \frac{a_0 + a_1}{2} + (\frac{a_1 - a_0}{2})i + (\frac{a_2 + a_3}{2})j + (\frac{a_3 - a_2}{2})k$$

je u $\mathbb{H}(\mathbb{Z})$ neparan, i $\alpha^{'} = (1+i)\alpha_0$. Ostali slučajevi ($a_0$ i a_2 neparni, ili a_0 i a_3 neparni) dozvoljavaju faktorizaciju $1+j$ ili $1+k$ i tretiraju se na isti način.

(b) $N(\alpha^{'}) \equiv 0 \pmod 4$.
Onda su svi a_i neparni, i stoga kongruenti $\pm 1 \pmod 4$. U svakom slučaju, $N(\alpha^{'}) \equiv 4 \pmod 8$. U ovom slučaju moramo razmotriti moguće kombinacije kongruencija modulo 4, što načelno daje šesnaest različitih podslučajeva. Međutim, ovi slučajevi se mogu grupisati u dve grupe po osam podslučajeva, u zavisnosti od toga da li je ukupan broj a_i-ova koji su $a_i \equiv 1 \pmod 4$ paran ili neparan.

Tvrđenje A. Ako je $a_i \equiv 1 \pmod 4$, gde je ukupan broj takvih a_i-ova paran, tada postoji neparan kvaternion α_1, takav da je $\alpha^{'} = (1+i)(1+j)\alpha_1$.

Dokaz. Možemo pretpostaviti da je $a_0 \equiv 1 \pmod 4$. Pretpostavimo da su $a_0 \equiv a_1 \equiv 1 \pmod 4$ i $a_2 \equiv a_3 \equiv \pm 1 \pmod 4$. Kao i u slučaju (a) imamo $\alpha' = (1+i)\alpha_0$ gde je

$$\alpha_0 = \frac{a_0+a_1}{2} + (\frac{a_0-a_1}{2})i + (\frac{a_2+a_3}{2})j + (\frac{a_3-a_2}{2}).$$

Primetimo da su $\frac{a_0+a_1}{2}$ i $\frac{a_2+a_3}{2}$ neparni, dok su $\frac{a_0-a_1}{2}$ i $\frac{a_3-a_2}{2}$ parni. Prema slučaju (a) tada važi $\alpha_0 = (1+j)\alpha_1$, gde je α_1 neparan jer je $N(\alpha_0) \equiv 2 \pmod 4$. Dakle $\alpha' = (1+i)(1+j)\alpha_1$.
Pretpostavimo sada da je $a_0 \equiv a_2 \equiv 1 \pmod 4$ i $a_1 \equiv a_3 \equiv \pm 1 \pmod 4$. Postupajući kao i ranije možemo napisati $\alpha' = (1+j)(1+k)\alpha_1$, pri čemu je α_1 neparan. Tada primetimo da je $(1+j)(1+k) = (1+i)(1+j)$. Poslednji slučaj, $a_0 \equiv a_3 \equiv 1 \pmod 4$ i $a_1 \equiv a_2 \equiv \pm 1 \pmod 4$, se pokazuje na sličan način, koristeći $(1+k)(1+i) = (1+i)(1+j)$.

Tvrđenje B. Ako je $a_i \equiv 1 \pmod 4$, gde je ukupan broj takvih a_i-ova neparan, tada postoji neparan kvaternion α_1, takav da je $\alpha' = (1+i)(1-k)\alpha_1$.

Dokaz. Ponovo možemo pretpostaviti, bez gubitka opštosti, da su tri a_i-a

kongruentna $1 \pmod 4$, pri čemu je a_0 među njima. Ako je $a_0 \equiv a_1 \equiv a_2 \equiv 1 \pmod 4$ i $a_3 \equiv -1 \pmod 4$, tada kao u slučaju (a) imamo $\alpha' = (1+i)\alpha_0$ sa

$$\begin{aligned}\alpha_0 &= \frac{a_0+a_1}{2} + (\frac{a_0-a_1}{2})i + (\frac{a_2+a_3}{2})j + (\frac{a_3-a_2}{2})k \\ &= b_0 + b_1 i + b_2 j + b_3 k.\end{aligned}$$

Sada su b_0 i b_3 neparni, dok su b_1 i b_2 parni. Tada važi

$$\begin{aligned}\alpha_0 &= (1-k)(\frac{b_0+b_3}{2} + (\frac{b_1-b_2}{2})i + (\frac{b_1+b_2}{2})j + (\frac{b_0+b_3}{2})k) \\ &= (1-k)\alpha_1,\end{aligned}$$

α_1 je neparan. Dakle, $\alpha_0 = (1+i)(1-k)\alpha_1$. Preostali slučajevi se pokazuju analogno.

Sada dokazujemo jedinstvenost.
Pretpostavimo suprotno, tj. da postoje dve različite faktorizacije kvaterniona α u obliku $\alpha = 2^{l_1}\pi\alpha_0$ i $\alpha = 2^{l_2}\rho\alpha_1$, gde su $l_1, l_2 \in \mathbb{N}_0$, $\pi, \rho \in \{1, 1+i, 1+$

$j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ i $\alpha_0, \alpha_1 \in \mathbb{H}(\mathbb{Z})$ neparni kvaternioni. Koristimo normu kvaterniona da analiziramo faktore:

$$N(\alpha) = N(2^{l_1}\pi\alpha_0) = 2^{2l_1}N(\pi)N(\alpha_0)$$
$$N(\alpha) = N(2^{l_2}\rho\alpha_1) = 2^{2l_2}N(\rho)N(\alpha_1)$$

Iz jednakosti fakorizacija α imamo:

$$2^{2l_1}N(\pi)N(\alpha_0) = 2^{2l_2}N(\rho)N(\alpha_1).$$

Podelom obe strane jednačine sa $2^{2\min(l_1,l_2)}$, dobijamo:

$$2^{2(\max(l_1,l_2)-\min(l_1,l_2))}\frac{N(\pi)}{N(\rho)} = \frac{N(\alpha_1)}{N(\alpha_0)}.$$

Pretpostavimo, bez gubitka opštosti da je $l_1 \leq l_2$. Tada imamo:

$$2^{2(l_1-l_2)}\frac{N(\pi)}{N(\rho)} = \frac{N(\alpha_1)}{N(\alpha_0)}.$$

Kako su α_0 i α_1 neparni kvaternioni iz $\mathbb{H}(\mathbb{Z})$, zaključujemo da je eksponent $2(l_2 - l_1)$ jednak nuli, što implicira da je $l_1 = l_2$.

Sada pokazujemo jednakost faktora π i ρ. Pretpostavimo da je $\pi \neq \rho$. Kako su π i ρ kvaternioni iz skupa $\{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$, možemo da primetimo da su njihove norme stepeni broja 2, pa odnos normi kvaterniona π i ρ mora biti 1. Sa druge strane, razlika $\pi\alpha_0 - \rho\alpha_1$ je kvaternion čija je norma nula, a to znači da su kvaternioni α_0 i α_1 proporcionalni sa faktorom $\frac{\rho}{\pi}$. Međutim pošto su α_0 i α_1 naparni kvaternioni iz $\mathbb{H}(\mathbb{Z})$, ova pretpostavka je kontradiktorna. Stoga, zaključujemo da važi $\pi = \rho$.

Sada, kada znamo da su $\pi = \rho$ i $l_1 = l_2$, ostaje da pokažemo da su α_0 i α_1 jednaki kvaternioni. Razlika $\pi\alpha_0 - \rho\alpha_1$ mora biti nula kvaternion, što znači da je $\alpha_0 = \alpha_1$.

Na osnovu ovoga zaključujemo da faktorizacija $\alpha = 2^l\pi\alpha_0$, gde su $l \in \mathbb{N}_0$, $\pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ i $\alpha_0 \in \mathbb{H}(\mathbb{Z})$ neparan, zaista jeste jedinstvena. $\square$

Primer 2.3. *Neka je* $\alpha = 16 + 4i + 12j + 8k$ *kvaternion sa celobrojnim koeficijentima. Prateći dokaz leme 2.5. pokažimo da broj* α *ima jedinstvenu faktorizaciju* $\alpha = 2^l\pi\alpha_0$*, gde je* $l \in \mathbb{N}, \pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ *i* $\alpha_0 \in \mathbb{H}(\mathbb{Z})$ *neparan.. Kako je* $\alpha = 16+4i+12j+8k$ *paran* *kvaternion čiji su svi koeficijenti stepeni broja 2, lako možemo da zaključimo da je* $l = 2$. *Tada je*

$$\alpha^{'} = \frac{\alpha}{2^l} = \frac{1}{4}(16 + 4i + 12j + 8k) = 4 + i + 3j + 2k.$$

Kako je $N(\alpha^{'}) = 16 + 1 + 9 + 4 = 30 \equiv 2 \pmod 4$ *važi slučaj pod (a). Posmatrajmo koeficijente kvaterniona* $\alpha^{'}$. $a_0 = 4, a_1 = 1, a_2 = 3$ *i* $a_3 = 2$. *Kako su* a_0 *i* a_3 *parni, a* a_1 *i* a_2 *neparni, na osnovu dokaza leme zaključujemo da je* $\pi = 1 + k$ *i koristimo sledeću formulu kako bismo izračunali* α_0*:*

$$\begin{aligned} \alpha_0 &= \frac{a_0 + a_3}{2} + (\frac{a_1 + a_2}{2})i + (\frac{a_2 - a_1}{2})j + (\frac{a_3 - a_0}{2})k \\ &= 3 + 2i + j - k. \end{aligned}$$

Kako je $N(\alpha_0) = 9 + 4 + 1 + 1 = 15$, α_0 *je neparan kvaternion.*
Tada je $\alpha = 2^2(1 + k)(3 + 2i + j - k)$.

PRIMER 2.4. *Naći jedinstvenu faktorizaciju kvaterniona* $\alpha = 1 + 3i - j - 3k$. *Kao i u prethodnom primeru, koristimo dokaz leme 2.5. Odmah možemo videti da je* $l = 0$ *i* $\alpha^{'} = \alpha$. *Računajući normu kvaterniona* $\alpha^{'}$, $N(\alpha^{'}) = 20 \equiv 0 \pmod 4$, *zaključujemo da važi slučaj pod (b). Kako su koeficijenti kvaterniona* $\alpha^{'}$ *jednaki* $a_0 = 1 \equiv 1 \pmod 4$, $a_1 = 3 \equiv -1 \pmod 4$, $a_2 = -1 \equiv -1 \pmod 4$ *i* $a_3 = -3 \equiv 1 \pmod 4$, *vidimo da važi tvrđenje A. Za traženje kvaterniona* α_0 *koristimo formulu:*

$$\begin{aligned} \alpha_0 &= \frac{a_0 + a_3}{2} + (\frac{a_1 + a_2}{2})i + (\frac{a_2 - a_1}{2})j + (\frac{a_3 - a_0}{2})k \\ &= -1 + i - 2j - 2k. \end{aligned}$$

Sada, kako je $N(\alpha_0) = 10 \equiv 2 \pmod 4$, *koristimo pravila slučaja pod (a) kako bismo izračunali* α_1. *Koeficijenti kvaterniona* α_0 *su* $b_0 = -1$, $b_1 = 1$, $b_2 = -2$ *i* $b_3 = -2$, *pa je:*

$$\begin{aligned} \alpha_1 &= \frac{b_0 + b_1}{2} + (\frac{b_1 + b_0}{2})i + (\frac{b_2 + b_3}{2})j + (\frac{b_3 - b_2}{2})k \\ &= i - 2j. \end{aligned}$$

Kako je $N(\alpha_1) = 5$, α_1 *je neparan, tada je* $\alpha = 2^0(1 + k)(1 + i)(i - 2j)$. *U dokazu leme videli smo da važi* $(1 + k)(1 + i) = (1 + i)(1 + j)$, *pa je* $\alpha = (1 + i)(1 + j)(i - 2j)$.

PRIMER 2.5. *U ovom primeru ćemo pokazati kako tražimo faktorizaciju kvaterniona* α *kada važi tvrđenje B. Neka je dat kvaternion* $\alpha = -2+2i+2j+2k$.

Vidimo da je $l = 1$ i $\alpha^{'} = -1 + i + j + k$, gde je $N(\alpha^{'}) = 4 \equiv 0 \pmod 4$, pa zaključujemo da važi slučaj pod (b). Kako su $a_0 = -1 \equiv -1 \pmod 4$, $a_1 = 1 \equiv 1 \pmod 4$, $a_2 = 1 \equiv 1 \pmod 4$ i $a_3 = 1 \equiv 1 \pmod 4$ imamo da je $\alpha_0 = -i + j$ i $N(\alpha) = 2$. Sada prelazimo na slučaj pod (a) i za $b_0 = 0$, $b_1 = -1$, $b_2 = 1$ i $b_3 = 0$ nalazimo da je $\alpha_1 = j$. Tada je $\alpha = 2(1+i)(1+k)j$.

Definišimo podprsten racionalnih brojeva označen sa $\mathbb{Z}\left[\frac{1}{2}\right]$ kao:

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{k}{2^n} : k \in \mathbb{Z}, n \in \mathbb{N}\right\}.$$

Teorema 2.4. *Neka su $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$, pri čemu je β neparan broj. Tada postoji $(\alpha, \beta)_D$. Osim toga, važi sledeća verzija Bezuove relacije: postoje γ, $\delta \in \mathbb{H}(\mathbb{Z}[\frac{1}{2}])$ takvi da je $(\alpha, \beta)_D = \gamma\alpha + \delta\beta$.*

Dokaz. Oponašamo dokaz Euklidovog algoritma za najveći zajednički delilac dva cela broja. Prema lemi 2.4., nalazimo $\gamma_0, \delta_0 \in \mathbb{H}(\mathbb{Z})$, $N(\delta_0) < N(\beta)$ tako da važi

$$\alpha = \gamma_0\beta + \delta_0.$$

Prema lemi 2.5., imamo $\delta_0 = 2^{l_0}\pi_0\delta_0^{'}$, gde je $\delta_0^{'}$ neparan, a $N(\delta_0^{'}) \leqslant N(\delta_0) < N(\beta)$. Ponovo koristeći leme 2.4. i 2.5., imamo

$$\beta = \gamma_1\delta_0^{'} + \delta_1,$$

pri čemu je $\delta_1 = 2^{l_1}\pi_1\delta_1^{'}$, $N(\delta_1^{'}) \leqslant N(\delta_1) < N(\delta_0^{'})$ i $\delta_1^{'}$ neparan. Ponavljajući ovaj postupak, dobijamo kvaternione $\gamma_i, \delta_i, \delta_i^{'} \in \mathbb{H}(\mathbb{Z})$ tako da važi:

$$\delta_{i-1}^{'} = \gamma_{i+1}\delta_i^{'} + \delta_{i+1},$$

i $\delta_{i+1} = 2^{l_{i+1}}\pi_{i+1}\delta_{i+1}^{'}$, $N(\delta_{i+1}^{'}) \leqslant N(\delta_{i+1}) < N(\delta_i^{'})$ i $\delta_{i+1}^{'}$ neparan. Poslednje dve jednačine su:

$$\delta_{k-2}^{'} = \gamma_k\delta_{k-1}^{'} + \delta_k$$
$$\delta_{k-1}^{'} = \gamma_{k+1}\delta_k^{'},$$

s obzirom da su δ_i-ovi niz kvaterniona u $\mathbb{H}(\mathbb{Z})$ sa strogo opadajućim normama. Tvrdimo da je $(\alpha, \beta)_r = \delta_k^{'}$. Očigledno, $\delta_k^{'}$ je desni delilac $\delta_{k-1}^{'}, \delta_{k-2}^{'}, \dots, \delta_1^{'}, \beta, \alpha$. Ako je δ desni delilac α i β onda je i desni delilac δ_0, pa samim tim i $\delta_0^{'}$, prema jedinstvenom deljenju u lemi 2.5.. Stoga je δ desni delilac $\delta_k^{'}$. Na kraju, preformulišemo prethodni sistem kao:

$$\begin{aligned}
\delta_0^{'} &= 2^{-l_0}\pi_0^{-1}(\alpha - \gamma_0\beta) \\
\delta_1^{'} &= 2^{-l_1}\pi_1^{-1}(\beta - \gamma_1\delta_0^{'}) \\
&\dots \\
\delta_k^{'} &= 2^{-l_k}\pi_k^{-1}(\delta_{k-2}^{'} - \gamma_k\delta_{k-1}^{'}).
\end{aligned}$$

Budući da je π_i invertibilan u $\mathbb{H}(\mathbb{Z}[\frac{1}{2}])$, ovo izražava $\delta_k^{'}$ kao

$$\delta_k^{'} = \gamma\alpha + \delta\beta,$$

pri čemu su $\gamma, \delta \in \mathbb{H}(\mathbb{Z}[\frac{1}{2}])$. $\square$

Lema 2.6. *Za $\alpha \in \mathbb{H}(\mathbb{Z})$ i $m \in \mathbb{Z}$, pri čemu je m neparan, važi:*

$$(m, \alpha)_D = 1 \textit{ ako i samo ako je } (m, N(\alpha))_D = 1.$$

Dokaz.
($\Rightarrow$) Pretpostavimo da važi $(m, \alpha)_D = 1$. Koirsteći Bezuovu relaciju 2.4., postoje $\gamma, \delta \in \mathbb{H}(\mathbb{Z}[\frac{1}{2}])$ takvi da važi

$$(m, \alpha)_D = 1 = \gamma m + \delta\alpha.$$

Zatim, imamo

$$N(\delta)N(\alpha) = N(1 - \gamma m) = (1 - \gamma m)(1 - \overline{\gamma} m) = 1 - (\gamma + \overline{\gamma})m + N(\gamma)m^2$$

ili

$$1 = N(\delta)N(\alpha) + (\gamma + \overline{\gamma})m - N(\gamma)m^2.$$

Pošto su $N(\delta), N(\gamma)$ i $\gamma + \overline{\gamma}$ elementi skupa $\mathbb{Z}[\frac{1}{2}]$, možemo naći $k \in \mathbb{N}$ tako da su $2^k N(\delta), 2^k(\gamma + \overline{\gamma}), 2^k N(\gamma)$ racionalni brojevi. Neka $\beta \in \mathbb{H}(\mathbb{Z})$ bude desni delilac koji je zajednički za $N(\alpha)$ i m. Pošto je m neparan, β je neparan kvaternion.
Iz izraza

$$2^k = (2^k N(\delta))N(\alpha) + (2^k(\gamma + \overline{\gamma}))m - (2^k N(\gamma))m^2,$$

primećujemo da je β desni delilac broja 2^k. Posmatrajući norme, zaključujemo da je $N(\beta)$ delilac broja 2^{2k}. S obzirom na to da je $N(\beta)$ neparan, mora važiti $N(\beta) = 1$, drugim rečima, β je invertibilan.

($\Leftarrow$) Pretpostavimo da važi $(m, N(\alpha))_D = 1$. Želimo pokazati da $(m, \alpha)_D = 1$. Suprotno pretpostavci, pretpostavimo da postoji desni delilac $\delta \in \mathbb{H}(\mathbb{Z}[\frac{1}{2}])$ koji deli i m i α. To znači da δ deli i $N(\alpha) = \alpha\overline{\alpha}$. Odavde sledi $(N(\alpha), m)_D = \delta$ što dovodi do kontradikcije sa našom pretpostavkom $(N(\alpha), m)_D = 1$. Stoga, mora da važi $\delta = 1$. $\square$

Lema 2.7. *Neka je $p \in \mathbb{N}$ neparan, prost broj. Pretpostavimo da postoji $\alpha \in \mathbb{H}(\mathbb{Z})$, takav da α nije deljiv sa p, ali da je $N(\alpha)$ deljiv sa p. Neka je $(\alpha, p)_D = \delta$. Tada je δ prost broj u $\mathbb{H}(\mathbb{Z})$ i $N(\delta) = p$.*

Dokaz.
Pišemo $p = \gamma\delta$, za neki kvaternion $\gamma \in \mathbb{H}(\mathbb{Z})$. Prvo primećujemo da γ nije jedinični kvaternion. Inače p i δ bi bili asocirani i time bi p delio α, što je u suprotnosti sa našom pretpostavkom. Dalje, pošto p deli $N(\alpha)$, sledi iz leme 2.6. da δ nije jedinični kvaternion. S druge strane, primenom normi dobijamo

$$p^2 = N(p) = N(\gamma)N(\delta),$$

gde je $N(\gamma) \neq 1 \neq N(\delta)$. Moramo imati $N(\gamma) = N(\delta) = p$.
Iz $N(\delta) = p$ sledi da je δ prost u $\mathbb{H}(\mathbb{Z})$. Zaista, ako je $\delta = xy$ faktorizacija δ u $\mathbb{H}(\mathbb{Z})$, primenom normi dobijamo $N(\delta) = p = N(x)N(y)$, pa je ili $N(x) = 1$ ili $N(y) = 1$. U svakom slučaju, x ili y je jedinični kvaternion. $\square$

Teorema 2.5. *Za svaki neparan prost broj $p \in \mathbb{N}$, postoji prost $\delta \in \mathbb{H}(\mathbb{Z})$, takav da je $N(\delta) = p = \delta\overline{\delta}$. Posebno, p nije prost u $\mathbb{H}(\mathbb{Z})$.*

Dokaz. Prema tvrđenju 1.4., postoje $x, y \in \mathbb{Z}$, takvi da je $1+x^2+y^2 \equiv 0 \pmod{p}$. Neka je $\alpha = 1 + xi + yj$. Jasno je da p ne deli α, ali deli $N(\alpha) = 1 + x^2 + y^2$. Tada važi lema 2.7. i $\delta = (\alpha, p)_D$ je željeni prost broj u $\mathbb{H}(\mathbb{Z})$. $\square$

Sada možemo da pokažemo sledeće:

Posledica 2.3. *Kvaternion $\delta \in \mathbb{H}(\mathbb{Z})$ je prost u $\mathbb{H}(\mathbb{Z})$ ako i samo ako je $N(\delta)$ prost u $\mathbb{Z}$.*

Dokaz. Tokom dokaza leme 2.7. smo videli da ako je $N(\delta)$ prost, tada je δ prost u $\mathbb{H}(\mathbb{Z})$. Dakle, treba dokazati obratnu implikaciju.
Neka je δ prost u $\mathbb{H}(\mathbb{Z})$. Pretpostavimo prvo da je δ paran. Prema lemi 2.5., imamo $\delta = 2^l\pi\delta_0$, gde je $l \in \mathbb{N}, \pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$, a δ_0 neparan. Napomenimo da 2 nije prost u $\mathbb{H}(\mathbb{Z})$ jer važi $2 = (1+i)(1-i)$. Pošto je prema pretpostavci δ prost u $\mathbb{H}(\mathbb{Z})$, mora važiti $l = 0, N(\delta_0) = 1$ (pošto je δ_0 neparan) i $\pi \in \{1+i, 1+j, 1+k\}$, tako da $N(\delta) = 2$, kao što je potrebno.
Sada pretpostavimo da je δ neparan. Neka $p \in \mathbb{N}$ bude neparan, prost broj koji deli $N(\delta)$. Treba da pokažemo da je $N(\delta) = p$. Neka je $\alpha = (p, \delta)_D$. Tada je $\delta = \gamma\alpha$, za neki $\gamma \in \mathbb{H}(\mathbb{Z})$. Iz leme 2.6. sledi da α nije jedinični kvaternion u $\mathbb{H}(\mathbb{Z})$. Pošto je δ prost u $\mathbb{H}(\mathbb{Z})$, zaključujemo da γ mora biti jedinični kvaternion u $\mathbb{H}(\mathbb{Z})$, tako da su α i β asocirani. Dakle, δ je desni delilac broja p, recimo $p = \psi\delta$ za neki $\psi \in \mathbb{H}(\mathbb{Z})$. Primena normi i uzimajući u obzir da p deli $N(\delta)$ daje

$$p = N(\psi)(\frac{N(\delta)}{p}).$$

Ako je $N(\psi) = 1$, tada su p i δ asocirani, što znači da je p prost u $\mathbb{H}(\mathbb{Z})$, što je u suprotnosti sa teoremom 2.5. Stoga, $\dfrac{N(\delta)}{p} = 1$, pa $N(\delta) = p$. □

Kao posledica aritmetike $\mathbb{H}(\mathbb{Z})$, dobijamo Lagranžov poznati rezultat o zbiru četiri kvadrata.

Posledica 2.4. *Svaki prirodan broj je zbir četiri kvadrata.*

Dokaz. Neka je $n \in \mathbb{N}$. Rezultat je očigledan za $n = 0$ i $n = 1$, pa možemo pretpostaviti $n \geqslant 2$. Neka je $n = 2^{r_0}p_1^{r_1}...p_k^{r_k}$ faktorizacija broja n na proste faktore, gde su p_i neparni prosti brojevi. Prema teoremi 2.5., možemo pronaći $\delta_i \in \mathbb{H}(\mathbb{Z})$, tako da je $p_i = N(\delta_i) = \delta_i\overline{\delta_i}$, dok je $2 = (1+i)(1-i)$. Stoga, svaki prosti faktor koji se pojavljuje u broju n može biti zapisan kao zbir kvadrata, a multiplikativnost kvaternionske norme daje konačno predstavljanje broja n u tom obliku. □

Kao što pokazuje primer nakon tvrđenja 2.5., ne možemo očekivati jedinstvenu faktorizaciju na proste brojeve u $\mathbb{H}(\mathbb{Z})$. Sada ćemo ograničiti pažnju na skup celobrojnih kvaterniona α za koje važi $N(\alpha) = p^k$, gde je p neparan, prost broj. Pokazaćemo da za ovo α možemo dobiti neku vrstu jedinstvene faktorizacije.

Najpre ćemo navesti Jakobijevu teoremu, koju ćemo koristiti u daljem tekstu.

Teorema 2.6. *Neka je n neparan pozitivan ceo broj. Tada je $r_4(n) = 8\sum_{d|n} d$.*

Neka dakle p bude neparan prost broj. Prema Jakobijevoj teoremi

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$$

ima $8(p+1)$ celobrojnih rešenja, svako odgovara celobrojnom kvaternionu $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ norme p. Ako je $p \equiv 1 \pmod 4$, tada je jedno a_i neparno, dok su ostali parni. Ako je $p \equiv 3 \pmod 4$, tada je jedno a_i parno, dok su ostali neparni. U svakom slučaju, jedna koordinata, nazovimo je a_i^0, je posebno odabrana. Ako $a_i^0 \neq 0$, tada između osam asociranih elemenata $\epsilon\alpha$, tačno jedna ima $|a_i^0|$ kao svoju nultu komponentu.(Obratimo pažnju na apsolutnu vrednost ovde!). Ako je $a_i^0 = 0$, kao što bi moglo biti kada je $p \equiv 3 \pmod 4$, tada će dva asocirana elementa $\epsilon\alpha$ i $-\epsilon\alpha$ imati obe $a_0 = 0$. U ovom slučaju možemo odabrati bilo koju kao posebno odabranu.
Dakle, postoji $p+1$ posebno odabranih rešenja

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p,$$

tako da odgovarajući kvaternion α zadovoljava ili $\alpha \equiv 1 \pmod 2$ ili $\alpha \equiv i + j + k \pmod 2$. U ovoj listi rešenja, kako α tako i $\overline{\alpha}$ se pojavljuju kad god je $a_0 > 0$, dok je samo jedan od para uključen kada je $a_0 = 0$. Tako formiramo skup

$$S_p = \{\alpha_1, \overline{\alpha_1}, ..., \alpha_s, \overline{\alpha_s}, \beta_1, ..., \beta_t\},$$

gde α_i ima $a_0^i > 0$, β_j ima $b_0^j = 0$ i $\beta_j = \sqrt{-N(\alpha_i)}$. Primetimo da je $2s + t = |S_p| = p + 1$.

Definicija 2.18. *Redukovani niz nad skupom S_p je niz koji se sastoji od elemenata iz skupa S_p i ne sadrži uzastopne podnizove oblika $\alpha_i\overline{\alpha_i}, \overline{\alpha_i}\alpha_i, \beta_j^2 (i = 1, ..., s; j = 1, ..., t)$. Dužina niza je broj elemenata koji se pojavljuju.*

Teorema 2.7. *Neka je $k \in \mathbb{N}$ i neka je $\alpha \in \mathbb{H}(\mathbb{Z})$ takav da je $N(\alpha) = p^k$. Tada α ima jedinstvenu faktorizaciju $\alpha = \epsilon p^r \omega_m$, gde je ϵ jedinični kvaternion u $\mathbb{H}(\mathbb{Z})$, ω_m je redukovani niz dužine m nad skupom S_p, i $k = 2r + m$.*

Dokaz. Prvo ćemo dokazati da ovakva faktorizacija postoji. Dakle, fiksiramo $\alpha \in \mathbb{H}(\mathbb{Z})$ sa $N(\alpha) = p^k$. Prema tvrđenju 2.5., α je proizvod prostih brojeva u $\mathbb{H}(\mathbb{Z})$:

$$\alpha = \delta_1 ... \delta_n.$$

Prema posledici 2.3., moramo imati $N(\delta_i) = p$ $(1 \leqslant i \leqslant n)$, i stoga $n = k$. Pošto je $N(\delta_i) = p$, nalazimo jedinični kvaternion ϵ_i i $\gamma_i \in S_p$ tako da je $\delta_i = \epsilon_i \gamma_i$. Stoga,

$$\alpha = \epsilon_1 \gamma_1 \epsilon_2 \gamma_2 ... \epsilon_k \gamma_k.$$

Hoćemo da pokažemo da za svaki $\gamma \in S_p$ i svaki jedinični kvaternion $\epsilon \in \mathbb{H}(\mathbb{Z})$ možemo pronaći $\gamma' \in S_p$ i jedinični kvaternion ϵ', tako da važi

$$\gamma \epsilon = \epsilon' \gamma'.$$

Pošto je ϵ jedinični kvaternion u $\mathbb{H}(\mathbb{Z})$, to znači da $\epsilon \in \{\pm 1, \pm i, \pm j, \pm k\}$. Prvo, razmotrimo slučaj kada je $\epsilon = \pm 1$. U tom slučaju, $\gamma \epsilon = \pm \gamma$, pa možemo uzeti $\gamma' = \gamma$ i $\epsilon' = \pm 1$.
Za ostale slučajeve, kada je $\epsilon = \pm i, \pm j$ ili $\pm k$, možemo primeniti sledeće. Neka je $\gamma = a + bi + cj + dk \in S_p$. Ako je $\epsilon = i$ tada je

$$\gamma \epsilon = (a + bi + cj + dk)i = -b + ai - dj + ck = -(b - ai + dj - ck).$$

Odavde vidimo da je $\epsilon' = -1$, a $\gamma' = b - ai + dj - ck \in S_p$.
Ako je $\epsilon = -i$, tada je $\epsilon' = 1$ i $\gamma' = b - ai + dj - ck$. Ostali slučajevi se pokazuju na analogan način.

U prethodnoj faktorizaciji α, ovo omogućava da se svi ϵ_i pomere na levo i da se zapiše

$$\alpha = \epsilon \gamma_1' ... \gamma_k'$$

gde je $\gamma_i' \in S_p$ i ϵ jedinični kvaternion u $\mathbb{H}(\mathbb{Z})$. Tako smo napisali α kao proizvod jediničnog kvaterniona i niza iz skupa S_p, ali ovaj niz nije nužno redukovan. Pravimo ga redukovanim tako što pomeramo svaki faktor p na levo, ako postoji pojava $\alpha_i \overline{\alpha_i}, \overline{\alpha_i} \alpha_i$ ili β_j^2 u nizu. Tada dobijamo kraći niz, za koga ponavljamo postupak. To dokazuje postojanje.
Jedinstvenost dokazujemo pomoću argumenta brojenja. Prvo, prema Jakobijevoj teoremi postoje tačno

$$8 \sum_{i=0}^{k} p^i = 8(\frac{p^{k+1} - 1}{p - 1})$$

kvaterniona $\alpha \in \mathbb{H}(\mathbb{Z})$ sa $N(\alpha) = p^k$. Sada brojimo koliko ima redukovanih nizova dužine m nad skupom S_p. Postoji $p+1$ mogućih izbora za prvi element i p mogućih izbora za svaki od sledećih elemenata (jer moramo izbegavati podnizove oblika $\alpha_i\overline{\alpha_i}, \overline{\alpha_i}\alpha_i$ i β_j^2). Dakle, broj redukovanih nizova dužine m je

$$\begin{cases} 1, & m = 0 \\ (p+1)p^{m-1}, & m \geqslant 1. \end{cases}$$

Dakle, ukupan broj izraza oblika $\epsilon p^r \omega_m$, gde je ϵ jedinični kvaternion, ω_m redukovani niz dužine m i $2r + m = k$ je

$$\begin{cases} 8(1 + \sum_{r=0}^{\frac{k}{2}-1}(p+1)p^{k-2r-1}), & \text{ako je } k \text{ paran,} \\ 8(\sum_{r=0}^{\frac{k-1}{2}}(p+1)p^{k-2r-1}), & \text{ako je } k \text{ neparan.} \end{cases}$$

U oba slučaja dobijamo $8(\dfrac{p^{k+1}-1}{p-1})$ izraza, koji se poklapaju sa brojem $\alpha \in \mathbb{H}(\mathbb{Z})$ sa $N(\alpha) = p^k$. Pošto, prema delu o postojanju, svaki takav α može biti napisan u ovakvom obliku, pa ova faktorizacija mora biti jedinstvena. $\square$

Definicija 2.19. *Označimo sa Λ' skup u $\mathbb{H}(\mathbb{Z})$ na sledeći način:*

$$\begin{aligned} \Lambda' = \{\alpha &= a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod 2 \\ &\textit{ili} \\ \alpha &\equiv i + j + k \pmod 2,\ N(\alpha) \textit{ stepen broja } p\} \end{aligned}$$

Lako je videti, redukcijom po modulu 2, da je Λ' zatvoren u odnosu na množenje. Jasno je da sadrži skup S_p.

Posledica 2.5. *Svaki element $\alpha \in \Lambda'$ sa normom $N(\alpha) = p^k$ ima jedinstvenu faktorizaciju $\alpha = \pm p^r \omega_m$, gde je $r \in \mathbb{N}$, ω_m redukovani niz dužine m nad skupom S_p, i $k = 2r + m$.*

Dokaz. Prema teoremi 2.7., α se može napisati na jedinstven način kao $\alpha = \epsilon p^r \omega_m$, r i ω_m koji imaju željene osobine, a ϵ je jedinični kvaternion u $\mathbb{H}(\mathbb{Z})$. Redukcijom po modulo 2, dobijamo $\alpha \equiv \epsilon\omega_m \pmod 2$. Svaki $\alpha_i, \beta_j \in S_p$ koji se pojavi u ω_m ima $\alpha_i, \beta_j \equiv 1 \pmod 2$ ili $\alpha_i, \beta_j \equiv i + j + k$

(mod 2). Za sada, označimo ovaj drugi slučaj sa γ. Onda, po modulu 2, imamo kongruencije:

$$\alpha \equiv \begin{cases} \epsilon & \text{ako se paran broj } \gamma \text{ pojavljuje u } \omega_m; \\ \epsilon(i+j+k) & \text{ako se neparan broj } \gamma \text{ pojavljuje u } \omega_m. \end{cases}$$

S druge strane, pošto je $\alpha \in \Lambda^{'}$, sam α mora zadovoljiti $\alpha \equiv 1 \pmod 2$ ili $\alpha \equiv i+j+k \pmod 2$. Stoga, vidimo da u svakom slučaju mora važiti $\epsilon \equiv 1 \pmod 2$, drugim rečima, $\epsilon = \pm 1$. $\square$

Sada ako se vratimo na primer faktorizacije broja 13, videćemo da smo tu rekli da faktorizacija broja 13 na proste kvaternione nije jedinstvena, što ukazuje na složenost tog procesa u ovom specifičnom prstenu. Međutim, teorema 2.7. tvrdi da postoji jedinstvena faktorizacija za određene klase kvaterniona čija je norma određeni stepen broja p. Ova neslaganja se mogu objasniti složenom prirodom faktorizacije u prstenu kvaterniona i specifičnim karakteristikama tog prstena. Takođe je važno napomenuti da, iako neujednačenosti u faktorizaciji postoje, postoji i određena klasa kvaterniona gde se može postići jedinstvenost faktorizacije. Ovo pokazuje da se faktroizacija u prstenu kvaterniona razlikuje od faktorizacije u običnim prstenovima celih brojeva zbog specifičnih svojstava kvaterniona.

Zaključak

Aritmetika celobrojnih kvaterniona predstavlja duboku i izazovnu oblast matematike koja pruža bogatstvo teorijskih koncepata i praktičnih primena. Kroz istraživanje celobrojnih kvaterniona, stičemo dublje razumevanje algebarskih struktura i razvijamo veštine analitičkog razmišljanja koje se protežu izvan konvencionalnih aritmetičkih pravila.

Osnovna svojstva celobrojnih kvaterniona, poput nekomutativnosti, izazivaju nas da se suočimo s kompleksnim problemima aritmetike. Deljenje, faktorizacija i pronalaženje najvećeg zajedničkog delioca postaju složeniji procesi u ovom kontekstu. Uprkos izazovima, aritmetika celobrojnih kvaterniona pruža nam dublje uvide u prirodu matematičkih struktura i podstiče nas da razvijamo nove metode za rešavanje problema.

Kroz proučavanje celobrojnih kvaterniona, otvaramo vrata praktičnim primenama u različitim disciplinama. Ovi kvaternioni igraju ključnu ulogu u modeliranju trodimenzionalnih rotacija, što je od suštinskog značaja u oblastima u rešavanju komplikovanih problema iz oblasti fizike, računarstva i inženjeringa.

Iako aritmetika celobrojnih kvaterniona može biti izazovna, istraživanje ove oblasti donosi dublje zadovoljstvo i zadovoljenje razvijanja veština rešavanja kompleksnih matematičkih problema. Sve u svemu, celobrojni kvaternioni pružaju nam priliku da se upustimo u dublje razmišljanje, razvijemo inovativne pristupe i otkrijemo fascinantne aspekte matematičkog sveta.

Bibliografija

[1] G. Davidoff, P. Sarnak, A. Valette. *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, New York, 2003.

[2] A. Lipkovski. *Linearana algebra i analitička geometrija*, Beograd, 2007.

[3] V. Ilić. *Kvaternioni i njihova primena u geometriji*, Beograd, 2011.

[4] S. Krešić-Jurić. *Algebarske strukture, skripta*, Split, 2013.

[5] P. Stehlik. *Kvaternioni i prostorne rotacije*, Osijek, 2020.

[6] B. Barbarić. *Algebra kvaterniona i primjene*, Zagreb, 2021.

[7] I. Gogić. *Kvaternioni i Frobeniusov teorem*, 2021.

[8] https://en.wikipedia.org/wiki/Quaternion

Biografija

Rođena sam 28. marta 1992. godine u Kruševcu. Završila sam Osnovnu školu „Vladislav Savić Jan" 2007. godine, nakon čega sam upisala srednju Ekonomsko - trgovinsku školu u Kruševcu. Godine 2011. počela sam osnovne studije na Matematičkom fakultetu u Beogradu. Po završetku osnovnih studija stekla sam stručni naziv diplomirani matematičar. 2019. godine upisala sam master studije na smeru profesor matematike i računarstva. Tokom studija živela sam uglavnom u Beogradu.

2019. godine vratila sam se u Kruševac i započela rad u Fabrici eksploziva i pirotehnike u Trayal korporaciji. Nakon tri i po godine ponovo sam se vratila u Beograd i počela raditi u Osnovnoj školi „Branko Ćopić" u Rakovici.