Vsote popolnih kvadratov

seminarska naloga pri predmetu Seminar 1
FMF Ljubljana

Primož Pušnik

april 2011

1 Uvod

V matematiki poznamo številne probleme, ki so razumljivi matematično neizobraženim ljudem, ko pa jih v roke dobi matematik, se izkažejo za izredno težke. S takšnimi in drugačnimi problemi so se ukvarjali že v antiki; Evklid se je "igral" s premicami, Pitagora je "premetaval kvadrate". Ta dva in še mnogi drugi veliki matematiki so se ukvarjali z navidez lahkimi problemi. Ker pa poti do rešitev niso bile enostavne, so včasih " zašli" na stranpoti ter tako izdelali pripomočke, ki so jih lahko uporabili na mnogih drugih področjih matematike. Žal pa so rešitve teh problemov, kolikor so jih doslej sploh našli, po navadi dostopne samo pravim matematikom. Pomislimo samo na slavni Fermatov problem in Catalanovo hipotezo, ki sta bila razrešena šele pred kratkim. Do danes pa še vedno ni znano, ali lahko med dvema popolnima kvadratoma vedno najdemo praštevilo. Ne vemo, če je praštevil oblike $n! - 1$ neskončno itd.

Poleg zelo zahtevnih matematičnih problemov imamo tudi probleme z rešitvami, ki so razumljive vsem, ki poznajo "malo" več srednješolske matematike. Mi si bomo pobližje ogledali problem, s katerim so se ukvarjali že Fermat, Lagrange in Gauss. Govori o tem katera naravna števila lahko zapišemo kot vsoto dveh, treh ali štirih popolnih kvadratov.

2 Vsote dveh kvadratov

V tej seminarski nalogi se bomo zaradi lažjega izražanja najprej omejili le na naravna števila. Poleg tega bomo privzeli, da je 0 naravno število, s čimer se bomo izognili obravnavanju dodatnih primerov.

V tem poglavju bomo klasificirali vsa naravna števila, ki jih lahko zapišemo, kot vsoto dveh popolnih kvadratov. Števila bi lahko klasificirali povsem elementarno, brez uporabe algebre, a kljub temu se bomo naloge lotili malo drugače, bolj "algebraično", s pomočjo Gaussovih celih števil.

Definicija 2.1. Množico $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, opremljeno s klasičnima operacijama seštevanja in množenja, imenujemo Gaussova števila.

Osnovne lastnosti Gaussovih števil:

- Gaussova števila sestavljajo komutativen kolobar (podkolobar obsega kompleksnih števil).
- Norma Gaussovega števila $z = a + bi$ je enaka $N(z) = z\overline{z} = a^2 + b^2$.
- Norma je multiplikativna, to pomeni $N(zw) = N(z)N(w)$.
- Edini obrnljivi elementi kolobarja so $1, -1, i$ in $-i$.
- Števili z in w sta si asociirani, če obstaja tak obrnljiv element t kolobarja, da je $z = w \cdot t$.
- Neničelen element je nerazcepen, če nima drugih deliteljev kot obrnljivih elementov in asociiranih elementov.

- Če je $N(z)$ praštevilo, potem je z nerazcepno Gaussovo število.

Trditev 2.1. *Kolobar Gaussovih števil je Evklidski kolobar.*

Dokaz. Naj bosta $a, b \neq 0$ Gaussovi števili. Kvocient $\frac{a}{b} = p + qi$ je kompleksno število z racionalnima komponentama p in q. Naj bo m celo število, ki je najbližje p-ju, n pa celo število, ki je najbližje q. Pišimo $p = m + r$, $q = n + s$, $|r| \leq \frac{1}{2}$ in $|s| \leq \frac{1}{2}$. Naj bo $\gamma = m + ni, \delta = r + si$. Število γ pripada kolobarju Gaussovih števil. Ker je $\frac{a}{b} = \gamma + \delta$, dobimo $a = b\gamma + b\delta$. Razlika $a - b\gamma = b\delta = x$ je Gaussovo število. Norma kompleksnih števil je multiplikativna, zato je $N(x) = N(b)N(\delta)$. Hkrati pa je $N(\delta) = r^2 + s^2 \leq \frac{1}{2}$, zato je $N(x) \leq \frac{1}{2}N(b) < N(b)$. Torej smo za vsaki dve števili a in b iz Gaussovega kolobarja našli taki števili γ in x, da je $a = b\gamma + x$ in $N(x) < N(b)$.

■

Posledica. *Ker je kolobar Gaussovih števil Evklidski, je posledično glavni kolobar in zato tudi kolobar z enolično faktorizacijo.*

Lema 2.1. *Za vsako praštevilo oblike $p = 4k+1$ obstaja tako naravno število m, da $p|(m^2 + 1)$.*

Dokaz. Oglejmo si polinom $x^{p-1} - 1$ nad kolobarjem Z_p. Ker je $p = 4k + 1$, lahko pišemo

$$x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1).$$

Polinom $x^{p-1} - 1$ ima v Z_p natanko $p - 1$ ničel, kar je posledica malega Fermatovega izreka (ničle so $\overline{1}, \overline{2}, \ldots \overline{p-1}$).

Torej imata $x^{\frac{p-1}{2}} - 1$ in $x^{\frac{p-1}{2}} + 1$ skupaj natanko $p - 1$ različnih ničel. V celem komutativnem kolobarju ima polinom največ toliko ničel, kolikor je njegova stopnja, torej imata oba omenjena polinoma vsak po največ $\frac{p-1}{2}$ ničel, oziroma vsak ima natanko $\frac{p-1}{2} \geq 1$ ničel.

Pokazali smo obstoj $\overline{g} \in Z_p$, ki zadostuje pogoju $\overline{g}^{\frac{p-1}{2}} \equiv -\overline{1}$, oziroma $(g^{\frac{p-1}{4}})^2 \equiv -1 \pmod{p}$.

Izberimo $m := g^{\frac{p-1}{4}}, \frac{p-1}{4} \in \mathbb{N}, m \in \mathbb{N}$. Tako smo našli tako naravno število m, da $p|(m^2 + 1)$. ■

Opomba. Zgornjo trditev bi lahko pokazali tudi s pomočjo Wilsonovega izreka, ki pravi, da je $(p-1)! \equiv -1 (\text{mod } p)$ natanko tedaj, ko je p praštevilo.

Opomba. Fermatov izrek pravi, če je p praštevilo in je $gcd(n, p) = 1$, tedaj je $n^{p-1} \equiv 1 (\text{mod } p)$.

Sedaj smo se dovolj dobro pripravili, da se lahko lotimo našega glavnega problema. Katera števila se da zapisati kot vsoto dveh kvadratov nenegativnih celih števil? Za lažje izražanje bomo uvedli še pojem lepega števila.

Definicija 2.2. Naravno število n je LEPO, kadar obstajata taki naravni števili x in y, da je $n = x^2 + y^2$.

Izrek 2.1. *Vsako praštevilo oblike $p = 4k + 1$ je LEPO.*

Dokaz. Naj bo p poljubno praštevilo oblike $4k+1$. Oglejmo si p kot element $\mathbb{Z}[i]$. Po lemi 2.1 obstaja $m \in \mathbb{N}$, da $p|m^2+1 = (m+i)(m-i)$.

Denimo, da je p nerazcepen v $\mathbb{Z}[i]$. Ker je $\mathbb{Z}[i]$ kolobar z enolično faktorizacijo, imamo dve možnosti: $p|m-i$ ali $p|m+i$. Denimo, da $p|m-i$, po konjugiranju $p|m+i$, oziroma če seštejemo pogoja, dobimo $p|2i$, kar implicira, da je $p \in \{1,2\}$.

Torej je p razcepen v $\mathbb{Z}[i]$, zato ga lahko faktoriziramo: $p = (a+bi)(c+di)$, pri čemer sta oba faktorja neobrnljiva, t.j. $a,b,c,d \geq 1$.

$$p^2 = N(p) = N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2)$$

Popolni kvadrat praštevila je produkt dveh naravnih števil, večjih od 1, torej je edina možnost, da je $p = a^2+b^2 = c^2+d^2$, oziroma $p = a^2+b^2$, za neka $a,b \in \mathbb{N}$. ■

Pokazali smo, da je vsako število oblike $4k+1$ lepo število, toda s tem še nismo našli vseh lepih števil. Nadalje se vprašamo, ali so še katera druga števila lepa. Zakaj je $45 = 6^2+3^2$, 15 pa ni lepo število.? Kakšnim kriterijem morajo zadoščati lepa števila? Z nekaj poskušanja vidimo, da je produkt lepih števil lepo število. Izkaže se, da to vedno drži.

Lema 2.2. *Produkt lepih števil je lepo število.*

Dokaz. Naj bosta $a = x^2+y^2$ in $b = u^2+v^2$ lepi števili, tedaj je

$ab = (x^2+y^2)(u^2+v^2) = (xu)^2+(xv)^2+(yu)^2+(yv)^2 = (xu)^2+2xyuv+(xv)^2+(yu)^2-2xyuv+(yv)^2 = (xu+yv)^2+(xv-yu)^2$.

Pokazali smo, da je produkt dveh lepih števil lepo število. Dokažimo z indukcijo, da je končen produkt lepih števil lepo število.

Naša indukcijska predpostavka je, da je produkt $n-1$ lepih števil vedno lepo število. Oglejmo si sedaj lepa števila $p_1, p_2, \ldots p_n$. Njihov produkt je enak $p_1p_2\cdots p_{n-1}p_n$. Produkt prvih $n-1$ števil je po indukcijski predpostavki lepo število, torej dobimo produkt dveh lepih števil, za katerega smo že na začetku pokazali, da je tudi lepo število. ■

Dejstvo, da je produkt lepih števil lepo število, nam je dalo zelo učinkovit način za iskanje lepih števil, vendar jih še ne moremo karakterizirati. Zakaj 15 ni lepo število? Razlog ne more biti to, da ni produkt lepih števil, ker je tudi $45 = 15 \cdot 3$ lepo, kot smo zapisali, pa ni produkt lepih števil. Lahko pa 45 pišemo kot $9 \cdot 5$, ti števili pa sta lepi. Ugibamo, da so vsa lepa števila tista, ki se dajo vsaj na en način zapisati kot produkt lepih praštevil in popolnih kvadratov (ne pozabimo, da so popolni kvadrati lepa števila). Razmislimo, kdaj tega ne moremo storiti. Težava se pojavi, kadar v praštevilskem razcepu našega števila obstaja nelepo praštevilo lihe stopnje. Tega praštevila ne moremo "pospraviti"v noben kvadrat v celoti, torej nam bo vedno ostal en nelep faktor. Ugibamo, da so lepa števila natanko tista, ki v praštevilskem razcepu nimajo nobenega nelepega praštevila v lihi stopnji.

Lema 2.3. *Naj bosta x in y tuji si naravni števili in p liho praštevilo, ki deli x^2+y^2, tedaj je $p \equiv 1 \pmod 4$.*

Dokaz. Po predpostavki izreka je

$$x^2+y^2 \equiv 0 (\text{mod } p),$$

oziroma

$$x^2 \equiv -y^2 (\text{mod } p).$$

Kongruence lahko potenciramo, zato je $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} y^{p-1} (\text{mod } p)$.
Največji skupni delitelj števil x in y je 1, zato p deli kvečjemu eno izmed njiju. Zaradi simetrije lahko predpostavimo, da p ne deli x. Tedaj pogoj $p|(x^2 + y^2)$ implicira, da p ne deli niti y.

Uporabimo mali Fermatov izrek $1 \equiv x^{p-1} \equiv (-1)^{\frac{p-1}{2}} y^{p-1} \equiv (-1)^{\frac{p-1}{2}} (\text{mod } p)$. Dobimo kongruenčno enačbo $(-1)^{\frac{p-1}{2}} \equiv 1 \text{ (mod } p)$, ki bo izpolnjena natanko tedaj, ko bo $p \equiv 1 \text{ (mod } 4)$. ■

Končno lahko karakteriziramo vsa lepa števila.

Izrek 2.2. *Naravno število n je lepo natanko tedaj, ko v praštevilski faktorizaciji ne vsebuje nobenega praštevila oblike $4k + 3$ lihe stopnje.*

Dokaz. Najprej pokažimo implikacijo v desno. Naj bo $n = x^2 + y^2$ lepo število. n lahko zapišemo kot $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$, pri čemer so $p_i, 1 \leq i \leq k$ različna praštevila. Naj bo $d = gcd(x, y)$ največji skupni delitelj števil x in y, $x = x_1 d$, $y = y_1 d$; $gcd(x_1, y_1) = 1$.

$$n = d^2 (x_1^2 + y_1^2)$$

$$x_1^2 + y_1^2 = \frac{{p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}}{d^2}.$$

Praštevilo, ki nastopa v praštevilski faktorizaciji števila n v lihi stopnji, deli $x_1^2 + y_1^2$, torej je po lemi 2.3 oblike $4t + 1$ za neko naravno število t.

Sedaj pokažimo še obratno implikacijo. Naj bo $n = m^2 u$, pri čemer kvadrat nobenega naravnega števila ne deli u. Če je n popolni kvadrat, je $u = 1$, torej je že izražen kot vsota dveh popolnih kvadratov. Eden izmed njiju je 0, sicer je n po predpostavki naloge produkt različnih praštevil oblike $4k + 1$.

Vsa taka praštevila so lepa, torej lahko n pišemo kot:

$$n = m^2 (x_1^2 + y_1^2)(x_2^2 + y_2^2) \cdots (x_t^2 + y_t^2) = m^2 (A^2 + B^2) = (mA)^2 + (mB)^2,$$

pri čemer prvi enačaj velja po izreku 2.1, drugi pa po lemi 2.2. ■

Dokaz izreka, da je vsako praštevilo oblike $4k + 1$ lepo, nam da misliti, ali se da vsako lepo praštevilo enolično zapisati kot vsoto dveh popolnih kvadratov.

Trditev 2.2. *Vsako lepo praštevilo se da zapisati kot vsota dveh popolnih kvadratov na natanko en način.*

Dokaz. Naj bo $p \in \mathbb{P}$ in $p = a^2 + b^2 = c^2 + d^2$.

Jasno je, da so $a, b, c, d > 0$, saj praštevilo ne more biti popolni kvadrat.

Očitno je $gcd(a, b) = gcd(c, d) = 1$, sicer p ne bi bilo praštevilo. Poračunajmo:

$$a^2 = p - b^2, c^2 = p - d^2,$$

$$a^2 c^2 \equiv (p - b^2)(p - d^2) \equiv b^2 d^2 (\text{mod } p),$$

$$(ac - bd)(ac + bd) \equiv 0(\mathrm{mod} p).$$

Sklepamo lahko, da $p|(ac - db)$ ali $p|(ac + bd)$.

Ker je $2p = a^2 + c^2 + b^2 + d^2 = (a - c)^2 + (b - d)^2 + 2ac + 2bd \geq 2ac + 2bc$, je $0 < ac + bc \leq p$.

Ocenimo lahko $0 < a^2, b^2, c^2, d^2 < p$, torej je $0 < a < b < c < d < \sqrt{p}$, $0 < ac, bd < p$, in končno $-p < ac - bd < p$.

Ob upoštevanju zgornjih ocen nam ostaneta dve možnosti:

- $ac - bd \equiv 0 \pmod{p}$, $-p < ac - bd < p$, torej je $ac - bd = 0$, oz. $ac = bd$.

  $gcd(a, b) = gcd(c, d) = 1$, zato $d = ka$, za nek $k \in \mathbb{N}$.

  Vstavimo to v enačbo $ac = bd = bka$, po krajšanju z a dobimo: $c = kb$.

  Nazadnje ugotovimo: $p = a^2 + b^2 = c^2 + d^2 = (kb)^2 + (ka)^2 = k^2(a^2 + b^2) = k^2 p \Rightarrow k = 1$, kar nam da $a = d$ in $b = c$.

- Vemo $ac + bd \equiv 0(\mathrm{mod}\ p)$, $0 < ac + bc \leq p$, torej $ac + bd = p$.

  Po že znani identiteti je

  $p^2 = (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 = p^2 + (ac - bd)^2 \Rightarrow ac = bd$,

  kar po sklepu iz prve točke implicira enoličnost zapisa.

■

3 Lagrangeov izrek

V prejšnjem poglavju smo poiskali vsa naravna števila, ki jih lahko zapišemo kot vsoto dveh popolnih kvadratov. Videli smo, da ne moremo vseh števil zapisati na željen način, zato se vprašamo, najmanj koliko kvadratov potrebujemo, da lahko vsa naravna števila zapišemo kot vsoto le-teh. Odgovor na to nam da znameniti Lagrangeov izrek, ki se da podobno kot prejšnji izrek dokazati povsem elementarno s pomočjo leme, ki jo bomo uporabili tudi mi, in principa neskončnega spusta (glej [1]). Toda mi že prej nismo pristopili povsem elementarno, ampak smo si pomagali s pomočjo Gaussovih števil. Gaussova števila imajo dve komponenti za dva kvadrata, zato se nam pri vsoti štirih kvadratov naravno ponujajo celoštevilski kvarternioni.

Definicija 3.1. Kvarternioni so števila oblike $a + bi + cj + dk$, pri čemer so a, b, c in d realna števila, i, j in k pa so imaginarne enote.

Kvarternioni s klasičnim seštevanjem in množenjem, definiranim z $ij = k$, $jk = i$, $ki = j$, $i^2 = j^2 = k^2 = -1$, postanejo realna štirirazsežna nekomutativna algebra.

Podobno kot pri kompleksnih številih se nam ponujajo celi kvarternioni oblike $a + bi + cj + dk$, pri čemer so a, b, c in d cela števila, toda v nasprotju z Gaussovimi števili kolobar teh števil ni Evklidski. Imajo pa kljub temu kvarternioni analog Gaussovih celih števil, in sicer Hurwitzova števila.

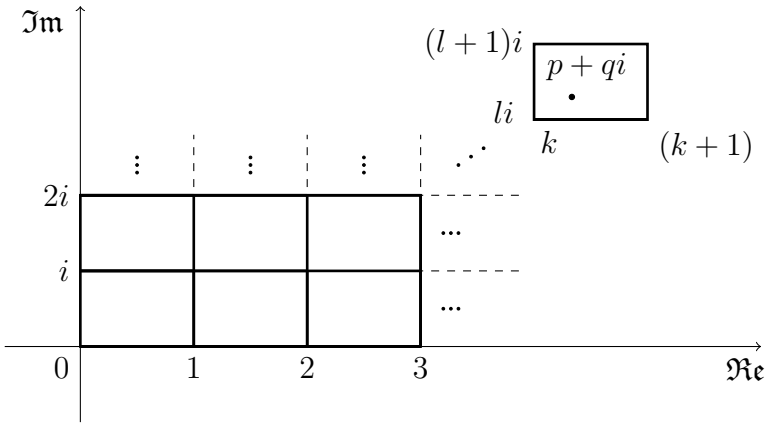
Definicija 3.2. Hurwitzovi kvarternioni so podkolobar kvartenionov, definiran z $\mathbb{K} = \{\frac{1}{2}a_0(1 + i + j + k) + ai + bj + ck | a_0, a, b, c \in \mathbb{Z}\}$.

Osnovne lastnosti Hurwitzovih števil (vse razen četrte veljajo tudi za kvarternione):

- Hurwitzova števila so nekomutativen kolobar (podkolobar kvarternionov).
- Norma Hurwitzovega števila $z = a+bi+cj+dk$ je enaka $N(z) = a^2+b^2+c^2+d^2$.
- Norma je multiplikativna, t.j. $N(zw) = N(z)N(w)$.
- Grupa obrnljivih elementov Hurwitzovih števil ima 24 elementov $\{\pm 1, \pm i \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\}$, pri čemer si lahko + in − poljubno izberemo.
- Števili a in b sta si asociirani, če obstaja tak obrnljiv element kolobarja, da je $a = b \cdot t$.
- Neničelen element je nerazcepen, če nima drugih deliteljev kot obrnljivih elementov in asociiranih elementov.

Trditev 3.1. *Hurwitzovi kvarternioni so Evklidski kolobar.*

Dokaz. Kvarternioni niso komutativni, zato lahko vpeljemo levo in desno deljenje. Kvarternion c je desni delitelj a, če je $a = kc$, za nek $k \in \mathbb{K}$. Dokažimo le, da je $\mathbb{K}$ Evklidski kolobar le za desne delitelje, za leve je dokaz podoben. Najprej preformulirajmo dokaz za to, da so Gaussova števila Evklidski kolobar. Denimo, da Gaussovo število a delimo z Gaussovim številom b. Oglejmo si kompleksno ravnino, tlakovano s kvadrati, kot na spodnji sliki 1.



Slika 1: Tlakovanje kompleksne ravnine.

Sedaj je takoj razvidno, da moramo za γ vzeti levo ogljišče pravokotnika, v katerem se nahaja $\frac{a}{b} = p + qi$, da bo $a = b\gamma + x$. Kot smo že dokazali, je tedaj $N(x) < N(b)$.

Poskusimo sedaj posplošiti to idejo na Hurwitzove kvarternione. Prostor kvarternionov je štiridimenzionalen z bazo $\{1, i, j, k\}$. Naš štiridimenzionalen prostor tlakujmo s hiperkockami $1 \times i \times j \times k$. Naj bosta $a, b \in \mathbb{K}$. Poiščimo, v kateri hiperkocki se nahaja $\frac{a}{b} = ab^{-1}$. Naj bo t oglišče, ki je najbližje $\frac{a}{b}$. Torej lahko zapišemo $\frac{a}{b} = t + w$, pri čemer je w neko Hurwitzovo število z racionalnimi koeficienti. Velja

$a = tb + wb$, $a, tb \in \mathbb{K}$, zato $wb \in \mathbb{K}$. Ocenimo $N(wb) = N(w)N(b) \leq N(b)$. Tukaj se vidi, zakaj kvarternioni niso Evklidski kolobar, kajti če je $\frac{a}{b}$ ravno v centru neke hiperkocke, se norma $N(bw)$, t.j. ostanka, ne zmanjša. Pri Hurwitzovih številih je ta prednost, če je $\frac{a}{b}$ slučajno v središču hiperkocke, v kateri se nahaja, tedaj lahko za t izberemo kar $\frac{a}{b}$, t.j. $\frac{a}{b} \in \mathbb{K}$. S tem smo dokazali, da je $\mathbb{K}$ res evklidski kolobar. ■

Podobno kot pri karakterizaciji števil v prvem poglavju tudi tukaj potrebujemo dve podobni lemi, ki nam bosta pomagali skonstruirati zapis števila kot vsoto štirih kvadratov.

Lema 3.1. *Za vsako liko praštevilo p obstajata naravni števili l in m, da $p|(1+l^2+m^2)$.*

Dokaz. Naj bosta $0 \leq x, y \leq \frac{p-1}{2}$. Denimo, da je $x^2 \equiv y^2 \pmod{p}$. To je možno le, če je $(x-y)(x+y) \equiv 0 \pmod{p}$. Ker je $x, y \leq \frac{p-1}{2}$, je $x+y \leq p-1 < p$, torej p ne deli $x+y$, p je praštevilo, zato $p|(x-y)$.

Ker je $|x-y| \leq |x|+|y| \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1 < p$, mora biti $x = y$.

Definiramo $A := \{x^2 | 0 \leq x \leq \frac{p-1}{2}\}$. Vsa števila v množici A dajo po zgornjem sklepu različne ostanke pri deljenju s p. Podobno dajo elementi množice $B := \{-1-x^2 | 0 \leq x \leq \frac{p-1}{2}\}$ različne ostanke pri deljenju s p.

V množicah A in B je skupaj $p+1$ števil, torej imata obe množici vsaj en skupen element, oziroma obstajata $l \in A$ in $m \in B$, da je $l^2 \equiv -1 - m^2 \ (mod\ p)$. ■

Opomba. Lema 3.1 je za praštevila oblike $4k+1$ direktna posledica leme 2.1, če vstavimo $l = 0$. Toda pravkar dokazana lema velja za vsa praštevila.

Lema 3.2. *Vsako praštevilo p je razcepno v $\mathbb{K}$.*

Dokaz. Po lemi 3.1 vemo, da obstajata taki naravni števili l in m, da $p|1+l^2+m^2$, oziroma $p|(1-li-mj)(1+li+mj)$.

Če je p nerazcepen v K, tedaj $p|(1-li-mj)$ ali $p|(a+li+mj)$. Toda niti $\frac{1}{p} - \frac{l}{p}i - \frac{m}{p}j$, niti $\frac{1}{p} + \frac{l}{p}i + \frac{m}{p}j$ ne leži v K, torej je p razcepen v $\mathbb{K}$. ■

Spomnimo se, kako smo skonstruirali izražavo lepih praštevil kot vsoto dveh kvadratov. To smo storili tako, da smo praštevilo p razcepili v kolobarju Gaussovih števil. Iz pogoja, da so Gaussova števila kolobar z enolično faktorizacijo smo ugotovili, da je praštevilo p razcepno v tem kolobarju. Povsem analogno gre tudi v primeru štirih kvadratov.

Trditev 3.2. *Naj bo p praštevilo. Tedaj obstajajo taka števila a, b, c, d, da je $p = a^2+b^2+c^2+d^2$ in $2a, 2b, 2c, 2d \in \mathbb{Z}$.*

Dokaz. Po lemi 3.2 je p razcepen v $\mathbb{K}$, torej lahko pišemo $p = (a+bi+cj+dk)\alpha$. Po konjugiranju dobimo $p = \overline{\alpha}(a-bi-cj-dk)$. Zmnožimo dobljeni enakosti in dobimo:

$p^2 = pp = (a+bi+cj+dk)\alpha\overline{\alpha}(a-bi-cj-dk) = (a+bi+cj+dk)|\alpha|^2(a-bi-cj-dk) = |\alpha|^2(a+bi+cj+dk)(a-bi-cj-dk) = |\alpha|^2(a^2+b^2+c^2+d^2)$.

Oba faktorja sta večja od 1, torej je $p = a^2+b^2+c^2+d^2$ za a, b, c, d, da je $2a, 2b, 2c, 2d$ naravno število. ■

Lema 3.3. *Naj bosta m in n taki naravni števili, ki ju lahko zapišemo kot vsoto štirih popolnih kvadratov nenegativnih celih števil, tedaj lahko tudi $m \cdot n$ zapišemo kot vsoto štirih nenegativnih kvadratov celih števil.*

Dokaz. $(x^2+y^2+z^2+w^2)(x_1^2+y_1^2+z_1^2+w_1^2) = (xx_1+yy_1+zz_1+ww_1)^2 + (xy_1 - yx_1 + zw_1 - wz_1)^2 + (xz_1 - zx_1 + wy_1 - yw_1)^2 + (xw_1 - wy_1 + yz_1 - zy_1)^2$. ■

Posledica. *Končen produkt števil, ki so vsote štirih popolnih kvadratov je vsota štirih popolnih kvadratov.*

Dokaz. Naj bo $n = m_1 m_2 \cdots m_k$, pri čemer so $m_i,\ 1 \leq i \leq k$ števila, ki jih lahko zapišemo kot vsoto štirih popolnih kvadratov. Dokažimo trditev z indukcijo na k. Bazni primer smo že pokazali v lemi 3.3. Naj bo naša indukcijska predpostavka, da se da vsako število, ki je proukt $k-1$ števil, ki so vsota štirih popolnih kvadratov, tudi samo take oblike. Torej lahko n po indukcjski predpostavki zapišemo kot $n = m_1 t$, pri čemer je t vsota največ štirih popolnih kvadratov. Po lemi 3.3 je tedaj tudi n vsota štirih popolnih kvadratov. ■

Izrek 3.1. *Vsako praštevilo p lahko zapišemo kot vsoto štirih kvadratov naravnih števil.*

Dokaz. Po trditvi 3.2 obstajajo taka nenegativna števila $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$, da je $p = a^2 + b^2 + c^2 + d^2$. Naj bo $2a = A, 2b = B, 2c = C, 2d = D$, tedaj je $n = \frac{A^2+B^2+C^2+D^2}{4}$.

Števila A, B, C in D so iste parnosti. Uporabimo sedaj lemo 3.3, tako da vstavimo

$A = xx_1 + yy_1 + zz_1 + ww_1$,
$B = xy_1 - yx_1 + zw_1 - wz_1$,
$C = xz_1 - zx_1 + wy_1 - yw_1$,
$D = xw_1 - wy_1 + yz_1 - zy_1$,
$x_1 = 1$, $y_1 = 1$, $z_1 = 1$, $w_1 = 1$.

Upoštevamo trditev leme in dobimo: $\frac{A^2+B^2+C^2+D^2}{4} = x^2 + y^2 + z^2 + w^2$, le še x, y, z in w moramo naračunati:

$A = x + y + z + w$,
$B = x - y + z - w$,
$C = x - z + w - y$,
$D = x - w + y - z$.

Poračunamo lahko, da je
$x = \frac{A+B+C+D}{4}$,
$y = \frac{A+D-C-B}{4}$,
$z = \frac{A+B-C-D}{4}$,
$w = \frac{A-B+C-D}{4}$.

Ker so A, B, C in D iste parnosti, so x, y, z in w cela števila; torej je $n = x^2 + y^2 + z^2 + w^2$ res vsota štirih popolnih kvadratov. ■

Posledica. *Vsako naravno število lahko zapišemo kot vsoto štirih popolnih kvadratov.*

Dokaz. Vsako naravno število ima končno mnogo prafaktorjev, torej ima končen prafaktorski razcep. Vsak prafaktor je praštevilo, torej je po izreku 3.1 vsota štirih popolnih kvadratov nenegativnih naravnih števil. Po posledici 3 je tudi naše naravno število vsota največ štirih popolnih kvadratov. ■

4 Zaključek

V članku nam je uspelo karakterizirati vsa števila, ki jih lahko zapišemo kot vsoto dveh kvadratov nenegativnih celih števil. Poleg tega smo pokazali, da se da vsako naravno število zapisati kot vsoto največ štirih popolnih kvadratov naravnih števil. Naravno se ponuja vprašanje, ali se da vsako število izraziti kot vsoto treh popolnih kvadratov? Do odgovora na to vprašanje je mnogo težje priti, kot do naših karakterizacij. V primeru dveh in štirih kvadratov smo imeli dve močni orodji, Gaussova in Hurwitzova števila, ki so podkolobar dvodimenzionalne algebre (obsega) kompleksnih števil, oziroma štiridimenzionalne algebre (obsega) kvarternionov. Vemo, da ne obstaja nobena trirazsežna algebra nad realnimi števili, ki bi bila tudi obseg, torej nimamo primernega orodja, da bi lahko analogno karakterizirali vsa števila, ki so vsota treh kvadratov nenegativnih celih števil. Presenetljivo lahko karakteriziramo vsa števila, ki so vsota največ treh popolnih kvadratov s pomočjo karakterizacije kvadratnih form nad obsegom celih števil. Dokaz pa poleg karakterizacije kvadratnih form zahteva temeljito znanje teorije kvadratnih kongruenc in poznavanje Dirichletovega izreka o praštevilih v aritmetičnem zaporedju. Izkaže se, da lahko naravno število zapišemo kot vsoto največ treh popolnih kvadratov natanko tedaj, ko ni oblike $4^\alpha(8k+7)$ (več o tem si lahko preberete v [3]).

Literatura

[1] J. Grasselli: *Elementarna teorija števil*, Ljubljana, DMFA-založništvo, 2009.

[2] I. Vidav: *Teorija števil in elementarna geometrija/izbor člankov*, DMFA-založništvo, 1996.

[3] L.J. Mordell: *Diophantine equations*, London, Academic Press, 1969.

[4] I. Vidav: *Algebra* , Ljubljana, DMFA-založništvo, 2003.

[5] I. N. Herstein: *Topics in Algebra*, London, Ginn and Company, 1964.