NYILATKOZAT

Név: Peremiczki Zsófia

ELTE Természettudományi Kar, szak: Matematika Bsc

NEPTUN azonosító: CZE4EJ

Szakdolgozat címe:
Gauss-egészek és kvaterniók

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2022.05.24.

Peremiczki Zsófia

a hallgató aláírása

Eötvös Loránd Tudományegyetem

Természettudományi Kar

Gauss-egészek és kvaterniók

Szakdolgozat

Peremiczki Zsófia

Matematika Bsc

Témavezető:

Dr. Kiss Emil

Algebra és Számelmélet Tanszék

ELTE
EÖTVÖS LORÁND
TUDOMÁNYEGYETEM

Budapest

2022

Tartalomjegyzék

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani témavezetőmnek, Dr. Kiss Emilnek, aki mindig azonnal megválaszolta az összes kérdésemet, folyamatosan segítette a szakdolgozatom létrejöttét. Megtisztelő, hogy egy ilyen nagy szakmai tudással rendelkező embertől tanulhattam ebben a korántsem egyszerű témában, amely iránt hétről-hétre egyre jobban fel is tudta kelteni az érdeklődésemet.

Külön köszönet illeti szaktársamat, Loreszt (Matúz Lórántot), aki bármilyen formázással vagy LaTeX-kóddal kapcsolatos kérdésben a segítségemre sietett, amikor szükség volt rá.

Bevezetés

A szakdolgozat témája a Gauss-egészeken keresztül a Pitagoraszi-számnégyesek, illetve a kvaterniókon keresztül a négy négyzetszám-tétel feldolgozása.

A Gauss-egészek Carl Friedrich Gauss-tól származnak. 1832-ben írt róluk először, egy másik matematikai probléma kapcsán, a kvadratikus reciprocitás, azaz egy bizonyos kongruencia megoldásának reményében. Ekkor még „egész komplex" számoknak nevezte őket. [1] Ez az elnevezés találó, ugyanis ennek a számkörnek az elemei azon komplex számokból állnak, amelyeknek mindkét együtthatója egész. Ezen Gauss-egészek létezése nem csak Gauss számára egyszerűsített le egy problémát: a Pitagoraszi-számnégyesek előállítását is megkönnyítik. Egy Pitagoraszi-számnégyes alatt pedig azt értjük, hogy létezik négy (egész) szám, amelyek közül három négyzetösszegét véve éppen a negyedik négyzetét kapjuk. Ilyen számnégyeseket nagyon könnyen alkothatunk: létezik hozzájuk egy konkrét képlet, amit később tétel formájában bizonyítunk.

A kvaterniók a komplex számok kibővítése, amelyek csoportjáról először Olinde Rodrigues írt 1840-ben, azonban a legtöbben Sir William Rowan Hamilton nevéhez kötik, aki a kvaterniókat 1843-ban fedezte fel. A matematika sok területén használják őket, alkalmazott matematika esetén például forgatások leírására. [2] A kvaterniók között is vannak egészek, de ezek közé már nem csak az egész együtthatósok tartoznak. A négy négyzetszám-tételt, azaz azt, hogy minden természetes szám előáll négy négyzetszám összegeként is egész kvaterniók segítségével látjuk be.

1 Gauss-egészek

Ebben a fejezetben először *Freud Róbert* és *Gyarmati Edit* 2014-es *Számelmélet* című könyve[3] alapján szedjük össze a Gauss-egészek legfontosabb tulajdonságait, miután néhány alapfogalmat bevezettünk.

1.1 Euklideszi-gyűrű

1.1.1 Definíció: (gyűrű)
Olyan struktúra, amely az összeadásra nézve Abel-csoport, a szorzásra nézve pedig félcsoport, és tetszőleges elemeire teljesülnek a disztributivitási szabályok (ha x, y, z gyűrűbeli elemek, akkor $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ és $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$).

◇

1.1.2 Definíció: (balideál)
Egy $\mathbf{R}$ *gyűrű egy* $\mathbf{B}$ *részhalmaza balideál, ha az összeadásra nézve részcsoport, és* $\forall b \in \mathbf{B}, r \in \mathbf{R}$ *elemre* $rb \in \mathbf{B}$.

◇

1.1.3 Definíció: (jobbideál)
Egy $\mathbf{R}$ *gyűrű egy* $\mathbf{J}$ *részhalmaza jobbideál, ha az összeadásra nézve részcsoport, és* $\forall j \in \mathbf{J}, r \in \mathbf{R}$ *elemre* $jr \in \mathbf{J}$.

◇

1.1.4 Definíció: (főideálgyűrű)
Egy $\mathbf{R}$ *szokásos gyűrű főideálgyűrű, ha minden ideálja főideál, azaz egy elemmel generálható.*

◇

Előbbi néhány definíció a későbbiekben, a kvaterniókról szóló részben is fontos lesz, ott azonban nem kommutatív a szorzás. Ebben a fejezetben még csak kommutatív gyűrűkről lesz szó.

1.1.5 Definíció: (Euklideszi-gyűrű)
$\mathbf{R}$ *euklideszi-gyűrű olyan kommutatív, egységelemes, nullosztómentes gyűrű, amelyben minden* $c \in \mathbf{R}$ *elemhez hozzárendelünk egy* $f(c) \geq 0$ *egész számot úgy, hogy* $f(c)$ *pontosan akkor nulla, ha* $c = 0$, *és minden* $a, b \in \mathbf{R}$, $b \neq 0$*-hoz létezik* $q, r \in \mathbf{R}$, *amelyekre* $a = bq + r$ *és* $f(r) < f(b)$.

◇

Tehát az **R** Euklideszi-gyűrűben van maradékos osztás, amely egy ismert tétel alapján azt jelenti, hogy **R** főideálgyűrű is. A főideálgyűrűkben pedig érvényes a számelmélet alaptétele, azaz ezeknek minden eleme (amely nem egység és nem nulla) egyértelműen felbontható véges sok felbonthatatlan szám szorzatára. [4]

1.2 Gauss-egészek

A Gauss-egészek számos tulajdonsága hasonlóan fogalmazható meg, mint az egész számok tulajdonságai, így a Gauss-egészek számelmélete és az egészek számelmélete valamilyen szinten össze is kapcsolható. Ehhez először definiáljuk a fogalmakat, és nézzük ezeknek néhány tulajdonságát.

1.2.1 Definíció: (Gauss-egész)
Az $\alpha = a + bi$ komplex szám Gauss-egész, ha $a, b \in \mathbb{Z}$.

◇

Ebből következik, hogy Gauss-egészek alkotják az egységnyi oldalú négyzetrács pontjait a komplex számsíkon (hiszen minden egész koordinátájú pontot hozzá tudunk rendelni egy Gauss-egészhez).

1.2.2 Definíció: (norma)
Az $\alpha = a + bi$ Gauss-egész normája: $N(\alpha) = |\alpha|^2 = a^2 + b^2$.

◇

1.2.3 Tétel:
Legyenek α, β tetszőleges Gauss egészek. Ekkor teljesülnek a következők:

(i) $N(\alpha) \geq 0$ *egész szám*

(ii) $N(\alpha) = 0$ *akkor és csak akkor, ha* $\alpha = 0$

(iii) $N(\alpha\beta) = N(\alpha)N(\beta)$.

1.2.4 Definíció: (osztó)
Legyenek α, β Gauss-egészek. β osztója α-nak, azaz $\beta|\alpha$, ha létezik γ Gauss-egész, amelyre $\alpha = \beta\gamma$.

◇

Ezen fogalmak bevezetésével már megfogalmazható a Gauss-egészek és egészek számelmélete közötti egyik fontos kapcsolat:

1.2.5 Tétel:
Ha α, β Gauss-egészekre $\alpha \mid \beta$, akkor normáikra $N(\alpha) \mid N(\beta)$ (ezek egész számok, így ezek körében értelmezve).

A tétel megfordítása nem teljesül, lássunk erre egy példát:

Példa:
Legyen $\alpha = 2 - i$, $\beta = 2 + i$. Ekkor $N(\alpha) = 2^2 + (-1)^2 = 5 = 2^2 + 1^2 = N(\beta)$.
Természetesen $5|5$ teljesül, azonban $2 + i \nmid 2 - i$, $\frac{2-i}{2+i} = \frac{(2-i)^2}{(2+i)(2-i)} = \frac{3-2i}{5} = \frac{3}{5} - \frac{2}{5}i$, ez pedig nem Gauss egész.

1.2.6 Definíció: (egység)
Egy Gauss-egész egység, ha minden Gauss-egésznek osztója.

◇

1.2.7 Tétel:
Legyen ε Gauss-egész. A következők ekvivalensek:

(i) ε *egység*

(ii) $\varepsilon \mid 1$

(iii) $N(\varepsilon) = 1$

(iv) $\varepsilon = 1, -1, i, -i$.

1.2.8 Tétel: (maradékos osztás a Gauss-egészek körében)
Ha $\alpha, \beta (\beta \neq 0)$ Gauss-egészek, akkor léteznek γ, ρ Gauss-egészek, amelyekkel $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

1.2.9 Definíció: (legnagyobb közös osztó)
Legyenek α, β Gauss-egészek, $\beta \neq 0$. Ezek legnagyobb közös osztója δ, ha δ osztója α-nak és β-nak is, és ha létezik ugyanilyen tulajdonságú γ, akkor $\gamma \mid \delta$. Jelölés: $(\alpha, \beta) = \delta$.

◇

1.3 Gauss-prímek

A Gauss-prímek a Gauss-egészek körében olyanok, mint a prímek az egészek körében. Emiatt minden prímekkel kapcsolatos definíció, állítás megfogalmazható a Gauss-prímekkel kapcsolatban. Ezek azért lesznek fontosak, mert segítségükkel kimondható, és bizonyítható a számelmélet alaptételének ezen számkörbeli megfelelője.

1.3.1 Definíció: (Gauss-felbonthatatlan)
Legyen $\pi \neq 0$ Gauss-egész, ami nem egység. π Gauss-felbonthatatlan, ha csak úgy bontható fel két Gauss-egész szorzatára, hogy valamelyik tényező egység, azaz ha $\pi = \alpha\beta$, akkor α vagy β egység.

◇

1.3.2 Definíció: (Gauss-prím)
Legyen $\pi \neq 0$ Gauss-egész, ami nem egység. π Gauss-prím, ha két Gauss-egésznek csak úgy lehet osztója, hogy legalább az egyik tényezőnek osztója, azaz ha $\pi \mid \alpha\beta$, akkor $\pi \mid \alpha$ vagy $\pi \mid \beta$.

◇

Természetesen a Gauss-egészek körében is ekvivalens a két fogalom, az egészek köréből ismert tétel itt is megfogalmazható:

1.3.3 Tétel:
Egy α Gauss-egész pontosan akkor Gauss-prím, ha Gauss-felbonthatatlan.

Bizonyítás:
Feltehető, hogy α nem nulla és nem egység.

Az egyik irány: α Gauss-prím $\Rightarrow$ α Gauss-felbonthatatlan.

Ehhez tegyük fel, hogy α Gauss-prím, és előáll a következő szorzatként: $\alpha = \beta\gamma$ (β, γ Gauss-egészek). Emiatt $\alpha \mid \beta\gamma$ is teljesül, ami a prímek definíciója szerint azt jelenti, hogy $\alpha \mid \beta$ vagy $\alpha \mid \gamma$.

Ha $\alpha \mid \beta$, az azt jelenti, hogy $\beta\gamma \mid \beta$, és mivel $\beta \neq 0$, ezért ekkor $\gamma \mid 1$, vagyis γ egység.

Ha $\alpha \mid \gamma$, az azt jelenti, hogy $\beta\gamma \mid \gamma$, és mivel $\gamma \neq 0$, ezért ekkor $\beta \mid 1$, vagyis β egység.

Mindkét esetben a Gauss-felbonthatatlanság definícióját kapjuk.

A másik irány: α Gauss-felbonthatatlan $\Rightarrow$ α Gauss-prím.

Tegyük fel, hogy α Gauss-felbonthatatlan. Induljunk ki az $\alpha \mid \beta\gamma$ oszthatóságból (ezek most is Gauss-egészek).

Ha $\alpha \mid \beta$, akkor α Gauss-prím.
Ha nem, akkor mivel tudjuk, hogy α felbonthatatlan, és $(\alpha, \beta) \mid \alpha$, ezért $(\alpha, \beta) = 1$. Ekkor

$$(\alpha, \beta) = 1 = \alpha\tau_1 + \beta\tau_2, \text{ (ahol } \tau_1, \tau_2 \text{ megfelelő Gauss-egészek).}$$

Ezt balról szorozva γ-val kapjuk, hogy

$$\gamma = \gamma\alpha\tau_1 + \gamma\beta\tau_2$$

A jobb oldali összeg mindkét tagja osztható α-val, ezért a bal oldal is osztható vele, azaz $\alpha \mid \gamma$, így α Gauss-prím.

□

1.3.4 Tétel: (a számelmélet alaptétele)
Minden nullától és egységtől különböző Gauss-egész egyértelműen (tényezők sorrendjétől és egységszerestől eltekintve) felbontható véges sok Gauss-felbonthatatlan szorzatára.

Bizonyítás:
A felbonthatóság létezésének bizonyítása:

Legyen α Gauss-egész nem nulla és nem egység. Ha α Gauss-felbonthatatlan, akkor önmaga a felbontása.

Tehát feltehetjük, hogy α nem Gauss-felbonthatatlan. Ekkor pedig létezik nemtriviális Gauss-felbonthatatlan osztója, mert a legkisebb normájú nemtriviális osztójának Gauss-felbonthatatlannak kell lennie. Ezen osztója legyen α_1, ezzel pedig $\alpha = \alpha_1\beta_1$ valamilyen egységtől különböző β_1 Gauss-egésszel.

Ha β_1 is Gauss-felbonthatatlan, akkor megkaptuk α felbontását, ha nem, akkor ehhez is van olyan Gauss-felbonthatatlan α_2 Gauss-egész, amellyel $\alpha_1 = \alpha_2\beta_2$ valamilyen egységtől különböző β_2 Gauss-egésszel. Ugyanezt folytatjuk α_2-vel, majd tovább, ameddig szükséges.

Ez az eljárás egy idő után véget ér, mert egyre kisebb normájú Gauss-egészeket veszünk, ezen normák pedig mindig pozitívak, így egy idő után eljutunk egy Gauss-felbonthatatlan α_n Gauss-egészhez, amelyre így $\alpha_n = \beta_n$, ezzel pedig a felbontás a következő:

$$\alpha = \beta_1\beta_2...\beta_n.$$

A felbonthatóság egyértelműségének bizonyítása:

Indirekt tegyük fel, hogy α-nak létezik két lényegesen különböző felbontása:

$$\alpha = \beta_1..\beta_n = \gamma_1..\gamma_m$$

($\beta_1, ..\beta_n, \gamma_1, ..\gamma_m$ Gauss-felbonthatatlanok).

Ha van olyan γ_i tényező, amely egységszerese valamelyik β_j, akkor γ_i-vel leoszthatunk, és az $\frac{\alpha}{\gamma_i}$-nek kapjuk két lényegesen különböző Gauss-felbontását.

Ezt addig ismételjük, amíg olyan Gauss-egészhez nem jutunk, amelynek kétféle felbontásában nincsenek olyan tényezők, melyek egymásnak egységszeresei. Feltehetjük, hogy α már ilyen (eljutottunk hozzá egy nagyobb Gauss-egésztől).

Mivel

$$\beta_1..\beta_n = \gamma_1..\gamma_m,$$

ezért

$$\beta_1 \mid \gamma_1..\gamma_m.$$

β_1 Gauss-felbonthatatlan, illetve a *1.3.3* tételből tudjuk, hogy minden Gauss-felbonthatatlan egyben Gauss-prím is, ezért β_1 Gauss-prím, azaz biztosan osztója valamelyik γ_i tényezőnek. De ekkor γ_i Gauss-felbonthatatlansága miatt β_1 egység, vagy γ_i egységszerese, ez pedig nem lehetséges.

□

1.3.5 Tétel: (az összes Gauss-prím)
Ha ε egy tetszőleges egység, akkor az összes Gauss-prím megadható a következő három módszer valamelyikével:

(i) $\varepsilon(1+i)$

(ii) εq, *ahol* $q = 4k+1$ *alakú prím valamely egész* k*-ra*

(iii) π, *ahol* $N(\pi) = 4k+1$ *alakú (pozitív) prím valamely (pozitív) egész* k*-ra: minden* $N(\pi)$*-hez (egységszerestől eltekintve) két Gauss-prím tartozik, amelyek egymás konjugáltjai (normáik ekkor triviálisan megegyeznek).*

Ennek a tételnek a segítségével könnyen ellenőrizhető egy Gauss-egészről, hogy Gauss-prím-e, vagy sem. Nézzünk is erre néhány példát.

Példa:
Triviálisan Gauss-prím az $1+i$, illetve a $-1+i$, hiszen ez utóbbi megyegyezik $i(1+i)$-vel.

A $2-5i$ és $2+5i$ is Gauss-prímek: $(2+5i)(2-5i) = 4+25 = 29$, és $29 = 4 \cdot 7 + 1$,
tehát $k = 7$-re $4k+1$ alakú.
Azonban az $5-2i$ és az $5+2i$ esetében hiába ugyanez a szorzat, ezek az előbbieknek egységszeresei (pontosabban i-szeresei), így a számelmélet alaptétele miatt már nem lehetnek azoktól különböző Gauss-prímek.

Példa:
A $9-2i$ nem Gauss-prím, mert $(9-2i)(9+2i) = 81+4 = 85$ nem prímszám, és nem is egy prímszám négyzete.

A -13 sem Gauss-prím, mert bár $4k-1$ alakú, de negatív. Emellett egységszerese a 13-nak, amely egy prím, de ez pedig már nem $4k-1$ alakú.

1.4 A két-négyzetszám-tétel

Egy diofantikus egyenlet olyan egész együtthatós egyenlet, amelynek megoldásai is egészek. Az $x^2+y^2 = n$ diofantikus egyenlet megoldhatóságát és megoldásszámát taglaló tétel az eddigieknek egy alkalmazása:

1.4.1 Tétel: (két-négyzetszám-tétel)
Legyen az $n \in \mathbb{Z}^+$ *kanonikus alakja* $n = 2^{\alpha} p_1^{\beta_1} ... p_r^{\beta_r} q_1^{\gamma_1} ... q_s^{\gamma_s}$*, ahol* $p_1, ..p_r$ $4k+1$ *alakú prímek,* $q_1, ..q_s$ $4k-1$ *alakú prímek, és az összes kitevő nemnegatív egész.*
Az $x^2+y^2 = n$ *diofantikus egyenlet akkor és csak akkor oldható meg, ha* γ_i *páros* $\forall i$*-re, és ekkor a megoldásszám* $4 \prod_{j=1}^{r} (\beta_j + 1)$.

Kimondható ennek egy magasabb dimenziós változata is, ez viszont nem arról szól, mikor van megoldás, hanem arról, hogy mikor nincs:

1.4.2 Tétel: (három-négyzetszám-tétel)
Az $n \in \mathbb{Z}$ *akkor és csak akkor nem áll elő három négyzetszám összegeként, ha* $n = 4^k(8m+7)$ *(*$k, m \in \mathbb{Z}$*).*

Példa:
Ha $n = 4^1(8 \cdot 1 + 7) = 60$, akkor nincs ilyen előállítás, azonban ha hozzáadunk 1-et (így biztosan nem lesz olyan alakú, mint a 60), akkor 61-et kapunk, ami pedig előáll három négyzetszám összegeként:

$$61 = 9 + 25 + 36 = 3^2 + 4^2 + 6^2.$$

Ezzel persze nem láttuk be, hogy minden esetben igaz a tétel, de erre a nehéz bizonyításra ebben a dolgozatban nem térünk ki.

A dolog érdekessége az, hogy még magasabb dimenziót tekintve, négy négyzetszám összegeként minden pozitív egész szám előáll. Ennek a tételnek a kimondása és bizonyítása majd később következik, a kvaterniók bevezetése után (*2.3.1*).

1.5 Pitagoraszi-számnégyesek bevezetése

Ebben a részben egy cikk[5], és annak korábbi, nem kiadott változata alapján foglaljuk össze az eredményeket.

Ha $a, b, c, d \in \mathbb{Z}$ Pitagoraszi-számnégyes, akkor $a^2 + b^2 + c^2 = d^2$ teljesül. Ezt abban az esetben vizsgáljuk, amikor ezek relatív prímek, azaz $(a, b, c, d) = 1$. Ebből világos, hogy nem lehet mindegyik szám páros, hiszen akkor a 2 is osztójuk lenne. Tehát lennie kell köztük páratlan számnak: ha b és c páros, akkor a és d páratlan, ez könnyen belátható a 4-gyel való osztási maradékok segítségével:

Ha valamelyik szám $2k + 1$ alakú, akkor négyzetre emelve 1-gyel lesz kongruens mod 4, a $2k$ alakú számok pedig nyilván 0-val. Ebből és $(a, b, c, d) = 1$-ből már következik, hogy a bal oldalon pontosan egy szám páratlan (persze ekkor a négyzete is az), és a jobb oldal is páratlan.

A Pitagoraszi-számnégyesek előállításáról szóló tétel bizonyítása a fő célunk, amelyhez szükségünk lesz egy lemmára.

1.5.1 Lemma:
Legyenek x, y pozitív egészek, γ Gauss-egész, $xy = \gamma\overline{\gamma}$, $(x, y, \gamma, \overline{\gamma}) = 1$. Ekkor léteznek m, n, p, q pozitív egészek, amelyekkel

$$x = (m + ni)(m - ni),$$
$$y = (p + qi)(p - qi),$$
$$\gamma = (m + ni)(p + qi),$$
$$\overline{\gamma} = (m - ni)(p - qi).$$

Adott x, y, γ-hoz pontosan négy (m, n, p, q) számnégyes van, és minden ilyenre teljesül, hogy $(x, \gamma) = m + ni$, $(y, \gamma) = p + qi$, hiszen γ éppen x és y nagyobbik szorzótényezőinek szorzata.

Bizonyítás:
Definiáljuk a következő Gauss-egészeket:

$$\alpha := (x, \gamma) = m + ni,$$
$$\beta := (y, \gamma) = p + qi.$$

Ezeket konjugálva kapjuk:

$$\overline{\alpha} = m - ni = (x, \overline{\gamma})$$

$$\overline{\beta} = p - qi = (y, \overline{\gamma})$$

Nézzük α és $\overline{\beta}$ legnagyobb közös osztóját. $xy = \gamma\overline{\gamma}$ miatt felírható a következő:

$$\frac{x}{\alpha} \cdot \frac{y}{\overline{\beta}} = \frac{\gamma}{\alpha} \cdot \frac{\overline{\gamma}}{\overline{\beta}}$$

Ebből látható, hogy

$$\frac{x}{\alpha} \text{ és } \frac{\overline{\gamma}}{\overline{\beta}}$$

osztói egymásnak, mert

$$\left(\frac{x}{\alpha}, \frac{\gamma}{\alpha}\right) = (m - ni, p + qi) = (p + qi, m - ni) = \left(\frac{y}{\overline{\beta}}, \frac{\overline{\gamma}}{\overline{\beta}}\right) = 1.$$

$(\alpha, \overline{\beta})$ osztója lesz $x, y, \gamma, \overline{\gamma}$ legnagyobb közös osztójának, ami viszont feltétel szerint 1, így $(\alpha, \overline{\beta}) = 1$.

$(\alpha, \overline{\beta}) = 1$ miatt $\frac{\overline{\gamma}}{\overline{\beta}}$ és $\left(\alpha\frac{\overline{\gamma}}{\overline{\beta}}, \overline{\beta}\frac{\overline{\gamma}}{\overline{\beta}}\right)$ egymás egységszeresei, és

$$\left(\alpha\frac{\overline{\gamma}}{\overline{\beta}}, \overline{\beta}\frac{\overline{\gamma}}{\overline{\beta}}\right) = \left((m + ni)\frac{(m - ni)(p - qi)}{p - qi}, (p - qi)\frac{(m - ni)(p - qi)}{p - qi}\right),$$

tehát $(x, \overline{\gamma}) = \overline{\alpha} = m - ni$ is egységszerese ezeknek.

Ennek felhasználásával és α-t egy megfelelő Gauss-egységgel szorozva azt kapjuk, hogy

$$\frac{\overline{\gamma}}{\overline{\beta}} = \overline{\alpha}.$$

Ezt rendezve $\gamma = \alpha\beta$, balról α-val szorozva pedig $\alpha\frac{\overline{\gamma}}{\overline{\beta}} = \alpha\overline{\alpha}$-t kapjuk, amely x-nek egységszerese. Mivel x és $\alpha\overline{\alpha}$ is pozitív egészek, így ezek megegyeznek. Azt hozzávéve, hogy $xy = \gamma\overline{\gamma}$ kapjuk, hogy

$$y = \frac{\gamma\overline{\gamma}}{x} = \beta\overline{\beta}.$$

Könnyen belátható a lemma utolsó része is, azaz, hogy négy ilyen számnégyes van, ez abból következik, hogy a Gauss-egészek körében négy egység van: $\{1, -1, i, -i\}$.

□

1.6 Pitagoraszi-számnégyesek előállítása

1.6.1 Tétel:
Ha $(a, b, c, d) = 1$, a, d páratlanok és $a^2 + b^2 + c^2 = d^2$, akkor a, b, c, d a következő alakúak ($m, n, p, q \in \mathbb{Z}$):

$$a = m^2 + n^2 - p^2 - q^2,$$
$$b = 2(mq + np),$$

$$c = 2(-mp + nq),$$
$$d = m^2 + n^2 + p^2 + q^2.$$

(Az $n = 0 = q$ választással $a = m^2 - p^2$, $b = 0$, $c = -2mp$, $d = m^2 + p^2$, amivel Pitagoraszi-számhármast kapunk.)[5]

Bizonyítás:
Az eredeti $a^2+b^2+c^2 = d^2$ egyenletből kivonva a^2-et és leosztva 4-gyel, illetve a jobb oldalon egy azonosság felhasználásával kapjuk a következőt:

$$\left(\frac{c}{2}\right)^2 + \left(\frac{b}{2}\right)^2 = \frac{d+a}{2} \cdot \frac{d-a}{2}$$

Ezt tovább alakítva, a Gauss-egészek körében:

$$\left(-\frac{c}{2} + \frac{b}{2}i\right) \cdot \left(-\frac{c}{2} - \frac{b}{2}i\right) = \frac{d+a}{2} \cdot \frac{d-a}{2}$$

Erre alkalmazzuk az előző lemmát:

$$x := \frac{d+a}{2}$$
$$y := \frac{d-a}{2}$$
$$\gamma := -\frac{c}{2} + \frac{b}{2}i$$

Hogy használhassuk a lemmát, még be kell látnunk, hogy ezek legnagyobb közös osztója az 1. Ezt indirekten könnyen megtehetjük: ha létezne egy Gauss-egész, ami osztója $\frac{d+a}{2}$-nek és $\frac{d-a}{2}$-nek is, akkor ezek összegének, azaz d-nek is osztója lenne, és különbségüknek, azaz a-nak is. Osztója még $-\frac{c}{2} + \frac{b}{2}i$-nek és $-\frac{c}{2} - \frac{b}{2}i$-nek is, ebből pedig összegüknek, azaz $-c$-nek, és különbségüknek, azaz bi-nek is osztója. Így osztója lenne a, b, c-nek is, de feltettük, hogy $(a, b, c) = 1$, így ellentmondásba ütközünk.

Így már megkaphatjuk a lemma segítségével, hogy adott m, n, p, q egészekre teljesülnek:

$$\frac{d+a}{2} = (m + ni)(m - ni),$$
$$\frac{d-a}{2} = (p + qi)(p - qi),$$
$$-\frac{c}{2} + \frac{b}{2}i = (m + ni)(p + qi).$$

Az első kettőből

$$d + a = 2(m^2 + n^2),$$
$$d - a = 2(p^2 + q^2).$$

Ezeket összeadva, kivonva

$$d = m^2 + n^2 + p^2 + q^2,$$

$$a = m^2 + n^2 - p^2 - q^2.$$

A harmadikból

$$-\frac{c}{2} + \frac{b}{2}i = (mp - nq) + (mq + np)i.$$

A két oldal valós és képzetes részeit egymással egyenlővé téve kapjuk, hogy

$$-\frac{c}{2} = mp - nq$$

$$\frac{b}{2} = mq + np.$$

Ezekből kifejezve b, c-t:

$$c = 2(-mp + nq)$$

$$b = 2(mq + np).$$

□

Nézzünk meg egy konkrét előállítást, amelyet a tétel alkalmazásával kaphatunk. Ehhez csak m, n, p és q értékeit kell megválasztanunk tetszőleges egész számnak, ügyelve arra, hogy $(a, b, c, d) = 1$ teljesüljön, illetve a és d páratlanok legyenek. Ezt könnyen megtehetjük, ha a négy paraméter közül pontosan egyet választunk páratlannak.

Példa:
Legyenek a paraméterek értékei a következők:

$$m = 1,\ n = 2,\ p = 4,\ q = 6$$

Ezekből a következőképpen kapjuk a számnégyes tagjait:

$$a = m^2 + n^2 - p^2 - q^2 = 1^2 + 2^2 - 4^2 - 6^2 = -47$$

$$b = 2(mq + np) = 2(1 \cdot 6 + 2 \cdot 4) = 28$$

$$c = 2(-mp + nq) = 2(-1 \cdot 4 + 2 \cdot 6) = 16$$

$$d = m^2 + n^2 + p^2 + q^2 = 1^2 + 2^2 + 4^2 + 6^2 = 57$$

Nézzük, hogy valóban Pitagoraszi-számnégyest kaptunk-e:

$$a^2 + b^2 + c^2 = (-47)^2 + 16^2 + 28^2 = 2209 + 256 + 784 = 3249 = 57^2 = d^2,$$

azaz a $\{-47, 16, 28, 57\}$ valóban Pitagoraszi-számnégyes, és az is látható, hogy ezek relatív prímek.

2 | Négy négyzetszám-tétel

Ebben a fejezetben az $x^2 + y^2 + u^2 + v^2 = n,\ n \in \mathbb{N}, x, y, u, v, \in \mathbb{Z}$ diofantikus egyenlet megoldásait keressük. Maga a négy négyzetszám-tétel éppen arról szól, hogy ennek az egyenletnek bármilyen (a feltételnek megfelelő) jobb oldallal van megoldása, vagyis az eddigiekkel ellentétben most nem kell más kikötéseket tennünk, ahogy például a három négyzetszám-tétel esetében meg kellett határoznunk, hogy milyen alakú n-re nincs megoldás.

Ezt úgy is megfogalmazhatjuk, hogy keressük egy természetes szám négy négyzetszámra való felbontásait. Amit később bizonyítunk, az az, hogy ilyen felbontás mindig létezik, a számáról pedig néhány érdekes részeredményt olvashatunk a dolgozatban.

2.1 Kvaterniók

A kvaterniók hasonlóak a komplex számokhoz, csak ezeket nem kettő, hanem négy dimenzióban értelmezzük. Ezek esetében a valós számok körét nem csak i-vel, hanem i, j, k-val egészítjük ki, amelyekre igazak a következők:

- $i^2 = j^2 = k^2 = ijk = -1$
- $ij = k$, $ji = -k$
- $jk = i$, $kj = -i$
- $ki = j$, $ik = -j$

Ezen tulajdonságú i, j, k elemek segítségével megadhatjuk a kvaterniókat: olyan $a+bi+cj+dk$ alakú számok, ahol $a, b, c, d \in \mathbb{R}$. A kvaterniók gyűrűjét $\mathbb{H}$-val jelöljük.

Legyen $\alpha = a+bi+cj+dk$ egy kvaternió, azaz $a, b, c, d \in \mathbb{R}$. A továbbiakban ezt használjuk a definíciókban.

2.1.1 Definíció: (konjugált)
Az α konjugáltja $\overline{\alpha} = a - bi - cj - dk$.

$\diamond$

2.1.2 Definíció: (norma)
Az α normája $N(\alpha) = a^2 + b^2 + c^2 + d^2$.

$\diamond$

Ez megegyezik $\alpha\overline{\alpha}$-val és $\overline{\alpha}\alpha$-val is, hiszen

$$\overline{\alpha}\alpha = \alpha\overline{\alpha} = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 - b^2i^2 - c^2j^2 - d^2k^2$$

(a vegyes tagok kiejtik egymást), és mivel $i^2 = j^2 = k^2 = -1$, ez épp a norma.

2.1.3 Definíció: (valós rész)
Az α valós része a.

◇

2.1.4 Definíció: (képzetes rész)
Az α képzetes része $bi + cj + dk$.

◇

2.1.5 Definíció: (kvaternió inverze)
Az α kvaternió inverze az az α^{-1} kvaternió, amelyre $\alpha\alpha^{-1} = 1$.

◇

2.1.6 Definíció: (tisztán képzetes kvaternió)
Az α kvaternió tisztán képzetes, ha valós része 0 ($a = 0$), azaz $\alpha = bi + cj + dk$.

◇

2.1.7 Definíció: (nyom)
Az α nyoma $tr(\alpha) = \alpha + \overline{\alpha} = 2a$.

◇

Ezekből következik:

2.1.8 Állítás:
$\alpha^2 - tr(\alpha)\alpha + N(\alpha) = 0$.

Bizonyítás:
Ezt könnyen ellenőrizhetjük az eddigieket alkalmazva:

$$\alpha^2 - \mathrm{tr}(\alpha)\alpha + N(\alpha) = \alpha^2 - (\alpha + \overline{\alpha}) \cdot \alpha + \alpha\overline{\alpha} = \alpha^2 - \alpha^2 - \overline{\alpha}\alpha + \alpha\overline{\alpha} = \alpha\overline{\alpha} - \overline{\alpha}\alpha$$

Természetesen $\alpha\overline{\alpha} = \overline{\alpha}\alpha$, így a végeredmény valóban 0.

□

2.1.9 Állítás:
Ha $\alpha_1, \alpha_2 \in \mathbb{H}$, akkor $\overline{\alpha_1\alpha_2} = \overline{\alpha_2} \cdot \overline{\alpha_1}$.

Bizonyítás:
Legyen $\alpha_1 = a_1 + b_1i + c_1j + d_1k$ és $\alpha_2 = a_2 + b_2i + c_2j + d_2k$.

Nézzük először az egyenlőség bal oldalát.

$$\overline{\alpha_1\alpha_2} = \overline{(a_1 + b_1i + c_1j + d_1k)(a_2 + b_2i + c_2j + d_2k)}.$$

Tehát először összeszorozzuk α_1-et és α_2-t, majd konjugálunk. A szorzás kifejtve:

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

$$= a_1 a_2 + a_1 b_2 i + a_1 c_2 j + a_1 d_2 k + b_1 a_2 i + b_1 b_2 i^2 + b_1 c_2 ij + b_1 d_2 ik +$$

$$+ c_1 a_2 j + c_1 b_2 ji + c_1 c_2 j^2 + c_1 d_2 jk + d_1 a_2 k + d_1 b_2 ki + d_1 c_2 kj + d_1 d_2 j^2$$

Erre alkalmazzuk a kvaterniók szorzási szabályait, és kiemelünk i, j, k-t:

$$(a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + i(a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) +$$

$$+ j(a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) + k(a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)$$

Ebből konjugálással kapjuk az eredményt:

$$\overline{\alpha_1 \alpha_2} =$$

$$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) - i(a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) -$$

$$- j(a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) - k(a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)$$

Most nézzük meg az egyenlőség jobb oldalát.

Itt $\overline{\alpha_2} = a_2 - b_2 i - c_2 j - d_2 k$ és $\overline{\alpha_1} = a_1 - b_1 i - c_1 j - d_1 k$, tehát

$$\overline{\alpha_2} \cdot \overline{\alpha_1} = (a_2 - b_2 i - c_2 j - d_2 k)(a_1 - b_1 i - c_1 j - d_1 k).$$

A bal oldal kiszámításához hasonlóan ezt is fejtsük ki, majd alkalmazzuk a szorzási szabályokat, és emeljünk ki $-i, -j, -k$-t.

$$(a_2 - b_2 i - c_2 j - d_2 k)(a_1 - b_1 i - c_1 j - d_1 k) =$$

$$= a_2 a_1 - a_2 b_1 i - a_2 c_1 j - a_2 d_1 k - b_2 a_1 i + b_2 b_1 i^2 + b_2 c_1 ij + b_2 d_1 ik -$$

$$- c_2 a_1 j + c_2 b_1 ji + c_2 c_1 j^2 + c_2 d_1 jk - d_2 a_1 k + d_2 b_1 ki + d_2 c_1 kj + d_2 d_1 k^2 =$$

$$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) - i(a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) -$$

$$- j(a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) - k(a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)$$

Ez pedig éppen az, amit a másik oldalra is kaptunk, tehát valóban $\overline{\alpha_1 \alpha_2} = \overline{\alpha_2} \cdot \overline{\alpha_1}$.

□

Ennek az állításnak a használatával könnyen belátható a következő:

2.1.10 Állítás:
Ha $\alpha_1, \alpha_2 \in \mathbb{H}$, akkor normáikra: $N(\alpha_1 \alpha_2) = N(\alpha_1) N(\alpha_2)$.

Bizonyítás:

$$N(\alpha_1\alpha_2) = \alpha_1\alpha_2\overline{\alpha_1\alpha_2} = \alpha_1\alpha_2\overline{\alpha_2}\cdot\overline{\alpha_1} = \alpha_1 N(\alpha_2)\overline{\alpha_1} = N(\alpha_1)N(\alpha_2)$$

Az első egyenlőség a norma definíciójából, a második a *2.1.9* állításból következik. A harmadik triviális, a negyedik pedig amiatt lesz igaz, hogy a norma valós számként felcserélhető bármely kvaternióval.

□

A kvaterniók egy szűkebb csoportja a Hurwitz-kvaterniók, más néven egész kvaterniók, ezek esetében a, b, c, d mindegyike egész, vagy minden együttható egy egész páratlan számnak a fele. Ezt vehetjük a Gauss-egészek megfelelőjének magasabb dimenzióban.

Az egész kvaterniókat $\mathbb{E}$-vel jelöljük. Egy egész kvaternió paritása a normája paritása alapján adódik.

Definiálunk még egy speciális kvaterniót:

$$\sigma = \frac{1+i+j+k}{2}.$$

Ennek normája $N(\sigma) = 4\cdot(\frac{1}{2})^2 = 1$, illetve azt is érdemes megjegyezni, hogy $\overline{\sigma} = 1-\sigma$.

2.1.11 Állítás:
A Hurwitz-kvaterniók gyűrűt alkotnak.

Bizonyítás:
Egy α kvaternió pontosan akkor van $\mathbb{E}$-ben, ha a $\{\sigma, i, j, k\}$ elemek egész együtthatós lineáris kombinációja, így elég ezeket vizsgálni.

Számoljunk ki néhány lehetőséget:

$$\sigma^2 = \frac{1+i+j+k}{2}\cdot\frac{1+i+j+k}{2} =$$

$$= \frac{1+i^2+j^2+k^2+2i+2j+2k+ij+ik+ji+jk+ki+kj}{4} =$$

$$= \frac{1-3+2(i+j+k)}{4} = \frac{-2+2(i+j+k)}{4} =$$

$$= \frac{2+2(i+j+k)-4}{4} = \frac{1+i+j+k}{2} - 1.$$

$$\sigma i = \frac{1+i+j+k}{2}\cdot i = \frac{-1+i+j-k}{2}.$$

$$i\sigma = i\cdot\frac{1+i+j+k}{2} = \frac{-1+i-j+k}{2}$$

Hasonlóan lehetne igazolni a többi szorzatra is, hogy $\mathbb{E}$-beli elemet kapunk, tehát valóban gyűrű.

□

2.2 A kvaterniók számelmélete algebrai szemmel

A következőkben az egész kvaterniók $\mathbb{E}$ gyűrűjében dolgozunk, egy cikk felhasználásának segítségével[5]. Ehhez majd szükségünk lesz néhány alapvető algebrai, gyűrűkkel kapcsolatos fogalomra, amelyeket a Gauss-egészek fejezetében már definiáltunk.

A kvaterniók körében is létezik oszthatóság:

2.2.1 Definíció: (oszthatóság)
Egy $\alpha \in \mathbb{E}$ balról osztható $\beta \in \mathbb{E}$ kvaternióval, ha létezik $\gamma \in \mathbb{E}$ kvaternió, amire $\alpha = \beta\gamma$, ennek jelölése $\beta \mid \alpha$.

$\diamond$

Emiatt definiálhatunk egységeket is:

2.2.2 Definíció: (egység)
Egy egész kvaternió egység, ha $\mathbb{E}$ minden elemét osztja (balról).

$\diamond$

2.2.3 Állítás:
Egy $\varepsilon \in \mathbb{E}$ pontosan akkor egység, ha normája 1.

2.2.4 Állítás:
Az egységek $\mathbb{E}$-ben a következők:

$$\pm 1,\ \ \pm i,\ \ \pm j,\ \ \pm k,\ \ \frac{\pm 1 \pm i \pm j \pm k}{2},$$

tehát összesen 24 darab van belőlük.

Bizonyítás:
Nézzük meg, hogy pontosan miért is ezek az egységek $\mathbb{E}$-ben: az első nyolc triviális, így a maradék 16-ról lesz szó.

Ha $\alpha = \frac{a+bi+cj+dk}{2} \mid 1$, akkor $N(\alpha) \mid N(1) = 1$, azaz $N(\alpha) = 1$.

$$1 = N(\alpha) = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2 + \left(\frac{d}{2}\right)^2 = \frac{a^2+b^2+c^2+d^2}{4}$$

Azaz $a^2+b^2+c^2+d^2 = 4$, ami mivel a $(\pm 2)^2 = 4$ esetben azt jelentené, hogy az egység a felsorolás első nyolc egységének valamelyike, de most a többit nézzük, csak úgy lehetséges, hogy $a, b, c, d = \pm 1$, azaz valóban $\frac{\pm 1 \pm i \pm j \pm k}{2}$ alakúak.

$\square$

A következő tétel a maradékos osztásról szintén hasonlóan fogalmazható meg, mint a Gauss-egészek esetében.

2.2.5 Tétel:
Az egész kvaterniók $\mathbb{E}$ gyűrűje bal euklideszi, azaz $\forall \alpha, \gamma \in \mathbb{E}$ $(\gamma \neq 0)$ $\exists \beta, \delta \in \mathbb{E}$, amelyekkel $\alpha = \beta\gamma + \delta$ és $N(\delta) < N(\gamma)$, azaz van maradékos osztás $\mathbb{E}$-ben.[6]

Bizonyítás:
Belátjuk, hogy $\mathbb{E}$ bal euklideszi gyűrű.

Legyenek $\alpha, \beta \in \mathbb{E}$ nem nulla kvaterniók olyanok, hogy

$$\beta^{-1}\alpha = x_0 + x_1 i + x_2 j + x_3 k.$$

Keressük meg azt az $\mathbb{E}$-beli elemet, amely a lehető „legközelebb" van $\beta^{-1}\alpha$-hoz.

Legyenek c_0, c_1, c_2, c_3 azonos paritású egészek, amelyekre igaz, hogy

$$|2x_i - c_i| \leq 1,\ i = 0, 1, 2, 3$$

Válasszuk úgy c_i-t, hogy legalább egy i-re szigorú egyenlőtlenség is teljesül.

Tudjuk, hogy az összes $\mathbb{E}$-beli kvaternió felírható a következő alakban is:

$$\omega = \frac{1}{2}(c_0 + c_1 i + c_2 j + c_3 k)$$

Tehát ω is egész kvaternió.

Nézzük a következő műveletet:

$$\beta^{-1}\alpha - \omega = x_0 + x_1 i + x_2 j + x_3 k - \left(\frac{1}{2}(c_0 + c_1 i + c_2 j + c_3 k)\right) =$$

$$= \frac{1}{2}(2x_0 - c_0) + \frac{1}{2}(2x_1 - c_1)i + \frac{1}{2}(2x_2 - c_2)j + \frac{1}{2}(2x_3 - c_3)k,$$

ennek a kvaterniónak a normája 1-nél kisebb.

Vezessünk be egy jelölést: $\gamma = \beta(\beta^{-1}\alpha - \omega)$

Ezt használva kapjuk a következőt:

$$\alpha = \beta\omega + \gamma, \text{ és teljesül, hogy } N(\gamma) < N(\beta),$$

hiszen tudjuk, hogy kvaterniók szorzatának normája megegyezik a normák szorzatával, amely pedig szükségképpen nagyobb vagy egyenlő, mint bármelyik (szorzatbeli) kvaternió normája.

Ebből kiderül, hogy az $\mathbb{E}$ gyűrűben létezik baloldali euklideszi osztás, azaz valóban bal euklideszi.

□

Ennek legfontosabb következménye, hogy a Hurwitz-kvaterniók körében is érvényes a számelmélet alaptétele, azaz, hogy minden $\mathbb{E}$-beli kvaternió felbontható irreducibilis kvaterniók szorzatára (ennek bizonyítása később, a *2.2.8* állításban).

Az egész kvaterniók körébe áthozhatjuk a Gauss-egészeknél látott definíciókat; teljesen hasonlóan adódik, hogy melyek a felbonthatatlanok.

2.2.6 Definíció: (felbonthatatlan)
Az $\alpha \in \mathbb{E}$ (amely nem egység) felbonthatatlan, ha felírva

$$\alpha = \beta\gamma$$

alakban, ahol $\beta, \gamma \in \mathbb{E}$, β és γ egyike csak egység lehet.

$\diamond$

2.2.7 Állítás:
Ha egy $\alpha \in \mathbb{E}$-re $N(\alpha) = p$, ahol p $\mathbb{Z}$-beli prím, akkor α felbonthatatlan.

Bizonyítás:
Tegyük fel, hogy $N(\alpha) = p$ prím, de α felbontható, azaz $\alpha = \beta\gamma$ valamely $\beta, \gamma \in \mathbb{E}$-re. Ekkor

$$p = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma),$$

azaz β és γ normáinak szorzata p, de mivel a normák nemnegatív egész számok, és p prím, ez csak két módon lehetséges:

$$N(\beta\gamma) = 1 \cdot p \text{ vagy } N(\beta\gamma) = p \cdot 1,$$

ez mindkét esetben azt jelentené, hogy β és γ valamelyike egység, azaz α felbonthatatlan.

$\square$

2.2.8 Állítás:
Minden $\mathbb{E}$-beli elem felbomlik felbonthatatlanok szorzatára.

Bizonyítás:
Indirekt tegyük fel, hogy van olyan $\alpha \in \mathbb{E}$, amely nem bomlik fel. Vegyük a legkisebb normájút ezek közül.

α biztosan nem felbonthatatlan, mert akkor lenne egy egytényezős felbontása.

Emiatt $\exists \beta, \gamma \in \mathbb{E}$, amelyekre $\alpha = \beta\gamma$. $N(\beta)$ és $N(\gamma)$ kisebb, mint $N(\alpha)$, és mivel α volt a legkisebb normájú elem, ami nem bomlik fel, β és γ felbomlik. Legyenek ezek a felbontások a következők:

$$\beta = \prod_{i=1}^{k} \beta_i^{b_i} \text{ és } \gamma = \prod_{j=1}^{l} \gamma_j^{c_j},$$

ahol $\beta_i, \gamma_j \in \mathbb{E}$ felbonthatatlanok, $b_i, c_j \in \mathbb{Z}^+$. Ekkor

$$\alpha = \beta\gamma = \prod_{i=1}^{k} \beta_i^{b_i} \prod_{j=1}^{l} \gamma_j^{c_j},$$

ezzel pedig α-nak egy felbontását kaptuk felbonthatatlanok szorzatára, ami ellentmondás, hiszen feltettük, hogy nincs ilyen.

$\square$

A továbbiakban használni fogjuk a következő jelöléseket:

2.2.9 Jelölés
$(a,b)_r$: jobbideál, melynek elemei $ax+by\ \forall x,y\in\mathbb{E}$.
$(a,b)_l$: balideál, melynek elemei $xa+yb\ \forall x,y\in\mathbb{E}$.

2.2.10 Állítás:
$\mathbb{E}$-ben minden J jobbideál főideál, azaz $\exists\theta\in J$, hogy J elemei pontosan a $\theta\xi$ elemek, ahol $\xi\in\mathbb{E}$.

Bizonyítás:
Feltehetjük, hogy J nem csak nullából áll, mert ebben az esetben $\theta=0$ jó lenne.

Ekkor legyen θ J-nek az egyik olyan eleme, amelynek a legkisebb a normája.

Mivel J jobbideál, ezért ha egy $\xi\in\mathbb{E}$ elemmel szorozzuk jobbról, akkor az is J-ben lesz, azaz $\theta\xi\in J$, $\forall\xi\in\mathbb{E}$.

Fordítva, ha tudjuk, hogy $\alpha\in J$, akkor ezt osszuk el maradékosan θ-val:

$$\alpha=\theta\gamma+\delta$$

Ha $\delta=0$, akkor az $\xi=\gamma$ választás jó lesz.

Ha $\delta\neq 0$, akkor a normákra igaz, hogy $N(\delta)<N(\theta)$, és

$$\delta=\alpha-\theta\gamma\in J,$$

de ez nem lehetséges, mert θ volt az ideál legkisebb normájú eleme.

□

2.2.11 Állítás:
Legyen $\alpha\in\mathbb{E}$, $p\in\mathbb{Z}$ prím olyan, amely nem osztója α-nak, de $N(\alpha)$-nak, azaz α normájának igen. Ekkor α felírható $\pi\alpha'$ alakban, ahol $N(\pi)=p$, és π egyértelműen meghatározott (jobb egységszeres erejéig).
Ha egy π elem p-normájú balosztója α-nak, akkor π generálja az $(\alpha,p)_r$ jobbideált. (Ez minden ilyen π-re teljesül.)

Bizonyítás:
Használjuk a *2.2.10* állítást. Legyen $\mathbf{R}=(\alpha,p)_r$ a π által generált jobbideál.
Abból, hogy $\alpha,p\in\mathbf{R}$, következik, hogy π balosztója α-nak és p-nek is.

Legyen τ az az osztója p-nek, amellyel $p=\pi\tau$, és legyen $\alpha=\pi\gamma$. Ekkor ha τ egység, akkor innen $\pi=p\tau^{-1}$ és ezért $\alpha=p\tau^{-1}\gamma$, azaz p balosztója α-nak.

A *2.1.10* állítás használatával:

$$N(\pi)N(\tau)=N(\pi\tau)=N(p)=p^2$$

A bal oldal két egész szám szorzata, így vagy $1\cdot p^2=p^2\cdot 1$, vagy $p\cdot p$ alakú.

Ha π normája p^2, akkor τ egység, de ekkor p egységszerese π-nek, és így $\pi \mid \alpha$ miatt $p \mid \alpha$ is, amiről feltettük, hogy nem igaz, így ellentmondásba ütközünk.

Ha π normája 1, akkor π egység, és $\mathbf{R}$ jobbideál léte miatt $\exists \tau_1, \tau_2 \in \mathbb{E}$, melyekre

$$\alpha\tau_1 + p\tau_2 = 1.$$

Ezt balról szorozva $\overline{\alpha}$-val kapjuk:

$$\overline{\alpha}\alpha\tau_1 + \overline{\alpha}p\tau_2 = \overline{\alpha}.$$

Ebből látjuk, hogy p osztója $\overline{\alpha}$-nak, így α-nak is, ami megint ellentmond a tétel feltételének.

Az utolsó eset az, hogy π normája p. Ekkor mivel $N(\pi)$ egy $\mathbb{Z}$-beli prím, π felbonthatatlan a Hurwitz-kvaterniók körében. Így π p-normájú balosztója α-nak.

Tegyük fel, hogy π_1 is megfelel az állítás feltételeinek, azaz p normájú balosztója α-nak. Ekkor $\alpha, p \in (\pi_1)_r$, ezért $\pi \in (\pi)_r = (\alpha, p)_r \subseteq (\pi_1)_r$, tehát π_1 balról osztja π-t. Emiatt $\pi = \pi_1$ egység, így $(\pi_1)_r = (\pi)_r = (\alpha, p)_r$.

□

2.3 Lagrange tételének bizonyítása

2.3.1 Tétel: (Lagrange)
Minden pozitív egész előáll négy négyzetszám összegeként, azaz minden $n \in \mathbb{N}^+$ számhoz létezik egész együtthatós kvaternió, amelynek normája n.

A tételnek a bizonyítása 4 részből áll.

Az elsőről már korábban volt szó: tudjuk a *2.2.5* tételből, hogy az $\mathbb{E}$ gyűrű euklideszi.

A következő állítás segítségével pedig megkapjuk, hogy elég a tételt prímekre igazolni, hiszen az összetett számok felírhatóak prímek szorzataként.

2.3.2 Állítás:
Ha van két olyan számunk, amelyeket már előállítottunk négy négyzetszám összegeként, akkor szorzatuk is előállítható ilyen módon.

Bizonyítás:
Legyenek $x, y \in \mathbb{E}$, amelyekre:

$$x = x_0 + x_1 i + x_2 j + x_3 k,$$

$$y = y_0 + y_1 i + y_2 j + y_3 k.$$

Nézzük a következő egyenlőséget:

$$N(x)N(y) = (x_0^2 + x_1^2 + x_2^2 + x_3^2)(y_0^2 + y_1^2 + y_2^2 + y_3^2) =$$

$$= (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3)^2 + (x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)^2 +$$
$$+(x_0y_2 - x_1y_3 + x_2y_0 + x_3y_1)^2 + (x_0y_3 + x_1y_2 - x_2y_1 + x_3y_0)^2,$$

azaz valóban előáll a szorzat is négy négyzetszám összegeként.

□

Kvaternió normával megfogalmazva azt kaptuk, hogy ha létezik olyan egész kvaternió, amelynek normája n, és olyan is, amelynek m, akkor nm normájú kvaternió is létezik, hiszen ez a *2.1.10* állítás alapján ennek a két kvaterniónak a szorzata.

Tehát elég megmutatni, hogy minden p pozitív prímszámhoz találhatunk egy $\mathbb{E}$-beli kvaterniót, amelynek a normája épp p.

Legyen először $p = 2$, ez az $1 + i$ kvaternió normája: $N(1 + i) = 1^2 + 1^2 + 0^2 + 0^2$, ezért innentől elég a $p > 2$ esetet vizsgálnunk.

2.3.3 Állítás:
Minden $p > 2$ prímszámhoz van olyan $a, b \in \mathbb{Z}$, hogy $p \mid 1 + a^2 + b^2$.

Bizonyítás:
A négyzetszámok $\frac{p+1}{2}$ maradékosztályt alkotnak mod p, hiszen:

$$x^2 \equiv y^2 \pmod{p} \text{ pontosan akkor, ha } x^2 - y^2 \equiv 0 \pmod{p},$$

ami azt jelenti, hogy $p \mid x^2 - y^2 = (x - y)(x + y)$, azaz két eset lehetséges:

$$p \mid x - y \Longleftrightarrow x \equiv y \pmod{p} \text{ vagy } p \mid x + y \Longleftrightarrow x \equiv -y \pmod{p}.$$

Ha nézzük az $1^2, 2^2, 3^2, .., (p - 1)^2$ maradékosztályait, akkor pontosan $\frac{p-1}{2}$-t kapunk, hiszen ez $p - 1$ szám, viszont mindent kétszer számoltunk, például $1^2 \equiv (p - 1)^2 \pmod{p}$. Mivel $p - 1$ egy páros szám (p páratlan), valóban minden maradékosztálynak megvan a párja.

A $\frac{p+1}{2}$ pedig úgy jön ki, hogy ezekhez hozzávesszük a 0 maradékosztályát, azaz $\frac{p-1}{2}+1 = \frac{p+1}{2}$ van összesen.

Tehát a^2 alakú maradékosztály $\frac{p+1}{2}$ van, és $-1-b^2$ alakúból szintén ennyi van (mert létezik $x \to -1 - x$ bijekció a mod p maradékosztályokon).

Ezeket összeadva $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p$, így található két egybeeső maradékosztály, azaz van olyan $a, b \in \mathbb{Z}$, amelyekre:

$$a^2 \equiv -1 - b^2 \pmod{p}, \text{ ami pontosan azt jelenti, hogy } p \mid 1 + a^2 + b^2.$$

□

A bizonyítás utolsó lépése az, hogy belátjuk, hogy létezik p-normájú elem $\mathbb{E}$-ben.

2.3.4 Állítás:
Van olyan elem $\mathbb{E}$-ben, amelynek normája p.

Bizonyítás:
Ehhez a *2.2.11* állításra lesz szükségünk.

$\alpha \in \mathbb{E}$-t válasszuk a következőképp:

$$\alpha = 1 + ai + bj, \text{ennek normája } N(\alpha) = 1^2 + a^2 + b^2 + 0^2.$$

Tudjuk, hogy α felírható $\pi\alpha'$ alakban, ahol $N(\pi) = p$, és π jobb egységszeres erejéig egyértelmű.

$\alpha = \alpha'\pi$, azaz $(\alpha')^{-1}\alpha = (\alpha')^{-1}\alpha'\pi = \pi$, és ez a π megfelelő.

□

Ezzel beláttuk, hogy $\mathbb{E}$-ben van p-normájú elem, de a négy négyzetszám-tétel bizonyításának befejezéséhez az is kéne, hogy ne csak $\mathbb{E}$-beli, hanem egész együtthatós p-normájú kvaternió is létezzen. A következő részben belátjuk, hogy minden $\mathbb{E}$-beli kvaterniónak van olyan egységszerese, amely egész együtthatós, ezzel befejezve a bizonyítást.

2.4 Primér kvaterniók

Erre a részre, amely *Rédei* könyvére[6] épül, a megoldások számának megértéséhez lesz szükségünk. Először a primér kvaternió fogalmát nézzük, amihez először egy bizonyos elemről, az $1 + i$-ről lesz szó.

A *2.2.7* állítás miatt nyilvánvaló, hogy ez felbonthatatlan, hiszen a normája $N(1 + i) = 2$ prím. Először ennek a maradékosztályait nézzük.

Ehhez szükség lesz a kongruenciákra: baloszthatóság esetében $\beta \mid \alpha$ azt jelenti, hogy $\exists\gamma$, amire $\alpha = \beta\gamma$, ekkor $\alpha_1 \equiv \alpha_2 \pmod{\beta}$ azt jelenti, hogy $\beta \mid \alpha_1 - \alpha_2$, ilyen esetben van lehetőség a kongruenciák jobbról való beszorzására ($\alpha, \beta, \gamma, \alpha_1, \alpha_2 \in \mathbb{E}$).

2.4.1 Állítás:
Az $\mathbb{E}$ *gyűrűben mindössze négy* $1 + i$ *szerinti maradékosztály van:* $0, 1, \sigma, \sigma + 1$.

Bizonyítás:
Minden $\mathbb{E}$-beli kvaternió felírható a *2.1.11* állítás bizonyításának eleje szerinti módon, azaz a következő alakban az a, b, c, d egészekkel:

$$a\sigma + bi + cj + dk.$$

Nézzük meg, mi történik, ha balról szorozzuk $1+i$-vel a σ-t (természetesen jobbról szorozva is hasonló eredményre jutnánk):

$$(1 + i)\sigma = (1 + i) \cdot \frac{1 + i + j + k}{2} = \frac{1 + i + j + k + i + i^2 + ij + ik}{2} =$$

$$= \frac{2i + 2k}{2} = \frac{2 - 2 + 2i + 2j + 2k - 2j}{2} = \frac{2 \cdot (1 + i + j + k)}{2} + \frac{-2 - 2j}{2} =$$

$$= 2\sigma - 1 - j,$$

ez pedig egy egész együtthatós kvaternió, vagyis az $(1+i)\mathbb{E}$ olyan egész együtthatós kvaterniókból áll, amelyeknek a normája páros, hiszen $N(1+i) = 2$, és bármely $\alpha \in \mathbb{E}$-re

$$N((1+i)\alpha) = N(1+i)N(\alpha) = 2 \cdot N(\alpha).$$

Ebből következik, hogy az állításban felsorolt négy maradékosztály mind különböző, hiszen bármely kettőnek a különbségét véve vagy nem egész együtthatós, vagy páratlan normájú kvaterniót kapnánk. A különbség lehet:

$$1, -1, \sigma, -\sigma, \sigma - 1, \sigma + 1,$$

és mivel σ nem egész együtthatós, ± 1-et hozzáadva sem lesz az, a ± 1 normája pedig 1, ami páratlan.

Már tudjuk, hogy ezek valóban mind különbözőek, azt kell belátnunk még, hogy nincs több maradékosztály.

Az $1+i$ balosztója a 2-nek, ezért minden egész szám benne van a 0 és az 1 maradékosztályaik közül az egyikben (hiszen egy egész vagy páros, vagy páratlan). Ekkor $1 \equiv -1 \pmod{1+i}$, tehát az előjelektől eltekinthetünk.

Nézzük $1 + j$-nek egy felírását, amelyben szerepel az $1 + i$:

$$1 + j = (1 + i) \cdot (1 + i)^{-1} \cdot (1 + j) = (1 + i) \cdot \frac{(1 - i)(1 + j)}{2} =$$

$$= (1 + i) \cdot \frac{1 - i + j + k}{2},$$

és mivel $\frac{1-i+j-k}{2}$ egy $\mathbb{E}$-beli egység, ezért $1 + j$ és $1 + i$ balosztói egymásnak, azaz jobb egységszeresek.

Ebből következik, hogy

$$1 + j \equiv 1 + i \equiv 0 \pmod{1+i}, \text{ azaz } 1 \equiv -j \pmod{1+i}$$

A baloszthatóság miatt a kongruenciát jobbról szorozhatjuk be bármivel, legyen ez most k:

$$1 \cdot k \equiv -j \cdot k = -i \pmod{1+i},$$

és mivel az előjelek nem számítanak, $k \equiv i \pmod{1+i}$.

Nézzük $bi + cj + dk + b + c + d$-t, ez megegyezik, azzal, hogy
$b(1 + i) + c(1 + j) + d(1 + k)$, ami mod $1 + i$ kongruens nullával, ebből pedig felírható a következő:

$$a\sigma + bi + cj + dk \equiv a\sigma - b - c - d \pmod{1+i}$$

Ha az ebben szereplő egészeket redukáljuk mod 2, akkor mindegyikből 0 vagy 1 lesz, azaz végül 0-t, 1-et, σ-t és $\sigma+1$-et kaphatunk, azaz valóban csak ez a négy maradékosztály létezik mod $1 + i$.

□

Következmény:
Ha az α kvaternió egész együtthatós, és páros normájú, akkor osztható $1+i$-vel.

Valóban, láttuk, hogy a 0 maradékosztályában páros normájú egész együtthatós kvaterniók vannak, így a σ és $\sigma+1$ maradékosztályaiban lévők a nem egész együtthatósok, az 1 maradékosztályában pedig bár egész együtthatós kvaterniók vannak, de normájuk páratlan.

Ebből az is egyértelmű, hogy az egész együtthatós kvaterniók pontosan azok, amelyek a 0 vagy az 1 maradékosztályában vannak mod $1+i$.

Azt már tudjuk, hogy a σ és a $\sigma+1$ mod p maradékosztályok elemei nem egész együtthatós kvaterniók, azonban ezek normájáról még nem esett szó. Ezzel kapcsolatban jön most egy állítás.

2.4.2 Állítás:
Azon kvaterniók, amelyek a σ vagy a $\sigma+1$ maradékosztályában vannak (természetesen mod $1+i$) páratlan normájúak.

Bizonyítás:
Először nézzük a σ maradékosztályát: legyen δ egy kvaternió, ami a σ maradékosztályában van. Ez azt jelenti, hogy

$$\delta \equiv \sigma \pmod{1+i},$$

ezt jobbról szorozva $\overline{\sigma}$-tal:

$$\delta\overline{\sigma} \equiv \sigma\overline{\sigma} = N(\sigma) = 1 \pmod{1+i}$$

Tehát a $\delta\overline{\sigma}$ az 1 maradékosztályában van, ezért ez egy páratlan normájú egész együtthatós kvaternió, így δ is páratlan normájú, hiszen felhasználva, hogy $\sigma, \overline{\sigma}$ egységek:

$$N(\delta\overline{\sigma}) = N(\delta)N(\overline{\sigma}) = N(\delta)\cdot 1 = N(\delta).$$

Most δ legyen olyan kvaternió, ami a $\sigma+1$ maradékosztályában van. Ekkor

$$\delta \equiv \sigma + 1 \pmod{1+i},$$

ezt jobbról szorozva σ-val kapjuk, hogy:

$$\delta\sigma \equiv (\sigma+1)\sigma \equiv \overline{\sigma}\sigma = 1 \pmod{1+i},$$

felhasználva, hogy $\overline{\sigma} = 1-\sigma \equiv \sigma+1 \pmod 2$. Tehát hasonlóan az előző esethez, δ páratlan normájú.

□

Tehát azt kaptuk, hogy a négy mod $1+i$ maradékosztályból egyben vannak páros normájú, és háromban páratlan normájú kvaterniók. Ahogy korábban említettük, a páros normájúak azok a kvaterniók, amelyek oszthatók $1+i$-vel, azaz $\mathbb{E}$-ben is a páros normájú kvaterniók oszthatók $1+i$-vel.

Megjegyzés:
Ha egy $\mathbb{E}$-beli kvaternió balról osztható $1+i$-vel, akkor jobbról is, azaz mindkét irányból való oszthatóság szempontjából ugyanazok a mod $1+i$ maradékosztályok, így az ilyen kongruenciákat nem csak jobbról, hanem balról is szorozhatjuk bármilyen $\mathbb{E}$-beli kvaternióval.

Az $x^2+y^2+u^2+v^2=n$ diofantikus egyenletnek pontosan annyi megoldása van, ahány n normájú egész együtthatós kvaternió létezik. Ahhoz, hogy egy jó gyűrűt kapjunk kvaterniókból, az egész együtthatósokhoz hozzá kell vennünk azokat is, amelyekben minden együttható egy páratlan szám fele. A következőkben azt vizsgáljuk, hogy ekkor mennyivel nő a megoldásszám.

Először nézzük meg azt az esetet, amikor n páratlan. Legyen $\alpha \in \mathbb{E}$, normája pedig n. Ha α-t balról szorozzuk a 24 egységgel, akkor megkapjuk bal egységszereseit, természetesen ez 24 elemet jelent. Ezek között keressük azt, amely egész együtthatós, ezt fogjuk primérnek nevezni. Ilyenből pontosan egy van:

2.4.3 Állítás:
α bal egységszeresei között egyetlen olyan van, ami egész együtthatós. Ez legyen $\alpha' = a+bi+cj+dk$, ekkor igazak a következők:

$$a+b+c+d \equiv 1 \pmod 4,$$

$$a-1 \equiv b \equiv c \equiv d \pmod 2.$$

Bizonyítás:
Először értsük meg, hogy pontosabban miről is van szó. Az eddigiektől eltérően, most nem az $1+i$, hanem a $2(1+i)$ maradékosztályait nézzük, amivel azt szeretnénk elérni, hogy minden egység különböző maradékosztályba kerüljön.

Először lássuk be, hogy az $1+i$ maradékosztályai 16 további részre bomlanak, azaz mivel $1+i$ szerint 4 volt, $2(1+i)$ szerint $4 \cdot 16 = 64$ darab lesz.

Legyenek $\alpha, \beta, \gamma \in \{0, 1, \sigma, \sigma+1\}$. Tekintsük a $2\alpha + (1+i)\beta + \gamma$ elemeket. Mivel 4^3-féleképpen választhatjuk ki, hogy α, β, γ közül melyik melyik maradékosztályban van, ezért ez összesen 64 elemet jelent.

Belátjuk, hogy ezek az elemek páronként inkongruensek mod $2(1+i)$.

Indirekt tegyük fel, hogy létezik $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2$ ($\alpha_1 \neq \alpha_2$, $\beta_1 \neq \beta_2$, $\gamma_1 \neq \gamma_2$ közül legalább egy teljesül), amelyekre:

$$2\alpha_1 + (1+i)\beta_1 + \gamma_1 \equiv 2\alpha_2 + (1+i)\beta_2 + \gamma_2 \pmod{2(1+i)}.$$

Tudjuk, hogy $1+i \mid 2$, vagyis az α-k és β-k együtthatói oszthatóak $1+i$-vel, ezért:

$$\gamma_1 \equiv \gamma_2 \pmod{1+i},$$

ami pedig csak úgy lehetséges, hogy $\gamma_1 = \gamma_2$. Ezt tehát elhagyhatjuk. Ezután osszuk le (balról) $1+i$-vel a fenti kongruenciát.

Mivel $2 = (1+i)(1-i)$, ez tovább alakítható:

$$(1-i)\alpha_1 + \beta_1 \equiv (1-i)\alpha_2 + \beta_2 \pmod 2.$$

$1+i \mid 1-i$, hiszen $1-i = (1+i)(-i)$, vagyis az eddigiekhez hasonlóan:

$$\beta_1 \equiv \beta_2 \pmod{1+i},$$

tehát $\beta_1 = \beta_2$, így ezt is elhagyhatjuk, és leoszthatunk (balról) $1-i$-vel, így kapjuk:

$$\alpha_1 \equiv \alpha_2 \pmod{1+i},$$

ami azt jelenti, hogy $\alpha_1 = \alpha_2$, vagyis az eredeti kongruenciánkban minden együttható páronként megegyezett egymással, tehát az elemek valóban mind különböző maradékosztályban vannak $2(1+i)$ szerint.

Azt is be kell még látnunk, hogy ezek az összes mod $2(1+i)$ maradékosztály elemeit reprezentálják.

Legyen $\delta \in \mathbb{E}$ tetszőleges. Ez benne van $1+i$ valamelyik maradékosztályában a négy közül. Legyen $\gamma \in \{0, 1, \sigma, \sigma+1\}$ a megfelelő reprezentáns. Ekkor

$$\delta - \gamma = (1+i)\delta' \text{ valamely } \delta' \in \mathbb{E}\text{-re.}$$

Ezt δ'-vel kétszer megismételve kapjuk β-t, majd α-t.

Így megkaptuk, hogy ez valóban egy teljes maradékrendszer mod $2(1+i)$, tényleg 64 osztály van.

Most legyen δ páratlan normájú kvaternió, reprezentánsa: $2\alpha + (1+i)\beta + \gamma$, ahogy $\gamma \neq 0$. Mivel γ-ra kikötést tettünk, ez összesen $4 \cdot 4 \cdot 3 = 48$ osztályt jelent. Ebből vegyük ki az 1 és a $2\sigma+1$ osztályát, amikben páratlan normájú egész együtthatós kvaterniók vannak. Ami nem triviális, az az, hogy ezek a kvaterniók pontosan a primérek lesznek. Ezt két lépésben látjuk be.

Elsőként belátjuk, hogy ebben a két osztályban pontosan azok a kvaterniók vannak, amelyeket az állítás is említ, azaz azok az $a + bi + cj + dk$ egész együtthatós kvaterniók, amelyekre

$$a+b+c+d \equiv 1 \pmod 4, \text{ és } a-1 \equiv b \equiv c \equiv d \pmod 2.$$

Nézzük az 1 osztályát. Ebben az $1 + 2(1+i)\gamma$ alakúak vannak, ahol $\gamma \in E$. Az $(1+i)\gamma$ alakúakról már beláttuk, hogy ezek pontosan a páros normájú egész együtthatósak. Tehát az 1 osztályában az $1 + 2x + 2yi + 2uj + 2vk$ alakú kvaterniók vannak, ahol $x, y, u, v \in \mathbb{Z}$, és $x^2 + y^2 + u^2 + v^2$ páros, így $x + y + u + v$ is páros.

Az, hogy $(1+2x) - 1, 2y, 2u, 2v$ páronként kongruensek mod 2 triviális, hiszen mindegyik szám páros.

A másik kongruenciához kéne, hogy:

$$1 + 2x + 2y + 2u + 2v \equiv 1 \pmod 4,$$

azaz

$$2(x+y+u+v) \equiv 0 \pmod 4.$$

$x^2+y^2+u^2+v^2$ szükségképpen páros, hiszen $1+i$-nek osztójának kell lennie $x+yi+uj+vk$-nak. Mivel bármely $z \in \mathbb{Z}$-re teljesül, hogy $z \equiv z^2 \pmod 2$, ezért

$$x \equiv x^2 \pmod 2,\ y \equiv y^2 \pmod 2,\ u \equiv u^2 \pmod 2,\ v \equiv v^2 \pmod 2,$$

amiket összeadva kapjuk, hogy

$$x+y+u+v \equiv x^2+y^2+u^2+v^2 \equiv 0 \pmod 2,$$

azaz $x+y+u+v$ is páros.

Visszatérve a $2(x+y+u+v) \equiv 0 \pmod 4$ kongruenciára, a bal oldalon két páros szám szorzata áll, így természetesen néggyel is osztható lesz, azaz valóban igaz, hogy 0-val kongruens mod 4.

Hasonlóan végezzük el ezt az $1+2\sigma$ osztályára is.
Ebben az $1+2\sigma+2(x+yi+uj+vk)$ alakúak vannak, ahol $x^2+y^2+u^2+v^2$ páros, így ezek az $1+(2x+1)+(2y+1)i+(2u+1)j+(2v+1)k$ alakú kvaterniók $(x,y,u,v \in \mathbb{Z})$.

A mod 2 kongruencia itt is triviális, hiszen $1+(2x+1)-1, 2y+1, 2u+1, 2v+1$ mind páratlanok.

A mod 4 kongruencia a következő:

$$1+(2x+1)+(2y+1)+(2u+1)+(2v+1) \equiv 1 \pmod 4,$$

azaz

$$2x+2y+2u+2v+4 \equiv 2(x+y+u+v) \equiv 0 \pmod 4,$$

ez pedig ugyanaz, amit az 1 maradékosztályának esetében már beláttunk.

A második bizonyítandó dolog az, hogy minden páratlan normájú kvaterniónak egyetlen bal egységszerese esik ennek a két osztálynak az uniójába.

Legyen ρ egység. Ekkor ha $\rho\delta \equiv 1$ vagy $\rho\delta \equiv 2\sigma+1 \pmod{2(1+i)}$, akkor ρ^{-1}-zel (ami szintén egy egység) szorozva azt kapjuk, hogy az a $2 \cdot 24$ elem, ami egyrészt egységszer 1, másrészt egységszer $2\sigma+1$, lefedi mind a 48 páratlan osztályt.

Ahhoz, hogy megkapjuk, hogy minden osztályhoz pontosan egy jó egység van, a fordított irányt kell megmutatnunk: azt, hogy ez a 48 konkrét elem páronként különböző osztályba esik mod $2(1+i)$.

Legyenek ρ_1, ρ_2 egységek, amelyek kongruensek mod $2(1+i)$. Szorozzuk be mindkettőt balról ρ_1^{-1}-zel:

$$\rho_1^{-1}\rho_1 = 1 \equiv \rho_1^{-1}\rho_2 =: \rho \pmod{2(1+i)}.$$

Tehát $\rho = a+bi+cj+dk$ egy mod $2(1+i)$ 1-gyel kongruens egység. Együtthatóira teljesül, hogy egészek, és $a+b+c+d \equiv 1 \pmod 4$, a páratlan, b, c, d páros (így $a-1, b, c, d$ kongruensek

mod 2). Ilyen feltételeknek egyetlen egység felel meg, az 1. Így $1 = \rho = \rho_1^{-1}\rho_2$, azaz $\rho_1 = \rho_2$.

Most legyenek $\rho_1(2\sigma + 1), \rho_2(2\sigma + 1)$ egységek, amelyek kongruensek mod $2(1 + i)$. Ez azt jelenti, hogy

$$2(1 + i) \mid \rho_2(2\sigma + 1) - \rho_1(2\sigma + 1) = (\rho_2 - \rho_1)(2\sigma + 1)$$

Ezt balról szorozva ρ_1 inverzével kapjuk, hogy

$$2(1 + i) \mid (\rho_1^{-1}\rho_2 - 1)(2\sigma + 1).$$

Vegyük mindkét oldal normáját, ezekre is teljesül az oszthatóság:

$$N(2(1 + i)) = 2^2 + 2^2 = 8 \mid N(\rho_1^{-1}\rho_2 - 1) \cdot N(2\sigma + 1) = N(\rho_1^{-1}\rho_2 - 1) \cdot 7,$$

a jobb oldalon felhasználva, hogy $2\sigma + 1 = 2 \cdot \frac{1+i+j+k}{2} + 1 = 2 + i + j + k$, aminek normája $2^2 + 3 \cdot 1^2 = 7$. Azaz leegyszerűsítve, mivel $(7, 8) = 1$

$$8 \mid N(\rho_1^{-1}\rho_2 - 1).$$

Használjuk a következő jelölést: $\rho := \rho_1^{-1}\rho_2$ (ez is egység). Ezzel, és a norma egy tulajdonságát használva

$$N(\rho - 1) = (\rho - 1)\overline{(\rho - 1)} = (\rho - 1)(\overline{\rho} - 1) = \rho\overline{\rho} - \rho - \overline{\rho} + 1$$

A *2.1.7* definíció alapján

$$\rho\overline{\rho} - \rho - \overline{\rho} + 1 = 1 + \rho\overline{\rho} - 2 \cdot \mathrm{Re}(\rho) = 2 - 2\mathrm{Re}(\rho)$$

Mivel $|\mathrm{Re}(\rho)| \leq 1$, ezért csak úgy teljesülhet az oszthatóság, hogy $\mathrm{Re}(\rho) = 1$, ekkor pedig $\rho = 1$, így $\rho_1 = \rho_2$.

Az utolsó lehetőség az, hogy $\rho_1(2\sigma + 1)$ és ρ_2 mod $2(1 + i)$ kongruens egységek. Ezeket balról szorozva ρ_1 inverzével:

$$2\sigma + 1 \equiv \rho_1^{-1}\rho_2 =: \rho \pmod{2(1 + i)}.$$

Ebben az osztályban azok az $a+bi+cj+dk$ kvaterniók vannak, amelyek együtthatói egészek, a páros, b, c, d páratlan, és összegük kongruens 1-gyel mod 4, de ilyen egység nincs.

Ezzel beláttuk, hogy páratlan n esetén minden n-normájú $\mathbb{E}$-beli kvaterniónak pontosan egy olyan bal egységszerese van, ami primér.

□

Ezzel teljesen beláttuk a négy négyzetszám-tételt.

Következmény:
Az $\alpha \in \mathbb{E}$ egész együtthatós, páratlan normájú kvaterniónak pontosan 8 egész együtthatós bal egységszerese van, speciálisan akkor is, ha α primér.

Bizonyítás:
Legyen α egész együtthatós, $N(\alpha)$ páratlan, ρ pedig egység. Ekkor

$$\alpha \equiv 1 \pmod{1+i},$$

ezt ρ-val szorozva:

$$\rho\alpha \equiv \rho \pmod{1+i}$$

A bal oldal akkor lesz egész együtthatós, ha 1-gyel kongruens mod $1+i$, ekkor pedig $\rho \equiv 1 \pmod{1+i}$, azaz ρ is egész együtthatós, amiből 8 darab van.

□

Tehát ha az $x^2+y^2+u^2+v^2=n$ diofantikus egyenletünk egy megoldása (x,y,u,v), akkor $\alpha = x+yi+uj+vk$ egész együtthatós, és $N(\alpha)=n$.

Ha β az egyetlen primér bal egységszerese α-nak, akkor $N(\beta)=n$, és β bármely bal egységszeresének a normája is n. Azaz $N(\beta)=n$ minden primér megoldásához 24 bal egységszeres megoldás tartozik $\mathbb{E}$-ben, és 8 az egész együtthatós kvaterniók között.

2.5 Hurwitz eredménye példákkal

Egy természetes szám négy négyzetszámként való felbontásainak számáról Hurwitz bizonyította kvaterniók használatával Jacobi tételét:

2.5.1 Tétel: (Jacobi)
Legyen n pozitív egész, és N a megoldásszáma a következő diofantikus egyenletnek:

$$x^2+y^2+u^2+v^2=n, \text{ ahol } x,y,u,v \in \mathbb{Z}.$$

Jelölje $f(k)$ a k szám pozitív egész osztóinak összegét.

Ekkor ha n páratlan, akkor $N = 8 \cdot f(n)$.

Ha pedig n páros, azaz előáll $n = 2^t m$ alakban valamely $t > 0$ és m páratlan számokra, akkor $N = 24 f(m)$.[7]

Ezt nem bizonyítjuk, de nézzünk néhány példát a tétel alkalmazására, hogy valóban kijön-e az előírt megoldásszám.

Példa:
Nézzünk meg először két egyszerű példát a páratlan esetre.

$$n := 1 = x^2+y^2+u^2+v^2$$

Ennek triviálisan csak kétféle összetételű $\{x,y,u,v\}$ számnégyes lehet a megoldása:

$$\{1,0,0,0\}$$

$$\{-1,0,0,0\}$$

Mindkét esetben 4 lehetőség van az egyes ismeretlenek megválasztására, így $2 \cdot 4 = 8$ előállítás van.

Ennek egyenlőnek kéne lennie $8 \cdot f(n)$-nel, és mivel 1-nek az egyetlen pozitív osztója önmaga, az összeg is 1 lesz, tehát ez valóban 8-cal egyezik meg.

Nézzük az $n = 3$ esetet.

Ekkor 3 olyan szám kell, amely négyzete 1, a negyedik tag pedig 0.

$$\{1, 1, 1, 0\}$$

$$\{1, 1, -1, 0\}$$

$$\{1, -1, -1, 0\}$$

$$\{-1, -1, -1, 0\}$$

Az első és negyedik lehetőség megint 4-4-féleképpen lehetséges.

A második és harmadik eset szintén szimmetrikus, így elég az egyiket megnéznünk, legyen ez a második.

Itt a két 1-es "helye" $\binom{4}{2} = 6$-féleképpen választható, a maradék két elemet pedig minden esetben felcserélhetjük, így új lehetőséget kapva, így összesen $6 \cdot 2 = 12$ lehetőségünk van.

Összeadva:

$2 \cdot 4 + 2 \cdot 12 = 32 = 8 \cdot f(n) = 8 \cdot (1 + 3) = 8 \cdot 4$, tehát valóban teljesül a tétel.

Nézzünk meg két példát a páros esetre is, legyen $n = 2$.

Itt azt is meg kell néznünk, hogy milyen $r > 0$, és m páratlan pozitív egésszel teljesül, hogy $n = 2^r m$.

$$2 = n = 2^r m = 2^1 \cdot 1,$$

tehát $m = 2$ és $r = 1$ (ez utóbbinak most nincs jelentősége).

Mivel $2 = 1 + 1 + 0 + 0$, ezért a lehetőségeink:

$$\{1, 1, 0, 0\}$$

$$\{1, -1, 0, 0\}$$

$$\{-1, -1, 0, 0\}$$

Az első és harmadik eset itt is azonosítható egymással, ugyanannyiféleképp választhatjuk az x, y, u, v értékeit ezekben az esetekben.

Egészen pontosan mindkét esetben rögzíthetjük a két 0-t, összesen $\binom{4}{2} = 6$-féleképpen, a maradék ilyenkor pedig egyértelmű.

Hasonló ehhez a második eset is, ott a 0-k rögzítése után még felcserélhetjük, hogy melyik helyen áll az 1, és melyiken a -1, így összességében $\binom{4}{2} \cdot 2 = 12$ lehetőség van.

Összeadva:

$$2 \cdot 6 + 12 = 24 = 24 \cdot 1 = 24 \cdot f(m),$$

hiszen az m-nek egyetlen osztója az 1.

És utoljára nézzük meg az $n = 4$ esetet, amelynek felbontásaiban már nem mindig csak $0, 1, -1$ szerepel.

Ennek a felbontása a következő:

$$4 = 2^2 \cdot 1 = 2^r m, \text{ azaz } r = 2 \text{ és } m = 1$$

Ebből pedig $f(m) = 1$ megint. A lehetséges esetek:

$$\{1, 1, 1, 1\}$$

$$\{1, 1, 1, -1\}$$

$$\{1, 1, -1, -1\}$$

$$\{1, -1, -1, -1\}$$

$$\{-1, -1, -1, -1\}$$

$$\{2, 0, 0, 0\}$$

$$\{-2, 0, 0, 0\}$$

Az első és az ötödik esetnél 1-1 lehetőségünk van, hiszen mind a négy szám ugyanaz.

A második és a negyedik eset 4-4-féleképpen jöhet ki, csakúgy, mint az utolsó kettő.

Már csak a harmadik eset maradt ki, de ehhez hasonlót is láttunk már: a lehetőségek száma 6.

Összeadva:

$$1 + 4 + 6 + 4 + 1 + 4 + 4 = 24 = 24 \cdot 1 = 24 \cdot f(m).$$

Jacobi tételének bizonyításához szükségünk lenne $\mathbb{E}$-ben a prímfelbontás egyértelműségére. Ennek pontos megfogalmazását nem adjuk meg, az alábbi állítás bizonyos esetekben ezt helyettesíti. Ez egy prím normájú kvaternióról szól, amiről az eddigiek alapján tudjuk, hogy létezik ilyen, hiszen minden természetes szám előáll kvaternió normájaként.

2.5.2 Állítás:
Legyenek $\theta, \eta, \pi \in \mathbb{E}$, és $N(\pi) = p$ valamely $\mathbb{Z}$-beli prímre. Ekkor ha $\pi \mid \theta$ és $p \mid \overline{\theta}\eta$, de $p \nmid \theta$, akkor $\pi \mid \eta$.

Bizonyítás:
A *2.2.11* állítás miatt $(p,\theta)_r = (\pi)_r$, és $\exists \tau_1, \tau_2 \in \mathbb{E}$, melyekre $\pi = \theta\tau_1 + p\tau_2$.
Ezt konjugálva, és jobbról szorozva η-val:

$$\overline{\pi}\eta = (\overline{\tau_1} \cdot \overline{\theta} + \overline{\tau_2} \cdot \overline{p})\eta = \overline{\tau_1} \cdot \overline{\theta} \cdot \eta + p \cdot \overline{\tau_2} \cdot \eta,$$

és mivel tudjuk, hogy $p \mid \overline{\theta}\eta$, így az összeg mindkét tagja osztható p-vel, amiből következik, hogy $\overline{\pi}\eta$ is osztható p-vel.

$N(\pi) = p$ miatt $p = \overline{\pi}\pi$, így $\overline{\pi}\pi \mid \overline{\pi}\eta$, ebből pedig nyilvánvaló, hogy $\pi \mid \eta$.

□

Jacobi tételének speciális esete, amikor $n = p$ páratlan prím. A tétel szerint ebben az esetben $8(p+1)$ megoldás van. Az előző szakaszban írottak alapján tehát igaz a következő:

2.5.3 Tétel: (prím normájú egész kvaterniók)
Az $\mathbb{E}$ gyűrűben $\forall p \in \mathbb{Z}, p > 2$ prím esetében pontosan $24(p+1)$ p-normájú egész kvaternió létezik.
Az ebből kimaradó $p = 2$ prím esetében csak az $1 + i$-nek és annak bal egységszereseinek a normája 2.

Az eddigiek alapján elindulhatunk annak vizsgálatában, hogy hány megoldás van, amikor n egy páratlan prím hatványa.

2.5.4 Állítás:
Legyen $p \in \mathbb{Z}$ prím és $l \geq 0$. Legyen $\pi_1 \in \mathbb{E}$ rögzített, $N(\pi_1) = p$. Nézzük az összes olyan $\alpha \in \mathbb{E}$-t, amelyre $N(\alpha) = p^l$ és $\alpha\pi_1$ nem osztható p-vel. Ilyen α-ból pontosan $24p^l$ darab van.
Bizonyítás:
A bizonyítás eszköze az l szerinti indukció lesz.

Ha $l = 0$, akkor teljesül az állítás, hiszen $24p^0 = 24$, és pontosan ennyi egység van.

Tegyük fel, hogy $p \nmid \alpha$. A *2.2.11* állításból következik, hogy α felírható
$\alpha = \alpha_2\pi_2$-ként, ahol $N(\pi_2) = p$ és α_2 jobb egységszeres, π_2 pedig bal egységszeres erejéig egyértelmű.

A három egész kvaternióról szóló *2.5.2* állítást alkalmazzuk a következő választásokkal:

$$\theta = \overline{\alpha},\ \eta = \pi_1,\ \pi = \pi_2.$$

Így kapjuk, hogy ha $p \mid \alpha\pi_1$, akkor π_2 és $\overline{\pi_1}$ bal egységszeresek.
Fordítva pedig a bal egységszerességből következik, hogy $p \mid \alpha\pi_1$.

A *2.5.3* tétel alapján bal egységszerestől eltekintve a p-normájú elemek száma $p+1$. Emiatt π_2-t p-féleképpen választhatjuk, α_2-t pedig adott π_2-re az indukciós feltevés szerint $24p^{l-1}$-féleképpen.

Így $\alpha = \alpha_2\pi_2$ pedig $p \cdot 24p^{l-1} = 24p^l$-féleképpen választható meg.

□

Irodalomjegyzék

[1] Israel Kleiner. From numbers to rings: The early history of ring theory. 1998.

[2] Simon L. Altmann. Hamilton, rodrigues and the quaternion scandal. *Mathematics Magazine*, 1989.

[3] Gyarmati Edit és Freud Róbert. Számelmélet. 2014.

[4] Kiss Emil. Bevezetés az algebrába. 2007.

[5] Lee M. Goswick, Emil W. Kiss, Gabor Moussong, and Nandor Simanyi. Sums of squares and orthogonal integral vectors. 2011.

[6] Rédei László. Algebra. *Az egész kvaterniók gyűrűje (81.)*, 1954.

[7] Dr. Adolf Hurwitz. Vorlesungen über die zahlentheorie der quaternionen. *Vorlesung 11.*, 1919.