Eötvös Loránd Tudományegyetem
Természettudományi Kar

Kovács Sebestyén

Diofantikus egyenletek elemi megoldásai

BSc szakdolgozat
Alkalmazott matematika szakirány

Témavezető:

Dr. Gyarmati Katalin, egyetemi docens
Algebra és Számelmélet Tanszék

Budapest, 2023.

Köszönetnyilvánítás

Köszönetemet fejezem ki Dr. Gyarmati Katalin tanárnőnek, hogy lehetőséget adott nekem a szakdolgozat témájának megismerésére, feldogozására, és hogy a konzultációk alkalmával a számelmélethez kapcsolódó ismereteimet is bővítette, ami nélkülözhetetlen volt a dolgozat írásakor. Továbbá hálás vagyok, hogy bármikor rendelkezésemre állt, és választ adott a felmerülő kérdéseimre.

Budapest, 2023. május 20.

Kovács Sebestyén

Tartalomjegyzék

Bevezetés

„Ουτοσ τοι Διοφαντον εχει
ταφοσ α μεγα θαυμα και
ταφοσ εκ τεχνησ μετρα βιοιο
λεγει εκτην κουριζειν βιοτου
θεοσ ωπασε μοιρην
δωδεκατην δ επιθεισ μηλα
πορεν χνοαειν τη δ αρ εφ
εβδοματη το γαμηλιον ηψατο
φεγγοσ, εκ δε γαμων πεμπτω
παιδ επενευσεν ετει αιαι,
τηλυγετον δειλον τεκοσ ημισυ
πατροσ τουδ εκαη κρυεροσ
μετρον ελων βιοτου πενθοσ δ
αυ πισυρεσσι παρηγορεων
ενιαυτοισ τηδε ποσου σοφιη
τερμ επερησε βιου”

Anthologia Palatina (XIV, 126)

Alexandriai Diophantosz (250 körül) görög matematikus életéről igen keveset lehet tudni. Fennaradt viszont egy időmértékes verselésű sírfelirat (vö. fenti mottó), amelynek kiváló fordítását Szász Károly (1576) tollából olvashatjuk:

E kő alatt nyugszik Diophant porháza;
Hány évet élt? - maga ekkép magyarázza:
Mint gyermek játszá le élete hatodát,
Tizenkettedrészét mint ifju élte át.
Még hetede mulva hű nőjét találta;
Öt év mulva lőn egy gyermekkel megáldva.
De ez csak félannyi időt élt, mint atyja,
Kitől őt a halál ölébe ragadja.
Négy évig gyászlá még agg apja őt sírva;
Mondd meg, mily korában szállt tehát a sírba?

Ebben az epigrammában, ami állítólag Diophantosz sírkövére volt vésve a korabeli szokásoknak megfelelően egy feladványt olvashatunk, amely arra kérdez rá, hogy hány éves korában halt meg Diophantosz. Ha x jelöli életkorát, akkor

$$x \cdot \left(\frac{1}{6} + \frac{1}{12} + \frac{1}{7}\right)$$

korában született meg a fia, aki $\frac{x}{2}$ évet élt, és 4 évvel korábban halt meg apjánál. Innen azt kapjuk, hogy

$$x \cdot \left(\frac{1}{6} + \frac{1}{12} + \frac{1}{7}\right) + 5 + \frac{x}{2} + 4 = x, \qquad \text{azaz} \qquad x = 84.$$

A fentiekből is látható, hogy Diophantosz 14 évig volt gyerek, ifjúsága 7 évig tartott, 33 évesen nősült meg, 38 évesen fia született, aki 42 évig élt, négy évvel korábban halt meg atyjánál.

Dolgozatunkban olyan (többnyire) egész együtthatós egy, ill. többváltozós algebrai egyenleteket tanulmányozzuk, amelyek megoldásai egész (olyakor racionális) számok. Ezeket az egyenleteket Alexandriai Diophantosz görög matematikus iránti tiszteletből diofantoszi vagy diofantikus egyenleteknek nevezik.

A diofantoszi egyenletekkel kacsolatban az alábbi kérdésekre keresünk választ

- Megoldható az adott egyenlet?
- Véges, vagy végtelen sok megoldás van-e?
- Kiszámítható-e az összes megoldás?

A diofantoszi egyenletek közé sorolhatjuk, pl. a polinomiális egyenelet mellet igen híres még a Pell-egyenletet, de találkozhatunk gyökös, illetve exponenciális diofantoszi egyenletekkel is. Ide sorolhatók a – babiloniaiak ismerte – pitagoraszi számhármasok előállításának problémaköre is.

A dolgozatban az $a, b \in \mathbb{Z}$ számok legnagyobb közös osztóját, illetve legkisebb közös többszörösét általában az

$$\mathrm{lnko}(a, b), \qquad \text{ill.} \qquad \mathrm{lkkt}(a, b)$$

szimbólumokkal, az egyszerűség kedvéért – olykor – a rövidebb

$$(a, b) \qquad \text{ill.} \qquad [a, b]$$

szimbólumokkal fogjuk jelölni, ha ez utóbbi nem okoz félreértést.
A szakdolgozatom első fejezete olyan diofantikus egyenletekről szól, melyekhez semmilyen előzetes háttértudás nem szükséges, ezek az úgynevezett lineáris diofantikus egyenletek, melyekkel már általános iskolában is találkozhatunk. A második fejezetben a kongruenciamódszer segítségével megadunk egy olyan nevezetes diofantikus egyenletet, melynek meglepő módon egyetlenegy megoldása sincsen. A harmadik fejezetben megismerkedhetünk a Gauß-egészekkel,

és a Legrende-szimbólum segítségével megadjuk a Gauß-prímek explicit képletét is. Ezt felhasználva pedig megoldjuk a kétnégyzetszám problémát a negyedik fejezetben. Ezek után egyéb nevezetes megoldott diofantikus egyenletekre adunk példát az ötödik fejezetben, melyek megoldásai hasonlóak a kétnégyzetszám probléma megoldásához. A szakdolgozatomat a John Pell angol matematikusról elnevezett diofantikus egyenletek egyik osztályával, a Pell-egyenletekkel zárom.

1. fejezet

Lineáris diofantikus egyenletek

A diofantikus egyenletek legegyszerűbb példája, a lineáris diofantikus egyenletek, ahol minden változó csak az első hatványon szerepel. Ezek egyszerűen tárgyalhatók, ez következik most.

Tétel (vö. [2]). Legyen $a, b \in \mathbb{Z}$: $a \cdot b \neq 0$. Ekkor az

$$ax + by = c \tag{1.0.1}$$

diofantikus egyenlet pontosan akkor megoldható $\mathbb{Z}^2$-en, ha $\text{lnko}(a, b)|c$.

Bizonyítás.

1. lépés. Ha az (1.0.1) egyenlet megoldható, akkor alkalmas $\alpha, \beta \in \mathbb{Z}$ számok esetén $a\alpha + b\beta = c$. Mivel

$$\text{lnko}(a, b)|a \qquad \text{és} \qquad \text{lnko}(a, b)|b,$$

ezért

$$\text{lnko}(a, b)|a\alpha + b\beta = c.$$

2. lépés. Tegyük fel, hogy $\text{lnko}(a, b)|c$, azaz van olyan $t \in \mathbb{Z}$, hogy

$$\text{lnko}(a, b) \cdot t = c.$$

Az euklideszi algoritmust felhasználva megmutatható, hogy ekkor alkalmas $u, v \in \mathbb{Z}$ számokkal

$$\text{lnko}(a, b) = au + bv.$$

Ekkor

$$c = \text{lnko}(a, b) \cdot t = (au + bv) \cdot t = a(ut) + b(vt) = c,$$

így az

$$x := ut, \qquad y := vt$$

választással $ax + by = c$. ■

Ha az $a \cdot x + b \cdot y = c$ lineáris diofantikus egyenletnek egyenletnek van megoldása, akkor végtelen sok megoldása van. Mielőtt felítnánk az egyenlet megoldáshalmazának szerkezetét, belátunk egy segédállítást.

Lemma (vö. [2]. Ha $a, b, c \in \mathbb{Z}$, akkor igaz az

$$a|bc \qquad \Longleftrightarrow \qquad \frac{a}{\mathrm{lnko}(a,b)} \,\Big|\, c$$

ekvivalencia.

Bizonyítás. Írjuk fel az $a, b, c \in \mathbb{Z}$ számokat az

$$a = \prod_{k=1}^{n} p_i^{\alpha_i}, \qquad b = \prod_{k=1}^{n} p_i^{\beta_i}, \qquad c = \prod_{k=1}^{n} p_i^{\gamma_i}$$

kanonikus alakban, ahol $i = 1,2,\ldots,n$ esetén $\alpha_i, \beta_i, \gamma_i$ nemnegatív egész számok (megengedünk 0 kitevőt is). Ekkor

$$\mathrm{lnko}(a,b) = \prod_{k=1}^{n} p_i^{\min\{\alpha_i,\beta_i\}}$$

miatt

$$\frac{a}{\mathrm{lnko}(a,b)} = \prod_{k=1}^{n} p_i^{\alpha_i - \min\{\alpha_i,\beta_i\}}$$

pontosan akkor osztja a c számot, ha minden $i = 1,2,\ldots,n$ index esetén

$$\alpha_i - \min\{\alpha_i, \beta_i\} \le \gamma_i.$$

Ez egyenértékű azzal, hogy minden $i = 1,2,\ldots,n$ indexre $\alpha_i \le \beta_i + \gamma_i$, azaz $a|bc$, ugyanis tetszőleges $i = 1,2,\ldots,n$ indexre

- az $\alpha_i - \min\{\alpha_i, \beta_i\} \le \gamma_i$ esetben

$$\alpha_i \le \min\{\alpha_i, \beta_i\} + \gamma_i \le \beta_i + \gamma_i;$$

- az $\alpha_i \le \beta_i + \gamma_i$ esetben $\alpha_i \le \beta_i + \gamma_i$ és $\alpha_i \le \alpha_i + \gamma_i$ miatt

$$\alpha_i \le \min(\alpha_i, \beta_i) + \gamma_i. \quad ■$$

Nem nehéz belátni azt sem, hogy ha $a|bc$ és $\mathrm{lnko}(a,b) = 1$, akkor $a|c$ is teljesül.

Tétel (vö. [2]). Ha valamely $a, b \in \mathbb{Z}$: $a \cdot b \neq 0$ esetén az $(x_0, y_0) \in \mathbb{Z}^2$ megoldása az (1.0.1) diofantikus egyenletnek, akkor (1.0.1) összes (x', y') megoldása a következő alakba írható

$$\left.\begin{aligned} x' &= x_0 + t \cdot \frac{b}{\operatorname{lnko}(a,b)}, \\ y' &= y_0 - t \cdot \frac{a}{\operatorname{lnko}(a,b)} \end{aligned}\right\} \qquad (t \in \mathbb{Z}). \tag{1.0.2}$$

Bizonyítás.

1. lépés. Belátjuk, hogy bármely $t \in \mathbb{Z}$ esetén $(x', y') \in \mathbb{Z}$ megoldása az (1.0.1) egyenletnek. Valóban, mivel (x_0, y_0) megoldása (1.0.1)-nek, azaz $ax_0 + by_0 = c$, ezért

$$ax' + by' = ax_0 + \frac{abt}{\operatorname{lnko}(a,b)} + by_0 - \frac{tba}{\operatorname{lnko}(a,b)} = ax_0 + by_0 = c.$$

2. lépés. Megmutajuk, hogy ha $(x_0, y_0) \in \mathbb{Z}^2$ megoldása (1.0.1)-nek, akkor minden megoldás (1.0.2) alakú. Mivel az

$$ax_0 + by_0 = c, \qquad ax' + by' = c$$

egyenlőségpár az

$$a(x' - x_0) + b(y' - y_0) = 0, \qquad \text{azaz az} \qquad a(x' - x_0) = b(y_0 - y')$$

egyenlőség következménye, ezért az utóbbit $\dfrac{1}{\operatorname{lnko}(a,b)}$-vel szorozva

$$\frac{a}{\operatorname{lnko}(a,b)}(x' - x_0) = \frac{b}{\operatorname{lnko}(a,b)}(y_0 - y') \tag{1.0.3}$$

adódik. Innen pedig

$$\operatorname{lnko}\left(\frac{a}{\operatorname{lnko}(a,b)}, \frac{b}{\operatorname{lnko}(a,b)}\right) = 1$$

miatt (vö. Lemma)

$$\frac{b}{\operatorname{lnko}(a,b)} \,\Big|\, (x' - x_0)$$

következik. Következésképpen van olyan $t \in \mathbb{Z}$, hogy

$$\frac{b}{\operatorname{lnko}(a,b)} \cdot t = x' - x_0, \qquad \text{így} \qquad x' = x_0 + t \cdot \frac{b}{\operatorname{lnko}(a,b)}.$$

Ezt (1.0.3)-be helyettesítve

$$\frac{a}{\text{lnko}(a,b)} \cdot \frac{tb}{\text{lnko}(a,b)} = \frac{b}{\text{lnko}(a,b)} \cdot (y_0 - y'),$$

ahonnan a $\dfrac{b}{\text{lnko}(a,b)}$ törttel osztva, majd átrendezve

$$y' = y_0 - t \cdot \frac{a}{\text{lnko}(a,b)}$$

adódik. ■

Megjegyezzük, hogy ha $a, b \in \mathbb{Z}$: $a \cdot b \neq 0$, akkor igaz az

$$\exists\, x, y \in \mathbb{Z}: \quad ax+by = c \quad \Longleftrightarrow \quad ax-c = -by \quad \Longleftrightarrow \quad b|(ax-c) \quad \Longleftrightarrow \quad ax \equiv c \pmod{b}$$

ekvivalencialánc.

Példa. A fenti megjegyzés értelmében

$$52x + 23y = 65 \quad \Longleftrightarrow \quad 52x \equiv 65 \pmod{23} \Longleftrightarrow \quad 6x \equiv -4 \pmod{23} \quad \Longleftrightarrow$$

$$\Longleftrightarrow \quad 3x \equiv -2 \,(23) \quad \Longleftrightarrow \quad 3x \equiv 21 \pmod{23},$$

így például $x_0 = 7$. A fentiek alapján b_0 kiszámítható:

$$52 \cdot 7 + 23b_0 = 65, \qquad \Longrightarrow \qquad b_0 = \frac{65 - 364}{23} = -13.$$

A $(7, -13)$ pár egy megoldás, a tétel szerint az összes megoldása az

$$52x + 23y = 65$$

diofasntikus egyenletnek $(52{,}23) = 1$ következtében tetszőleges $t \in \mathbb{Z}$ esetén

$$x' = 7 + 23t, \qquad y' = -13 - 52t$$

alakú.

Tétel (vö. [2]). Legyen $2 \leq k \in \mathbb{N}$, ill. legyenek $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ olyan számok, amelyekre $\prod_{i=1}^{k} a_i \neq 0$, továbbá tegyük fel, hogy $c \in \mathbb{Z}$. Ekkor az

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k = c \tag{1.0.4}$$

diofantikus egyenlet pontosan akkor megoldható $\mathbb{Z}^k$-n, ha $\text{lnko}(a_1, \ldots, a_k)|c$.

Példa. (vö. [7]) Megoldjuk a

$$15x + 10y + 7z = 4$$

difantikus egyenletet. Mivel a bal oldal

$$7z + 5(3x + 2y)$$

alakú ezért $(3,2) = 1$ miatt minden $t \in \mathbb{Z}$ szám esetény van olyan $x, y \in \mathbb{Z}$, hogy

$$3x + 2y = t.$$

Így a

$$7z + 5t = 4$$

egyneletnek megoldása a $(z_0, t_0) = (2, -2)$ pár. Az utóbbi egyenlet összes megoldása így

$$z = 2 - 5l, \qquad t = -2 + 7l$$

alakú, ahol $l \in \mathbb{Z}$ tetszőleges.

2. fejezet

Magasabb fokú diofantikus egyenletek, a kongruencia-módszer

Az elsőfokú diofantikus egyenletek után rátérhetünk a magasabb fokúakra is. Ehhez nyújt segítséget a kongurencia-módszer.

Kongruencia-módszer (vö. [4]). Ha létezik olyan $0 < m \in \mathbb{Z}$, hogy

$$f(x_1, x_2, ..., x_n) \equiv 0 \quad (m)$$

nem oldható meg, ahol $f \in \mathbb{Z}[x_1, x_2, ..., x_n]$, akkor az

$$f(x_1, x_2, ..., x_n) = 0$$

diofantikus egyenletnek sincsen megoldása.

A kongruencia-módszert alkalmazva adhtatunk egy $\mathbb{Z}^2 - \{0,0\}$-án megoldhatatlan egyenletet.

Feladat. Legyen $(a, b, c) \in \mathbb{Z}^3$. A kongruencia-módszert felhasználva mutassuk meg, hogy az

$$a^2 + b^2 = 3c^2 \tag{2.0.1}$$

egyelnetnek nek nincsen a triviálistól különböző megoldása!

Megoldás. Tegyük fel indirekt módon, hogy a (2.0.1) egyenletnek van a triviálistól különböző (a, b, c) megoldása, majd legyen

$$d := \text{lnko}(a, b, c).$$

A (2.0.1) egyenlet d^2-vel leosztva azt kapjuk, hogy

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

azaz

$$\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) \in \mathbb{Z}^3$$

is megoldás. Mivel ezek a számok relatív prímek, ezért elég azt belátni, hogy nincs olyan megoldás-hármas, amelyek legnagyobb közös osztója 1-gyel egyenlő. Ha (a, b, c) hármas megoldása a (2.0.1) egyenletnek, akkor a kongrencia-módszer és az előző megfigyelés szerint $(a, b, c) \in \mathbb{Z}^3$ választható olyannak, hogy $\text{lnko}(a, b, c) = 1$ legyen. Mindez azt jelenti, hogy

$$3|(a^2 + b^2)$$

és ha k négyzetszám, akkor

$$k \equiv 0 \quad (3) \qquad \text{vagy} \qquad k \equiv 1\,(3).$$

Így külön-külön is igaz, hogy $3|a^2$ és $3|b^2$, ahonnan már következik, hogy

$$9|a^2, \qquad 9|b^2, \qquad 9|a^2 + b^2 = 3c^2,$$

és fennállnak a $3|a$, $3|b$, $3|c$ oszthatósági relációk. Ez ellentmond annak, hogy

$$\text{lnko}(a, b, c) = 1. \quad \blacksquare$$

3. fejezet

Gauß-egészek

Ez a fejezet a [2] tankönyv 7.4. szakaszának felhasználásával készült.

Léteznek nevzetesebb megoldhatatlan egyenletek, de ezek tárgyalásához néhány fogalomra szükség van. A továbbiakban azt szeretnénk eldönteni, hogy mely $n \in \mathbb{N}$ esetén létezik olyan $(x, y) \in \mathbb{Z}^2$ pár, hogy

$$x^2 + y^2 = n \tag{3.0.1}$$

és (3.0.1)-nek hány különböző megoldása lehetséges.

Definíció. Gauß-egészeknek nevezzük az $a + bi$ alakú komplex számokat, ahol $a, b \in \mathbb{Z}$. A Gauß-egész számok halmazát $\mathbb{G}$-vel jelöljük.

Az egész számok mintájára bevezethetünk néhány egyszerű fogalmat.

Definíció. Azt mondjuk, hogy az $\alpha \in \mathbb{G}$ Gauß-egész **osztható** a $\beta \in \mathbb{G}$ Gauß-egésszel, ha alkalmas $\gamma \in \mathbb{G}$ Gauß-egésszel $\beta = \alpha\gamma$ teljesül. Erre a szokásos $\alpha|\beta$ jelölést használjuk.

A továbbiakban hasznos lesz egy komplex szám abszolútértékének négyzetére egy új jelölést bevezetni.

Definíció. Az $\alpha = a + bi \in \mathbb{G}$ Gauß-egész **normá**jának nevezzük és $N(\alpha)$-val jelöljük az

$$N(\alpha) := |\alpha|^2 = a^2 + b^2$$

nemnetatív valós számot.

Megjegyezzük, hogy a komplex számokra érvényes $|\alpha\beta|^2 = |\alpha|^2|\beta|^2$ azonosság segítségével belátható, hogy az $\alpha, \beta \in \mathbb{G}$ Gauß–egészek normájára

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

Lemma (vö. [2]). Bármely $\alpha, \beta \in \mathbb{G}$ Gauß-egész esetén igaz az

$$\alpha|\beta \qquad \Longrightarrow \qquad N(\alpha)|N(\beta)$$

implikáció.

Bizonyítás. Az előző észrevétel felhasználásával látható, hogy alkalmas $\gamma \in \mathbb{G}$ esetén $\beta = \alpha\gamma$. Ekkor

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

ahonnan $N(\alpha)|N(\beta)$ következik. ■

Definíció. Ha az $\epsilon \in \mathbb{G}$ számra fennáll, hogy minden $\alpha \in \mathbb{G}$ esetén $\epsilon|\alpha$, akkor ϵ-t **Gauß-egység**nek nevezzük.

Megmutatjuk, hogy négy különböző szám van, amiket ha tetszőleges $\mathbb{G}$-beli elemmel elosztunk, akkor $\mathbb{G}$-ben maradunk.

Tétel (vö. [2]). $\mathbb{G}$ egységeit pontosan a következő négy szám:

$$1; \qquad -1; \qquad \imath; \qquad -\imath.$$

Bizonyítás. Egyrészt tetszőleges $\alpha \in \mathbb{G}$ számra

$$\alpha = 1 \cdot \alpha = (-1) \cdot (-\alpha) = \imath \cdot (-\imath \cdot \alpha) = (-\imath) \cdot (\imath\alpha),$$

másrészt pedig, ha $\epsilon \in \mathbb{G}$ egység, akkor

$$\epsilon|1 \qquad \text{és} \qquad 0 \leq N(\epsilon)|N(1) = 1,$$

azaz $\epsilon := a + b\imath$ esetén $N(\epsilon) = a^2 + b^2 = 1$, ahonnan

$$a = \pm 1, \quad b = 0 \qquad \text{vagy} \qquad a = 0, \quad b = \pm 1$$

következik. ■

Felmerül a kérdés, hogy ahogy egész számok halmazán van maradékos osztás, úgy létezik-e maradékos osztás a Gauß-egészeknél is.

Tétel (vö. [2]). Bármely $\alpha, \beta \in \mathbb{G}$, $\beta \neq 0$ Gauß-egész esetén van olyan $\gamma, \delta \in \mathbb{G}$ Gauß-egész, hogy

$$\alpha = \beta\gamma + \delta, \tag{3.0.2}$$

ahol $N(\delta) < N(\beta)$.

Bizonyítás. Mivel $\beta \neq 0$ ezért (3.0.2) avval egyenértékű, hogy

$$\frac{\alpha}{\beta} - \gamma = \frac{\delta}{\beta},$$

azaz $N(\delta) < N(\beta)$ következtében

$$\left|\frac{\alpha}{\beta} - \gamma\right| = \left|\frac{\delta}{\beta}\right| < 1.$$

Azt kell belátnunk, hogy tetszőleges $\rho := \frac{\alpha}{\beta}$ Gauß-racionálishoz van olyan $\gamma \in \mathbb{G}$ Gauß-egész, hogy $|\rho - \gamma| < 1$. Ez viszont igaz, ugyanis ha tekintjük a komplex számsíkon a racionális koordinátájú

$$\rho = \frac{\alpha}{\beta} = a + bi$$

pontokat ($(a, b) \in \mathbb{Q}^2$), akkor legyen γ a ρ-t tartalmazó egységyzet ρ-hoz legközelebbi csúcsa. Ekkor

$$|\rho - \gamma| \leq \quad \text{"egységnégyzet átlójának a fele"} \quad = \frac{\sqrt{2}}{2} < 1.$$

Így tehát valamely $\gamma \in \mathbb{G}$ Gauß-egészre

$$\left|\frac{\alpha}{\beta} - \gamma\right| < 1,$$

azaz van olyan $\delta \in \mathbb{G}$, amelyre

$$N(\delta) < N(\beta) \qquad \text{és} \qquad \frac{\alpha}{\beta} - \gamma = \frac{\delta}{\beta}$$

teljesül. Ezt átrendezve kapjuk a tétel állítását. ■

Ha az $\alpha \in \mathbb{G}$ Gauß-egész normáját a

$$\phi(\alpha) := N(\alpha)$$

módon jelöljük akkor bármely $\alpha, \beta \in \mathbb{G}$, $\beta \neq 0$ esetén

$$\phi(\alpha\beta) = N(\alpha\beta) = N(\alpha)N(\beta) \geq N(\alpha) \cdot 1 = \phi(\alpha).$$

Ezzel a következő eredményt láttuk be.

Tétel. A fent értelmezett ϕ leképezéssel a $(\mathbb{G}, \phi)$ struktúra euklideszi gyűrű, azaz $\mathbb{G}$-ben igaz a számelmélet alaptétele, bármely két $\mathbb{G}$-beli számnak van kitüntetett osztója, továbbá valamely $\pi \in \mathbb{G}$ pontosan akkor felbonthatatlan, ha π prím.

Definálhatjuk az euklideszi gyűrű fogalmaát.

Definició (vö. [4]). Az $\mathbb{E}$ gyűrűt **euklideszi gyűrű**nek nevezzük, ha valamely $\mathbb{E}$-beli $*$ műveletre nézve teljesülnek az alábbi tulajdonságok:

(i). minden $(a, b) \in \mathbb{E}^2$-re

$$a * b = b * a$$

($*$ művelet kommutatív);

(ii). $a * b = 0$-ból következik, hogy $a = 0$ vagy $b = 0$ ($\mathbb{E}$ nullosztómentes);

(iii). minden $a \in \mathbb{E}$, $a \neq 0$-hoz hozzá van rendelve egy $\phi(a) \geq 0$ egész szám, hogy $\mathbb{E}$-ben tudunk ϕ szerint maradékosan osztani: tetszőleges $(a, b) \in \mathbb{E}^2$, $b \neq 0$ esetén létezik olyan $(r, q) \in \mathbb{E}^2$, hogy

$$a = b * q + r, \qquad \text{ahol} \qquad r = 0 \quad \text{vagy} \quad \phi(r) < \phi(b);$$

(iv). bármely $(a, b) \in \mathbb{E}^2$, $a \neq 0, b \neq 0$ esetén $\phi(ab) \geq \phi(a)$ teljesül.

A Gauß-prímek felsorolásában sokat fog segíteni a következő tétel.

Tétel ([2], 7.4.14.).

1. Minden π Gauß-prímhez pontosan egy p pozitív prím létezik, hogy $\pi | p$.
2. Minden $p > 0$ prímszám vagy Gauss-prím, vagy $p = \pi_1 \overline{\pi_1}$, ahol π_1 és $\overline{\pi_1}$ már Gauss-prímek, valamint $N(\pi_1) = p$.

Bizonyítás.

1. A tételbeli p-re vonatkozó állítást két lépésben igazoljuk.

   1. lépés (egzisztencia).. Ha π Gauss-prím, akkor nem 0 és nem egység $\mathbb{G}$-ben, ezért $N(\pi) > 1$. Alkalmazzuk $N(\pi)$-re a számelmélet alaptételét és a Gauss-prímek definícióját, ahol p_i pozitív prímek, majd vegyük észre, hogy

   $$\pi | \pi\overline{\pi} = \prod_{i=1}^{r} p_i.$$

Ekkor π Gauss-prím osztja a szorzatot, ezért szükségszerűen valamelyik tényezőt is osztja.

2. lépés (unicitás).. Tegyük fel indirekt módon, hogy létezik két különböző $p > 0$ és $q > 0$, hogy p prím és q is prím, továbbá $\pi|p$, $\pi|q$. Ekkor $\text{lnko}(p, q) = 1$ miatt alkalmas$(u, v) \in \mathbb{Z}^2$-re

$$pu + qv = \text{lnko}(p, q) = 1.$$

Emiatt pedig $\pi|\,(pu + qv) = 1$. Ez ellentmond annak, hogy π Gauss-prím, tehát nem egység.

2. Ha p pozitív prím nem Gauß-prím, akkor a számelmélet alaptétele szerint egyértelműen bomlik fel egységszerestől és sorrendtől eltekintve Gauss-prímek szorzatára:

$$p = \prod_{i=1}^{r} \pi_i.$$

Vegyük a két szám normáját:

$$p^2 = N(p) = \prod_{i=1}^{r} N(\pi_i),$$

ahol $r \geq 2$ $p^2 = p \cdot p$, és a számelmélet alaptétele szerint a két előállítás megegyezik:

$$r = 2 \quad \text{és} \quad p = \pi_1\pi_2 \quad \text{és} \quad N(\pi_1) = N(\pi_2) = p,$$

továbbá a

$$\pi_1\pi_2 = p = N(\pi_1) = \pi_1\overline{\pi_1}$$

egyenlőség után már látszik, hogy $\pi_2 = \overline{\pi_1}$, és itt π_1 és $\pi_2 = \overline{\pi_1}$ is Gauss-prím. ■

Ahhoz, hogy explicit képletet adjunk az összes Gauß-prímre, definiálnunk kell a Legendre-szimbólumot.

Definíció (Legrende-szimbólum). Legyen p páratlan prím, továbbá $a \in \mathbb{Z}$ olyan, amelyre $\text{lnko}(a, p) = 1$. Ekkor az

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{az} \quad x^2 \equiv a \ (p) \quad \text{kongruencia megoldható,} \\ -1 & \text{az} \quad x^2 \equiv a \ (p) \quad \text{kongruencia nem oldható meg.} \end{cases}$$

formulával értelmezett számot **Legendre-szimbólum**nak nevezzük.

Ismeretes számelméletből a következő lemma.

Lemma (vö. [2]). Az $a \in \mathbb{Z}$ szám pontosan akkor kvadratikus maradék (mod p), ha

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

illetve akkor és csak akkor kvadratikus nemmaradék (mod p), ha

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Az előző tétel következményeként kapjuk az következő lemmát.

Lemma (vö. [2]). Ha p páratlan prím, $a \in \mathbb{Z}$ pedig olyan, amelyre $\text{lnko}(a,p) = 1$, akkor

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Az előző lemmának most néhány következményét tárgyaljuk.

Tétel(vö. [2]). Legyen $a, b \in \mathbb{Z}$, továbbá $p \in \mathbb{N}$ páratlan prím. Ekkor igazak az alábbi állítások.

1. Ha $a \equiv b \pmod{p}$, akkor $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Bizonyítás. Először vegyük észre, hogy (2)-nél

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\left(\frac{p-1}{2}\right)} b^{\left(\frac{p-1}{2}\right)} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Tehát mind a három egyenlet két oldalának a különbsége csak 0, -2, 2 lehet felhasználva, hogy

$$\left(\frac{a}{p}\right) \in \{-1,1\}.$$

Továbbá a legutóbbi lemma és az előző érvelés szerint a három egyenlet két oldalának a külöbsége osztható a p páratlan prímmel, így ez a három szám csak 0 lehet. ■

Most kimondunk további két, Legendre-szimbólummal kapcsolatos tételt bizonyítás nélkül. Az első a legkisebb pozitív prímászámnak az Legendre-szimbólumával kapcsolatos.

Tétel (vö. [2]).

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

A második pedig arról, hogy egy páratlan prím egy másik páratlan prím szerinti Legendre-szimbóluma visszavezethető arra az esetre, ha a másik páratlan prímnek nézzük a Legendre-szimbólumát az egyik páratlan prím szerint.

Tétel (Kvadratikus reciprocitás (vö. [2])). Ha p és q különböző páratlan prímek, akkor

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Most már meg tudjuk adni az explicit képletet a Gauß-felbonthatatlanokra.

Tétel (vö. [2]). Az összes Gauss-prímszám az alábbi számok, és egységszereseik:

1. $1+\imath$,
2. p, ahol $p \in \mathbb{Z}$ olyan prím, hogy alkalmas $k \in \mathbb{Z}$ esetén $p = 4k+3$ ($4k+3$ alakú prím),
3. π és $\overline{\pi}$, ahol $N(\pi)$ valemely $4k+1$ alakú prím, $k \in \mathbb{Z}$.

Bizonyítás. Az előző tétel szerint az összes Gauß-prímet valamely $p > 0$ egész prím Gauß-felbontásából kaphatjuk meg. Három eset lehetséges:

1. eset.. Ha $p = 2$, akkor $p = -\imath(1+\imath)^2$. Az $1+\imath$ nyilván Gauß-prím, ellenkező esetben ui. $1+\imath = \alpha\beta$, ahol $N(\alpha) \geq 2$, $N(\beta) \geq 2$, ennélfogva

$$2 = N(1+\imath) = N(\alpha)N(\beta) \geq 2 \cdot 2 = 4,$$

ami nem lehetséges.

2. eset.. Ha p egy $4k+3$ alakú prím, akkor p Gauß-prím. Tegyük fel ugyanis, hogy p nem Gauß-prím. Egy korábbi tétel következtében

$$p = N(\pi_1) = \pi_1\overline{\pi_1},$$

ahol π_1 Gauß-prím. Ha $\pi_1 = a+b\imath$, akkor $a^2+b^2 = p$, ami lehetetlen, ugyanis a bal oldalt 4-gyel osztva 3-at kapunk maradékul, míg a jobb oldal 0,1 vagy 2 maradékot ad.

3. eset.. Tegyük fel, hogy p egy $4k+1$ alakú prím. Ekkor p nem Gauss-prím. Tegyük fel

ugyanis indirekt módon, hogy p Gauß-prím. Ekkor egy korábbi tétel szerint

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{4k+1-1}{2}} = 1,$$

ezért van olyan $x \in \mathbb{Z}$, hogy $x^2 \equiv -1 \pmod{p}$. Az iménti kongruenciát oszhatóságra átírva azt kapjuk, hogy

$$p | x^2 + 1 = (x + \imath)(x - \imath).$$

Mivel p az indirekt feltevés szerint Gauß-prím, ezért a fenti szorzat valamelyik tagját osztja. Ha $p | x + \imath$, akkor van olyan $a + b\imath \in \mathbb{G}$, hogy

$$x + 1 \cdot \imath = p \cdot (a + b\imath) = pa + pb\imath,$$

ahonnan pb=1, és $p|1$, ami nem lehetséges, mert feltettük, hogy p Gauß-prím, és nem egység. Hasonlóan látható, hogy ha $p | x - \imath$, akkor valamilyen $b \in \mathbb{Z}$-re $pb = -1$ ugyancsak nem lehetséges. Tehát a $4k + 1$ alakú prímek nem Gauss-prímek, ezért alkalmazhatjuk egy korábbi tételünket ([2], 7.4.14.), ami szerint

$$p = \pi_1 \overline{\pi_1}.$$

Itt π_1 és $\overline{\pi_1}$ már Gauß-prímek, a számelmélet alaptétele szerint a felbontás egységszerestől eltekintve egyértelmű, így p felbontásában már nem találunk új Gauß-prímet, de vegyük észre, hogy itt $p = N(\pi_1) = N(\overline{\pi_1})$. ■

4. fejezet

A két-négyzetszám-probléma

Ezt és a következő két fejezetet [4] alapján tárgyalom.

Ennyi előkészület után már rátérehetünk a két-négyzetszám-problémára, amely azt a kérdést hivatott megválaszolni, hogy mely természetes számok írhatók fel két négyzetszám összegeként.

A tetszőleges $x, y, u, v \in \mathbb{C}$ számra fennálló

$$\left(x^2 + y^2\right) \cdot \left(u^2 + v^2\right) = (xu - yv)^2 + (xv + yu)^2$$

azonosságból következik, hogy ha két természetes szám előáll két négyzetszám összegeként, akkor a szorzatuk is előáll két négyzetszám összegeként. Így a probléma megoldásához elég azt eldönteni, hogy mely prímek állnak elő két négyzetszám összegeként.

Tétel (vö. [2]. Valamely p prím pontosan akkor írható fel két négyzetszám összegeként, ha $p = 2$ vagy a p egy $4k + 1$ alakú prím, ahol $k \in \mathbb{N}$.

Bizonyítás.

1. lépés. Ha p prím nem $4k+1$ alakú, és $p \neq 2$, akkor néggyel osztva hármat ad maradékul, míg két négyzetszám összege néggyel osztva nem adhat hármat maradékul, csak 0-t, 1-et, vagy 2-t, hiszen négyzetszám négyes maradéka 0, vagy 1. A konguenciamódszert alkalmazva látható, hogy p ekkor nem írható fel két négyzetszám összegeként.

2. lépés. Ha $p = 2$, akkor $p = 1^2 + 1^2$ egyszerű eset.

3. lépés. Ha $p = 4k + 1$, ahol $k \in \mathbb{Z}$, akkor p nem Gauß-prím, és ezért valamilyen $\pi_1 = a + bi$ Gauß-felbonhatatlanra teljesül, hogy $p = \pi_1\overline{\pi_1}$, sőt $N(\pi_1) = p$. A

$$p = N(\pi_1) = a^2 + b^2$$

egyenlőségből már látható, hogy p felírható két négyzetszám összegeként. ■

Ezután rátérhetünk arra a problémára, hogy mely összetett számok állnak elő két négyzetszám összegeként, illetve hányféleképpen.

Tétel (vö. [2]). Legyen a $2 < n \in \mathbb{N}$ prímtényezős felbontása

$$n = 2^{\alpha} \cdot \prod_{i=1}^{r} p_i^{\beta_i} \cdot \prod_{j=1}^{s} q_j^{\gamma_j} \tag{4.0.1}$$

alakú, ahol $i = 1,2,\dots,r$ és $j = 1,2,\dots,s$ esetén β_i, γ_j nemnegatív egész számok, p_i egy $(4k-1)$ alkú prímosztója n-nek, q_j egy $(4k+1)$ alakú prímosztója n-nek, $0 \leq \alpha \in \mathbb{Z}$. Ekkor az

$$x^2 + y^2 = n \tag{4.0.2}$$

egyenlet megoldásainak a száma

- 0, ha valamely i-re β_i páratlan,
- $4 \cdot \prod_{j=1}^{s} (\gamma_j + 1)$, ha $i = 1,2,\dots,r$ esetén $2 | \beta_i$.

Bizonyítás. Az n (4.0.1) felbontásában csak $j = 1,\dots,s$-re lesznek a q_j számok nem Gauß-prímek. Ekkor egy korábbi tétel szerint a q_j számok így írhatóak fel Gauß-felbonthatatlanok szorzataként: $q_j = \pi_j \overline{\pi_j}$. Használjuk fel, hogy $2 = -i\,(1+i)^2$. Ekkor a (4.0.1) felbontás így alakítható át:

$$n = \left(-\imath\,(1+\imath)^2\right)^{\alpha} \prod_{i=1}^{r} p_i^{\beta_i} \prod_{j=1}^{s} (\pi_j \overline{\pi_j})^{\gamma_j} = \epsilon_1\,(1+i))^{2\alpha} \prod_{i=1}^{r} p_i^{\beta_i} \prod_{j=1}^{s} (\pi_j \overline{\pi_j})^{\gamma_j}\,. \tag{4.0.3}$$

Itt a $(-\imath)^{\alpha} = \epsilon_1$ szám Gauß-egység, és a többi tényező mind Gauß-prím. Másfelől, ha $(x,y) \in \mathbb{Z}^2$ kielégíti az (4.0.2) egyenletet, akkor $(x+\imath y)\,(x-\imath y) = n$, azaz $(x+\imath y)\,|n$ a $\mathbb{G}$ gyűrűben. Fel tudjuk írni $x+\imath y$ kanonikus alakját is, valamely ϵ_2 egység felhasználásával:

$$x + \imath y = \epsilon_2\,(1+\imath)^{\delta} \prod_{i=1}^{r} p_i^{\phi_i} \prod_{j=1}^{s} \pi_j^{\mu_j}\,(\overline{\pi_j})^{\nu_j} \tag{4.0.4}$$

alkalmas $\delta \leq 2\alpha$, $\mu_j \leq \gamma_j$, $\nu_j \leq \gamma_j$ számokkal. Képezzük az előző egyenlet konjugáltját, és vegyük észre, hogy

$$\overline{1+\imath} = 1 - \imath = -\imath\,(1+\imath)\,,$$

valamint legyen

$$\overline{\epsilon_2} \cdot (-\imath)^{\delta} = \epsilon_3$$

egy másik egység:

$$x - \imath y = \overline{\epsilon_2}(-\imath(1+\imath))^{\delta} \prod_{i=1}^{r} p_i^{\phi_i} \prod_{j=1}^{s} \pi_j^{\nu_j} (\overline{\pi_j})^{\mu_j} = \epsilon_3 (1+\imath)^{\delta} \prod_{i=1}^{r} p_i^{\phi_i} \prod_{j=1}^{s} \pi_j^{\nu_j} (\overline{\pi_j})^{\mu_j}. \quad (4.0.5)$$

Most (4.0.4)-et és (4.0.5)-öt összeszorozva azt kapjuk, hogy

$$(x + \imath y)(x - \imath y) = x^2 + y^2 = n = \epsilon_2 \epsilon_3 (1+\imath)^{2\delta} \prod_{i=1}^{r} p_i^{2\phi_i} \prod_{j=1}^{s} \pi_j^{\mu_j + \nu_j} \prod_{j=1}^{s} (\overline{\pi_j})^{\nu_j + \mu_j}. \quad (4.0.6)$$

A számelmélet alaptétele szerint az n egész szám egységszorzóktól (és sorrendtől) eltekinte egyételműen bomlik fel Gauß-prímek szorzatára, ezért a (4.0.3) és a (4.0.6) előállítás egységszorzóktól eltekintve megegyezik. Tehát, ha van olyan $(x, y) \in \mathbb{Z}^2$, ami kielégíti a (4.0.2) egyenletet, akkor az n szám prímtényezős felbontásában lévő kitevők és az $x + \imath y$ szám Gauß-prímtényezős felbontásában lévő kitevők között az alábbi kapcsolat áll fenn:

$$\delta = \alpha, \qquad \beta_i = 2\phi_i, \qquad \gamma_j = \mu_j + \nu_j.$$

Következésképpen β_i páros. Ebben az esetben az (x, y) pár pontosan akkor megoldás, ha $x + \imath y$ előáll (4.0.4) alakban. Hányféleképpen nézhet ki (4.0.4)-ben $x + \imath y$ megoldás?

- ϵ_2 egység négyféle lehet,
- $\delta = \alpha$: ez egyértelmű,
- $\phi_i = \dfrac{\beta_i}{2}$ ezek is egyértelműek,
- $0 \leq \mu_j \leq \gamma_j$: ezek $(\gamma_j + 1)$-féle értéket vehetnek fel, és ekkor már a $\nu_j = \gamma_j - \mu_j$ számok egyértelműek. Az eseteket összeszorozva kapjuk a különböző megoldások számát. ■

Megjegyzés. Ha (x, y) számpár megoldása a (4.0.2) egyenletnek, akkor az

$$(x, y), \qquad (-x, y), \qquad (x, -y) \qquad \text{és} \qquad (-x, -y)$$

számpárokatt különböző megoldásoknak tekintjük.

5. fejezet

Egyéb nevezetes diofantikus egyenletek

Most a két-négyzetszám-prolémához hasonló nevezetes diofantikus egyenleteket fogunk megoldani. Arra a kérdésre keressük a választ, hogy mely p prímekre oldható meg az

$$x^2 + ay^2 = p \qquad \big((x, y) \in \mathbb{Z}^2,\ a \in \mathbb{N}\big) \tag{5.0.1}$$

diofantikus egyenlet. Legyen először $a := 2$.

Amíg a két-négyzetszám-problémánál a Gauß-egészeket vizsgáltuk, most egy másik gyűrűt vezetünk be.
Jelölje továbbra is $\mathbb{G}$ a Gauß-egészek halmazát. Ekkor a

$$\{a + bi\sqrt{2} \in \mathbb{C} :\ (a, b) \in \mathbb{Z}^2\}$$

gyűrűt a $\mathbb{G}(\sqrt{2})$ szimbólummal jelöljük.
Megjegyezzük, hogy $\mathbb{G}(\sqrt{2})$ az a legszűkebb olyan gyűrű, ami tartalmazza a Gauß-egészek halmazát, és a $\sqrt{2} \in \mathbb{R}$ számot. Hasonlóan definálható $z \in \mathbb{C}$ nem Gauß-egész esetén a $\mathbb{G}(z)$ gyűrű is, illetve teszőleges $\mathbb{K}$ gyűrű és $\alpha \notin \mathbb{K}$ szám esetén a $\mathbb{K}(\alpha)$ gyűrű is.

Definíció. Valamely

$$c + di\sqrt{a} := \alpha \in \mathbb{G}(\sqrt{a})$$

szám esetén az

$$N(\alpha) := |\alpha|^2 = c^2 + ad^2$$

nemnegatív számot α normájának nevezzük.

Megjegyezzük, hogy az oszhatóság, felbonthatatlanság, egységek hasonlóan definálhatóak ebben a számkörben is. Felmerül a kéredés, hogy tudunk-e maradékosan osztani $G(\sqrt{2})$-ben. Erre ad választ a következő

Tétel.A

$$\phi(\alpha) := N(\alpha) \qquad (\alpha \in \mathbb{G}(\sqrt{2}))$$

választással a $(\mathbb{G}(\sqrt{2}), \phi)$ struktúra euklideszi gyűrű.

Bizonyítás. Hasonlóan, mint a hogy a Gauß-egészeknél bizonyítottuk a maradékos osztás tételét. Itt is elég annyit belátnunk, hogy

$$\forall \alpha \in \mathbb{Q}(\imath\sqrt{2}) \quad \exists \gamma \in \mathbb{G}(\sqrt{2}) : \qquad |\alpha - \gamma| < 1,$$

ahol

$$\mathbb{Q}(\imath\sqrt{2}) = (a + b\imath\sqrt{2} : (a, b) \in \mathbb{Q}^2).$$

Ha $\alpha \in \mathbb{Q}(\imath\sqrt{2})$, akkor az α számot tartalmazza egy négypontú téglalap a komplex számsíkon, melynek csúcsai $\mathbb{G}(\sqrt{2})$-beli számokból állnak.A legszűkebb ilyen téglalap vízszintes oldalának a hossza 1, függőleges oldalának a hossza $\sqrt{2}$. Legyen γ ennek a téglalapnak az α-hoz legközelebbi csúcsa. Ekkor

$$|\alpha - \gamma| \leq \quad \text{"téglalap átlójának a fele"} \quad = \frac{\sqrt{3}}{2} < 1.$$

Evvel a bizonyítást befejeztük. ■

Megmutatjuk, hogy ebben a gyűrűben az egységek ugyanazok, mint $\mathbb{Z}$-ben.

1. Lemma. A $\mathbb{G}(\sqrt{2})$ számgyűrű egységei a következő két szám: $1, -1$.

Bizonyítás. Ez a két szám nyilván egység, másfelől, ha $\epsilon|\alpha$ minden $\alpha \in \mathbb{G}$-re, akkor $\epsilon|1$, ezért $N(\epsilon)|N(1) = 1$, tehát $N(\epsilon) = 1$, azaz $\epsilon = \pm 1$. ■

Tetszőleges p prím, illetve $(x, y) \in \mathbb{Z}^2$ esetén most azt vizsgáljuk, hogy az

$$x^2 + 2y^2 = p \tag{5.0.2}$$

egyenlet mikor oldható meg. A bizonyítás menete ugyanaz lesz, mint a két-négyzetszám-problémánál.

2. Lemma. Ha p olyan pozitív prímszám, hogy valamely $k \in \mathbb{N}$ esetén fennáll a $p = 8k+1$ egyenlőség, vagy valamely $l \in \mathbb{N}$ esetén $p = 8l + 3$, akkor van olyan $z \in \mathbb{Z}$, hogy

$$z^2 + 2 \equiv 0 \qquad (\mathrm{mod}\ p).$$

Bizonyítás. Azt kell beleátnunk, hogy ekkor $\left(\frac{-2}{p}\right) = 1$. Használjuk fel, hogy

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}}.$$

A feltétel szerint két eset lehetséges.

1.eset. Ha a p prímre és valamely $k \in \mathbb{N}$-re fennáll, hogy $p = 8k + 1$, akkor

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{8k+1-1}{2}} \cdot (-1)^{\frac{(8k+1)^2-1}{8}} = (-1)^{4k} \cdot (-1)^{\frac{64k^2+16k+1-1}{8}} =$$

$$= (-1)^{4k} \cdot (-1)^{8k^2+2k} = 1.$$

2.eset. Ha p prímre és valamely $l \in \mathbb{N}$-re fennáll, hogy $p = 8l + 3$, akkor

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{8l+3-1}{2}} \cdot (-1)^{\frac{(8l+3)^2-1}{8}} = (-1)^{4l+1} \cdot (-1)^{\frac{64l^2+48l+9-1}{8}} =$$

$$= (-1)^{4l+1} \cdot (-1)^{8l^2+6l+1} = 1. \quad \blacksquare$$

3. Lemma. Ha p egész prímre teljesül, hogy valamely $k \in \mathbb{N}$, ill. $l \in \mathbb{N}$ számra $p = 8k + 1$ vagy $p = 8l + 3$, akkor p nem prím $\mathbb{G}(\sqrt{2})$-ben.

Bizonyítás. Az állítással ellentétben tegyük fel, hogy p prím $\mathbb{G}(\sqrt{2})$-ben. Ekkor az előző lemma szerint van olyan $z \in \mathbb{Z}$, hogy

$$p | z^2 + 2 = \left(z + \imath\sqrt{2}\right) \cdot \left(z - \imath\sqrt{2}\right).$$

Az indirekt feltevés miatt p prím $\mathbb{G}(\sqrt{2})$-ben, ezért p a fenti szorzat valamelyik tényezőjét is osztja. Ha $p | \left(z + \imath\sqrt{2}\right)$, akkor van olyan $u + v\imath\sqrt{2} \in \mathbb{G}(\sqrt{2})$, hogy

$$p \cdot (u + v\imath\sqrt{2}) = z + 1 \cdot \imath\sqrt{2}.$$

Tehát

$$pu + (pv)\,\imath\sqrt{2} = z + 1 \cdot \imath\sqrt{2}.$$

Ennélfogva $pv = 1$, ami nem lehetséges, mert p egész prím, nem $\mathbb{Z}$-beli egység. Ha $p | \left(z - \imath\sqrt{2}\right)$, akkor hasonló gondolatmenettel látható, hogy valamilyen $v \in \mathbb{Z}$ számra pv=-1, ami szintén lehetetlen. Ezzel a lemmát bebizonyítottuk. $\blacksquare$

Az iménti három lemma felhasználásával be tudjuk látni, hogy az (5.0.1) egyenlet mely prímekre oldható meg.

Tétel. Legyen p pozitív prímszám. Az (5.0.2) egyenletnek akkor és csak akkor odható meg a $\mathbb{Z}^2$ halmazon, ha $p = 2$, illetve ha van olyan $k \in \mathbb{N}$, hogy $p = 8k + 1$ vagy ha van olyan $l \in \mathbb{N}$, hogy $p = 8l + 3$.

Bizonyítás. A tételt két lépésben igazoljuk.

1.lépés. Ha p=2, akkor $p = 0^2 + 2 \cdot 1^2$. Egy teljes maradékrendszer vizsgálatával látható, hogy ha alkalmas $(x, y) \in \mathbb{Z}^2$ számpárral $p = x^2 + 2y^2$, akkor p 8-cal osztva 0, 1, 2, 3 vagy 4 maradékot ad. Ha p prím, akkor ezek közül csak az 1 és a 3 forduhat elő, mint 8-al vett osztási maradék (vagy $p = 2$).

2.lépés. Ha $p = 8k+1$, vagy $p = 8k+3$, ahol $k \in \mathbb{Z}$ és p prím, akkor az előző lemma szerint p nem prím a $\mathbb{G}(\sqrt{2})$ euklideszi gyűrűben, ezért alkalmas $\alpha \in \mathbb{G}(\sqrt{2}), \beta \in \mathbb{G}(\sqrt{2})$ számokra $p = \alpha \cdot \beta$, ahol $\alpha \neq \pm 1$ és $\beta \neq \pm 1$. Ha

$$\alpha = u + \imath v\sqrt{2} \in \mathbb{G}(\sqrt{2}),$$

és vesszük az egyenőség két oldalának a normáját, akkor a

$$p^2 = N(p) = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$$

egyenlőséghez jutunk. Ekkor $N(\alpha) = N(\beta) = p$, mert α és β nem egység $\mathbb{G}(\sqrt{2})$-ben, $N(\alpha) > 1$ $N(\beta) > 1$. Ezért a

$$p = N(\alpha) = u^2 + 2v^2$$

egyenlőség a kívánt felbontást adja. ■

A fenti három lemma segítségével belátott tételhez hasonlóan meg tudjuk mondani, hogy valamely p prím esetén mikor oldható meg a

$$p = x^2 + 3y^2 \tag{5.0.3}$$

egyenlet a $\mathbb{Z}^2$ halmazon.

Tétel. Valamely p prím esetén az (5.0.3) pontosan akkor oldható meg, ha $p = 3$, vagy alkalmas $k \in \mathbb{N}$ számra $p = 12k + 1$, vagy valamilyen $l \in \mathbb{N}$ egész esetén $p = 12l + 7$.

Bizonyítás. (Vázlat) Az előző tétel bizonyítását „leutánozzuk” vázlatosan.

1.lépés. Vegyük észre, hogy

$$\mathbb{G}(\sqrt{3}) = (a + b \cdot \epsilon : (a, b) \in \mathbb{Z}^2) := G(\epsilon), \qquad \epsilon = -\frac{1}{2} + \imath \cdot \frac{\sqrt{3}}{2}$$

ϵ egy harmadik primitív egységgyök. Itt $\mathbb{G}(\sqrt{3})$ euklideszi gyűrű, ennek bizonyításához megint csak azt kell látni, hogy

$$\forall \alpha \in \mathbb{Q}(\sqrt{3}\imath) \quad \exists \gamma \in \mathbb{G}(\epsilon), |\alpha - \gamma| < 1.$$

Ez hasonlóan a korábbi érvelésekhez azért igaz, mert rögzített $\alpha \in \mathbb{Q}(\epsilon)$-t tartalmazza egy négyzet a komplex számsíkon, melynek csúcsai $\mathbb{G}(\epsilon)$-beli számok.(Azért négyzet, mert $|\epsilon| = 1$.) Ekkor ha γ a legszűkebb ilyen négyzetnek az α-hoz legközelebbi csúcsa, akkor

$$|\alpha - \gamma| \leq \quad \text{„négyzet átlójának a fele”} \quad = \frac{\sqrt{2}}{2} < 1.$$

2.lépés. Ha $p = 3$, akkor $p = 0^2 + 3 \cdot 1^2$ triviális. Egy mod 12 teljes maradékrendszert megvizsgálva látható, hogy ha valamilyen $(x, y) \in \mathbb{Z}^2$ számpárral $p = x^2 + 3y^2$, akkor a p prím 12-vel osztva 0-t, 1-et, 3-at, 4-et, 7-et vagy 9-et ad maradékul. Ha p prím, akkor ezek közül csak az 1 és a 7 forduhat elő, mint 12-vel vett osztási maradék (vagy $p = 3$).

3.lépés. A korábbiakhoz hasonlóan belátható, hogy $\mathbb{G}(\sqrt{3})$ egységei: $1, -1$.

4.lépés. Megmutatjuk, hogy ha a p prím $12k + 1$ vagy $12k + 7$ alakú, ahol $k \in \mathbb{N}$, akkor az $x^2 + 3 \equiv 0 \ (p)$ kongruencia megoldható, azaz ilyenkor $\left(\frac{-3}{p}\right) = 1$. Valóban, a kvadratikus reciprocitási tételt és a Legrende-szimbólummal kapcsolatos azonosságokat használva azt kapjuk, hogy

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Így tehát

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & (\text{ha} \quad p \equiv 1 \ (3)), \\ \\ -1 & (\text{ha} \quad p \equiv 2 \ (3)). \end{cases}$$

Tehát, ha alkalmas $k \in \mathbb{Z}$ egész szám esetén a p prím $12k + 1$ vagy $12k + 7$ alakú, akkor $\left(\frac{-3}{p}\right) = 1$.

5.lépés. Ezután indirekt módon bebizonyítható, hogy ha a p szám $12k + 1$ vagy $12k + 7$ alakú prím, ahol $k \in \mathbb{N}$ tetszőleges szám, akkor p nem felbonthatlan $\mathbb{G}(\sqrt{3})$-ban. A valódi felbontást felírva, ha vesszük a felbontásban szereplő számok normáját, megkapjuk az (5.0.3) egyenlet egyik megoldását. ■

Megjegyzés. Tetszőleges $a \in \mathbb{N}$ nem négyzetszám estén nem működik a fenti eljárás az (5.0.1) egyenletet megoldására. Például az $a := 5$ esetben a $\mathbb{G}(\sqrt{5})$ gyűrű nem euklideszi, ugyanis itt is csak az 1 és a -1 számok az egységek, és például a 6 számnak van két különböző, $\mathbb{G}(\sqrt{5})$-beli

felbonthatatlanokra való felbontása:

$$6 = 2 \cdot 3 = (1 + \sqrt{5}\imath) \cdot (1 - \sqrt{5}\imath).$$

Ezután azzal a problémával foglalkozunk, hogy mely természetes számok írhatóak fel három, illetve négy négyzetszám összegeként. Először a három-négyzetszám-problémát vizsgáljuk.

Tétel. Egy $n \in \mathbb{N}$ természetes szám pontosan akkor nem írható fel három négyzetszám összegeként, ha van olyan $(\alpha, k) \in \mathbb{N}^2$, hogy $n = 4^\alpha \cdot (8k + 7)$.

Bizonyítás. Csak azt látjuk be, hogy ha valamilyen α, k természetes számokra

$$n = 4^\alpha \cdot (8k + 7),$$

akkor az n természetes szám nem írható fel három négyzetszám összegeként. Ezt α szerinti teljes indukcióval látjuk be.

- Legyen $\alpha := 0$, azaz valamilyen $k \in \mathbb{N}$ számmal $n = 8k+7$. Egy teljes maradékrendszer vizsgálatával belátható, hogy egy természetes szám négyzete 8-cal osztva csak 0, 1 és 4 maradékot adhat. Három négyzetszám összege ezért 8-cal osztva csak 0,1,2,3,4,5,6 maradékot adhat, 7-et nem.
- Tegyük fel, hogy valamely $\alpha \in \mathbb{N}$ és $k \in \mathbb{N}$ számokra

  $$n = 4^\alpha \cdot (8k + 7),$$

  s n nem írható fel három négyzetszám összegeként. Azt állítjuk, hogy ebben az esetben az

  $$n' := 4^{\alpha+1} \cdot (8k + 7)$$

  szám sem írható fel három négyzetszám összegeként. Ellenkező esetben ui valamiyen $(x, y, z) \in \mathbb{Z}^3$ számhármasra

  $$n' = 4^{\alpha+1} \cdot (8k + 7) = x^2 + y^2 + z^2.$$

  Tudjuk, hogy minden négyzetszám néggyel osztva 0 vagy 1 maradékot ad, és a feltevés szerint $4|x^2 + y^2 + z^2$. Következésképpen az összeg minden tagja osztható néggyel:

  $$4|x^2, \quad 4|y^2, \quad 4|z^2,$$

  emiatt

  $$2|x \quad 2|y, 2|z.$$

Tehát

$$n = \frac{n'}{4} = \frac{x^2}{4} + \frac{y^2}{4} + \frac{z^2}{4} = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$$

is előállna három négyzetszám összegeként, ami az indukciós feltevés miatt nem lehetséges. ■

Habár három négyzetszám összegekén bizonyos természetes számokat nem tudunk felírni, de négy négyzetszám összegeként már igen. Erről szól az alábbi

Tétel (Lagrange). Minden természetes szám felírható négy négyzetszám összegeként.

Ennek a tételnek a bizonyítása megtalálható [4]-ben.

6. fejezet

Pell-egyenletek

Ebben a fejezetben a diofantikus egyenletek egy speciális osztályával, a Pell-egyenletekkel foglalkozunk.

Definició (vö. [4]). Az

$$x^2 - Dy^2 = 1 \qquad \big((x,y) \in \mathbb{Z}^2,\ 0 < D \in \mathbb{N} \quad \text{és } D \text{ nem négyzetszám}\big) \qquad (6.0.1)$$

egyenletet **Pell-egyenlet**nek nevezzük.

Ha a (6.0.1) egyenlet nem Pell-egyenlet, azaz D pozitív négyzetszám, akkor csak az $(1,0)$ és a $(-1,0)$ lesz megoldása (6.0.1)-nak. Ezek a vektorok ugyanis mindig megoldások, de ha valamilyen $0 < k \in \mathbb{N}$ egészre $D = k^2$, és ha $(x,y) \in \mathbb{Z}^2$ megoldása (6.0.1)-nek, akkor

$$x^2 - Dy^2 = x^2 - k^2y^2 = (x - ky)(x + ky) = 1.$$

Az előző egyenlőség szerint ilyenkor két eset lehetséges:

1.eset.

$$\left.\begin{aligned} x - ky &= 1, \\ x + ky &= 1. \end{aligned}\right\}$$

Ekkor azt kapjuk, hogy $x = 1$, $y = 0$.

2.eset.

$$\left.\begin{aligned} x - ky &= -1, \\ x + ky &= -1. \end{aligned}\right\}$$

Ekkor pedig átrendezve az adódik, hogy $x = -1$, $y = 0$.

A megoldások száma más lesz, ha (6.0.1)-ben kikötjük, hogy D nem négyzetszám, azaz Pell-egyenletről beszélünk.

A Pell-egyenletek megoldhatóságának vizsgálatára szükségünk lesz az alábbi segédállításokra.

1. Lemma. Ha a $k \in \mathbb{N}$ és az $n \in \mathbb{N}$ számok pozitívak, valamint ha $\alpha := \sqrt[k]{n}$, akkor igaz az

$$\alpha \in \mathbb{Q} \qquad \Longrightarrow \qquad \alpha \in \mathbb{Z}$$

implikáció.

Bizonyítás. A feltétel szerint valamilyen $(p, q) \in \mathbb{Z}^2$, $q \neq 0$, $\text{lnko}(p, q) = 1$ számpárral

$$\alpha = \frac{p}{q}.$$

Ekkor α gyöke az

$$f(x) := x^k - n$$

egész együtthatós polinomnak, ezért Rolle-tétele miatt teljesül, hogy

$$p|n \quad \text{és} \quad q|1. \quad \blacksquare$$

Ahhoz, hogy belássuk, hogy minden Pell-egyenletnek végtelen sok megoldása létezik, szükségünk lesz Dirichlet approximációs tételére.

Dirichlet approximációs tétele (vö. [4]). Minden α irracionális számhoz létezik végtelen sok $1 \leq q_n \leq n$ egész szám, hogy alkalmas $p_n \in \mathbb{Z}$ számmal fennáll az

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$$

becslés.

Bizonyítás. Legyen α tetszőleges irracionális szám. Osszuk fel egyenletesen a $[0,1]$ interallumot n egyenlő részre $n-1$ osztóponttal, azaz tekintsük a

$$\left\{\frac{k}{n} \in \mathbb{R} : \ k = 1,2,3,\ldots,n-1\right\}$$

halmazt, majd tekintsük a $(0,1)$intervallumbeli $(n+1)$ darab

$$\{\alpha\}, \{2\alpha\}, \{3\alpha\}, \ldots, \{(n+1)\alpha\}.$$

irracionális számot ($\{x\}$ jelölje x valós szám törtrészét). Ezen számok mindegyike beleesika $(0,1)$ intervallum valamely fenti felosztás szerinti részinvervallumába. Tudjuk,

hogy n részintervallum van, ezért a skatulyaelv miatt lesz két szám, amely ugyanannak a részintervallumnak a belső pontja, azaz

$$\text{alkalmas} \quad r_1, r_2 \in \{1,2,\dots,n+1\}, \quad r_1 > r_2, \quad \text{ill.} \quad k \in \{0,1,\dots n-1\},$$

számokkal

$$\{r_1\alpha\},\ \{r_2\alpha\} \in \left(\frac{k}{n},\ \frac{k+1}{n}\right).$$

Ekkor tehát

$$\{r_1\alpha\} - \{r_2\alpha\} < \frac{1}{n}.$$

Legyen

$$p_i := [r_i\alpha] \qquad (i = 1,2),$$

ahol $[x]$ az x valós szám egész részét. Ekkor azt kapjuk, hogy

$$|r_1\alpha - p_1 - (r_2\alpha - p_2)| = |(r_1 - r_2)\alpha - (p_1 - p_2)| < \frac{1}{n}.$$

Legyen

$$q := r_1 - r_2 > 0 \qquad \text{és} \qquad p := p_1 - p_2.$$

Ekkor nyilvánvalóan $1 \le q \le n$. Látható, hogy ilyenkor

$$|q\alpha - p| < \frac{1}{n} \qquad \Longleftrightarrow \qquad \left|\alpha - \frac{p}{q}\right| < \frac{1}{q\cdot n}$$

Azt kaptunk, hogy minden n pozitív egész számhoz van olyan $1 \le q \le n$ szám és alkalmas p egész szám, hogy

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q\cdot n}.$$

Definiáljunk a fenti becsléshez egy alkamas

$$\left(\frac{p_n}{q_n}\right)$$

sorozatot, ahol $1 \le q_n \le n$ egész szám és egy másik p_n egészre fennáll, hogy

$$0 \le \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n\cdot n}.$$

Tudjuk, hogy $n \mapsto \dfrac{1}{n}$ sorozat nullához tart, ezért a közrefogási elvet alkalmazva látható, hogy

$$\frac{p_n}{q_n} \longrightarrow \alpha \qquad (n \to \infty).$$

Innen már következik, hogy az

$$n \mapsto \frac{p_n}{q_n}$$

sorozatnakvégtelen sok különböző tagja van, ugyanis véges sok racionális számokból álló sorozat nem konvergálhat irracionális számhoz. Vegyük észre azt is, hogy a fenti sorozatban végelen sok q_n van, ugyanis ha csak véges sok különböző q_n lenne, akkor végtelen sok különböző p_n lenne a sorozatban, és ekkor a

$$n \mapsto \left|\frac{p_n}{q_n}\right|$$

sorozatnak lenne végtelenhez tartó részsorozata, alkalmas indexsorozattal

$$\frac{p_{n_k}}{q_{n_k}} \longrightarrow \pm\infty \qquad (k \to \infty)$$

azaz

$$\left|\alpha - \frac{p_{n_k}}{q_{n_k}}\right| \longrightarrow \infty \qquad (k \to \infty)$$

teljesülne, ami az

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n \cdot n} \qquad (1 \leq n \in \mathbb{N})$$

feltétel miatt nem lehetséges. Ezért végtelen sok különböző $1 \leq q_n \leq n$ számmal és alkalmas p_n egész számmal igaz, hogy

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n \cdot n} \leq \frac{1}{q_n^2},$$

ahonnan a tétel állítása már következik. ■

Most több lépésen keresztül nekilátunk bebizonyítani, hogy minden Pell-egyenletnek végtelen sok megoldása létezik. A következő lemma bizonyításában használni fogjuk Dirichlet approximációs tételét.

2. Lemma. Tegyük fel, hogy $D \in \mathbb{N}$ nem négyzetszám. Ekkor van olyan $t \in \mathbb{Z}$, hogy

$$0 < |t| < 2\sqrt{D} + 1$$

és az

$$x^2 - Dy^2 = t \qquad ((x, y) \in \mathbb{Z}^2)$$

diofantikus egyenletnek végtelen sok olyan megoldása van, amely megoldásokban a második koordináták mind különböznek, azaz, ha

$$(x_1, y_1), (x_2, y_2), \ldots \quad \text{megoldások,}$$

akkor igaz az

$$i \neq j \qquad \Longrightarrow \qquad y_i \neq y_j$$

implikáció.

Bizonyítás. Feltettük, hogy $D \in \mathbb{N}$ nem négyzetszám, ezért az első lemma miatt $\sqrt{D}$ irracionális. Ekkor Dirichlet approximációs tétele szerint végtelen sok olyan q_n egész szám van, amelyre $1 \leq q_n \leq n$ és mindegyik q_n-hez van olyan $p_n \in \mathbb{Z}$, hogy

$$\left|\sqrt{D} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

Vegyük észre, hogy ekkor $p_n > 0$, ugyanis ellenkező esetben

$$\left|\sqrt{D} - \frac{p_n}{q_n}\right| = \left|\sqrt{D} + \frac{-p_n}{q_n}\right| \geq \sqrt{D} \geq 1 \geq \frac{1}{q_n^2}$$

is igaz lenne, ami az approximáció miatt nem lehetséges. Mekkora lehet ekkorqlinebreak $|p_n^2 - Dq_n^2|$ értéke? Nagyon nagy nem, ugyanis a Dirichlet-féle approximációs tételet és a háromszög-egyenlőtlenséget alkalmazva azt kapjuk, hogy

$$\begin{aligned}
\left|p_n^2 - Dq_n^2\right| &= \left|p_n - \sqrt{D}q_n\right| \cdot \left|p_n + \sqrt{D}q_n\right| = q_n^2 \cdot \left|\frac{p_n}{q_n} - \sqrt{D}\right| \cdot \left|\frac{p_n}{q_n} + \sqrt{D}\right| = \\
&= q_n^2 \cdot \left|\frac{p_n}{q_n} - \sqrt{D}\right| \cdot \left|\frac{p_n}{q_n} - \sqrt{D} + 2\sqrt{D}\right| \leq \\
&\leq q_n^2 \cdot \left|\frac{p_n}{q_n} - \sqrt{D}\right| \cdot \left(\left|\frac{p_n}{q_n} - \sqrt{D}\right| + 2\sqrt{D}\right) < \\
&< q_n^2 \cdot \frac{1}{q_n^2} \cdot \left(\frac{1}{q_n^2} + 2\sqrt{D}\right) = \frac{1}{q_n^2} + 2\sqrt{D} \leq 1 + 2\sqrt{D},
\end{aligned}$$

amiből következik, hogy minden $n \in \mathbb{N}$ számra

$$-1 - 2\sqrt{D} \leq p_n^2 - Dq_n^2 \leq 1 + 2\sqrt{D}$$

teljesül

$$\text{és} \quad p_n^2 - Dq_n^2 \neq 0, \quad \text{mert D nem négyzetszám, és így } \sqrt{D} \text{ irracionális.}$$

Legyen

$$I := [-1 - 2\sqrt{D}, 1 + 2\sqrt{D}]$$

intervallum, és legyen J az I-beli nem nulla egész számok halmaza. Látható, hogy ekkor minden $n \in \mathbb{N}$ számra $\left(p_n^2 - Dq_n^2\right) \in J$, és J véges sok egész számokat tartalmazó halmaz. A skatulyaelv szerint van olyan $t \in J$, hogy végtelen sok k számra

$$p_k^2 - Dq_k^2 = t.$$

A megoldások második koordinátái azért lesznek különbözőek, mert a bizonyításban szereplő $n \mapsto q_n$ sorozat injektív volt. ■

A fenti lemma segítségével meg tudunk adni a (6.0.1) egyenlet egy konkrét, nemtriviális megoldását (azaz egy olyan (u, v) megoldást, amelyre $(u, v) \neq (\pm 1, 0)$).

3. Lemma. Minden Pell-egyenletnek létezik nemtriviális megoldása.

Bizonyítás. Az előző lemma szerint van olyan $t \in \mathbb{Z}$, amelyre fennáll a

$$0 < |t| < 2\sqrt{D} + 1$$

becslés, és a

$$x^2 - Dy^2 = t \qquad ((x, y) \in \mathbb{Z}^2, x > 0, y > 0) \tag{6.0.2}$$

diofantikus egyenletnek végtelen sok megoldása van, ahol a második koordináták mind különböznek. Azonban modulo $|t|$ legfeljebb $|t|^2$ megoldáspár létezhet, ezért a skatulyaelvet alkalmazva látható, hogy van olyan $(x_1, y_1, x_2, y_2) \in \mathbb{N}^4$, csupa pozitív koordinátájú vektor, hogy

$$\left.\begin{array}{lcl} y_1 & \neq & y_2, \\ x_1 & \equiv & x_2 \pmod{|t|}, \\ y_1 & \equiv & y_2 \pmod{|t|}, \\ x_1^2 - Dy_1^2 & = & x_2^2 - Dy_2^2 = t. \end{array}\right\} \tag{6.0.3}$$

Legyen

$$u := \frac{x_1x_2 - Dy_1y_2}{|t|}, \qquad \text{ill.} \qquad v := \frac{x_1y_2 - x_2y_1}{|t|}.$$

Azt állítjuk, hogy az $(u, v) \in \mathbb{Z}^2$ nemtriviális megoldása a (6.0.1) egyenletnek. Az állításunkat három lépésben igazoljuk.

1.lépés. A (6.0.3) miatt

$$x_1x_2 - Dy_1y_2 \equiv x_1^2 - Dy_1^2 = t \equiv 0 \pmod{|t|}, \quad \text{tehát } u \text{ egész},$$

$$x_1y_2x_2y_1 \equiv x_1y_1 - x_1y_1 = 0 \equiv 0 \pmod{|t|}, \quad \text{így } v \text{ is egész.}$$

2.lépés. Az (u, v) definícióját és (6.0.3) felhasználva azt kapjuk, hogy

$$\begin{aligned} u^2 - Dv^2 &= \left(\frac{x_1x_2 - Dy_1y_2}{|t|}\right)^2 - D\left(\frac{x_1y_2 - x_2y_1}{|t|}\right)^2 = \\ &= \frac{x_1^2x_2^2 - 2Dx_1x_2y_1y_2 + D^2y_1^2y_2^2 - Dx_1^2y_2^2 + 2Dx_1x_2y_1y_2 - Dx_2^2y_1^2}{t^2} = \\ &= \frac{x_1^2 \cdot (x_2^2 - Dy_2^2) - Dy_1^2 \cdot (x_2^2 - Dy_2^2)}{t^2} = \\ &= \frac{(x_1^2 - Dy_1^2) \cdot (x_2^2 - Dy_2^2)}{t^2} = \frac{t \cdot t}{t^2} = 1. \end{aligned}$$

Tehát (u, v) megoldás.

3.lépés. Már csak azt kell bebizonyítanunk, hogy $(u, v) \neq (\pm 1, 0)$, azaz $v \neq 0$. Tegyük fel indirekt módon, hogy $v = 0$. Ekkor

$$x_1y_2 = x_2y_1,$$

ezért

$$x_2 = x_1 \cdot \left(\frac{y_2}{y_1}\right) \quad \text{és} \quad y_2 = y_1 \cdot \left(\frac{x_2}{x_1}\right) \quad \text{és} \quad \frac{x_2}{x_1} = \frac{y_2}{y_1}.$$

Legyen

$$\lambda := \frac{y_2}{y_1} = \frac{x_2}{x_1} > 0.$$

Ekkor megint (6.0.3)-et használva kapjuk, hogy

$$t = x_2^2 - Dy_2^2 = (\lambda \cdot x_1)^2 - D(\lambda \cdot y_1)^2 = \lambda^2\left(x_1^2 - Dy_1^2\right) = \lambda^2 \cdot t.$$

Így t-vel leosztva, és figyelembe véve, hogy $0 < \lambda$, az következik, hogy $\lambda = 1$, azaz $y_1 = y_2$. Ez azonban nem lehetséges, mert olyan két megoldást választottunk, ahol a második koordináták különböznek. Ezért (u, v) nemtriviális egész megoldása a (6.0.1) diofantikus egyenletnek. ■

Még egy lemmára szükségünk lesz, hogy bebizonyítsuk fejezetünk tételét.

4. Lemma. Ha (x_1, y_1) és (x_2, y_2) megoldásai a (6.0.1) diofantikus egyenletnek, akkor az

$$u + \sqrt{D}v := \left(x_1 + \sqrt{D}y_1\right) \cdot \left(x_2 + \sqrt{D}y_2\right)$$

egyenlőséggel (u, v)-t definiálva (u, v) is megoldása lesz a (6.0.1) diofantikus egyenletnek.

Bizonyítás. A bizonyítás elején megjegyezzük, hogy mivel most $\sqrt{D}$ irracionális szám, ezért tetszőleges $(a, b, c, d) \in \mathbb{Z}^4$ számnégyesre igaz az alábbi ekvivalencia:

$$a + b\sqrt{D} = c + d\sqrt{D} \qquad \Longleftrightarrow \qquad a = c \quad \text{és} \quad b = d.$$

Emiatt tételben lévő $u + v\sqrt{D}$ egyértelműen definiált. Ekkor

$$u + \sqrt{D}v = (x_1x_2 + Dy_1y_2) + \sqrt{D}\,(x_1y_2 + x_2y_1) \qquad \Longleftrightarrow \qquad u = x_1x_2 + Dy_1y_2,$$

és $v = x_1y_2 + x_2y_1$. Így a képletbe behelyettesítve azt kapjuk, hogy

$$\begin{aligned} u^2 - Dv^2 &= (x_1x_2 + Dy_1y_2)^2 - D\,(x_1y_2 + x_2y_1)^2 = \\ &= x_1^2x_2^2 + D^2x_1^2x_2^2 - Dx_1^2y_2^2 - Dx_2^2y_1^2 = x_1^2(x_2^2 - Dy_2^2) - Dy_1^2(x_2^2 - Dy_2^2) = \\ &= (x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = 1 \cdot 1 = 1. \quad \blacksquare \end{aligned}$$

A lemmáink után bebizonyíthatjuk, hogy minden Pell-egyenletnek végtelen sok megoldása van.

Tétel. Minden $0 < D \in \mathbb{Z}$ nem négyzetszám által megadott Pell-egyenletnek végtelen sok megoldása van.

Bizonyítás. A harmadik lemmában láttuk, hogy van nemtriviális megoldás, ebből negálással könnyen tudunk pozitív koordinátákból álló megoldást készíteni. Legyen (x_1, y_1) egy ilyen megoldás, amely pozitív koordinátákkal rendelkezik és így nemtriviális. Minden természetes számhoz hozzárendelünk egy megoldást. Az n-edik megoldást így értelmezzük:

$$x_n + y_n\sqrt{D} := \left(x_1 + y_1\sqrt{D}\right)^n.$$

Ekkor a 4. lemmából teljes indukcióval következik, hogy ezek a vektorok valóban megoldások, nyilván pozitívak, és különbözőek is, ugyanis ha $i < j$, akkor

$$x_j + y_j\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)^j = \left(x_1 + y_1\sqrt{D}\right)^{j-i} \cdot \left(x_1 + y_1\sqrt{D}\right)^i >$$

$$> 1 \cdot \left(x_1 + y_1\sqrt{D}\right)^i = x_i + y_i\sqrt{D}.$$

Ezért ezek a megoldások valóban különbözőek, így a fejezet tételét bebizonyítottuk. ■

Irodalomjegyzék

[1] *Diofantoszi egyenlet*, Wikipédia (2023. 01. 04.) (https://hu.wikipedia.org/wiki/Diofantoszi_egyenlet).

[2] Freud, R.; Gyarmati, E.: *Számelmélet*, Nemzeti Tankönyvkiadó, Budapest, 2006.

[3] Gyarmati, K.: *Elemi számelmélet*, (2022. 10. 17.) (http://gyarmatikati.web.elte.hu/jegyzet/szamelm1.pdf).

[4] Gyarmati, K.: *Számelmélet 2*, (2022. 10. 17.) (http://gyarmatikati.web.elte.hu/targyak/szamelmelet_2/szamelmelet2.html).

[5] Gyarmati, E.; Turán, P.: *Számelmélet*, Tankönyvkiadó, Budapest, 1988.

[6] Niven, I., Zuckerman, H. S., Montgomery, H. L.: *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc, New York, Chichester, Brisbane, Toronto, Singapure, 1991.

[7] Simo, Orsolya.: *Diofantikus egyenletek megoldása elemi módszerekkel*, szakdolgozat, Eötvös Loránd Tudományegyetem, Budapest, 2010.