# Prímfaktorizációs kvadratikus testek

Matematika BSc szakdolgozat

*Szerző:*
Domanovszki Bettina Daniella

*Témavezető:*
Dr. Waldhauser Tamás
*SZTE Bolyai Intézet*
*Algebra és Számelmélet Tanszék*

Szegedi Tudományegyetem Bolyai Intézet

2009

# Tartalomjegyzék

# 1 Bevezetés

A kvadratikus testek feletti egyértelmű prímfaktorizáció létezése számelméleti problémák vizsgálata során merült fel. A híres Fermat-féle két négyzetszám tétel számos bizonyítása közül az egyik legszebb, és legegyszerűbb bizonyítás azon alapszik, hogy a $\mathbb{Q}\left(\sqrt{-1}\right)$ komplex kvadratikus test algebrai egészeinek gyűrjén, vagyis a Gauss egészek gyűrűjén létezik egyértelmű prímfaktorizáció, vagyis Gauss-gyűrű. A nagy Fermat-tételt $n = 3$-ra Euler az Euler-egészek, vagyis $\mathbb{Q}\left(\sqrt{-3}\right)$ algebrai egészeinek segítségével igazolta. Ezen gondolatmenet mintájára próbálták az általános esetet is hasonló módon bebizonyítani, és eközben merült fel az a probléma, hogy algebrai egészek milyen gyűrűiben létezik egyértelmű prímfelbontás.

Gauss azt sejtette, hogy kilenc olyan komplex kvadratikus test létezik, amelyeken a prímfaktorizáció egyértelmű, és ezen sejtését 1801-ben publikálta a Disquisitiones Arithmeticae című könyvében. Ezek a kvadratikus testek pedig a következők:

$$\mathbb{Q}\left(\sqrt{m}\right), \text{ ahol } m = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

1934-ben Hans Heilbronn és Edward Linfoot megmutatta, hogy a fenti kilenc értékre vett komplex kvadratikus test valóban prímfaktorizációs, és ezen a kilencen kívül legfeljebb még egy prímfaktorizációs komplex kvadratikus test létezhet. Később, 1952-ben Kurt Heegner moduláris formákat és egyenleteket használva bebizonyította, hogy ez a tizedik test nem létezik. Ez a bizonyítás azonban hiányos volt, és csak akkor fogadták el, amikor 1967-ben Harold Stark teljes bizonyítást adott, kitöltve a Heegner gondolatmenetében lévő hézagokat. A számelméletben Heegner számnak hívjuk az olyan négyzetmentes, pozitív egész $m$ számot, melyre a komplex kvadratikus test, $\mathbb{Q}\left(\sqrt{-m}\right)$ prímfaktorizációs. A Stark-Heegner tétel szerint pontosan kilenc Heegner szám van (a fenti $m$ értékek ellentettjei): $1, 2, 3, 7, 11, 19, 43, 67, 163$.

Érdekességképpen megemlítjük, hogy a Heegner-számok a számelmélet különböző területein felbukkannak, olykor meglehetősen meglepő összefüggésekben. Az Euler féle prím-generáló polinom, azaz $n^2 + n + 41$ prím számokat ad $n = 0, \ldots, 39$-re, ami összefügg azzal, hogy a legnagyobb Heegner szám: $163 = 4 \cdot 41 - 1$. Rabinowitz bizonyította be, hogy $n^2 + n + p$ prím számokat ad $n = 0, \ldots, p - 2$-re akkor és csakis akkor, ha a $\mathbb{Q}\left(\sqrt{1 - 4p}\right)$ kvadratikus test prímfaktorizációs. Érdekesség még a Ramanujan féle konstans, amely nem más, mint az $e^{\pi\sqrt{163}}$ transzcendens szám, amely majdnem egész, hiszen nagyon közel van egy egész számhoz:

$$e^{\pi\sqrt{163}} = 262\,537\,412\,640\,768\,743,999\,999\,999\,999\,25\ldots \approx 640\,320^3 + 744.$$

A dolgozatban a kvadratikus test algebrai egészeinek gyűrűjén vizsgáljuk az egyértelmű prímfelbontás létezését. Be fogjuk látni, hogy a következő $m$ értékekre a komplex kvadratikus test euklideszi, következésképpen főideálgyűrű, vagyis létezik rajta prímfaktorizáció:

$$m = -1, -2, -3, -7, -11.$$

Megnézzük továbbá azt az esetet is, amikor $m = -19$. Ekkor Dedekind-Hasse norma segítségével látjuk be, hogy létezik egyértelmű prímfelbontás a kvadratikus testen.

Ezen ismereteinket az $x^2 + m = y^3$ alakú diofantoszi egyenletek megoldásában használjuk. Legegyszerűbb példa ezen megoldás menetére az $x^2 + 1 = y^3$ egyenlet megoldása. Első lépésben átírjuk az egyenletünk bal oldalát szorzat alakba:

$$(x + i)(x - i) = y^3.$$

Könnyen megmutatható, hogy a baloldalon szereplő két tényező relatív prím a Gauss-egészek $\mathbb{Z}[i]$ gyűrűjében. Mivel ezen a gyűrűn létezik egyértelmű prímfelbontás, ezért $x+i$-nek és $x-i$-nek is „köbszámnak" kell lennie, vagyis

$$x+i=(a+bi)^3=a^3-3ab^2+\left(3a^2b-b^3\right)i \qquad (a,b\in\mathbb{Z})\,.$$

Ebből következik, hogy $x=a^3-3ab^2$, illetve $1=3a^2b-b^3$. Ez utóbbi egyenletből kapjuk, hogy $b=-1$ és $a=0$, amiből kapjuk, hogy egyenletünk egyetlen megoldása: $x=0,\ y=1$.

# 2 Kvadratikus testek

## 2.1 Algebrai egészek

**2.1. Definíció.** Egy komplex számot *algebrai számnak* nevezünk, ha gyöke valamely nemzéró $f(x) \in \mathbb{Q}[x]$ polinomnak.

A fenti definícióból a következő tétel egyszerűen adódik.

**2.2. Tétel.** *Egy komplex szám akkor és csak akkor algebrai szám, ha gyöke valamely nemzéró $g(x) \in \mathbb{Z}[x]$ polinomnak.*

**2.3. Tétel.** *Bármely $\alpha$ algebrai számhoz egyetlen olyan $g(x) \in \mathbb{Q}[x]$ irreducibilis főpolinom létezik, amelynek $\alpha$ gyöke. Ezt a $g(x)$ polinomot az $\alpha$ algebrai szám minimálpolinomjának nevezzük. Amennyiben $f(x)$ olyan polinom $\mathbb{Q}[x]$-ben, amelynek $\alpha$ gyöke, akkor fennáll a $g(x) \mid f(x)$ oszthatóság.*

**2.4. Definíció.** Egy $\alpha$ algebrai számot *$n$-edfokú algebrai számnak* nevezünk, ha minimálpolinomja $n$-edfokú.

Belátható, hogy a következő definíció és tétel egymással ekvivalens.

**2.5. Definíció.** Egy algebrai számot *algebrai egésznek* nevezünk, ha minimálpolinomja egész együtthatós polinom.

**2.6. Tétel.** *Egy komplex szám akkor és csakis akkor algebrai egész, ha gyöke valamely $\mathbb{Z}[x]$-beli főpolinomnak.*

Az összes algebrai számok halmaza (a komplex számok körében megszokott összeadás, szorzás műveletével) testet alkot. Ezt a testet az *algebrai számok testének* nevezzzük. Az algebrai egészek részgyűrűt alkotnak az algebrai számok testében.

**2.7. Tétel.** *A racionális számok közül csak $\mathbb{Z}$ elemei algebrai egészek.*

*Bizonyítás.* Ha $\alpha$ racionális szám, akkor minimálpolinomja $x - \alpha$. Ez a polinom akkor és csakis akkor egész együtthatós, ha $\alpha \in \mathbb{Z}$. □

**2.8. Tétel.** *Egy $\alpha$ komplex szám akkor és csakis akkor algebrai, ha létezik $\beta$ algebrai egész és $k$ egész szám, hogy $\alpha = \beta/k$.*

*Bizonyítás.* Tegyük fel, hogy $\alpha = \beta/k$, ahol $\beta$ algebrai egész, és $k$ egész szám. Vegyük észre, hogy $\beta$ és $k$ algebrai számok. Az algebrai számok pedig testet alkotnak, tehát $\alpha$ algebrai szám.

A másik irány bizonyításához keressük az $\alpha$ algebrai számot $\beta/k$ alakban, ahol $k$ egész szám. Legyen $\alpha$ minimálpolinomja a következő:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Q}[x].$$

Legyen

$$a_i = \frac{r_i}{s_i}, \text{ ahol } \; r_i, s_i \in \mathbb{Z}, \; \text{lnko}\,(r_i, s_i) = 1 \qquad (i = 0, 1, 2, \ldots, n-1)\,.$$

A minimálpolinom értéke az $\alpha = \beta/k$ helyen 0, amiből $k^n$-nel való szorzás után kapjuk, hogy:

$$\beta^n + \frac{r_{n-1}k}{s_{n-1}}\beta^{n-1} + \ldots + \frac{r_1 k^{n-1}}{s_1}\beta + \frac{r_0 k^n}{s_0} = 0.$$

Ha $k = \prod_{i=1}^{n-1} s_i$, akkor a fenti egyenlet bal oldalán minden együttható egész szám, és ekkor a 2.6. Tétel mutatja, hogy $\beta$ algebrai egész. □

**2.9. Definíció.** Legyen $\alpha$ tetszőleges algebrai szám. Az $\alpha$ szám minimálpolinomjának bármely gyökét $\alpha$ *konjugáltjának* nevezzük. Az összes konjugáltak szorzata pedig $\alpha$ *normája*, amit $N(\alpha)$-val jelölünk. A Viéte-formulák szerint $N(\alpha)$ előjel erejéig nem más, mint $\alpha$ minimálpolinomjának konstans tagja, így $N(\alpha) \in \mathbb{Q}$.

**2.10. Tétel.** *Jelölje $\mathbb{Q}(\alpha)$ a komplex számok testének azt a legszűkebb résztestét, mely az n-edfokú $\alpha$ algebrai számot tartalmazza. Ekkor minden $\mathbb{Q}(\alpha)$-beli szám egyértelműen előáll*

$$c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0$$

*alakban, ahol $c_{n-1}, c_{n-2}, ..., c_1, c_0$ racionális számok.*

## 2.2 Algebrai egészek kvadratikus testekben

**2.11. Definíció.** A $\mathbb{Q}(\alpha)$ alakú testeket, ahol $\alpha$ másodfokú algebrai szám, *kvadratikus testeknek* nevezzük. A 2.10. Tétel szerint $\mathbb{Q}(\alpha) = \{a + b\alpha : a, b \in \mathbb{Q}\}$. Abban az esetben, ha $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, akkor azt mondjuk, hogy $\mathbb{Q}(\alpha)$ *valós* kvadratikus test, ellenkező esetben $\mathbb{Q}(\alpha)$ *komplex* kvadratikus test.

**2.12. Lemma.** *Egy $\alpha$ algebrai szám akkor és csakis akkor másodfokú, ha előáll $\alpha = a + b\sqrt{m}$ alakban, ahol $a, b \in \mathbb{Q}$,$b \neq 0$, és $m \in \mathbb{Z}\backslash\{1\}$ négyzetmentes szám.*

*Bizonyítás.* Ha $\alpha$ a tételben szereplő alakban áll elő, akkor minimálpolinomja a következő:

$$x^2 - 2ax + \left(a^2 - b^2 m\right).$$

Ebből látszik, hogy $\alpha$ másodfokú.

Tegyük fel, hogy $\alpha$ másodfokú algebrai szám. Vegyük a minimálpolinomját a következő alakban:

$$x^2 - 2ax + c \qquad (a, c \in \mathbb{Q}).$$

A másodfokú egyenlet megoldóképlete alapján

$$\alpha = a \pm \sqrt{a^2 - c^2}.$$

Az $a^2 - c^2$ racionális számot felírhatjuk $b^2 m$ alakban, ahol $b \in \mathbb{Q}$ és $m$ négyzetmentes egész szám. Így tehát $\alpha = a \pm b\sqrt{m}$, és szükség esetén $b$ előjelét megváltoztatva megkapjuk a kívánt előállítást. (Vegyük észre, hogy $m \neq 1$, hiszen $\alpha$ nem racionális.) □

**2.13. Definíció.** Az $\alpha = a + b\sqrt{m}$ másodfokú algebrai szám *konjugáltján* az $\overline{\alpha} = a - b\sqrt{m}$ számot értjük.

A fenti számolásokból látszik, hogy $\overline{\alpha}$ éppen $\alpha$ minimálpolinomjának másik gyöke, tehát a 2.9. Definíció szerinti (egyik) konjugáltja $\alpha$-nak. Ha $m < 0$, akkor $\overline{\alpha}$ éppen $\alpha$ komplex konjugáltja.

**2.14. Tétel.** *Ha $K$ kvadratikus test, akkor létezik olyan 1-től különböző, négyzetmentes $m$ egész szám, hogy $K = \mathbb{Q}(\sqrt{m})$.*

*Bizonyítás.* Legyen $K = \mathbb{Q}(\alpha)$, ahol $\alpha$ másodfokú. A 2.12. Lemma alapján tudjuk, hogy $\alpha = a + b\sqrt{m}$, ahol $a, b \in \mathbb{Q}$, tehát $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{m})$. □

**2.15. Tétel.** *Ha $m, n \neq 1$ négyzetmentes egész számok, és $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$, akkor $m = n$.*

*Bizonyítás.* Ha a tétel feltételei teljesülnek, akkor $\sqrt{m} = a + b\sqrt{n}$, alkalmas $a, b$ racionális számokkal. Négyzetreemelés után kapjuk, hogy

$$m = \left(a^2 + b^2 n\right) + 2ab\sqrt{n}.$$

Mivel $\sqrt{n}$ nem racionális, ezért $ab = 0$, ami azt jelenti, hogy $a = 0$ vagy $b = 0$. A második esetben a $\sqrt{m} = a$ egyenlőséget kapnánk, ami nem lehetséges, mert $\sqrt{m} \notin \mathbb{Q}$. Az első esetben $m = b^2 n$, és mivel $m$ négyzetmentes, ezért $b = 1$, vagyis $m = n$. □

A továbbiakban $m$ mindig egy rögzített (tetszőleges) négyzetmentes, 1-től különböző egész szám, $K$ pedig a $\mathbb{Q}(\sqrt{m})$ testet jelöli. Vegyük észre, hogy $m > 0$ esetén $K$ valós, $m < 0$ esetén pedig $K$ komplex kvadratikus test. A $K$-beli algebrai egészek gyűrűjét $\mathcal{O}_K$ jelöli. A továbbiakban az $\mathcal{O}_K$ gyűrű számelméleti tulajdonságait fogjuk vizsgálni. Szeretnénk, ha $\mathcal{O}_K$-ra is kaphatnánk a $\mathbb{Q}(\sqrt{m})$ test elemeinek a 2.12. Lemmában adott leírásához hasonló előállítást. Azt várnánk, hogy $\mathcal{O}_K = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$ de amint a következő tételben látni fogjuk, nem minden esetben ilyen egyszerű $\mathcal{O}_K$ elemeinek leírása.

**2.16. Tétel.** *A $K = \mathbb{Q}(\sqrt{m})$ kvadratikus test algebrai egészeinek gyűrűje $\mathcal{O}_K = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, ahol*

$$\omega = \begin{cases} \sqrt{m}, & \text{ha } m \equiv 2, 3 \pmod 4; \\ \frac{1+\sqrt{m}}{2}, & \text{ha } m \equiv 1 \pmod 4. \end{cases}$$

*Bizonyítás.* Legyen $\alpha = a + b\sqrt{m} \in K$, ahol $a, b \in \mathbb{Q}$. Ha $b = 0$, akkor $\alpha = a$, és a 2.7. Tétel szerint ebben az esetben $\alpha$ pontosan akkor algebrai egész, ha $a \in \mathbb{Z}$.

Tegyük fel most, hogy $b \neq 0$, ekkor $\alpha \notin \mathbb{Q}$, tehát minimálpolinomja másodfokú. A 2.12. Lemmában már láttuk, hogy az ilyen alakú $\alpha$ minimálpolinomja:

$$x^2 - 2ax + \left(a^2 - b^2 m\right).$$

Tegyük fel, hogy $\alpha \in \mathcal{O}_K$, azaz $2a \in \mathbb{Z}$ és $a^2 - b^2 m \in \mathbb{Z}$. Ekkor $4b^2 m = (2a)^2 - 4\left(a^2 - b^2 m\right) \in \mathbb{Z}$. Tekintsük $b$ és $m$ prímtényezős alakját:

$$b = \pm p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}, \text{ ahol } \beta_i \in \mathbb{Z} \quad (i = 1, 2, \ldots, r),$$
$$m = \pm p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r}, \text{ ahol } \delta_i \in \{0, 1\} \quad (i = 1, 2, \ldots, r),$$

mivel $m$ négyzetmentes. Feltehető, hogy $p_1 = 2$, ha nincs benne valamelyik prímtényezős felbontásban, akkor $\beta_1 = 0$, vagy $\delta_1 = 0$. Behelyettesítve kapjuk, hogy

$$4b^2 m = \pm p_1^{2\beta_1 + \delta_1 + 2} \prod_{i=2}^{r} p_i^{2\beta_i + \delta_i}.$$

A következő feltételeknek kell teljesülniük ahhoz, hogy $4b^2 m$ egész szám legyen:

$$2\beta_1 + \delta_1 + 2 \geq 0, \text{ vagyis}$$
$$\beta_1 \geq -1,$$

és $i = 2, 3 \ldots, r$ esetén

$$2\beta_i + \delta_i \geq 0, \text{ vagyis}$$
$$\beta_i \geq 0.$$

A fentiek szerint $b$ vagy egész, vagy „félegész" (azaz páratlan szám fele), tehát $b = \frac{l}{2}$, ahol $l \in \mathbb{Z}$. Korábban megállapítottuk, hogy $2a \in \mathbb{Z}$, ezért $a = \frac{k}{2}$, ahol $k \in \mathbb{Z}$. Ekkor

$$a^2 - b^2 m = \frac{k^2}{4} - \frac{l^2}{4} m = \frac{k^2 - l^2 m}{4} \in \mathbb{Z}, \text{ tehát}$$
$$4 \mid k^2 - l^2 m.$$

A következő négy eset lehetséges $k$ és $l$ paritásának függvényében:

(i) $k$ páratlan és $l$ páros: $k^2 - l^2 m \equiv 1 \not\equiv 0 \pmod 4$, ami ellentmondás;

(ii) $k$ páros és $l$ páratlan: $k^2 - l^2 m \equiv -m \not\equiv 0 \pmod 4$, mivel $m$ négyzetmentes, tehát ez is ellentmondás;

(iii) $k$ és $l$ páros: $k^2 - l^2 m \equiv 0 \pmod 4$, és ekkor $a, b \in \mathbb{Z}$;

(iv) $k$ és $l$ páratlan: $k^2 - l^2 m \equiv 1 - m \pmod 4$, ez akkor és csakis akkor lehetséges, ha $m \equiv 1 \pmod 4$.

A fentieket összegezve $m \not\equiv 1 \pmod 4$ esetén

$$\mathcal{O}_K = \left\{ a + b\sqrt{m} : a, b \in \mathbb{Z} \right\},$$

és ekkor készen vagyunk. Figyeljük meg, hogy az $\mathcal{O}_K$ halmaz egy téglalaprácsot alkot a komplex számsíkon, amelynek alaptartománya olyan téglalap, melynek egyik oldala 1, másik oldala $\sqrt{|m|}$ hosszúságú (lásd az 1. ábrát).

Az $m \equiv 1 \pmod 4$ esetben pedig azt kapjuk, hogy

$$\mathcal{O}_K = \left\{ \frac{k}{2} + \frac{l}{2}\sqrt{m} : k, l \in \mathbb{Z}, \text{ és } \ k \equiv l \pmod 2 \right\},$$

és ekkor következő egyenlőséget kell belátnunk:

$$\left\{ a + b\sqrt{m} : a, b \in \mathbb{Z} \text{ vagy } a, b \text{ félegész} \right\} = \left\{ a + b\frac{1 + \sqrt{m}}{2} : a, b \in \mathbb{Z} \right\}.$$

A bal oldalon szereplő halmaz az $1, \sqrt{m}$ számok által kifeszített rács kiegészítve az alaptartományok középpontjaival, mely a 2. ábrán látható. A jobb oldalon szereplő halmaz pedig az $1, \frac{1+\sqrt{m}}{2}$ számok által kifeszített rács, amely a 3. ábrán figyelhető meg. Az ábrákról látszik, hogy a két rács megegyezik. □

## 2.3 Norma és egységek kvadratikus testekben

A 2.9. Definíció értelmében az $\alpha = a + b\sqrt{m} \in K$ szám normája $N(\alpha) = \alpha \cdot \overline{\alpha} = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - b^2 m$. Vegyük észre, hogy $m < 0$ esetén $N(\alpha) = |\alpha|^2$. Vizsgálni fogjuk, hogy az $N$ norma mely $m$-ekre euklideszi, illetve Dedekind-Hasse norma (lásd a 3.4. Definíciót). Előkészületként a norma néhány alaptulajdonságát bizonyítjuk be.

**2.17. Tétel.** *Tetszőleges $K$ kvadratikus test esetén teljesülnek az alábbiak.*

(i) *A norma multiplikatív, azaz bármely $\alpha, \beta \in K$ esetén $N(\alpha\beta) = N(\alpha)\,N(\beta)$.*

(ii) *Ha $\alpha \in \mathcal{O}_K$, akkor $N(\alpha) \in \mathbb{Z}$.*

(iii) *Bármely $\alpha, \beta \in \mathcal{O}_K$ esetén, ha $\alpha \mid \beta$, akkor $N(\alpha) \mid N(\beta)$.*

(iv) *Ha $\alpha \in \mathcal{O}_K$, akkor $\alpha$ pontosan akkor egység az $\mathcal{O}_K$ gyűrűben, ha $N(\alpha) = \pm 1$.*

*Bizonyítás.* A tétel első állításának bizonyításához elsőként azt kell megmutatni, hogy ha $\alpha$,$\beta \in K$, akkor $\overline{\alpha\beta} = \overline{\alpha}\cdot\overline{\beta}$. Ezt egy könnyű számolással ellenőrizhetjük. Ezután könnyen adódik, hogy

$$N(\alpha\beta) = \alpha\beta\cdot\overline{\alpha\beta} = \alpha\beta\cdot\overline{\alpha}\,\overline{\beta} = \alpha\overline{\alpha}\cdot\beta\overline{\beta} = N(\alpha)\,N(\beta).$$

Következik a második állítás bizonyítása. Ha $\alpha$ algebrai egész $K$-ban, akkor minimálpolinomja egész együtthatós, és a 2.9. Definícióból tudjuk, hogy $\alpha$ minimálpolinomjának kontans tagja megegyezik $\alpha$ normájával, tehát $N(\alpha)$ egész szám.

A harmadik állítás igazolásához tegyük fel, hogy $\beta = \alpha\gamma$, ahol $\gamma \in \mathcal{O}_K$. Az első tulajdonság szerint $N(\beta) = N(\alpha)\,N(\gamma)$, a második tulajdonság szerint itt mindhárom norma egész szám, következésképpen $N(\alpha) \mid N(\beta)$.

A negyedik állítás bizonyítása a következőképpen történik. Ha $N(\alpha) = \pm 1$, és $\alpha$ algebrai egész, akkor $\alpha\cdot\overline{\alpha} = \pm 1$, azaz $\alpha$ egység. Fordítva, tegyük fel, hogy $\alpha$ algebrai egész és egység. Akkor létezik olyan $\beta$ algebrai egész $K$-ban, hogy $\alpha\beta = 1$, ahonnan $N(\alpha\beta) = N(\alpha)\,N(\beta) = 1$ következik, és innen $N(\alpha) = \pm 1$, mivel mind $\alpha$, mind $\beta$ normája egész szám a második tulajdonság alapján. □

**2.18. Tétel.** *Legyen $K = \mathbb{Q}(\sqrt{m})$ komplex kvadratikus test. Ha $m \neq -1, -3$, akkor $\mathcal{O}_K$ egységei 1 és $-1$. Ha $m = -1$, akkor $\mathcal{O}_K$ egységei a negyedik egységyökök, $m = -3$ esetén pedig a hatodik egységyökök.*

*Bizonyítás.* A 2.17. Tétel (iv) pontja szerint olyan $\alpha$ algebrai egészeket kell keresni a $K$ testben, amelyeknek normája 1 vagy $-1$. A 2.16. Tétel szerint $\alpha = a + b\sqrt{m}$, ahol $a, b \in \mathbb{Z}$ vagy $\alpha = (a + b\sqrt{m})/2$, ahol $a, b$ páratlan számok, és így a normája $N(\alpha) = a^2 - mb^2$ vagy $N(\alpha) = (a^2 - mb^2)/4$.

Először nézzük az első lehetőséget. Ekkor olyan $a$ és $b$ egész számokat keresünk, amelyekre $a^2 - mb^2 = \pm 1$. Mivel $m$ negatív, $a^2 - mb^2 \geq 0$, ezért csak az $a^2 - mb^2 = 1$ egyenlet megoldásait kell keresnünk. Nyilvánvaló, hogy $a = 1$, $b = 0$ valamint $a = -1$, $b = 0$ megoldások. Ha $m < -1$, akkor nincs más megoldás, ugyanis ekkor $a^2 - mb^2 \geq -mb^2 \geq 2b^2 \geq 2$, ha $b \neq 0$. Ha $m = -1$, akkor még további megoldásként adódik az $a = 0$, $b = 1$ valamint az $a = 0$, $b = -1$ lehetőség is.

Most térjünk át az $\alpha = (a + b\sqrt{m})/2$ esetre. Ekkor a 2.16. Tétel szerint $m \equiv 1 \pmod 4$. Ha $m < -3$, akkor az $(a^2 - mb^2)/4 = 1$ egyenletnek nincs páratlan $a$, $b$ megoldása, mert ha $a$ és $b$ páratlan lenne, akkor $a^2 - mb^2 \geq 1 - m > 4$. Végül tekintsük az $m = -3$ esetet. Ekkor az $a^2 + 3b^2 = 4$ egyenlet megoldásai (páratlan $a$-ra és $b$-re): $a = \pm 1$, $b = \pm 1$. Ezzel kimerítettük az összes lehetőséget. A kapott megoldások pontosan azok, amelyek a tételben szerepelnek. □

# 3 Euklideszi és prímfaktorizációs kvadratikus testek

Ebben a fejezetben azt vizsgáljuk, hogy milyen $m < 0$ értékekre lesz $\mathcal{O}_K$ prímfaktorizációs gyűrű, azaz Gauss-gyűrű. Tudjuk, hogy tetszőleges $R$ integritástartományra

$$R \text{ euklideszi gyűrű} \Longrightarrow R \text{ főideálgyűrű} \Longrightarrow R \text{ prímfaktorizációs gyűrű},$$

és általában ezen implikációk egyike sem fordítható meg. Az általunk vizsgált $\mathcal{O}_K$ gyűrűk esetén (sőt nemcsak másodfokú, hanem tetszőleges végesfokú algebrai számtestekre) a második implikáció megfordítva is igaz, vagyis $\mathcal{O}_K$ akkor és csakis akkor prímfaktorizációs, ha főideálgyűrű. Ennek igazolásához a Dedekind-gyűrűk elméletére van szükség [1].

**3.1. Definíció.** A $K$ test *prímfaktorizációs*, ha algebrai egészeinek gyűrűje prímfaktorizációs gyűrű (Gauss-gyűrű). A $K$ test *euklideszi*, ha algebrai egészeinek gyűrűje euklideszi gyűrű.

Felidézzük az euklideszi norma definícióját, és definiálunk egy általánosabb normát, amelynek segítségével a főideálgyűrűk jellemezhetők. A továbbiakban legyen $R$ tetszőleges integritástartomány.

**3.2. Definíció.** A $\|\cdot\|\colon R \longrightarrow \mathbb{N}_0$ leképezés *norma*, ha

(N) $$\forall \alpha \in R : \|\alpha\| = 0 \Longleftrightarrow \alpha = 0.$$

**3.3. Definíció.** A $\|\cdot\|$ norma *euklideszi norma*, ha (N) mellett teljesül még a következő feltétel:

(E) $$\forall \alpha, \beta \in R, \beta \neq 0 : \beta \mid \alpha \;\; vagy \;\; \exists \kappa \in R : 0 < \|\alpha - \beta\kappa\| < \|\beta\|.$$

**3.4. Definíció.** A $\|\cdot\|$ norma *Dedekind-Hasse norma*, ha (N) mellett teljesül még a következő feltétel:

(DH) $$\forall \alpha, \beta \in R, \beta \neq 0 : \beta \mid \alpha \;\; vagy \;\; \exists \kappa, \tau \in R : 0 < \|\alpha\tau - \beta\kappa\| < \|\beta\|.$$

Az euklideszi norma definíciójában általában az (E) feltétel helyett a következő feltétel használatos:

(E') $$\forall \alpha, \beta \in R, \beta \neq 0 : \; \exists \kappa \in R : 0 \leq \|\alpha - \beta\kappa\| < \|\beta\|.$$

Világos, hogy $\beta \mid \alpha$ akkor és csakis akkor, ha $\|\alpha - \beta\kappa\| = 0$, tehát az (E') és az (E) feltételek valóban ekvivalensek. A Dedekind-Hasse norma esetében ilyen átfogalmazás nem lehetséges.

**3.5. Tétel.** *Ha $R$-en létezik Dedekid-Hasse norma, akkor $R$ főideálgyűrű.*

*Bizonyítás.* Legyen $I \subseteq R$ ideál. Ha $I = \{0\}$, akkor nyilván $I = (0)$. Ha $I \neq \{0\}$, akkor legyen legyen $\beta$ minimális normájú eleme az $I\backslash\{0\}$ halmaznak. A „szívó" tulajdonság miatt tetszőleges $\xi \in R$ esetén $\xi\beta \in I$, vagyis $(\beta) \subseteq I$.

A másik irányú tartalmazás igazolásához azt kell megmutatnunk, hogy minden $\alpha \in I$ elem osztható $\beta$-val. Ha $\beta \mid \alpha$, akkor készen vagyunk, ha pedig $\beta \nmid \alpha$, akkor léteznie kell olyan $\kappa, \tau \in R$ elemeknek, hogy $0 < \|\alpha\tau - \beta\kappa\| < \|\beta\|$. A „szívó" tulajdonság miatt $\alpha\tau \in I$ és $\beta\kappa \in I$, így a különbségük is eleme $I$-nek, de nem lehet 0, ezért $\alpha\tau - \beta\kappa \in I\backslash\{0\}$. Ez viszont ellentmond annak, hogy $\beta$ normája minimális. Így tehát $I = (\beta)$. □

**Megjegyzés.** A fenti tétel megfordítása is igaz, vagyis egy $R$ integritástartomány akkor és csakis akkor főideálgyűrű, ha létezik rajta Dedekind-Hasse norma.

## 3.1 Euklideszi kvadratikus testek

**3.6. Tétel.** *Kizárólag a következő $m$ értékekre lesz a $K = \mathbb{Q}(\sqrt{m})$ komplex kvadratikus test euklideszi:*

$$m = -1, -2, -3, -7, -11.$$

Ezt a tételt nem bizonyítjuk, mert annak ellenőrzése, hogy csakis erre az öt számra igaz, hogy $K$ euklideszi, nehéz. Csak azt látjuk be, hogy erre az öt számra $K$ euklideszi.

**3.7. Tétel.** *A következő $m$ értékekre a $K = \mathbb{Q}(\sqrt{m})$ kvadratikus test euklideszi:*

$$m = -1, -2, -3, -7, -11.$$

*Bizonyítás.* Először tekintsük az $m \equiv 2, 3 \pmod 4$ esetet. Ekkor $\mathcal{O}_K$ elemei egy téglalaprácsot alkotnak a komplex számsíkon. A rács alaptartománya olyan téglalap, amelynek oldalai 1, illetve $\sqrt{|m|}$ hosszúak (lásd az 1. ábrát). Be fogjuk látni, hogy $N$ akkor és csakis akkor euklideszi norma, ha a sík minden pontját lefedik a rácspontok köré rajzolt egységnyi sugarú körök.

Világos, hogy az $N$ norma teljesíti az (N) feltételt. Már csak azt kell belátnunk, hogy az (E') feltételt is teljesíti, ehhez pedig igazolnunk kell, hogy

$$\forall \alpha, \beta \in \mathcal{O}_K,\ \beta \neq 0\ \exists \kappa \in \mathcal{O}_K, \text{ hogy } N(\alpha - \beta\kappa) < N(\beta).$$

Mivel $\beta \neq 0$, és $N$ multiplikatív, ezért leoszthatunk $N(\beta)$-val, így az $N\left(\frac{\alpha}{\beta} - \kappa\right) < 1$ egyenlőtlenséget kapjuk. A norma az abszolútérték négyzete, ezért az utóbbi egyenlőtlenség akkor és csakis akkor állhat fenn, ha

$$\left|\frac{\alpha}{\beta} - \kappa\right| < 1. \tag{3.1}$$

Legyen tetszőleges $z \in \mathbb{C}$, $r \in \mathbb{R}^+$ esetén $C_r(z)$ a $z$ középpontú $r$ sugarú nyílt körlap: $C_r(z) = \{w \in \mathbb{C} : |w - z| < r\}$. Ekkor (3.1) ekvivalens azzal, hogy

$$\frac{\alpha}{\beta} \in C_1(\kappa).$$

A 2.8. Tétel szerint $K$ minden eleme előáll $\alpha/\beta$ $(\alpha, \beta \in \mathcal{O}_K)$ alakban, tehát azt kell belátnunk, hogy $\bigcup_{\kappa \in \mathcal{O}_K} C_1(\kappa) \supseteq K$. Megmutatjuk, hogy a tételben megnevezett öt $m$ értékre az $\mathcal{O}_K$ pontjai köré rajzolt egységsugarú körök nemcsak $K$-t, de az egész komplex számsíkot lefedik, azaz

$$\bigcup_{\kappa \in \mathcal{O}_K} C_1(\kappa) = \mathbb{C}.$$

A 4. ábrán látható $ABCD$ téglalap az 1. ábrán látható rács egy alaptartománya. Ha ezen téglalap minden pontját lefedjük a csúcsai köré rajzolt egységsugarú körökkel, akkor az egész sík lefedhető az $\mathcal{O}_K$ elemei köré rajzolt egységsugarú körökkel. A téglalap akkor lesz lefedve, ha a 4. ábrán látható kör lefedi a téglalap $E$ középpontját, tehát amikor

$$\frac{|\overline{BD}|}{2} < 1,$$

vagyis a Pitagorasz-tétel szerint

$$\frac{\left|\sqrt{|m|+1}\right|}{2} < 1.$$

Rendezések után kapjuk, hogy $|m| < 3$, vagyis $m = -1, -2$.

Most tekintsük azt az eset, amikor $m \equiv 1 \pmod 4$. Ekkor $\mathcal{O}_K$ elemei egy paralelogrammarácsot alkotnak a komplex számsíkon (lásd 3. ábra), amely a 2.16. Tétel szerint nem más, mint a fentebb tekintett téglalaprács kiegészítve a téglalapok középpontjaival (2. ábra). Az előző esethez hasonlóan azt kell belátnunk, hogy minden téglalapot lefed a csúcsai és a középpontja köré rajzolt öt egységkör. Az 5. ábrán az a határhelyzet látható, amikor a zárt körök még éppen lefedik a téglalapot, vagyis ha az $\overline{AD}$ szakasz hosszabb az ebben a helyzetben látottnál, akkor még a zárt körök sem fedik le a téglalapot, ha pedig rövidebb, akkor már a nyílt körök is lefedik.

Vegyük észre, hogy az $\overline{FG}$ szakasz hossza a Pitagorasz-tétel miatt egyenlő $\frac{\sqrt{3}}{2}$-vel. Ebből következik, hogy abban az esetben, amikor $\left|\overline{DF}\right| \geq \frac{\sqrt{3}}{2} + 1$, a nyílt körlapok nem fedik le a téglalapot (egyenlőség esetén a zárt körlapok már lefedik), viszont amikor

$$\left|\overline{DF}\right| < \frac{\sqrt{3}}{2} + 1,$$

akkor már a nyílt körlapok lefedik a téglalap minden pontját. Vegyük észre továbbá, hogy

$$\frac{\sqrt{|m|}}{2} = \left|\overline{DF}\right|.$$

Behelyettesítve, és átalakítva az előző egyenlőtlenséget, a következőt kapjuk:

$$\sqrt{|m|} < \sqrt{3} + 2.$$

Ha négyzetreemeljük mindkét oldalt, megkapjuk a felső korlátot $|m|$-re:

$$|m| < 7 + 4\sqrt{3} \approx 13,93,$$

vagyis $|m| < 13$, amelynek negatív egész megoldásai $m = -1, -2, \ldots, -12$, de ezek közül csak $m = -3, -7, -11$ teljesíti az $m \equiv 1 \pmod 4$ feltételünket. □

**Megjegyzés.** A fenti gondolatmenet azt is igazolja, hogy csak a tételbeli öt $m$ értékre lesz az $N$ norma euklideszi norma az $\mathcal{O}_K$ gyűrűn. Annak igazolása, hogy ezen öt érték kivételével $N$-től különböző euklideszi norma sincs, jóval nehezebb feladat.

## 3.2 Prímfaktorizációs kvadratikus testek

**3.8. Tétel.** *Kizárólag a következő $m$ értékekre lesz a $K = \mathbb{Q}(\sqrt{m})$ komplex kvadratikus test prímfaktorizációs:*

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

A tétel bizonyítása nehéz, mi csak az $m = -19$ esetre ellenőrizzük. Ez a klasszikus példa olyan főideálgyűrűre, amely nem euklideszi.

**3.9. Tétel.** *Legyen $K = \mathbb{Q}(\sqrt{-19})$. Ekkor az $\mathcal{O}_K$ gyűrűn a szokásos $N$ norma Dedekind-Hasse norma, következésképpen $\mathcal{O}_K$ főideálgyűrű.*

*Bizonyítás.* Tudjuk, hogy $\mathcal{O}_K = \mathbb{Z}[\omega]$, ahol $\omega = \frac{1+\sqrt{-19}}{2}$. Az világos, hogy (N) teljesül. Ahhoz, hogy (DH) teljesüljön, azt kell megmutatnunk, hogy

$$\forall \alpha, \beta \in \mathcal{O}_K, \beta \neq 0 : \beta \mid \alpha \quad \text{vagy } \exists \kappa, \tau \in \mathcal{O}_K : 0 < N(\alpha\tau - \beta\kappa) < N(\beta).$$

Vegyük észre, hogy ha $\tau = 0$, akkor $0 < N(\beta\kappa) < N(\beta)$, vagyis $0 < N(\kappa) < 1$. Ez ellentmond annak, hogy $N(\kappa) \in \mathbb{Z}$, tehát $\tau$ nem lehet 0. Ezért leoszthatunk $N(\beta\kappa)$-val és a norma multiplilativitása miatt a következőt kapjuk:

$$\forall \alpha, \beta \in \mathcal{O}_K, \beta \neq 0 : \frac{\alpha}{\beta} \in \mathcal{O}_K \quad \text{vagy} \quad \exists \kappa, \tau \in \mathcal{O}_K : 0 < N\left(\frac{\alpha}{\beta} - \frac{\kappa}{\tau}\right) < \frac{1}{N(\tau)}. \tag{3.2}$$

Mivel $\xi = \frac{\alpha}{\beta}$ a $K$ test tetszőleges eleme lehet, és mivel a norma az abszolútérték négyzete, ezért (3.2) így is megfogalmazható:

$$\forall \xi \in K \backslash \mathcal{O}_K : \exists \kappa, \tau \in \mathcal{O}_K : 0 < \left|\xi - \frac{\kappa}{\tau}\right| < \frac{1}{|\tau|}. \tag{3.3}$$

Jelölje tetszőleges $z \in \mathbb{C}$, $r \in \mathbb{R}^+$ esetén $C_r^\circ(z)$ a $z$ középpontú $r$ sugarú nyílt körlapot, amelynek középpontját eltávolítjuk: $C_r^\circ(z) = \{w \in \mathbb{C} : 0 < |z - w| < r\}$. Ezzel a jelöléssel (3.3) a következő alakot ölti:

$$\forall \xi \in K \backslash \mathcal{O}_K : \exists \kappa, \tau \in \mathcal{O}_K : \xi \in C^\circ_{\frac{1}{|\tau|}}\left(\frac{\kappa}{\tau}\right). \tag{3.4}$$

Ennek geometriai jelentése a következő: A 6. ábrán látható az $\mathcal{O}_K$ elemei alkotta paralelogrammarács. Rajzoljunk minden rácspont köré középpontjában kilyukasztott egységsugarú kört. Így ugyanazt a körrendszert kapjuk, mint a 3.7. Tételben, amikor azt vizsgáltuk, hogy az $N$ norma euklideszi-e. Ezután minden $\tau \in \mathcal{O}_K \backslash \{0\}$ számra készítsük el ennek az ábrának az „$\frac{1}{\tau}$-szorosát” (ez forgatást és zsugorítást jelent). Ha ezt a végtelen sok ábrát egymásra helyezve $\mathcal{O}_K$ pontjai kivételével az egész sík le lesz fedve, akkor $N$ Dedekind-Hasse norma.

Megmutatjuk, hogy $m = -19$ esetén már a $\tau = 1, 2, \overline{\omega}, \overline{\omega + 1}$ értékekhez tartozó négy körrendszer lefedi a $\mathbb{C} \backslash \mathcal{O}_K$ halmazt. A $\tau = 1$ esetet a 7. ábra mutatja. Ezt az ábrát kell origóból középpontosan felére zsugorítani a $\tau = 2$ esetben (8. ábra). A szemléletes ábrázolás érdekében, a $\tau = 1$ esetben kapott körrendszer által lefedett pontokat szürkére színezzük (9. ábra), és erre az ábrára helyezzük rá a $\tau = 2$ esetben kapott körrendszert (10. ábra). Ekkor már az egész sík le van fedve, kivéve a körök középpontjait. A feketével jelölt középpontokat nem kell lefednünk, ugyanis ezek $\mathcal{O}_K$ elemei. A szürke részre eső fehérrel jelölt középpontok már le vannak fedve, tehát a szürke részen kívül eső fehér pontok, vagyis az $\frac{a}{2} + \frac{b}{2}\omega$ $(a, b \in \mathbb{Z}, b$ páratlan) pontok lefedése a célunk.

Vegyük észre, hogy ha egy $\xi$ pontot le tudunk fedni, vagyis

$$\xi \in C^\circ_{\frac{1}{|\tau|}}\left(\frac{\kappa}{\tau}\right)$$

alkalmas $\tau, \kappa \in \mathcal{O}_K$ számokkal, akkor bármely $\gamma \in \mathcal{O}_K$ esetén $\xi + \gamma$ is lefedhető, nevezetesen

$$\xi + \gamma \in C^\circ_{\frac{1}{|\tau|}}\left(\frac{\kappa + \gamma\tau}{\tau}\right).$$

Ezért elegendő a kimaradt fehér pontokat $\mathcal{O}_K$ elemeivel való eltolás erejéig tekinteni, és így elegendő az $\frac{\omega}{2}$, $\frac{\omega+1}{2}$ pontokkal foglalkozni (lásd a 10. ábrát). Egyszerű számolás mutatja, hogy $\frac{\omega}{2}$ esetén $\tau = \overline{\omega}$ és $\kappa = 2$, míg $\frac{\omega+1}{2}$ esetén $\tau = \overline{\omega + 1}$ és $\kappa = 3$ megfelelő lesz. □

# 4 Alkalmazások

Amint már a bevezetésben volt róla szó, $x^2 + m = y^3$ alakú diofantoszi egyenleteket oldunk meg. Első lépésben szorzattá alakítjuk az egyenlet bal oldalát:

$$\left(x + \sqrt{-m}\right)\left(x - \sqrt{-m}\right) = y^3,$$

és a tényezőkről belátjuk, hogy relatív prímek. Tegyük fel, hogy a $K = \mathbb{Q}\left(\sqrt{-m}\right)$ kvadratikus test algebrai egészeinek gyűrűje, $\mathcal{O}_K$ prímfaktorizációs. Ekkor a bal oldalon szereplő tényezők külön-külön „köbszámok", tehát

$$\left(x + \sqrt{-m}\right) = \left(a + b\sqrt{-m}\right)^3 = a^3 - 3ab^2m + \left(3a^2b - mb^3\right)\sqrt{-m} \qquad (a, b \in \mathbb{Z}),$$

amiből következik, hogy $x = a^3 - 3ab^2m$, és $1 = 3a^2b - mb^3$. Ez utóbbi egyenlőségből $a$ és $b$ könnyen kifejezhető, visszahelyettesítve megkapjuk $x$-et és $y$-t is.

**4.1. Tétel.** *Az $x^2 + 4 = y^3$ diofantoszi egyenlet megoldásai $x = \pm 2$,$y = 2$, valamint $x = \pm 11$,$y = 5$.*

*Bizonyítás.* Először tekintsük azt az esetet, amikor $x$ páros. Ekkor $y$ is páros, ezért $y^3 \equiv 0 \pmod 8$. Mivel $x$ páros, két eset lehetséges: $x \equiv 0 \pmod 4$, vagy $x \equiv 2 \pmod 4$. Ha $x \equiv 0 \pmod 4$, akkor $y^3 \equiv x^2 + 4 \equiv 4 \pmod 8$, ami lehetetlen, következésképpen $x \equiv 2 \pmod 4$. Tehát kereshetjük a megoldást az $y = 2Y$, $x = 2X$ alakban, ahol $X$ páratlan szám. Ekkor egyszerűsítés után az egyenletünk az

$$X^2 + 1 = 2Y^3$$

alakot ölti, majd szorzattá alakítva kapjuk, hogy

$$(X + i)(X - i) = 2Y^3 = (1 + i)(1 - i)Y^3.$$

Figyeljük meg, hogy $X^2 + 1 \equiv 2 \pmod 4$, mert $X$ páratlan, így $Y^3$ páratlan. Rendezzük az egyenletet:

$$Y^3 = \frac{X + i}{1 + i} \cdot \frac{X - i}{1 - i} = \left(\frac{1 + X}{2} + \frac{1 - X}{2}i\right)\left(\frac{1 + X}{2} - \frac{1 - X}{2}i\right).$$

Vezessük be a következő jelöléseket:

$$a = \frac{1 + X}{2}, b = \frac{1 - X}{2}.$$

Mivel $X$ páratlan, $a$ és $b$ egész számok és egyenletünk a következő alakot ölti:

$$Y^3 = (a + bi)(a - bi).$$

Vegyük észre, hogy $a + b = 1$, így $\text{lnko}(a, b) = 1$. Megmutatjuk, hogy az $a + bi$ és $a - bi$ Gauss-egészek is relatív prímek. Legyen $d = \text{lnko}(a + bi, a - bi)$, ekkor $d$ osztja e két szám különbségét és összegét is:

$$d \mid (a + bi) - (a - bi) = 2bi,$$
$$d \mid (a + bi) + (a - bi) = 2a.$$

Tehát $N(d)$ osztja az $a+bi, 2bi, 2a$ számok normáját, vagyis az $Y^3, 4b^2, 4a^2$ számokat. Mivel $Y$ páratlan, $a$ és $b$ pedig relatív prímek, ezért $N(d)=1$, vagyis $d$ egység.

Tehát $a+bi$ és $a-bi$ valóban relatív prímek, ezért mindkettőnek „köbszámnak", vagyis egy Gauss-egész köbének kell lennie. Legyen

$$a+bi=(s+ti)^3=s^3-3st^2+\left(3s^2t-t^3\right)i.$$

Hasonlítsuk össze a valós és képzetes részeket:

$$a=s^3-3st^2,$$
$$b=3s^2t-t^3.$$

Ebből következik, hogy $a+b=s^3-3st^2+3s^2t-t^3$, másrészt tudjuk, hogy $a+b=1$, így tehát

$$1=s^3-3st^2+3s^2t-t^3=(s-t)\left(s^2+4st+t^2\right).$$

Mivel $s,t\in\mathbb{Z}$, így

$$(s-t)=\pm1 \text{ és } \left(s^2+4st+t^2\right)=\pm1.$$

Vonjuk ki a második egyenletet az első egyenlet négyzetéből:

$$(s-t)^2-\left(s^2+4st+t^2\right)=-6st=1-(\pm1).$$

Tehát $-6st=2$ vagy $-6st=0$. Az első eset nyilván lehetetlen, tehát $s=0$ vagy $t=0$. Ha $s=0$, akkor $a=0$ és $b=1-a=1$, ha pedig $t=0$, akkor $b=0$ és $a=1-b=1$. Tehát $X=\pm1$, és így

$$x=\pm2,\ y=2.$$

Most tekintsük azt az esetet, amikor $x$ páratlan. Felírhatjuk az eredeti egyenletünket a következő alakban:

$$y^3=(x+2i)(x-2i).$$

Belátjuk, hogy $x+2i$ és $x-2i$ relatív prímek. Legyen $d=\text{lnko}(x+2i,x-2i)$, ekkor $d$ osztja ezen két szám különbségét:

$$d\mid(x+2i)-(x-2i)=4i.$$

Tehát $N(d)$ osztja az $x+2i,\ 4i$ számok normáját, vagyis az $x^2+4, 16$ számokat. Mivel $x$ páratlan, ezért $N(d)=1$, vagyis $d$ egység.

Tehát $x+2i$ és $x-2i$ valóban relatív prímek, ezért mindkettőnek „köbszámnak" kell lennie. Legyen

$$x+2i=(q+ri)^3=q^3-3qr^2+\left(3q^2r-r^3\right)i.$$

A valós és képzetes részeket összehasonlítva kapjuk, hogy

$$x=q^3-3qr^2,$$
$$2=3q^2r-r^3.$$

Látjuk, hogy $r\mid 2$, így $r=\pm2$ vagy $r=\pm1$. Visszahelyettesítve az egyenletbe a következő lehetséges $(q,r)$ számpárokat kapjuk: $(1,1),(-1,1),(1,-2),(-1,-2)$. Az első két esetben $x$-re páros számot kapunk, a második két esetből pedig a következő megoldás adódik:

$$x=\pm11,\ y=5.$$

□

**4.2. Tétel.** *Az $x^2+2=y^3$ diofantoszi egyenlet megoldásai $x=\pm 5, y=3$.*

*Bizonyítás.* Ha $y$ páros, akkor $x^2 \equiv -2 \pmod 8$, ami lehetetlen, ezért $y$ és $x$ is páratlan. Felírhatjuk az egyenletünket a következő alakban:

$$y^3 = \left(x+\sqrt{-2}\right)\left(x-\sqrt{-2}\right).$$

Először megmutatjuk, hogy $x+\sqrt{-2}$ és $x-\sqrt{-2}$ relatív prímek a $\mathbb{Z}\left[\sqrt{-2}\right]$ gyűrűben. Jelölje $d$ ezen két szám legnagyobb közös osztóját. Ekkor $d$ osztja a különbségüket is:

$$d \mid \left(x+\sqrt{-2}\right) - \left(x-\sqrt{-2}\right) = 2\sqrt{-2}.$$

Tehát $N(d)$ osztja az $x+\sqrt{-2},\ 2\sqrt{-2}$ számok normáját, vagyis az $x^2+2, 8$ számokat. Mivel $x$ páratlan, ezért $N(d)=1$, vagyis $d$ egység.

Tehát $x+\sqrt{-2}$ és $x-\sqrt{-2}$ valóban relatív prímek, ezért „köbszámoknak" kell lenniük:

$$x+\sqrt{-2} = \left(a+b\sqrt{-2}\right)^3 = a^3-6ab^2+\left(3a^2b-2b^3\right)\sqrt{-2}.$$

Hasonlítsuk össze a valós és képzetes részeket:

$$\begin{aligned} x &= a^3-6ab^2, \\ 1 &= 3a^2b-2b^3. \end{aligned}$$

Látjuk, hogy $b \mid 1$, így $b=\pm 1$. Ha $b=-1$, akkor $a \notin \mathbb{Z}$, a $b=1$ esetben pedig $a=\pm 1$, amiből a következő megoldás adódik:

$$x=\pm 5,\ y=3.$$

□

**4.3. Tétel.** *Az $x^2+11=y^3$ diofantoszi egyenlet megoldásai $x=\pm 4, y=3$, valamint $x=\pm 58, y=15$.*

*Bizonyítás.* Ha $x$ páratlan, akkor $y^3=x^2+11 \equiv 4 \pmod 8$, ami lehetetlen. Tehát $x$-nek párosnak kell lennie, és ekkor $y$ páratlan. Azt is észrevehetjük, hogy $11 \nmid x$, hiszen ellenkező esetben azt kapjuk, hogy $y^3=x^2+11 \equiv 11 \pmod{121}$, ami nem lehetséges. Tehát $11 \nmid x$, és így $11 \nmid y$.

Felírhatjuk az eredeti egyenletünket a következő alakban:

$$y^3 = \left(x+\sqrt{-11}\right)\left(x-\sqrt{-11}\right).$$

Megmutatjuk, hogy $x+\sqrt{-11}$ és $x-\sqrt{-11}$ relatív prímek a $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ gyűrűben. Legyen $d=\text{lnko}\left(x+\sqrt{-11}, x-\sqrt{-11}\right)$, ekkor $d$ osztja ezen két szám különbségét:

$$d \mid \left(x+\sqrt{-11}\right) - \left(x-\sqrt{-11}\right) = 2\sqrt{-11}.$$

Tehát $N(d)$ osztja az $x+\sqrt{-11},\ 2\sqrt{-11}$ számok normáját, vagyis az $x^2+11, 44$ számokat. Mivel $x$ páros, és nem osztható 11-gyel, ezért $N(d)=1$, vagyis $d$ egység.

Tehát $x+\sqrt{-11}$ és $x-\sqrt{-11}$ valóban relatív prímek. Ekkor mindkettő „köbszám":

$$\begin{aligned} x+\sqrt{-11} &= \left(a+b\frac{1+\sqrt{-11}}{2}\right)^3 = \\ &= \left(a^3+\frac{3}{2}a^2b-\frac{15}{2}ab^2-4b^3\right)+\left(\frac{3}{2}a^2b+\frac{3}{2}ab^2-b^3\right)\sqrt{-11}. \end{aligned}$$

Hasonlítsuk össze a valós és képzetes részeket:

$$x = a^3 + \frac{3}{2}a^2b - \frac{15}{2}ab^2 - 4b^3,$$
$$1 = \frac{3}{2}a^2b + \frac{3}{2}ab^2 - b^3.$$

Az utóbbit átalakítva kapjuk, hogy

$$2 = b\left(3a^2 + 3ab - 2b^2\right),$$

amiből következik, hogy $b = \pm 1$, vagy $b = \pm 2$. A négy esetet megvizsgálva az $(a, b)$ számpárra a $(0, -1), (1, -1), (1, 2), (-3, 2)$ lehetőségek adódnak, és ezekből az eredeti egyenletre a következő megoldásokat kapjuk:

$$x = \pm 4, y = 3 \text{ és } x = \pm 58, y = 15.$$

□

**4.4. Tétel.** *Az $x^2 + 19 = y^3$ diofantoszi egyenlet megoldásai $x = \pm 18, y = 7$.*

*Bizonyítás.* A megoldás menete az előző példával analóg, ezért nem is dolgozzuk ki részletesen, csak vázlatot mutatunk. Az előző feladathoz hasonlóan belátható, hogy $x$ páros, és ekkor $y$ páratlan, valamint $19 \nmid x$, és így $19 \nmid y$.

Felírhatjuk az eredeti egyenletünket a következő alakban:

$$y^3 = \left(x + \sqrt{-19}\right)\left(x - \sqrt{-19}\right).$$

Megmutatható továbbá, hogy $x + \sqrt{-19}$ és $x - \sqrt{-19}$ relatív prímek a $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ gyűrűben. Ekkor mindkettő „köbszám”:

$$x + \sqrt{-19} = \left(a + b\frac{1 + \sqrt{-11}}{2}\right)^3 =$$
$$= \left(a^3 + \frac{3}{2}a^2b - \frac{27}{2}ab^2 - 7b^3\right) + \left(\frac{3}{2}a^2b + \frac{3}{2}ab^2 - 2b^3\right)\sqrt{-19}.$$

Hasonlítsuk össze a valós és képzetes részeket:

$$x = a^3 + \frac{3}{2}a^2b - \frac{27}{2}ab^2 - 7b^3,$$
$$1 = \frac{3}{2}a^2b + \frac{3}{2}ab^2 - 2b^3.$$

Az utóbbit átalakítva kapjuk, hogy

$$2 = b\left(3a^2 + 3ab - 4b^2\right),$$

amiből következik, hogy $b = \pm 1$, vagy $b = \pm 2$. A négy esetet megvizsgálva az $(a, b)$ számpárra az $(1, 1), (-2, 1)$ lehetőségek adódnak, és ezekből az eredeti egyenletre a következő megoldásokat kapjuk:

$$x = \pm 18,\ y = 7.$$

□

# Irodalomjegyzék

[1] David S. Dummit, Richard M. Foote, *Abstract Algebra*, John Wiley & Sons, Inc., Hoboken, NJ, 2004.

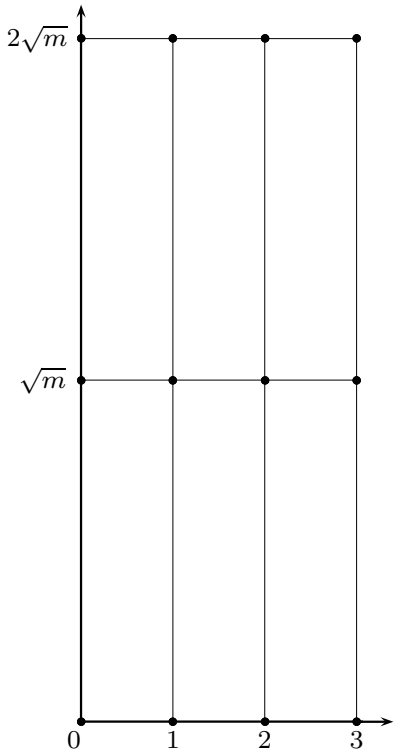
[2] Freud Róbert, Gyarmati Edit, *Számelmélet,* Nemzeti Tankönyvkiadó, Budapest, 2005.

[3] Erich Hecke, *Lectures on the Theory of Algebraic Numbers*, Graduate Texts in Mathematics 77, Springer-Verlag, New York-Berlin, 1981.

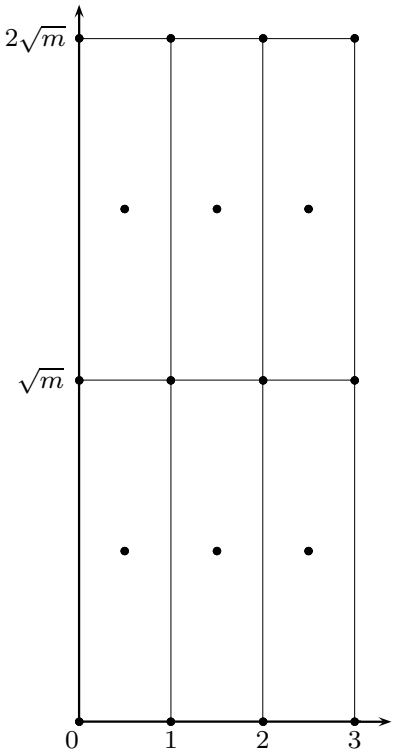
[4] Megyesi László, *Bevezetés a számelméletbe,* Polygon Jegyzettár, Polygon, Szeged, 2005.

[5] M. Ram Murty, Jody Esmonde, *Problems in Algebraic Number Theory,* Graduate Texts in Mathematics 190, Springer-Verlag, New York, 2005.

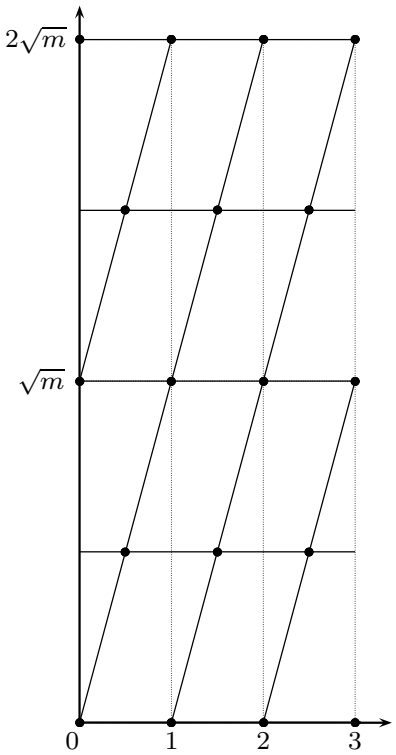
# 5 Melléklet



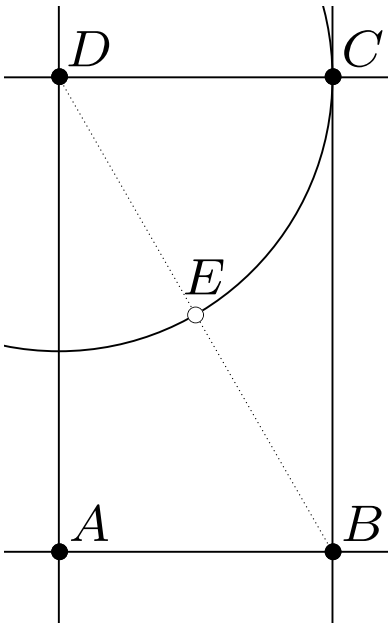

1. ábra



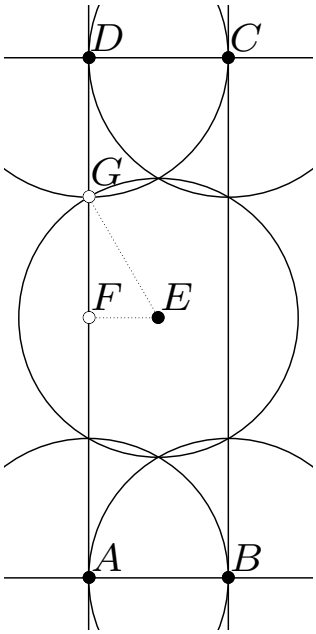

2. ábra



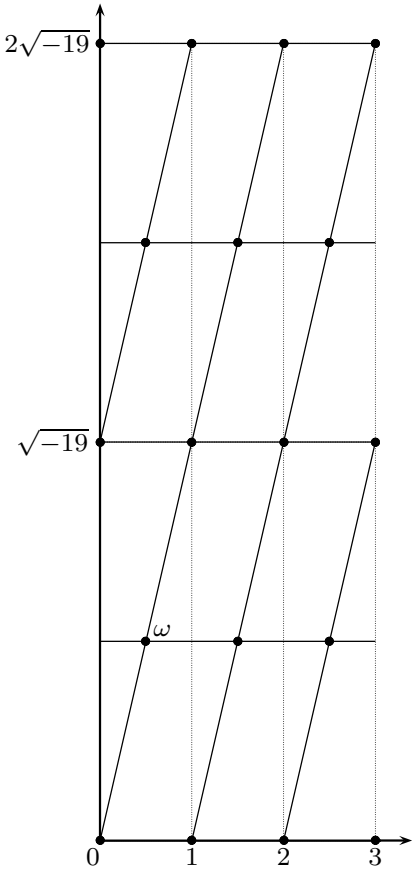

3. ábra



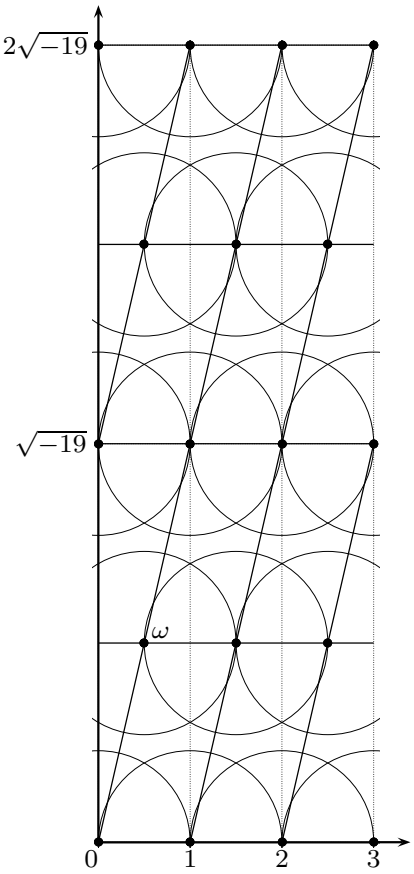

4. ábra



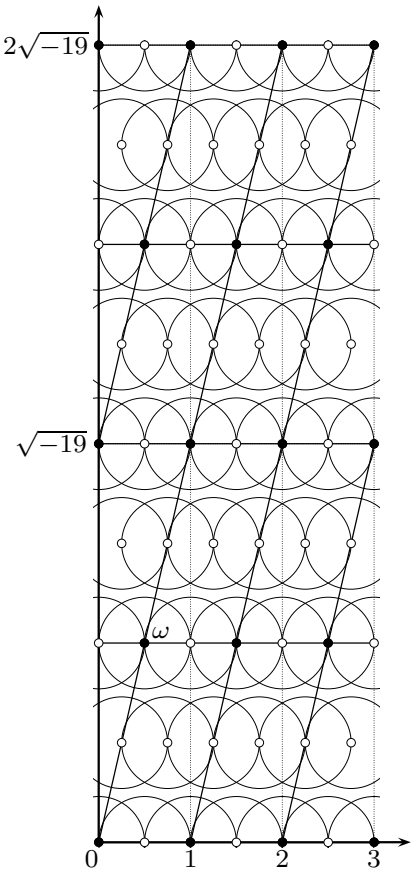

5. ábra



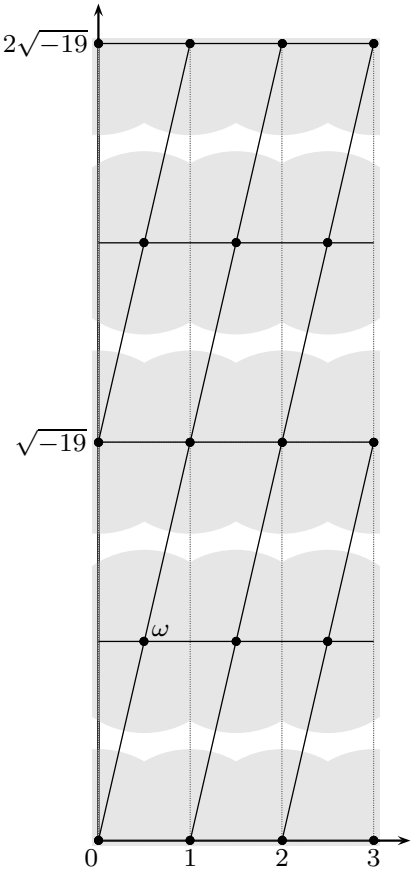

6. ábra



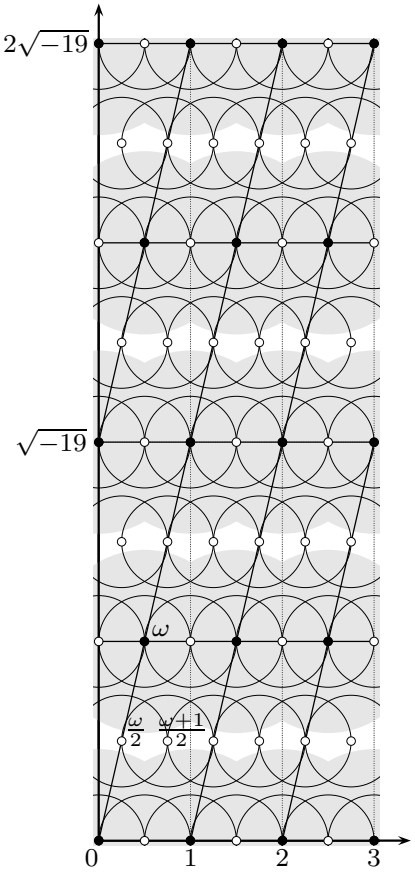

7. ábra




8. ábra




9. ábra




10. ábra

# 6 Nyilatkozat

Alulírott Domanovszki Bettina Daniella kijelentem, hogy a szakdolgozatban foglaltak saját munkám eredményei, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel. Tudomásul veszem, hogy szakdolgozatomat a Szegedi Tudományegyetem könyvtárában a kölcsönözhető könyvek között helyezik el, és az interneten is nyilvánosságra hozhatják.

Köszönetet szeretnék mondani témavezetőmnek, Dr. Waldhauser Tamásnak az érdekes témáért, és a sok segítségért, melynek köszönhetően ez a szakdolgozat elkészült.