



Monogenitási vizsgálatok algebrai számtestekben

doktori (PhD) értekezés

NYUL GÁBOR

Debreceni Egyetem

Debrecen, 2007

Ezen értekezést a Debreceni Egyetem Matematika és Számítástudományok Doktori Iskola Diofantikus és konstruktív számelmélet programja keretében készítettem a Debreceni Egyetem doktori (PhD) fokozatának elnyerése céljából.

Debrecen, 2007. január 31.

.....
Nyul Gábor
jelölt

Tanúsítom, hogy Nyul Gábor doktorjelölt 2003–2006 között a fent megnevezett doktori iskola Diofantikus és konstruktív számelmélet programjának keretében irányításommal végezte munkáját. Az értekezésben foglalt eredményekhez a jelölt önálló alkotó tevékenységével meghatározóan hozzájárult. Az értekezés elfogadását javaslom.

Debrecen, 2007. január 31.

.....
Dr. Gaál István
témavezető

Köszönetnyilvánítás

Köszönetet szeretnék mondani mindazoknak, akik segítettek abban, hogy eddig eljuthattam:

Elsősorban Édesanyámnak és Édesapámnak, hogy felneveltek és húsz éven át biztosították a hátteret, hogy tanulhassak. Ugyancsak köszönet illeti testvéremet, Balázst.

Általános iskolai és középiskolai matematikatanáraimnak, Győri Sándorné Erzsike néninek, Szabó Tiborné Erzsike néninek, Szántó Sándornak és Nagy Erzsébetnek, hogy megismertették velem a matematika alapjait és megszerettették velem ezt a tantárgyat. Rajtuk kívül a többi tanáromnak az egykori Új Élet Parki Általános Iskolából és a debreceni Fazekas Mihály Gimnáziumból.

A Matematikai Intézet és az Informatikai Kar azon oktatóinak, akik az egyetemi évek alatt betekintést nyújtottak a matematika különböző területeibe, továbbá a Matematika és Számítástudományok Doktori Iskola Diofantikus és konstruktív számelmélet doktori programja tanárainak, Dr. Győry Kálmánnak és Dr. Pethő Attilának.

A fent felsoroltakon kívül mindazoknak, akik akár a legcsekélyebb mértékben is hozzájárultak előrehaladásomhoz.

Végül, de messze nem utolsósorban témavezetőmnek, Dr. Gaál Istvánnak rengeteg segítségéért és állandó támogatásáért.

Tartalomjegyzék

1. Bevezetés	1
2. Diéder negyedfokú számtestek monogenitása	7
2.1. Negyedfokú számtestek monogenitása	7
2.2. Diéder negyedfokú számtestek	9
2.3. Az algoritmus	11
2.4. Numerikus példák	12
3. Bikvadratikus számtestek monogenitása	15
3.1. Bikvadratikus számtestek	15
3.2. Teljesen komplex bikvadratikus testek monogenitása	18
3.3. A tétel bizonyítása	20
3.4. Teljesen komplex bikvadratikus számtestek táblázata	24
4. Az index forma egyenlet p-adikus változata bikvadratikus számtestekben	27
4.1. A megoldás előkészítése	27
4.2. Az S -egység egyenlet a racionális egész számok gyűrűje felett	29
4.3. A racionális egészek gyűrűje feletti S -egység egyenlet megoldása	30
4.4. A kitevők lehetséges értékeinek leírása	32
4.5. Az S -egység egyenlet a negyedfokú test felett	37
4.6. A K feletti S -egység egyenlet megoldása: felső korlátok	41
4.7. A K feletti S -egység egyenlet megoldása: redukció	44
4.8. Az algoritmus	46
4.9. Első példa: egy teljesen komplex bikvadratikus test	47
4.10. Második példa: egy teljesen valós bikvadratikus test	51

4.11. Harmadik példa: egy teljesen valós bikvadratikus test, amikor bonyolultabb a megoldás	55
4.12. A példák számításigénye	60
5. Multikvadratikus számtestek monogenitása	61
5.1. Multikvadratikus számtestek	61
5.2. Három másodfokú számtest kompozitumának monogenitása .	61
5.3. Testindex multikvadratikus számtestekben	67
5.4. Monogenitás multikvadratikus számtestek egy rendjében . . .	68
6. Algebrai számtestek testindexe	71
6.1. Testindex	71
6.2. Kishi-féle harmadfokú testek	72
6.3. Legegyszerűbb negyedfokú testek	74

1. Bevezetés

A számelmélet két fejezete, a történetileg az ókorig visszanyúló diofantikus egyenletek elmélete és a sokkal fiatalabb algebrai számelmélet szoros kapcsolatban állnak egymással, például diofantikus egyenletek megoldásakor gyakran lehet algebrai számelméleti eszközöket, eredményeket felhasználni. Az értekezés tárgya az algebrai számelmélet egy klasszikus területének, az algebrai számtestek monogenitásának és ezzel rokon kérdéseknek a vizsgálata, mely ekvivalens bizonyos széteső forma diofantikus egyenletek, úgynevezett index forma egyenletek megoldásával.

Legyen K egy n -edfokú algebrai számtest és jelölje $\mathbb{Z}_K$ a K -beli algebrai egészek gyűrűjét. Nyilvánvaló, hogy ha $\alpha \in K$ primitív eleme K -nak, azaz $K = \mathbb{Q}(\alpha)$, akkor $(1, \alpha, \dots, \alpha^{n-1})$ bázisa K -nak $\mathbb{Q}$ felett. Ugyancsak jól ismert, hogy minden algebrai számtestben létezik egész bázis. Az algebrai számelmélet egy klasszikus kérdése annak vizsgálata, hogy létezik-e K -ban a fenti két tulajdonsággal egyszerre rendelkező bázis, azaz létezik-e olyan $\alpha \in \mathbb{Z}_K$ elem, hogy $(1, \alpha, \dots, \alpha^{n-1})$ egész bázisa K -nak. Az ilyen alakú egész bázist **hatvány egész bázis**nak, α -t pedig a hatvány egész bázis **generátor**ának nevezzük. K -t akkor hívjuk **monogén**nek, ha van hatvány egész bázisa. Egy algebrai számtest monogenitásának eldöntése mellett ugyancsak fontos probléma, hogy monogén testekben hogyan határozhatjuk meg az összes hatvány egész bázist generáló elemet.

Belátható, hogy ha $\alpha \in \mathbb{Z}_K$ primitív eleme K -nak, akkor $\mathbb{Z}[\alpha]^+$ véges indexű részcsoportha a $\mathbb{Z}_K^+$ additív csoportnak és ebben az esetben $I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+)$ -t α **index**ének nevezzük. Látható, hogy α pontosan akkor generál hatvány egész bázist K -ban, ha $I(\alpha) = 1$.

A K algebrai számtest m_K **minimális indexe**, illetve i_K **testindexe** rendre a K -beli primitív algebrai egészek indexeinek minimuma, illetve legnagyobb közös osztója. Világos, hogy $i_K \mid m_K$, továbbá K -ban akkor és csak akkor létezik hatvány egész bázis, ha $m_K = 1$, és így monogén K esetén $i_K = 1$. (Az utolsó állítás megfordítása nem igaz.)

Legyen $(\omega_1 = 1, \omega_2, \dots, \omega_n)$ egész bázisa K -nak, $l(\underline{x}) = x_1 + x_2\omega_2 + \dots + x_n\omega_n$ és $l^{(i)}(\underline{x}) = x_1 + x_2\omega_2^{(i)} + \dots + x_n\omega_n^{(i)}$, ahol $\omega_j^{(i)}$ jelöli ω_j -nek az i -edik relatív konjugáltját K -ban ($i, j = 1, \dots, n$). Ekkor ehhez az egész bázishoz

tartozó **diszkrimináns forma**

$$D_{K/\mathbb{Q}}(l(\underline{x})) = \prod_{1 \leq i < j \leq n} (l^{(i)}(\underline{x}) - l^{(j)}(\underline{x}))^2.$$

Legyen D_K a K számtest diszkriminánsa. A diszkrimináns forma felírható

$$D_{K/\mathbb{Q}}(l(\underline{x})) = (I(x_2, \dots, x_n))^2 \cdot D_K$$

alakban, ahol $I(x_2, \dots, x_n)$ egy racionális egész együtthatós, $n(n-1)/2$ -edfokú homogén polinom (lsd. például [11], Lemma 1.1.2.). Ezt a polinomot az $(\omega_1 = 1, \omega_2, \dots, \omega_n)$ egész bázishoz tartozó **index formának** nevezzük.

Bebizonyítható (lsd. például [11], Lemma 1.1.3.), hogy ha $\alpha = x_1 + x_2\omega_2 + \dots + x_n\omega_n \in \mathbb{Z}_K$ ($x_1, x_2, \dots, x_n \in \mathbb{Z}$) primitív eleme K -nak, akkor $I(\alpha) = |I(x_2, \dots, x_n)|$. Következésképpen A indexű primitív $\mathbb{Z}_K$ -beli elemek keresése (A adott természetes szám) ekvivalens az

$$I(x_2, \dots, x_n) = \pm A \quad (x_2, \dots, x_n \in \mathbb{Z})$$

index forma egyenlet, speciálisan a hatvány egész bázisok keresése ekvivalens a ± 1 jobb oldalú index forma egyenlet megoldásával.

A fentiek alapján a minimális index és a testindex is megadható az index forma segítségével, mivel

$$m_K = \min \{|I(x_2, \dots, x_n)| \mid x_2, \dots, x_n \in \mathbb{Z} \text{ és } I(x_2, \dots, x_n) \neq 0\}$$

és

$$i_K = \text{lko} \{I(x_2, \dots, x_n) \mid x_2, \dots, x_n \in \mathbb{Z}\}.$$

Az $\alpha, \beta \in \mathbb{Z}_K$ elemek **$\mathbb{Z}$ -ekvivalensek**, ha $\alpha - \beta \in \mathbb{Z}$. (Ez ekvivalenciareláció $\mathbb{Z}_K$ -n.) Ebben az esetben $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, ezért ha $\alpha, \beta \in \mathbb{Z}_K$ $\mathbb{Z}$ -ekvivalens primitív elemek, akkor $I(\alpha) = I(\beta)$. Speciálisan ha $\alpha, \beta \in \mathbb{Z}_K$ $\mathbb{Z}$ -ekvivalensek és α hatvány egész bázist generál, akkor β is. Ezek az észrevételek egyébként abból is adódnak, hogy az index forma független x_1 -től.

Legyenek $p_1, \dots, p_s$ különböző rögzített prímszámok. Ekkor az index forma egyenlet **p -adikus változata** az

$$I(x_2, \dots, x_n) = \pm p_1^{t_1} \cdot \dots \cdot p_s^{t_s}$$

egyenlet, ahol az ismeretlenek $x_2, \dots, x_n \in \mathbb{Z}$ az $\text{lko}(x_2, \dots, x_n) = 1$ feltétellel és $0 \leq t_1, \dots, t_s \in \mathbb{Z}$. Ennek megoldása ekvivalens az olyan K -beli primitív algebrai egészek meghatározásával, melyek indexe csak a rögzített prímekkel osztható.

Megjegyezzük, hogy a fenti fogalmak és azok tulajdonságai egyszerűen megfogalmazhatók $\mathbb{Z}_K$ helyett tetszőleges $\mathcal{O} \subseteq \mathbb{Z}_K$ rend esetén is.

Győry K. [26] bebizonyította, hogy az index forma egyenleteknek csak véges sok megoldásuk van, a megoldások abszolút értékére pedig effektív felső korlátot vezetett le. (A felső korlát legjobb ismert javítása [29]-ben található.) A bizonyítást az index forma egyenlet egységegyenletekre történő visszavezetésével és a Baker-módszert alkalmazva nyerte. Következményként adódik, hogy $\mathbb{Z}$ -ekvivalenciától eltekintve csak véges sok adott indexű primitív $\mathbb{Z}_K$ -beli elem létezik, speciálisan $\mathbb{Z}$ -ekvivalenciától eltekintve csak véges sok hatvány egész bázis generátor van.

Az eredmény effektív volta algoritmuselméleti szempontból azt jelenti, hogy az index forma egyenletek megoldása, adott indexű primitív algebrai egész elemek keresése, hatvány egész bázis generátorok keresése elvben elvégezhető, ha a korlátig végignézzük az összes lehetséges értéket. A felső korlátok azonban még a kis foksámú testek esetén is olyan nagyok, hogy a gyakorlatban ez a módszer önmagában nem kivitelezhető, így hatékony algoritmusok keresése továbbra is fontos feladat maradt.

Az index forma egyenlet p -adikus változata esetén szintén *Győry K.* [27] adott a megoldásokra effektív felső korlátot, melyre ugyancsak elmondhatók az előbb leírtak.

Ezek után a további vizsgálatoknak két fontos iránya van. Egyrészt adott típusú algebrai számtestek esetén lehet hatékony algoritmust keresni az index forma egyenlet, illetve az ehhez kapcsolódó algebrai számelméleti problémák megoldására. Igazán hatékony algoritmus csak harmadfokú (*Gaál I., N. Schulte* [23]) és negyedfokú (*Gaál I., Pethő A., M. Pohst* [19], [22]) esetben ismert. Létezik továbbá általános algoritmus ötödfokú (*Gaál I., Győry K.* [12]) és hatodfokú (*Y. Bilu, Gaál I., Győry K.* [4]) számtestekre, melyek kivitelezhetők ugyan, de még nem tekinthetők igazán hatékonyoknak.

A másik lehetséges irány szerint algebrai számtestek egy családjában (például egy parametrikus családban) kell megoldani ezeket a problémákat. Ez azt jelenti, hogy a megoldást a család összes teste esetén egyszerre

keressük.

Az ismertett problémakörrel sokan foglalkoztak, mely eredményekről több összefoglaló cikk [9], [10], [30], [31], illetve könyv [11] ad részletes áttekintést.

Az értekezés további fejezetei mind az eddig ismertett problémák valamelyikével foglalkoznak bizonyos algebrai számtestek esetén. Most röviden áttekintjük ezeket az eredményeket.

A 2. fejezetben egy olyan gyors algoritmust adunk, ami adott valós másodfokú számtest esetén megadja az összes olyan vegyes szignatúrájú diéder negyedfokú számtestet, melyben van hatvány egész bázis és melynek részteste az adott másodfokú test, egyúttal ezekben meghatározza az összes hatvány egész bázis generátort. Ehhez egyrészt *A. C. Kable* [33] eredményét használjuk fel, ami biztosítja azt is, hogy csak véges sok megfelelő negyedfokú test létezik. Másrészt alkalmazzuk *Gaál I.*, *Pethő A.* és *M. Pohst* [19], [22] módszerét negyedfokú számtestek index forma egyenleteinek megoldására, melyet a fejezet elején röviden össze is foglalunk. Algoritmusunkat példaként a $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$ másodfokú számtestekre alkalmaztuk, melyekre nyert numerikus eredményeket a fejezet végén ismertetjük.

A 3. és a 4. fejezetben bikvadratikus számtestekkel foglalkozunk. Így hívjuk azokat a negyedfokú algebrai számtesteket, melyek Galois-csoportja Klein-csoport vagy ekvivalens módon azokat, amik különböző négyzetmentes $m, n \in \mathbb{Z} \setminus \{0, 1\}$ számokkal $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ alakba írhatók. Ezekben a testekben sokan foglalkoztak a monogenitás problémájával, ezek összefoglalása a 3. fejezet első részében található.

Számunkra a legfontosabb eredmény az, hogy *K. S. Williams* [53] leírta a bikvadratikus számtestek egy egész bázisát, valamint diszkriminánsát, ami alapján *Gaál I.*, *Pethő A.* és *M. Pohst* [16] kiszámították a három kvadratikus forma szorzatára bomló index formát. Ugyancsak ők [21] adtak hatékony eljárást a teljesen valós bikvadratikus számtestek esetén az index forma egyenlet megoldására. A 3. fejezet célja az, hogy a teljesen komplex eset vizsgálatával teljessé tegye a monogenitás vizsgálatát bikvadratikus számtestekben. Egyszerűen ellenőrizhető szükséges és elégséges feltételt adunk hatvány egész bázis létezésére és leírjuk az összes hatvány egész bázist

generáló elemet. Kiderül, hogy a generátoroknak az egész bázisra vonatkozó együtthatói konstans vektorok egy kis elemszámú halmazából kerülhetnek ki. A bizonyítás fontos eleme, hogy teljesen komplex bikvadratikus számtestekben az index forma tényezői között van definit kvadratikus forma. Ebből az észrevételből kiindulva tetszőleges jobb oldalú index forma egyenlet is megoldható. Ezt alkalmazva nyerhető a fejezet végén található táblázat, melyben összefoglaljuk a 10^4 -nél kisebb diszkriminánsú teljesen komplex bikvadratikus számtesteket, kiszámolva testindexüket, minimális indexüket és a minimális indexszel rendelkező összes elemet.

A 4. fejezet olyan hatékony algoritmust ismertet, mely bikvadratikus számtestekben az index forma egyenlet p -adikus változatát oldja meg. Egy példától eltekintve p -adikus index forma egyenletet numerikusan eddig még nem oldottak meg. Látni fogjuk, hogy bikvadratikus számtesteknél az esetek jelentős részében lényegében egy $\mathbb{Z}$ feletti S -egység egyenlet megoldásával érhetünk célt. Kiderül azonban, hogy ha az egyenlet jobb oldalán szereplő prímekek valamelyike két különböző prímideál szorzatára bomlik fel a bikvadratikus számtest mindhárom résztestében, akkor még meg kell oldani egy S -egység egyenletet a negyedfokú test felett is. Az S -egység egyenletek megoldásához p -adikus és komplex logaritmusok lineáris formáira vonatkozó becsléseket és különböző redukciónak eljárásokat alkalmazunk. Az algoritmus illusztrálásaként három konkrét egyenletet is megoldunk.

A bikvadratikus számtesteket természetes módon lehet általánosítani, ha $\mathbb{Q}$ -hoz legalább két különböző $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ négyzetmentes szám négyzetgyökét adjungáljuk. Az így nyert multikvadratikus számtesteket vizsgáljuk az értekezés 5. fejezetében, melyeknél mindig feltesszük vagy más feltételekből következik, hogy a számtest fokszáma 2^n . Ezek monogenitásával kapcsolatban az itt ismertetettek az első eredmények. Azt látjuk be, hogy $n = 3$ esetén ha k_1, k_2, k_3 páronként relatív prímekek, $k_1 < 0$ és $k_2 \equiv k_3 \equiv 1 \pmod{4}$, akkor a multikvadratikus számtest nem monogén. Ezután tetszőleges n esetén igazoljuk, hogy páratlan diszkrimináns mellett a testindex páros, míg további megkötés nélkül az $\mathcal{O} = \mathbb{Z}[\sqrt{k_1}, \dots, \sqrt{k_n}]$ rend minden elemének indexe osztható 2-nek egy nagy kitevős hatványával. Ezekből az is következik, hogy a feltételek megtartása mellett rendre a maximális rendben illetve $\mathcal{O}$ -ban nincs hatvány egész bázis.

Az utolsó fejezetben algebrai számtestek két parametrikus családjára esetén határozzuk meg a testindexet. Először a Kishi-féle harmadfokú

testeket vizsgáljuk. Így nevezzük a $t^3 - a(a^2 + a + 3)(a^2 + 2)t^2 - (a^3 + 2a^2 + 3a + 3)t - 1 \in \mathbb{Z}[t]$ polinomok felbontási testét, ahol $a \in \mathbb{Z}$ olyan egész szám, amire egy jól meghatározott, a -tól függő egész szám négyzetmentes. A Kishi-féle harmadfokú testeknek megadjuk egy egész bázisát, majd kiszámítjuk az ehhez tartozó index formát, aminek vizsgálatával bebizonyítjuk, hogy a testindex minden ilyen test esetén 1. Ezután a legegyszerűbb negyedfokú testek családját tekintjük, amiket a $t^4 - at^3 - 6t^2 + at + 1 \in \mathbb{Z}[t]$ polinom felbontási testeként definiálunk, ahol $a \in \mathbb{Z} \setminus \{0\}$ olyan, hogy $a^2 + 16$ -nak az 1-en kívül nincs páratlan négyzetszám osztója. Ezekről a 2. fejezetben már leírt módszert felhasználva azt igazoljuk, hogy testindexük rendre 1 vagy 2 attól függően, hogy a páros vagy páratlan.

2. Diéder negyedfokú számtestek monogenitása

2.1. Negyedfokú számtestek monogenitása

Negyedfokú algebrai számtestekben az index forma egyenlet megoldásával, hatvány egész bázis keresésével *Gaál I.*, *Pethő A.* és *M. Pohst* [17], [18], [19], [20], [21], [22] egy cikksorozatban foglalkoztak részletesen. Ezek közül [19] és [22] egy olyan hatékony algoritmust ismertet, amely tetszőleges negyedfokú számtest esetén alkalmazható. Ez az eljárás az index forma egyenlet megoldását harmadfokú és negyedfokú Thue-egyenletek megoldására vezeti vissza. Most röviden ezt a módszert foglaljuk össze.

Legyen K egy tetszőleges negyedfokú algebrai számtest. Tegyük fel, hogy $\xi \in \mathbb{Z}_K$ primitív eleme K -nak, azaz $K = \mathbb{Q}(\xi)$. Legyen ξ definiáló polinomja $f(t) = t^4 + a_1t^3 + a_2t^2 + a_3t + a_4 \in \mathbb{Z}[t]$ és jelöljük ξ indexét $m = I(\xi)$ -vel.

Ha K egy egész bázisa $(\omega_1 = 1, \omega_2, \omega_3, \omega_4)$, akkor egy $d \in \mathbb{Z}$ közös nevező kiemelésével

$$\omega_i = \frac{1}{d} \sum_{j=1}^4 \lambda_{ij} \xi^{j-1} \quad (i = 1, \dots, 4)$$

írható, ahol $\lambda_{ij} \in \mathbb{Z}$ ($1 \leq i, j \leq 4$). A továbbiakban az $I(x_2, x_3, x_4) = \pm A$ index forma egyenlet megoldása helyett a vele ekvivalens problémával, A indexű $\alpha = x_1\omega_1 + x_2\omega_2 + x_3\omega_3 + x_4\omega_4 \in \mathbb{Z}_K$ ($x_1, x_2, x_3, x_4 \in \mathbb{Z}$) primitív elemek keresésével foglalkozunk. Ebből a szempontból feltehetjük, hogy $x_1 = 0$, ezért α felírható

$$\alpha = \frac{a + x\xi + y\xi^2 + z\xi^3}{d} \quad (1)$$

alakban, ahol $a, x, y, z \in \mathbb{Z}$ a következőképpen van meghatározva:

$$\begin{pmatrix} a \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \lambda_{11} & \lambda_{21} & \lambda_{31} & \lambda_{41} \\ \lambda_{12} & \lambda_{22} & \lambda_{32} & \lambda_{42} \\ \lambda_{13} & \lambda_{23} & \lambda_{33} & \lambda_{43} \\ \lambda_{14} & \lambda_{24} & \lambda_{34} & \lambda_{44} \end{pmatrix} \begin{pmatrix} 0 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \quad (2)$$

A továbbiakban azon $\alpha \in \mathbb{Z}_K$ értékekhez tartozó x, y, z együtthatókat fogjuk meghatározni, melyekre $I(\alpha) = A$. Ezekből (2) alapján kaphatjuk meg az eredeti index forma egyenlet megoldásait.

A módszer kulcsfontosságú eleme a következő eredmény.

2.1.1. TÉTEL (Gaál I., Pethő A., M. Pohst [19], Theorem 2.1.)

Az (1) alakban megadott $\alpha \in \mathbb{Z}_K$ elem indexe pontosan akkor A , ha az

$$F(u, v) = u^3 - a_2 u^2 v + (a_1 a_3 - 4a_4) u v^2 + (4a_2 a_4 - a_3^2 - a_1^2 a_4) v^3 = \pm \frac{d^6 A}{m} \quad (3)$$

egyenletnek van olyan $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ megoldása, hogy az (1)-beli x, y, z együtthatók teljesítik a következő egyenlőségeket:

$$\begin{aligned} Q_1(x, y, z) &= x^2 - a_1 xy + a_2 y^2 + (a_1^2 - 2a_2) xz + (a_3 - a_1 a_2) yz \\ &\quad + (-a_1 a_3 + a_2^2 + a_4) z^2 = u \quad , \\ Q_2(x, y, z) &= y^2 - xz - a_1 yz + a_2 z^2 = v \quad . \end{aligned} \quad (4)$$

L.-C. Kappe és *B. Warren* [34] eredménye (Theorem 1.) szerint ha $f(t)$ Galois-csoportja Klein-csoport, negyedrendű ciklikus csoport vagy nyolcadrendű diéder csoport, akkor $F(u, v)$ reducibilis $\mathbb{Q}$ felett, így a szorzattá alakításkor adódó elsőfokú tényező alapján (3) egyszerűen megoldható. Ha pedig $f(t)$ Galois-csoportja negyedfokú alternáló csoport vagy negyedfokú szimmetrikus csoport, akkor $F(u, v)$ irreducibilis $\mathbb{Q}$ felett, ezért (3) egy harmadfokú Thue-egyenlet.

A (3) egyenlet megoldása után annak összes (u, v) megoldására tekintenünk kell a (4) egyenletrendszerrel. (Ha (3) nem megoldható vagy (3) összes megoldása esetén (4)-nek nincs megoldása, akkor az index forma egyenletnek sincs megoldása, azaz K -ban nincs A indexű algebrai egész.)

A (4) egyenletrendszer megoldásainak meghatározásához legyen (u, v) egy rögzített megoldása (3)-nak. Jelöljük (x_Q, y_Q, z_Q) -val

$$Q_0(X, Y, Z) = uQ_2(X, Y, Z) - vQ_1(X, Y, Z) = 0$$

egy nem triviális megoldását. (A (4) megoldásai teljesítik ezt az egyenletet, ezért ha nincs nem triviális megoldás, akkor (4)-nek nincs megoldása. A nem triviális megoldás meghatározásához lsd. [40] Chapter 7., Theorem 3. és Theorem 5.)

Ha például $z_Q \neq 0$ (a többi eset hasonlóan kezelhető), akkor (4) tetszőleges (x, y, z) megoldásához léteznek olyan $p, q, r \in \mathbb{Q}$ racionális

paraméterek, hogy

$$x = rx_Q + p, \quad y = ry_Q + q, \quad z = rz_Q. \quad (5)$$

Mivel (4) összes (x, y, z) megoldása teljesíti a $Q_0(x, y, z) = 0$ egyenlőséget, ezért $Q_0(x_Q, y_Q, z_Q) = 0$ alapján könnyen kiszámítható $c_1, c_2, c_3, c_4, c_5 \in \mathbb{Z}$ értékekkel $r(c_1p + c_2q) = c_3p^2 + c_4pq + c_5q^2$ adódik. Az (5)-beli egyenleteket szorozzuk meg $(c_1p + c_2q)$ -val és használjuk az előző egyenlőséget, hogy (5)-ből kiküszöböljük r -et. Továbbá szorozzuk meg ezeket az egyenleteket p, q közös nevezőjének négyzetével, majd az így kapott p', q' egész paraméterek $\text{lko}(p', q')$ legnagyobb közös osztójának négyzetével osszuk el az egyenleteket. Ekkor a paramétereket ismét p -vel és q -val jelölve

$$\begin{aligned} k \cdot x &= f_x(p, q) = c_{11}p^2 + c_{12}pq + c_{13}q^2, \\ k \cdot y &= f_y(p, q) = c_{21}p^2 + c_{22}pq + c_{23}q^2, \\ k \cdot z &= f_z(p, q) = c_{31}p^2 + c_{32}pq + c_{33}q^2 \end{aligned} \quad (6)$$

adódik, ahol $k, c_{ij} \in \mathbb{Z}$, $k > 0$, a $p, q \in \mathbb{Z}$ paraméterek pedig relatív prímek. [22] szerint k osztja $\det(c_{ij})/\text{lko}\{c_{ij} \mid 1 \leq i, j \leq 3\}^3$ -t. Ez utóbbi kifejezés általában egy kis egész számot ad, ezért k -ra csak néhány lehetséges értéket enged meg.

Mindegyik k esetén a (6)-beli előállítást (4)-be helyettesítve

$$F_1(p, q) = Q_1(f_x(p, q), f_y(p, q), f_z(p, q)) = k^2u, \quad (7)$$

$$F_2(p, q) = Q_2(f_x(p, q), f_y(p, q), f_z(p, q)) = k^2v. \quad (8)$$

[22] (Theorem 2. és Theorem 3.) szerint (7) és (8) közül legalább az egyik negyedfokú Thue-egyenlet. Ezt megoldva kapjuk p, q -t, melyből (6) alapján adódnak a megfelelő x, y, z értékek.

Ha $F(u, v)$ irreducibilis, akkor a (3) Thue-egyenletet, illetve a (7), (8)-ból adódó Thue-egyenletet *Y. Bilu* és *G. Hanrot* [5] módszerével lehet gyorsan megoldani, amit beépítettek például a KASH-ba [6] is.

2.2. Diéder negyedfokú számtestek

Legyen $K = \mathbb{Q}(\xi)$ negyedfokú algebrai számtest és ξ definiáló polinomja $f(t) \in \mathbb{Z}[t]$. A továbbiakban olyan K negyedfokú algebrai számtesteket

vizsgálunk, melyeknél $f(t)$ Galois-csoportja nyolcadrendű diéder csoport. Ilyenkor az egyszerűség kedvéért azt mondjuk, hogy K **diéder negyedfokú számtest**.

Ha K egy diéder negyedfokú számtest, akkor K -nak egyetlen M másodfokú részteste van. Ismert továbbá az is, hogy ha M képzetes másodfokú részteste a K diéder negyedfokú számtestnek, akkor K csak teljesen komplex lehet. Ezért amennyiben K vegyes szignatúrájú, akkor M valós másodfokú számtest.

A. C. Kable [33] diéder negyedfokú számtestekben vizsgálta a hatvány egész bázis létezésének problémáját. Tételében szükséges és elégséges feltételt adott hatvány egész bázis létezésére ilyen negyedfokú testekben. Számunkra tételének alábbi két következménye lesz fontos.

2.2.1. LEMMA (A. C. Kable [33], Corollary 1.)

Legyen K diéder negyedfokú számtest, melynek másodfokú részteste M . Ha K -ban van hatvány egész bázis, akkor az előjel megfelelő választásával $D_K \pm 4D_M^3$ négyzetszám.

Ha K vegyes szignatúrájú diéder negyedfokú számtest, akkor $D_K < 0$ és M valós másodfokú test, így $D_M > 0$. Ezért a 2.2.1. lemmából adódik a következő állítás.

2.2.2. LEMMA (A. C. Kable [33], Corollary 2.)

Legyen K vegyes szignatúrájú diéder negyedfokú számtest, melynek másodfokú részteste M . Ha K -ban van hatvány egész bázis, akkor $|D_K| \leq 4D_M^3$. Következésképpen csak véges sok olyan monogén, vegyes szignatúrájú diéder negyedfokú számtest létezik, mely egy adott valós másodfokú számtestet résztestként tartalmaz.

A 2.2.2. lemma utolsó állítása azért is érdekes, mert ha a feltételek közül elhagyjuk a vegyes szignatúrát, akkor J. G. Huard, B. K. Spearman és K. S. Williams [32] (Theorem 2.) eredménye szerint az már nem teljesül.

Megjegyezzük még, hogy diéder negyedfokú számtestekben Gaál I., Pethő A. és M. Pohst [20] foglalkoztak index forma egyenletek megoldásával. Az általuk megadott módszer az index forma egyenlet megoldását visszavezeti bizonyos másodfokú polinomértékek keresésére másodrendű lineáris rekurzív sorozatokban. Ez az eljárás azonban nem működik minden diéder negyedfokú számtest esetén, jelentős részükre azonban igen.

Célunk a továbbiakban az lesz, hogy rögzített M valós másodfokú számtest esetén meghatározzuk az összes K vegyes szignatúrájú diéder negyedfokú számtestet, melynek másodfokú részteste M és melyben van hatvány egész bázis.

2.3. Az algoritmus

Adott M valós másodfokú számtest esetén a 2.2.2. lemma szerint csak véges sok olyan monogén, vegyes szignatúrájú diéder negyedfokú számtest létezik, melynek másodfokú részteste M . Ebben a részben ezek meghatározására adunk gyors algoritmust.

A 2.2.2. lemma értelmében a K vegyes szignatúrájú diéder negyedfokú számtestek közül elég csak azokat vizsgálni, melyekre $|D_K| \leq 4D_M^3$ teljesül. Amennyiben M részteste K -nak, akkor $D_M^{[K:M]} \mid D_K$, ezért esetünkben $D_M^2 \mid D_K$ ellenőrzése tovább szűkíti a szóba jöhető testek körét. Ezek után Gaál I., Pethő A. és M. Pohst-nak a 2.1. részben ismertetett eljárásával választjuk ki az így megmaradó testek közül azokat, amelyekben valóban van hatvány egész bázis. Egyúttal meghatározzuk azokat az elemeket, melyek hatvány egész bázist generálnak.

Ezek után megadható a problémára vonatkozó gyors algoritmus (Gaál I., Nyul G. [14]):

input: Egy M valós másodfokú számtest.

output: Az összes olyan monogén, vegyes szignatúrájú diéder negyedfokú K számtest, amely résztestként tartalmazza M -et. Ezen kívül ezekben a K testekben meghatározzuk az összes hatvány egész bázist generáló elemet.

1. Meghatározzuk az összes olyan vegyes szignatúrájú negyedfokú K számtestet, melynek diszkriminánsa az előbb írtaknak megfelelően teljesíti a következőket:

$$D_M^2 \mid D_K, \quad D_M^2 \leq |D_K| \leq 4D_M^3 \quad (9)$$

(A KASH [6] segítségével készíthető bizonyos számtesteket, esetünkben a vegyes szignatúrájú negyedfokú számtesteket felsoroló táblázat. Algoritmusunk ezen lépése ezt a táblázatot felhasználva hajtható

vége. Megjegyezzük, hogy a (9) feltétel kevés lehetséges K -t szolgáltat.)

2. Kiszámítjuk a K -t meghatározó elem definiáló polinomjának Galois-csoportját és K résztesteit. Azokat a K -kat hagyjuk meg, melyek esetén a Galois-csoport nyolcadrendű diéder csoport és melyek M -et tartalmazzák résztestként.

(A Galois-csoport és a résztestek meghatározása is végrehajtható például a KASH [6] segítségével.)

3. Megvizsgáljuk, hogy K monogén-e és elhagyjuk azokat a K -kat, melyekben nincs hatvány egész bázis. Ezzel együtt kiszámítjuk a K -beli hatvány egész bázisok összes lehetséges generátorát.

(Ebben a lépésben Gaál I., Pethő A. és M. Pohst [19], [22] módszerét alkalmazzuk. A 2.1. részben megjegyeztük, hogy diéder negyedfokú testek esetén a (3) egyenlet egyszerűen megoldható, mert bal oldala egy elsőfokú és egy másodfokú forma szorzatára bomlik. A (7), (8) egyenletek megoldásához szintén a KASH [6] használható.)

2.4. Numerikus példák

Az algoritmust példaként azokban az esetekben alkalmazzuk, amikor a valós másodfokú számtest $M = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$.

A következő táblázat a számítások eredményét tartalmazza. Mindegyik M esetén felsoroljuk azon K vegyes szignatúrájú diéder negyedfokú számtestek diszkriminánsát, amelyeknek részteste M és teljesítik (9)-et, azaz azokat a K testeket, melyek a 2.3. részben leírt algoritmus 1. és 2. pontja után megmaradtak. Mindegyik testnél megadjuk egy K -t meghatározó ξ elem $f(t)$ definiáló polinomját és az (1)-ben szereplő d közös nevezőt.

Ezután feltüntetjük az algoritmus 3. pontjának alkalmazásakor megoldásként adódó azon (x, y, z) koordinátákat, melyekre az ezekkel (1) szerint felírt α elem hatvány egész bázist generál K -ban. (Jegyezzük meg, hogy ha (x, y, z) megoldást szolgáltat, akkor $(-x, -y, -z)$ is, ezért közülük csak az egyiket soroljuk fel.)

Néhány testnél „nincs megoldás” szerepel. Ezek azok a testek, melyeket az algoritmus 3. pontjánál hagyunk el, azaz ezek a K vegyes szignatúrájú

diéder negyedfokú számtestek teljesítik (9)-et és másodfokú résztestük M , de a test mégsem tartalmaz hatvány egész bázist. Ilyen testek létezése azt is igazolja, hogy a 2.2.2. lemma első állítása nem megfordítható.

A példák kiszámításához a Maple programcsomagot, illetve a 2.3. részben írtaknak megfelelően a KASH [6] programcsomagot használtuk. Az algoritmus időigénye példánként mindössze néhány perc volt.

$$\begin{aligned}
M &= \mathbb{Q}(\sqrt{2}) \\
D_K &= -448, f(t) = t^4 - 2t^3 + t^2 + 2t - 1, d = 1 \\
&\quad (x, y, z) = (0, 1, -1), (1, -6, 4), (4, -3, 1), (1, 0, 0), (1, -2, 1) \\
D_K &= -1024, f(t) = t^4 - 2t^2 - 1, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (2, 0, -1) \\
D_K &= -1472, f(t) = t^4 - 2t^3 - 3t^2 - 2t - 1, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (0, 3, -1), (3, 2, -1) \\
D_K &= -1792, f(t) = t^4 - 2t^2 - 4t - 2, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (1, 1, -1) \\
D_K &= -1984, f(t) = t^4 - 2t^3 + t^2 - 2, d = 1 \\
&\quad (x, y, z) = (1, 0, 0) \\
D_K &= -2048, f(t) = t^4 - 2, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (1, 1, 1), (1, -1, 1)
\end{aligned}$$

$$\begin{aligned}
M &= \mathbb{Q}(\sqrt{3}) \\
D_K &= -1728, f(t) = t^4 - 2t^3 - 2t + 1, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (0, 2, -1) \\
D_K &= -3312, f(t) = t^4 - 2t^3 - t^2 + 2t - 2, d = 1 \\
&\quad (x, y, z) = (1, 0, 0) \\
D_K &= -3312, f(t) = t^4 + t^2 - 6t + 1, d = 3 \\
&\quad \text{nincs megoldás} \\
D_K &= -4608, f(t) = t^4 + 2t^2 - 2, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (3, 1, 1), (3, -1, 1) \\
D_K &= -4608, f(t) = t^4 - 2t^2 - 2, d = 1 \\
&\quad (x, y, z) = (1, 0, 0) \\
D_K &= -5616, f(t) = t^4 - 3t^2 - 6t - 3, d = 1 \\
&\quad (x, y, z) = (2, 1, -1), (1, 0, 0) \\
D_K &= -5616, f(t) = t^4 - 2t^3 + 3t^2 - 2t - 2, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (17, -10, 4), (9, -2, 4) \\
D_K &= -6336, f(t) = t^4 - 2t^3 - 4t^2 - 4t - 2, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (1, 3, -1) \\
D_K &= -6336, f(t) = t^4 - 2t^3 - 8t^2 - 6t - 3, d = 3 \\
&\quad \text{nincs megoldás}
\end{aligned}$$

$$\begin{aligned}
D_K &= -6768, f(t) = t^4 - 2t^3 + t^2 - 3, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (1, 0, 1), (4, -3, 1) \\
D_K &= -6768, f(t) = t^4 - t^2 - 6t - 2, d = 2 \\
&\quad (x, y, z) = (2, 1, -2), (2, -1, 0), (2, 1, 0), (1, 1, -1) \\
D_K &= -6912, f(t) = t^4 - 3, d = 1 \\
&\quad (x, y, z) = (1, 0, 0)
\end{aligned}$$

$$\begin{aligned}
M &= \mathbb{Q}(\sqrt{5}) \\
D_K &= -275, f(t) = t^4 - t^3 + 2t - 1, d = 1 \\
&\quad (x, y, z) = (0, 0, 1), (1, 0, 0), (2, -2, 1), (1, 2, -4), (0, 1, -1) \\
D_K &= -400, f(t) = t^4 - t^2 - 1, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (0, 1, 1), (1, 0, -1), (0, 1, -1) \\
D_K &= -475, f(t) = t^4 - t^3 - 2t^2 - 2t - 1, d = 1 \\
&\quad (x, y, z) = (1, 0, 0), (0, 2, -1), (2, 1, -1)
\end{aligned}$$

3. Bikvadratikus számtestek monogenitása

3.1. Bikvadratikus számtestek

Egy testet **bikvadartikus számtest**nek nevezzük, ha $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ alakú negyedfokú algebrai számtest, ahol $m, n \in \mathbb{Z} \setminus \{0, 1\}$ különböző négyzetmentes racionális egész számok.

A továbbiak során a $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ bikvadratikus számtest esetén használni fogjuk a következő jelöléseket. Legyen $l = \text{lko}(m, n) > 0$ és m_1, n_1 az $m = lm_1$ és $n = ln_1$ egyenlőségekkel definiálva.

Az m és n négyzetmentessége miatt a 4-gyel való oszthatóságuk szempontjából a következő kilenc esetet különböztethetjük meg, melyek mindegyikénél feltüntetjük, hogy abban az esetben mennyi lehet m, n és m_1n_1 4-gyel vett osztási maradéka:

m	n	m_1n_1
1	1	1
1	2	2
1	3	3
2	1	2
2	2	1 vagy 3
2	3	2
3	1	3
3	2	2
3	3	1

Miután K másodfokú résztestei $\mathbb{Q}(\sqrt{m}), \mathbb{Q}(\sqrt{n}), \mathbb{Q}(\sqrt{m_1n_1})$, így

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m}, \sqrt{m_1n_1}) = \mathbb{Q}(\sqrt{n}, \sqrt{m_1n_1}) \quad (10)$$

Ezek alapján *K. S. Williams* [53] megállapította, hogy minden bikvadratikus számtest esetén meg lehet m, n, m_1, n_1 -et úgy választani, hogy azok a 4-gyel való oszthatóság szempontjából az alábbi öt eset valamelyikébe tartozzanak, így a továbbiakban elég csak ezeket vizsgálni:

1. eset: $m \equiv 1 \pmod{4}, n \equiv 1 \pmod{4}, m_1 \equiv 1 \pmod{4}, n_1 \equiv 1 \pmod{4}$
2. eset: $m \equiv 1 \pmod{4}, n \equiv 1 \pmod{4}, m_1 \equiv 3 \pmod{4}, n_1 \equiv 3 \pmod{4}$
3. eset: $m \equiv 1 \pmod{4}, n \equiv 2 \pmod{4}$

4. eset: $m \equiv 2 \pmod{4}$, $n \equiv 3 \pmod{4}$
 5. eset: $m \equiv 3 \pmod{4}$, $n \equiv 3 \pmod{4}$

K. S. Williams [53] mindegyik esetben parametrikus formában meghatározott egy egész bázist (Theorem 2.), illetve megadta a test diszkriminánsát (Theorem 3.). Ezeket az esetek fenti számozásával ismertetjük.

A $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ bikvadratikus számtest egy egész bázisa a következő:

1. eset: $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right)$
 2. eset: $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right)$
 3. eset: $\left(1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{m_1n_1}}{2}\right)$
 4. eset: $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m_1n_1}}{2}\right)$
 5. eset: $\left(1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m_1n_1}}{2}\right)$

A $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ bikvadratikus számtest diszkriminánsa pedig:

1. és 2. eset: $D_K = l^2 m_1^2 n_1^2$
 3. és 5. eset: $D_K = 16l^2 m_1^2 n_1^2$
 4. eset: $D_K = 64l^2 m_1^2 n_1^2$

Ezeket az eredményeket felhasználva *Gaál I.*, *Pethő A.* és *M. Pohst* [16] esetenként kiszámították a fenti egész bázishoz tartozó index formákat:

1. eset:

$$\left(l(x_2 + \frac{x_4}{2})^2 - \frac{n_1}{4}x_4^2\right) \left(l(x_3 + \frac{x_4}{2})^2 - \frac{m_1}{4}x_4^2\right) \left(n_1(x_3 + \frac{x_4}{2})^2 - m_1(x_2 + \frac{x_4}{2})^2\right)$$

2. eset:

$$\left(l(x_2 - \frac{x_4}{2})^2 - \frac{n_1}{4}x_4^2\right) \left(l(x_3 + \frac{x_4}{2})^2 - \frac{m_1}{4}x_4^2\right) \left(n_1(x_3 + \frac{x_4}{2})^2 - m_1(x_2 - \frac{x_4}{2})^2\right)$$

3. eset:

$$(lx_2^2 - n_1x_4^2) \left(l(x_3 + \frac{x_4}{2})^2 - \frac{m_1}{4}x_4^2\right) (n_1(2x_3 + x_4)^2 - m_1x_2^2)$$

4. eset:

$$\left(\frac{l}{2}(2x_2 + x_4)^2 - \frac{n_1}{2}x_4^2\right) \left(2lx_3^2 - \frac{m_1}{2}x_4^2\right) \left(2n_1x_3^2 - \frac{m_1}{2}(2x_2 + x_4)^2\right)$$

5. eset:

$$(l(2x_2 + x_3)^2 - n_1x_4^2)(lx_3^2 - m_1x_4^2)\left(\frac{n_1}{4}x_3^2 - m_1\left(x_2 + \frac{x_3}{2}\right)^2\right)$$

T. Nakahara [43] bebizonyította, hogy végtelen sok bikvadratikus számtestben van hatvány egész bázis. Megmutatta azt is, hogy egy bikvadratikus számtest testindexe 1, 2, 3, 4, 6 vagy 12 lehet. Igazolta továbbá azt, hogy tetszőleges $N \in \mathbb{N}$ esetén végtelen sok olyan bikvadratikus számtest létezik, melynek testindexe 1, minimális indexe pedig nagyobb N -nél, következésképpen végtelen sok bikvadratikus számtestben nincs hatvány egész bázis.

Gaál I., Pethő A. és M. Pohst [16] új, elemi bizonyítást adtak arra, hogy a bikvadratikus számtestek testindexe mivel lehet egyenlő, sőt leírták, hogy m_1 , n_1 és l -től függően melyik értéket mikor veszi fel.

Bikvadratikus számtestek monogenitásával többen is foglalkoztak. $m = -1$ és $n > 0$ esetén *T. Funakura* [8] (Corollary 5.) bizonyította, hogy K pontosan akkor monogén, ha $n = 2, 3, 5$. *M.-N. Gras* és *F. Tanoé* [25] szükséges és elégséges feltételeket adtak bikvadratikus számtestekben hatvány egész bázis létezésére. *Y. Motoda* [41] bizonyos teljesen valós esetekben vizsgálta a monogenitás problémáját és adta meg a hatvány egész bázis generátorokat.

Szintén *Gaál I., Pethő A. és M. Pohst* [21] adott hatékony algoritmust a teljesen valós bikvadratikus számtestek esetén az $I(x_2, x_3, x_4) = \pm A$ index forma egyenlet megoldására, ahol $I(x_2, x_3, x_4)$ a megfelelő esethez tartozó, előbb felírt index forma, $A \in \mathbb{N}$ pedig rögzített szám. Módszerükben az index forma egyenlet megoldását szimultán Pell-egyenletek megoldására vezették vissza. Az eljárás illusztrálására az összes 10^6 -nál kisebb diszkriminánsú, teljesen valós bikvadratikus számtest esetén kiszámították a minimális indexet és meghatározták az összes ilyen indexű elemet.

A továbbiakban az lesz a célunk, hogy a teljesen komplex bikvadratikus számtestek vizsgálatával teljessé tegyük a monogenitás témakörét bikvadratikus számtestek esetén. Szükséges és elégséges feltételt fogunk adni a teljesen komplex bikvadratikus számtestek monogenitására, megadjuk a hatvány egész bázis generátorok keresésekor fellépő index forma egyenlet összes megoldását, végül egy, a fent említetthez hasonló táblázatot készítünk a teljesen komplex esetben is.

3.2. Teljesen komplex bikvadratikus testek monogenitása

Ebben a részben a teljesen komplex bikvadratikus számtestekben vizsgáljuk a monogenitás problémáját. A továbbiakban használjuk az előző részben bevezetett jelöléseket.

A $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ bikvadratikus számtest pontosan akkor teljesen komplex, ha m és n közül legalább az egyik negatív szám. Ilyenkor a 3.1. részben leírt eseteknél m és n előjelére is ügyelve az adódik, hogy m és n választható úgy, hogy a következő esetek valamelyike álljon fenn:

1. eset: $m > 0, n < 0, m \equiv 1 \pmod{4}, n \equiv 1 \pmod{4}, m_1 \equiv 1 \pmod{4}, n_1 \equiv 1 \pmod{4}$
2. eset: $m > 0, n < 0, m \equiv 1 \pmod{4}, n \equiv 1 \pmod{4}, m_1 \equiv 3 \pmod{4}, n_1 \equiv 3 \pmod{4}$
- 3/A. eset: $m > 0, n < 0, m \equiv 1 \pmod{4}, n \equiv 2 \pmod{4}$
- 3/B. eset: $m < 0, n > 0, m \equiv 1 \pmod{4}, n \equiv 2 \pmod{4}$
- 4/A. eset: $m > 0, n < 0, m \equiv 2 \pmod{4}, n \equiv 3 \pmod{4}$
- 4/B. eset: $m < 0, n > 0, m \equiv 2 \pmod{4}, n \equiv 3 \pmod{4}$
- 5/A. eset: $m > 0, n < 0, m \equiv 3 \pmod{4}, n \equiv 3 \pmod{4}$
- 5/B. eset: $m < 0, n < 0, m \equiv 3 \pmod{4}, n \equiv 3 \pmod{4}$

Ennek igazolására példaként tekintsük a 3.1. részben leírt 4. esetet. Ezen belül meg kell vizsgálni az összes lehetséges, lényegesen különböző előjelezést és felhasználjuk (10)-et:

- a.) $m \equiv 2 \pmod{4}, m > 0$ és $n \equiv 3 \pmod{4}, n < 0$. Ez a 4/A. eset.
- b.) $m \equiv 2 \pmod{4}, m < 0$ és $n \equiv 3 \pmod{4}, n > 0$. Ez a 4/B. eset.
- c.) $m \equiv 2 \pmod{4}, m < 0$ és $n \equiv 3 \pmod{4}, n < 0$. Ilyen feltételek mellett $m_1 n_1 \equiv 2 \pmod{4}, m_1 n_1 > 0$. Ez $m_1 n_1$ és n -nel a 4/A. esetben tartozik.

Ezekre az esetekre vonatkozóan természetesen a 3.1. részben felírt egész bázis, diszkrimináns és index forma változatlanul adódik.

A következő tételben olyan jellemzését adjuk a hatvány egész bázissal rendelkező teljesen komplex bikvadratikus számtesteknek, mely alapján könnyen ellenőrizhető, hogy egy adott teljesen komplex bikvadratikus számtest monogén-e. Továbbá amikor létezik a testben hatvány egész bázis, akkor meghatározzuk az összes hatvány egész bázist generáló elemet. A tétel érdekessége az is, hogy a korábban megadott egész bázishoz tartozó

index formával felírt, ± 1 jobb oldalú index forma egyenlet megoldása minden esetben a paramétereiktől nem függő, konstans vektorok egy véges halmazába tartozik.

3.2.1. TÉTEL (Nyul G. [45])

Legyen $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ a felsorolt esetek valamelyikébe tartozó teljesen komplex bikvadratikusszámtest.

Az 1., 2. és 3/A. esetben K nem monogén.

A további esetekben K -ban a hatvány egész bázis létezésének szükséges és elégséges feltétele:

3/B. eset: $m_1 = -1$, $l - 4n_1 = -1$ (és a feltétel miatt $n_1 > 0$).

4/A. eset: $m_1 = 2$, $n_1 = -1$, $l = 1$, azaz $m = 2$ és $n = -1$.

4/B. eset: $m_1 = -2$, $l - n_1 = \pm 2$ (és a feltétel miatt $n_1 > 0$).

5/A. eset: $n_1 = -1$, $4l - m_1 = 1$ (és a feltétel miatt $m_1 > 0$).

5/B. eset: $l = 1$, $n_1 - m_1 = \pm 4$ (és a feltétel miatt $m_1, n_1 < 0$).

Ha K monogén, akkor a megfelelő index formával vett $I(x_2, x_3, x_4) = \pm 1$ index forma egyenlet megoldásai:

3/B. eset:

$$(x_2, x_3, x_4) = \pm(1, 1, -2), \pm(1, -1, 2)$$

4/A. eset:

$$(x_2, x_3, x_4) = \pm(0, 0, 1), \pm(1, 0, -1)$$

4/B. eset:

$$(x_2, x_3, x_4) = \pm(0, 0, 1), \pm(1, 0, -1)$$

5/A. eset:

$m_1 = 3$, $n_1 = -1$, $l = 1$, azaz $m = 3$, $n = -1$ esetén

$$(x_2, x_3, x_4) = \pm(1, -2, 1), \pm(1, -2, -1), \pm(0, 1, 0), \pm(1, -1, 0)$$

A többi 5/A. esetbeli testre

$$(x_2, x_3, x_4) = \pm(1, -2, 1), \pm(1, -2, -1)$$

5/B. eset:

$$(x_2, x_3, x_4) = \pm(0, 1, 0), \pm(1, -1, 0)$$

MEGJEGYZÉS A tételben a 4/B. esetnél levő feltételre igaz, hogy minden olyan test, amelynél $l - n_1 = 2$ szerepel, megegyezik valamelyik olyan testtel, amelynél az egyenlőségben $l - n_1 = -2$ teljesül, és ez fordítva is igaz. Tekintsünk ugyanis a 4/B. esetben egy olyan testet, melynek a tétel értelmében létezik hatvány egész bázisa. Ekkor ha $m_1 = -2$, $l - n_1 = 2$, akkor legyen $n_1 = x$ (ez a 4/B. esetből kifolyólag pozitív páratlan egész) és így $l = x + 2$. Eszerint $m = lm_1 = -2(x + 2)$, $n = ln_1 = x(x + 2)$ és

$m_1 n_1 = -2x$. Ezzel szemben $m'_1 = -2$, $n'_1 = x + 2$, $l' = x$ választással $m' = l' m'_1 = -2x$, $n' = l' n'_1 = x(x + 2)$ és $l' - n'_1 = -2$, így (10) miatt $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m_1 n_1}, \sqrt{n}) = \mathbb{Q}(\sqrt{m'}, \sqrt{n'})$, továbbá ezek az új paraméterek is a 4/B. esetben tartoznak. Hasonlóan végezhető el ez a gondolatmenet fordítva is.

Az 5/B. esetben pedig az m -re és n -re vonatkozó feltételek szimmetriája miatt minden olyan test, amelyre $n_1 - m_1 = 4$ teljesül, megegyezik valamelyik olyannal, amelyre $n_1 - m_1 = -4$ áll fenn, és ez fordítva is igaz.

3.3. A tétel bizonyítása

A bizonyítás során a 3.1. részben felírt index formák közül mindig a megfelelővel oldjuk meg az $I(x_2, x_3, x_4) = \pm 1$ index forma egyenletet. Az index forma minden esetben három egész együtthatós kvadratikus forma szorzatára bomlik, így az index forma egyenlet csak úgy oldható meg, ha minden tényező értéke ± 1 . A teljesen komplex esetben pedig még az is teljesül, hogy a tényezőként adódó kvadratikus formák között mindig vannak definiték, a vizsgálatot érdemes ezek valamelyikével kezdeni.

1. eset: Ekkor $m_1 > 0$, $n_1 < 0$, $m_1 \equiv 1 \pmod{4}$, $n_1 \equiv 1 \pmod{4}$ és legyen $\tilde{n}_1 = |n_1| > 0$, amire $\tilde{n}_1 \equiv 3 \pmod{4}$.

Ekkor a megfelelő index forma első tényezője nem negatív, tehát a fent írtak értelmében 1-gyel egyenlő, amiből $l(2x_2 + x_4)^2 + \tilde{n}_1 x_4^2 = 4$ adódik. Itt mindkét tag nemnegatív egész értékű, továbbá $\tilde{n}_1 \equiv 3 \pmod{4}$ miatt $\tilde{n}_1 x_4^2 \equiv 0$ vagy $3 \pmod{4}$, így három lehetőség jöhet szóba:

a.) $l(2x_2 + x_4)^2 = 0$, $\tilde{n}_1 x_4^2 = 4$. Az utóbbi egyenlőség esetünkben $\tilde{n}_1 \equiv 3 \pmod{4}$ mellett nem teljesülhet.

b.) $l(2x_2 + x_4)^2 = 1$, $\tilde{n}_1 x_4^2 = 3$. Ez csak úgy lehetséges, ha $l = 1$, $2x_2 + x_4 = \pm 1$, $\tilde{n}_1 = 3$ (azaz $n_1 = -3$) és $x_4 = \pm 1$. Az index forma harmadik tényezője nem pozitív, így értéke -1 :

Ha $x_4 = 1$, akkor $x_2 = 0$ vagy -1 , így a harmadik tényező $-3 \left(x_3 + \frac{1}{2}\right)^2 - \frac{m_1}{4} = -1$, azaz $3(2x_3 + 1)^2 + m_1 = 4$. Ekkor csak $3(2x_3 + 1)^2 = 3$ és $m_1 = 1$ lehet, ezért $x_3 = 0$ vagy -1 .

Ha $x_4 = -1$, akkor $x_2 = 0$ vagy 1 , a harmadik tényező pedig

$-3\left(x_3 - \frac{1}{2}\right)^2 - \frac{m_1}{4} = -1$, azaz $3(2x_3 - 1)^2 + m_1 = 4$. Innen hasonlóan kapjuk, hogy $m_1 = 1$, $x_3 = 0$ vagy 1 .

A megmaradó esetekkel $((x_3, x_4) = (0, 1), (-1, 1), (0, -1), (1, -1))$ az index forma második tényezőjét véve azt kapjuk, hogy $\frac{l}{4} - \frac{m_1}{4} = \pm 1$, ami $l = m_1 = 1$ miatt lehetetlen.

c.) $l(2x_2 + x_4)^2 = 4$, $\tilde{n}_1 x_4^2 = 0$. Ekkor $x_4 = 0$, $l = 1$ és $x_2 = \pm 1$. Ebben az esetben az index forma második tényezője $x_3^2 = 1$, tehát $x_3 = \pm 1$, így a harmadik tényező $n_1 - m_1 = \pm 1$. Ez azonban ellentmond az 1. esetben fennálló $m_1 \equiv n_1 \pmod{4}$ feltételnek.

2. eset: Ekkor $m_1 > 0$, $n_1 < 0$, $m_1 \equiv 3 \pmod{4}$, $n_1 \equiv 3 \pmod{4}$ és legyen $\tilde{n}_1 = |n_1| > 0$, amire $\tilde{n}_1 \equiv 1 \pmod{4}$.

Az index forma első tényezője ebben az esetben is nem negatív, tehát 1 értékű, így $l(2x_2 - x_4)^2 + \tilde{n}_1 x_4^2 = 4$ teljesül. Az 1. esethez hasonlóan $\tilde{n}_1 x_4^2 \equiv 0$ vagy $1 \pmod{4}$ miatt három esetet különböztetünk meg:

a.) $l(2x_2 - x_4)^2 = 0$, $\tilde{n}_1 x_4^2 = 4$. Eszerint $\tilde{n}_1 = 1$ (azaz $n_1 = -1$), $x_4 = 2$ vagy -2 , amiből rendre $x_2 = 1$ vagy -1 . Ekkor az index forma nem pozitív harmadik tényezője $x_4 = 2$ esetén $-(x_3 + 1)^2 = -1$, így $x_3 = 0$ vagy -2 , illetve $x_4 = -2$ esetén $-(x_3 - 1)^2 = -1$, amiből $x_3 = 0$ vagy 2 .

A fennmaradó esetekben $((x_3, x_4) = (0, 2), (-2, 2), (0, -2), (2, -2))$ a második tényező $l - m_1 = \pm 1$. Ez ellentmond $m = lm_1$ páratlanságának.

b.) $l(2x_2 - x_4)^2 = 3$, $\tilde{n}_1 x_4^2 = 1$. Ekkor $l = 3$, $2x_2 - x_4 = \pm 1$, $\tilde{n}_1 = 1$ (azaz $n_1 = -1$), $x_4 = \pm 1$. Az index forma harmadik tényezője nem pozitív, így -1 értékű:

Ha $x_4 = 1$, akkor $x_2 = 0$ vagy 1 , ezért a harmadik tényező $-\left(x_3 + \frac{1}{2}\right)^2 - \frac{m_1}{4} = -1$, így $(2x_3 + 1)^2 + m_1 = 4$. Ekkor csak $(2x_3 + 1)^2 = 1$ és $m_1 = 3$ lehetséges, ahonnan $x_3 = 0$ vagy -1 .

Ha $x_4 = -1$, akkor $x_2 = 0$ vagy -1 , a harmadik tényező pedig $-\left(x_3 - \frac{1}{2}\right)^2 - \frac{m_1}{4} = -1$, ezért $(2x_3 - 1)^2 + m_1 = 4$. Innen az előzőekhez hasonlóan $m_1 = 3$, $x_3 = 0$ vagy 1 .

Az összes lehetséges esetben $((x_3, x_4) = (0, 1), (-1, 1), (0, -1), (1, -1))$

a második tényező $\frac{l}{4} - \frac{m_1}{4} = \pm 1$, ami viszont $l = m_1 = 3$ miatt nem lehetséges.

c.) $l(2x_2 - x_4)^2 = 4$, $\tilde{n}_1 x_4^2 = 0$. Ekkor $x_4 = 0$, $l = 1$ és $x_2 = \pm 1$. Ezek szerint a második tényező $x_3^2 = 1$, ezért $x_3 = \pm 1$ és a harmadik tényező $n_1 - m_1 = \pm 1$, ami $m_1 \equiv n_1 \pmod{4}$ miatt lehetetlen.

3/A. eset: Ekkor $m_1 > 0$, $n_1 < 0$ és legyen $\tilde{n}_1 = |n_1| > 0$. Az index forma első tényezője nem negatív, így $lx_2^2 + \tilde{n}_1 x_4^2 = 1$.

Ebben az esetben $\tilde{n}_1$ páros, ezért $lx_2^2 = 1$, $\tilde{n}_1 x_4^2 = 0$. Ekkor $l = 1$, $x_2 = \pm 1$, $x_4 = 0$. A második tényező $x_3^2 = 1$, tehát $x_3 = \pm 1$, a harmadik tényező pedig $4n_1 - m_1 = \pm 1$. De $m_1 \geq 1$, $n_1 \leq -1$ miatt $4n_1 - m_1 \leq -5$, ami ellentmondást eredményez.

3/B. eset: Ekkor $n_1 > 0$, $m_1 < 0$ és legyen $\tilde{m}_1 = |m_1| > 0$. Ebben az esetben a harmadik tényező nem negatív, tehát $n_1(2x_3 + x_4)^2 + \tilde{m}_1 x_2^2 = 1$.

Mivel n_1 páros, ezért $n_1(2x_3 + x_4)^2 = 0$, $\tilde{m}_1 x_2^2 = 1$, amiből $2x_3 + x_4 = 0$, $\tilde{m}_1 = 1$ (azaz $m_1 = -1$) és $x_2 = \pm 1$. Ekkor a második tényező $\frac{x_4^2}{4} = 1$, azaz $x_4 = 2$ vagy -2 , amiből rendre $x_3 = -1$ vagy 1 . Ezek alapján az első tényező $l - 4n_1 = \pm 1$. Amennyiben $l - 4n_1 = 1$ lenne, akkor $l \equiv 1 \pmod{4}$ teljesülne, így $m_1 = -1$ miatt $m \equiv 3 \pmod{4}$ volna, ami nem felel meg a 3/B. eset feltételeinek. Tehát $m_1 = -1$, $l - 4n_1 = -1$ és az index forma egyenlet megoldásai $(x_2, x_3, x_4) = \pm(1, 1, -2), \pm(1, -1, 2)$.

4/A. eset: Ekkor $m_1 > 0$, $n_1 < 0$ és legyen $\tilde{n}_1 = |n_1| > 0$. Ekkor a harmadik tényező nem pozitív, így értéke -1 , amiből $4\tilde{n}_1 x_3^2 + m_1(2x_2 + x_4)^2 = 2$.

Ennek első tagja osztható 4-gyel, így $4\tilde{n}_1 x_3^2 = 0$ és $m_1(2x_2 + x_4)^2 = 2$ lehet. Innen $x_3 = 0$, $m_1 = 2$ és $2x_2 + x_4 = \pm 1$. Ekkor az index forma második tényezője $-x_4^2 = -1$, tehát $x_4 = \pm 1$. Ha $x_4 = 1$, akkor $x_2 = 0$ vagy -1 , míg ha $x_4 = -1$, akkor $x_2 = 0$ vagy 1 .

Minden esetet figyelembe véve $((x_2, x_4) = (0, 1), (-1, 1), (0, -1), (1, -1))$ az ebben az esetben nem negatív első tényező $\frac{l}{2} - \frac{n_1}{2} = 1$, azaz $l - n_1 = 2$. Továbbá $l \geq 1$, $n_1 \leq -1$, amiből $l - n_1 \geq 2$. Mint láttuk, ebben egyenlőség áll fenn, tehát $l = 1$, $n_1 = -1$. Ebben az esetben ezek szerint $l = 1$, $m_1 = 2$, $n_1 = -1$ és az index forma egyenlet megoldásai $(x_2, x_3, x_4) = \pm(0, 0, 1), \pm(1, 0, -1)$.

4/B. eset: Ekkor $n_1 > 0$, $m_1 < 0$ és legyen $\tilde{m}_1 = |m_1| > 0$. Ebben az esetben a második tényező nem negatív, tehát 1 értékű, így $4lx_3^2 + \tilde{m}_1x_4^2 = 2$.

Az első tag osztható 4-gyel, így $4lx_3^2 = 0$, $\tilde{m}_1x_4^2 = 2$. Ezekből $x_3 = 0$, $\tilde{m}_1 = 2$ (azaz $m_1 = -2$), $x_4 = \pm 1$. Ekkor a harmadik tényező $(2x_2 + x_4)^2 = 1$, így $2x_2 + x_4 = \pm 1$. Ha $x_4 = 1$, akkor $x_2 = 0$ vagy -1 , ha pedig $x_4 = -1$, akkor $x_2 = 0$ vagy 1 .

Az összes esetet figyelve $((x_2, x_4) = (0, 1), (-1, 1), (0, -1), (1, -1))$ az első tényező $\frac{l}{2} - \frac{n_1}{2} = \pm 1$, azaz $l - n_1 = \pm 2$. Tehát ebben az esetben $m_1 = -2$, $l - n_1 = \pm 2$ és az index forma egyenlet megoldásai $(x_2, x_3, x_4) = \pm(0, 0, 1), \pm(1, 0, -1)$.

5/A. eset: Ekkor $m_1 > 0$, $n_1 < 0$ és legyen $\tilde{n}_1 = |n_1| > 0$. Ekkor az első tényező nem negatív, így $l(2x_2 + x_3)^2 + \tilde{n}_1x_4^2 = 1$. Ebből kiindulva két esetet kell megkülönböztetni:

a.) $l(2x_2 + x_3)^2 = 0$, $\tilde{n}_1x_4^2 = 1$. Ekkor $2x_2 + x_3 = 0$, $\tilde{n}_1 = 1$ (azaz $n_1 = -1$) és $x_4 = \pm 1$. Ezekkel a harmadik tényező $-\frac{x_3^2}{4} = -1$, azaz $x_3 = 2$ vagy -2 , amiből rendre $x_2 = -1$ vagy 1 . A második tényező ekkor $4l - m_1 = \pm 1$. Amennyiben $4l - m_1 = -1$ lenne, akkor $m_1 \equiv 1 \pmod{4}$ állna fenn. Másrészt $n \equiv 3 \pmod{4}$ és $n_1 = -1$ miatt $l \equiv 1 \pmod{4}$, tehát $m \equiv 1 \pmod{4}$ lenne, ami ellentmondás. Így az 5/A. eset a.) részében $n_1 = -1$, $4l - m_1 = 1$ és az index forma egyenlet megoldásai $(x_2, x_3, x_4) = \pm(1, -2, 1), \pm(1, -2, -1)$.

b.) $l(2x_2 + x_3)^2 = 1$, $\tilde{n}_1x_4^2 = 0$. Ekkor $l = 1$, $2x_2 + x_3 = \pm 1$, $x_4 = 0$. Ezek esetén a második tényező $x_3^2 = 1$, azaz $x_3 = \pm 1$. Ha $x_3 = 1$, akkor $x_2 = 0$ vagy -1 , ha $x_3 = -1$, akkor $x_2 = 0$ vagy 1 .

Az esetek mindegyikében $((x_2, x_3) = (0, 1), (-1, 1), (0, -1), (1, -1))$ a nem pozitív harmadik tényező $\frac{n_1}{4} - \frac{m_1}{4} = -1$, azaz $n_1 - m_1 = -4$. Ez $m_1 > 0$, $n_1 < 0$ egészekre csak $(m_1, n_1) = (1, -3), (2, -2), (3, -1)$ esetén teljesülhet, ahonnan $l = 1$ miatt rendre $(m, n) = (1, -3), (2, -2), (3, -1)$, amiből csak az utolsó felel meg az 5/A. eset feltételeinek. Marad tehát $m = 3$, $n = -1$, mely esetén a b.) részben az index forma egyenlet megoldásai $(x_2, x_3, x_4) = \pm(0, 1, 0), \pm(1, -1, 0)$. (Megjegyzendő, hogy az $m = 3$, $n = -1$ eleget tesz az a.) részben szereplő feltételeknek is.)

5/B. eset: Ekkor $m_1 < 0$, $n_1 < 0$ és legyen $\tilde{m}_1 = |m_1| > 0$, $\tilde{n}_1 = |n_1| > 0$.

Az index forma második tényezője ekkor nem negatív, tehát $lx_3^2 + \tilde{m}_1x_4^2 = 1$. Ez alapján két lehetőség van:

a.) $lx_3^2 = 0$, $\tilde{m}_1x_4^2 = 1$. Ekkor $x_3 = 0$, $\tilde{m}_1 = 1$ (azaz $m_1 = -1$) és $x_4 = \pm 1$. Ezek mellett az első tényező $4lx_2^2 + \tilde{n}_1 = 1$. Az első tag 4-gyel osztható, ezért $x_2 = 0$ és $\tilde{n}_1 = 1$, azaz $n_1 = -1$. Ezekkel az értékekkel azonban a harmadik tényező 0 lenne, ami nem lehetséges.

b.) $lx_3^2 = 1$, $\tilde{m}_1x_4^2 = 0$. Ekkor $l = 1$, $x_3 = \pm 1$, $x_4 = 0$. Ezesetben az első tényező $(2x_2 + x_3)^2 = 1$, azaz $2x_2 + x_3 = \pm 1$. Ezért ha $x_3 = 1$, akkor $x_2 = 0$ vagy -1 , ha pedig $x_3 = -1$, akkor $x_2 = 0$ vagy 1 . Minden lehetséges értéknél $((x_2, x_3) = (0, 1), (-1, 1), (0, -1), (1, -1))$ a harmadik tényező $\frac{n_1}{4} - \frac{m_1}{4} = \pm 1$, azaz $n_1 - m_1 = \pm 4$. Ekkor tehát $l = 1$, $n_1 - m_1 = \pm 4$ és az index forma egyenlet megoldásai $(x_2, x_3, x_4) = \pm(0, 1, 0), \pm(1, -1, 0)$.

Az pedig, hogy a kapott számhármassok valóban megoldások, a megfelelő eseteknél a feltételeket is figyelembe véve behelyettesítéssel könnyen ellenőrizhető. $\square$

3.4. Teljesen komplex bikvadratikus számtestek táblázata

A 3.2.1. tétel bizonyításában fontos észrevétel volt, hogy bikvadratikus számtestek esetén az index forma három darab egész együtthatós másodfokú forma szorzata, továbbá hogy a teljesen komplex esetben ezek közt van olyan tényező, amely definit. Ezen a módon teljesen komplex bikvadratikus számtestekben nem csak a ± 1 jobb oldalú, hanem tetszőlegesen rögzített $A \in \mathbb{N}$ esetén a $\pm A$ jobb oldalú index forma egyenlet is megoldható. Ezt használjuk az alábbi számításokban is.

A következő táblázatban (Nyul G. [45]) az összes olyan teljesen komplex bikvadratikus számtestet soroljuk fel a diszkriminánsok növekvő sorrendjében, melynek diszkriminánsa legfeljebb 10^4 . Ugyanilyen táblázatot a teljesen valós esetben Gaál I., Pethő A. és M. Pohst [21] adtak.

A testeknél szereplő m_1 , n_1 , l a fentieknek megfelelően a $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ test megfelelő paraméterei, D_K , i_K , m_K rendre a test diszkriminánsa, testindexe és minimális indexe. Ezen kívül mindegyik testnél megtalálható az $I(x_2, x_3, x_4) = \pm m_K$ egyenletnek az összes megoldása. (Ha (x_2, x_3, x_4) megoldás, akkor $(-x_2, -x_3, -x_4)$ is az, de csak az egyiket tüntetjük fel.)

D_K kiszámítása [53], míg i_K kiszámítása [16] alapján történt. m_K meghatározásához vettük i_K -nak $k \cdot i_K$ ($k \in \mathbb{N}$) többszöröseit mindaddig, amíg az index forma egyenlet $\pm k \cdot i_K$ jobb oldallal megoldható lett.

A számolásokat Maple-be írt program segítségével végeztük el, ami csupán néhány percet vett igénybe.

D_K	m_1	n_1	l	i_K	m_K	(x_2, x_3, x_4)
144	3	-1	1	1	1	$(1, -2, 1), (1, -1, 0), (0, 1, 0), (1, -2, -1)$
225	-3	5	1	2	2	$(0, 1, -1), (0, 0, 1), (1, 0, -1), (1, 1, -1)$
256	2	-1	1	1	1	$(0, 0, 1), (1, 0, -1)$
400	-1	-5	1	1	1	$(0, 1, 0), (1, -1, 0)$
441	-1	7	3	2	2	$(0, 1, -1), (1, 0, 1), (1, -1, 1), (0, 0, 1)$
576	-3	2	1	1	4	$(0, 1, -1), (0, 0, 1)$
576	-1	2	3	1	3	$(1, 1, -1), (1, 0, -1), (1, 0, 1), (1, -1, 1)$
784	7	-1	1	1	2	$(1, -1, 0), (0, 1, 0)$
1089	-1	11	3	2	4	$(3, -1, 2), (1, 1, -2)$
1225	-7	5	1	2	6	$(0, 1, -1), (1, 1, -1), (1, 0, -1), (0, 0, 1)$
1521	-3	13	1	2	10	$(2, 1, -1), (2, 0, -1), (1, 0, 1), (1, -1, 1)$
1600	5	-2	1	1	4	$(0, 1, -1), (0, 0, 1)$
1600	1	-2	5	1	4	$(0, 1, -1), (0, 0, 1)$
1936	11	-1	1	1	3	$(1, -1, 0), (0, 1, 0)$
2304	6	-1	1	1	5	$(0, 1, -1), (0, 1, 1), (1, -1, -1), (1, 1, -1)$
2304	-2	3	1	1	1	$(1, 0, -1), (0, 0, 1)$
2601	-3	17	1	2	20	$(0, 1, -1), (1, -1, 0), (1, 1, 0), (1, 0, -1), (1, 1, -1), (0, 0, 1)$
2704	-1	-13	1	1	3	$(0, 1, 0), (1, -1, 0)$
3025	-11	5	1	2	12	$(0, 0, 1), (0, 1, -1), (1, 1, -1), (1, 0, -1)$
3136	-7	2	1	1	8	$(0, 1, -1), (0, 0, 1)$
3136	-1	2	7	1	1	$(1, -1, 2), (1, 1, -2)$
3249	-1	19	3	2	14	$(1, 0, -1), (2, -1, 1), (1, 1, -1), (2, 0, 1)$
3600	15	-1	1	1	4	$(1, -1, 0), (0, 1, 0), (2, -4, 1), (2, -4, -1)$
3600	3	-5	1	1	2	$(1, -1, 0), (0, 1, 0)$
3600	3	-1	5	1	12	$(0, 1, -1), (1, -1, 1), (0, 1, 1), (1, -1, -1)$
4624	-1	-17	1	1	4	$(0, 1, 0), (1, -1, 0)$
4761	-1	23	3	2	8	$(2, -1, 1), (1, 0, -1), (2, 0, 1), (1, 1, -1)$
5776	19	-1	1	1	5	$(1, -1, 0), (0, 1, 0)$
5929	-1	11	7	2	4	$(2, -1, 2), (0, 1, -2)$
6400	10	-1	1	1	21	$(0, 1, -1), (1, 1, -1), (1, -1, -1), (0, 1, 1)$
6400	2	-5	1	1	3	$(1, 0, -1), (0, 0, 1)$
6400	2	-1	5	3	3	$(1, 0, -1), (0, 0, 1)$
7056	1	-7	3	1	18	$(1, -1, 0), (0, 1, 0)$
7056	1	-3	7	1	31	$(1, 0, -1), (1, 0, 1)$
7056	-1	-21	1	1	5	$(0, 1, 0), (1, -1, 0)$
7569	-3	29	1	2	26	$(3, 1, -1), (2, -1, 1), (3, 0, -1), (2, 0, 1)$
7744	-11	2	1	1	12	$(0, 0, 1), (0, 1, -1)$
7744	-1	2	11	3	3	$(1, -1, 2), (1, 1, -2)$
8281	-7	13	1	2	20	$(1, 1, 0), (1, -1, 0)$
8464	23	-1	1	1	6	$(1, -1, 0), (0, 1, 0)$
8649	-1	31	3	2	10	$(2, -1, 1), (2, 0, 1), (1, 0, -1), (1, 1, -1)$
9025	-19	5	1	2	24	$(1, 1, 0), (1, -1, 0)$

4. Az index forma egyenlet p-adikus változata bikvadratikus számtestekben

4.1. A megoldás előkészítése

Ebben a fejezetben az index forma egyenlet p-adikus változatának megoldásával foglalkozunk bikvadratikus számtestekben. A bikvadratikus számtestek esetén továbbra is megtartjuk a 3. fejezetben bevezetett jelöléseket.

Eszerint a továbbiakban is legyenek $m, n \in \mathbb{Z} \setminus \{0, 1\}$ különböző négyzetmentes egész számok, $l = \text{lko}(m, n) > 0$ és $m = lm_1$, $n = ln_1$. A $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ bikvadratikus számtestben fogunk dolgozni, amelyről a korábbiak alapján feltehetjük, hogy a 3.1. részben felsorolt öt eset valamelyikébe tartozik. Jelölje az ott megadott egész bázishoz felírt index formát $I(x_2, x_3, x_4)$. Legyenek továbbá K másodfokú résztestei $M_1 = \mathbb{Q}(\sqrt{n})$, $M_2 = \mathbb{Q}(\sqrt{m})$, $M_3 = \mathbb{Q}(\sqrt{m_1 n_1})$.

Legyenek $p_1, \dots, p_s$ különböző rögzített prímszámok. A fejezet hátralevő részében célunk hatékony algoritmust adni az index forma egyenlet p-adikus változatának, azaz az

$$I(x_2, x_3, x_4) = \pm p_1^{t_1} \cdot \dots \cdot p_s^{t_s} \quad (11)$$

egyenlet megoldására, ahol $x_2, x_3, x_4 \in \mathbb{Z}$, $0 \leq t_1, \dots, t_s \in \mathbb{Z}$ az ismeretlenek az $\text{lko}(x_2, x_3, x_4) = 1$ feltétel mellett.

Megjegyezzük, hogy eltekintve egy *N. P. Smart* [49] által megoldott példától (egy teljesen komplex ciklikus negyedfokú számtestben, a 2 és 3 prímeket használva) p-adikus index forma egyenletet eddig még nem oldottak meg.

Ahhoz, hogy a továbbiakban egységesen tudjuk kezelni az összes esetet, vezessük be az új, egész értékű $u_1, u_2, u_3, a, b, c, d, f, g, t$ paramétereket és x, y, z ismeretleneket a következő táblázat szerint:

eset	u_1	u_2	u_3	a	b	c	d	f	g	t	x	y	z
1.	m_1	n_1	l	n_1	4	m_1	4	n_1	4	1	x_4	$2x_2 + x_4$	$2x_3 + x_4$
2.	m_1	n_1	l	n_1	4	m_1	4	n_1	4	1	x_4	$2x_2 - x_4$	$2x_3 + x_4$
3.	m_1	$4n_1$	l	n_1	1	m_1	4	n_1	1	1	x_4	x_2	$2x_3 + x_4$
4.	m_1	n_1	l	n_1	2	$m_1/2$	1	$2n_1$	1	2	x_4	$2x_2 + x_4$	x_3
5.	m_1	n_1	$4l$	n_1	1	m_1	1	n_1	4	1	x_4	$2x_2 + x_3$	x_3

(Jegyezzük meg, hogy a 4. esetben m_1 páros, így $c \in \mathbb{Z}$.)

Korábban láttuk, hogy bikvadratikus számtestek esetén az index forma minden esetben három másodfokú forma szorzata. A tényezők 3.1. részbeli sorrendje mellett jelöljük ezek abszolút értékét rendre $F_i = F_i(x_2, x_3, x_4)$ -gyel ($i = 1, 2, 3$). Ekkor egyszerű számolással ellenőrizhető a következő állítás.

4.1.1. LEMMA (Gaál I., Pethő A., M. Pohst [21], Lemma 1.)

A fenti jelölésekkel

$$\pm u_1 F_1 \pm u_2 F_2 = \pm u_3 F_3. \quad (12)$$

Az index forma tényezőire kapható a következő egyenletrendszer is:

$$\begin{aligned} (ax)^2 - ny^2 &= \pm ab F_1 \\ (cx)^2 - mz^2 &= \pm cd F_2 \\ (fz)^2 - m_1 n_1 y^2 &= \pm fg F_3 \end{aligned} \quad (13)$$

Ezeknek az egyenleteknek a bal oldalai lineáris formák szorzatára bomlanak rendre M_1, M_2, M_3 -ban, melyeket a következő azonosság kapcsol össze:

$$tc(ax - \sqrt{n}y) - ta(cx - \sqrt{m}z) = \sqrt{m}(fz - \sqrt{m_1 n_1}y) \quad (14)$$

A (11) p-adikus index forma egyenlet megoldását egy $\mathbb{Z}$ feletti S-egység egyenlet megoldására fogjuk visszavezetni. Kiderül, hogy bizonyos esetekben ennek megoldása alapján az index forma faktorai már csak véges sok értéket vehetnek fel. Ilyenkor (11) megoldása a teljesen valós esetben Gaál I., Pethő A. és M. Pohst [21] szimultán Pell-egyenletekre vezető eljárásával, a teljesen komplex esetben pedig a 3.4. részben említett, definitséget kihasználó módszerrel fejezhető be. Látni fogjuk azonban, hogy ha van olyan prím $p_1, \dots, p_s$ között, amely két különböző prímideál szorzatára bomlik M_1, M_2, M_3 mindegyikében, akkor még meg kell oldani egy további S-egység egyenletet K felett is.

4.2. Az S-egység egyenlet a racionális egész számok gyűrűje felett

A továbbiakban feltesszük, hogy $x_2, x_3, x_4 \in \mathbb{Z}$, $0 \leq t_1, \dots, t_s \in \mathbb{Z}$ tetszőleges rögzített megoldása a (11) egyenletnek, így $F_1, F_2, F_3 \in \mathbb{Z}$. Mivel megfelelő előjellel $I(x_2, x_3, x_4) = \pm F_1 F_2 F_3$, ezért (12) miatt F_1, F_2, F_3 megoldása a

$$\begin{aligned} \pm u_1 F_1 \pm u_2 F_2 &= \pm u_3 F_3 \\ F_i &= p_1^{\alpha_{i1}} \cdot \dots \cdot p_s^{\alpha_{is}} \quad (i = 1, 2, 3) \end{aligned} \quad (15)$$

$\mathbb{Z}$ feletti S-egység egyenletnek.

Először a (15) S-egység egyenlet $f_1, f_2, f_3 \in \mathbb{N}$ primitív megoldásait fogjuk keresni, azaz azokat, melyekre $\text{lko}(f_1, f_2, f_3) = 1$. Ekkor világos, hogy (15) összes megoldása

$$F_i = f_i \cdot p_1^{a_{i1}} \cdot \dots \cdot p_s^{a_{is}} \quad (i = 1, 2, 3) \quad (16)$$

alakban áll elő, ahol $0 \leq a_1, \dots, a_s \in \mathbb{Z}$ tetszőleges.

Keressük f_1, f_2, f_3 -t a következő alakban

$$f_i = p_1^{a_{i1}} \cdot \dots \cdot p_s^{a_{is}} \quad (i = 1, 2, 3). \quad (17)$$

Legyen továbbá $j = 1, \dots, s$ esetén

$$a'_{ij} = a_{ij} + \text{ord}_{p_j}(u_i) \quad (i = 1, 2, 3). \quad (18)$$

Ezzel a $\pm u_1 f_1 \pm u_2 f_2 = \pm u_3 f_3$ egyenlet felírható

$$\pm u'_1 p_1^{a'_{11}} \cdot \dots \cdot p_s^{a'_{1s}} \pm u'_2 p_1^{a'_{21}} \cdot \dots \cdot p_s^{a'_{2s}} = \pm u'_3 p_1^{a'_{31}} \cdot \dots \cdot p_s^{a'_{3s}} \quad (19)$$

alakba, ahol u'_1, u'_2, u'_3 relatív prímek $p_1, \dots, p_s$ -hez. Ebben az esetben az u_1, u_2, u_3 -ból esetleg adódó, az összes tagban közös $p_1, \dots, p_s$ -hatványokkal osztva

$$\pm u'_1 p_1^{a''_{11}} \cdot \dots \cdot p_s^{a''_{1s}} \pm u'_2 p_1^{a''_{21}} \cdot \dots \cdot p_s^{a''_{2s}} = \pm u'_3 p_1^{a''_{31}} \cdot \dots \cdot p_s^{a''_{3s}}, \quad (20)$$

ahol $a''_{1j}, a''_{2j}, a''_{3j}$ ($j = 1, \dots, s$) közül már csak legfeljebb egy pozitív (hiszen u'_1, u'_2, u'_3 relatív prímek $p_1, \dots, p_s$ -hez).

Ha a (20) egyenletet ilyen feltételek mellett megoldjuk, akkor a''_{ij} -t annyival megnövelve, hogy legalább $\text{ord}_{p_j}(u_i)$ legyen, megkapjuk a'_{ij} -t ($i = 1, 2, 3; j = 1, \dots, s$), azaz (19) megoldásait.

Ezekből (18) segítségével adódik a_{ij} ($i = 1, 2, 3; j = 1, \dots, s$), majd (17)-ből f_1, f_2, f_3 , amiből (15) összes F_1, F_2, F_3 megoldásához (16) alapján jutunk.

4.3. A racionális egészek gyűrűje feletti S-egység egyenlet megoldása

A (20) egyenletben tetszőleges $j \in \{1, \dots, s\}$ esetén vagy $a''_{1j} = 0$, vagy

$$\begin{aligned} 0 < a''_{1j} &= \text{ord}_{p_j} \left(\pm u'_2 \cdot p_1^{a''_{21}} \cdot \dots \cdot p_s^{a''_{2s}} \pm u'_3 \cdot p_1^{a''_{31}} \cdot \dots \cdot p_s^{a''_{3s}} \right) \\ &= \text{ord}_{p_j} \left(1 \pm \frac{u'_2}{u'_3} \cdot p_1^{a''_{21}-a''_{31}} \cdot \dots \cdot p_s^{a''_{2s}-a''_{3s}} \right), \end{aligned}$$

hiszen a jobb oldal ekkor nem tartalmazza p_j -t tényezőként. Erre *K. Yu* [54] (ld. még [50]) p -adikus logaritmusok lineáris formáira vonatkozó becslését használva

$$\begin{aligned} a''_{1j} &= \text{ord}_{p_j} \left(\log_{p_j} \frac{u'_2}{u'_3} + (a''_{21} - a''_{31}) \log_{p_j} p_1 + \dots + (a''_{2s} - a''_{3s}) \log_{p_j} p_s \right) \\ &< C_1 \log H, \end{aligned} \tag{21}$$

ahol C_1 a tétel alapján kiszámítható konstans, $H = \max a''_{ij}$. Jegyezzük meg, hogy ha $a''_{1j} \neq 0$, akkor $a''_{2j} = a''_{3j} = 0$, tehát az előbbi képletben az $(a''_{2j} - a''_{3j}) \log_{p_j} p_j$ tag hiányzik és minden $k \neq j$ esetén a''_{2k} és a''_{3k} közül legfeljebb az egyik lehet pozitív.

Hasonló felső korlátot kaphatunk a''_{2j} , a''_{3j} -re is ($j = 1, \dots, s$), ahonnan $H < \overline{C}_1 \log H$ adódik, ami pedig egy felső korlátot ad H -ra.

A számolások egyszerűsítése végett, ha $u'_1 u'_2 u'_3$ -nek kevés prímosztója van, akkor érdemes azokkal kibővíteni a (11) jobb oldalán álló prímek halmazát, a szimmetria miatt ekkor ugyanis kevesebb esettel kell majd foglalkozni. Ilyenkor értelemszerűen majd csak azokat a megoldásokat kell figyelembe venni, melyeknél az újonnan vett prímek kitevői megegyeznek azzal a kitevővel, amivel az eredeti u'_1, u'_2, u'_3 -ben szerepelnek (lásd a harmadik példát).

A H korlátjára vonatkozó redukciót *B. M. M. de Weger* [52] LLL-redukciós algoritmust használó ötlete alapján végezzük el. Ennek az alábbi változatát fogjuk használni.

4.3.1. LEMMA (Gaál I., Járasi I., F. Luca [13], Lemma 4.1.)

Legyen p prímszám, $\vartheta_1, \dots, \vartheta_n \in \Omega_p$ (Ω_p a p -adikus számtest algebrai lezártjának teljessé tételét jelöli), $\Lambda = \sum_{i=1}^n x_i \vartheta_i$ (ahol $x_1, \dots, x_n \in \mathbb{Z}$), $X = \max_i |x_i|$ és c_1, c_2 pozitív konstansok. Tegyük fel, hogy $\text{ord}_p(\vartheta_i)$ $i = n$ esetén minimális. Legyen ekkor

$$\vartheta'_i = -\frac{\vartheta_i}{\vartheta_n} \quad (i = 1, \dots, n-1)$$

és

$$\Lambda' = \frac{\Lambda}{\vartheta_n} = -\sum_{i=1}^{n-1} x_i \vartheta'_i + x_n.$$

Legyen továbbá $0 < \mu \in \mathbb{Z}$ és tetszőleges $\vartheta \in \Omega_p$ esetén $\vartheta^{(\mu)}$ egy olyan racionális egész szám, hogy $\text{ord}_p(\vartheta - \vartheta^{(\mu)}) \geq \mu$. Jelöljük végül Γ_μ -vel a következő mátrix oszlopvektorai által kifeszített rácsot

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ \vartheta'_1 & \vartheta'_2 & \dots & \vartheta'_{n-1} & p^\mu \end{pmatrix}$$

valamint b_1 -gyel Γ_μ LLL-redukált bázisának első vektorát. Ha

$$\|b_1\| > 2^{\frac{n-1}{2}} \cdot \sqrt{n} \cdot X_0,$$

akkor az $\text{ord}_p(\Lambda) \geq c_1 + c_2 x_j$ egyenlőtlenségnek nincs olyan $x_1, \dots, x_n$ megoldása, melyre

$$\frac{\mu - 1 + \text{ord}_p(\vartheta_n) - c_1}{c_2} \leq X \leq X_0.$$

A lemma alkalmazása során μ -t úgy célszerű megválasztani, hogy a fenti jelölések mellett p^μ nagyságrendje X_0^n körüli legyen.

A 4.3.1. lemmának (21)-re történő alkalmazásával a H -ra kapott korlátot redukálni tudjuk. Az így kapott korlátra ismét végrehajtjuk a redukciót mindaddig, amíg a korlátot ezzel csökkenteni lehet.

A felső korlát általában 3-5 lépésen keresztül csökkenthető. A redukció elég hatékony, hiszen a korlátot első lépésben nagyságrendileg a logaritmusára csökkenti.

A végső lépésben kapott korlát alatti értékeket végigellenőrizve megkapjuk (20) összes megoldását, ahonnan a már leírt módon adódik (15) összes primitív megoldása.

4.4. A kitevők lehetséges értékeinek leírása

A (15) egyenlet egy adott f_1, f_2, f_3 primitív megoldása esetén (16) alapján (13) a következő alakba írható:

$$\begin{aligned} (ax)^2 - ny^2 &= \pm s_1 p_1^{a_1} \cdots p_s^{a_s} \\ (cx)^2 - mz^2 &= \pm s_2 p_1^{a_1} \cdots p_s^{a_s} \\ (fz)^2 - m_1 n_1 y^2 &= \pm s_3 p_1^{a_1} \cdots p_s^{a_s} \end{aligned} \quad (22)$$

ahol $s_1 = abf_1$, $s_2 = cdf_2$, $s_3 = fgf_3$. A továbbiak egyszerűsítése érdekében vezessük be a $P = p_1^{a_1} \cdots p_s^{a_s}$ jelölést is.

Jegyezzük még meg, hogy az $\text{lko}(x_2, x_3, x_4) = 1$ feltételből és x, y, z definíciójából könnyen adódik, hogy $\text{lko}(x, y, z) = 1$ vagy 2.

A továbbiakban feltesszük, hogy $2 \in \{p_1, \dots, p_s\}$. Ezt megtehetjük, hiszen ellenkező esetben a 2-t hozzávesszük a (11) egyenlet jobb oldalán álló prímelekhez, megoldjuk így az egyenletet, végül pedig csak azokat a megoldásokat vesszük figyelembe, melyeknél a 2 kitevője 0.

A most következő két állítás fontos szerepet fog játszani számításainkban.

4.4.1. LEMMA (i) Ha $p \notin \{p_1, \dots, p_s\}$ prímszám, akkor

$$p \nmid \text{lko}(x, y), \quad p \nmid \text{lko}(x, z), \quad p \nmid \text{lko}(y, z).$$

(ii) Ha $p_i \in \{p_1, \dots, p_s\} \setminus \{2\}$, akkor

$$\text{ord}_{p_i}(\text{lko}(x, y)) \leq \text{ord}_{p_i}(s_1)/2$$

$$\begin{aligned}\text{ord}_{p_i}(\text{lko}(x, z)) &\leq (\text{ord}_{p_i}(s_2) + 1)/2 \\ \text{ord}_{p_i}(\text{lko}(y, z)) &\leq \text{ord}_{p_i}(s_3)/2\end{aligned}$$

(iii) Ha $p_i = 2$, akkor

$$\begin{aligned}\text{ord}_2(\text{lko}(x, y)) &\leq (\text{ord}_2(s_1) + 3)/2 \\ \text{ord}_2(\text{lko}(x, z)) &\leq (\text{ord}_2(s_2) + 3)/2 \\ \text{ord}_2(\text{lko}(y, z)) &\leq (\text{ord}_2(s_3) + 2)/2\end{aligned}$$

BIZONYÍTÁS (i) Indirekt tegyük fel, hogy $p \mid x$ és $p \mid y$. Ekkor (22) első egyenlete alapján $p^2 \mid abf_1P$, amiből $p \notin \{p_1, \dots, p_s\}$ miatt $p^2 \mid ab$. Így a és b definíciója szerint $p = 2$ vagy $p^2 \mid n_1$. Előbbi nem lehetséges a $2 \in \{p_1, \dots, p_s\}$ feltevésünk, utóbbi pedig n_1 négyzetmentessége miatt.

Hasonlóan igazolható $p \nmid \text{lko}(x, z)$ és $p \nmid \text{lko}(y, z)$ is.

(ii/1) Legyen $\alpha \in \mathbb{N}$ olyan, hogy $p_i^\alpha \mid x, y$. Mivel $\text{lko}(x, y, z) \leq 2$ és $p_i \neq 2$, ezért ekkor $p_i \nmid z$. (22) első egyenlete alapján $p_i^{2\alpha} \mid s_1P$.

Indirekt tegyük fel, hogy $2\alpha > \text{ord}_{p_i}(s_1)$. Ekkor $p_i \mid P$, ahonnan (22) második és harmadik egyenlete alapján $p_i \mid mz^2$ és $p_i \mid f^2z^2$. Ezekből viszont $p_i \nmid z$ miatt $p_i \mid m$ és $p_i \mid f$ adódik. Utóbbiból $p_i \neq 2$ szerint $p_i \mid n_1$, ezért $p_i \mid l$ és így $p_i^2 \mid n_1l = n$, ami ellentmond n négyzetmentességének.

(ii/2) Legyen $\beta \in \mathbb{N}$ olyan, hogy $p_i^\beta \mid x, z$. Ekkor az előzőekhez hasonlóan $p_i \nmid y$ és (22) második egyenletéből $p_i^{2\beta} \mid s_2P$.

Indirekt tegyük fel, hogy $2\beta > \text{ord}_{p_i}(s_2) + 1$. Ekkor $p_i^2 \mid P$, így (22) első egyenlete alapján $p_i^2 \mid ny^2$. De $p_i \nmid y$, ezért $p_i^2 \mid n$, ami ellentmond annak, hogy n négyzetmentes.

(ii/3) Legyen $\gamma \in \mathbb{N}$ olyan, hogy $p_i^\gamma \mid y, z$. Ekkor a fentiekhez hasonlóan $p_i \nmid x$ és (22) harmadik egyenletéből $p_i^{2\gamma} \mid s_3P$.

Indirekt tegyük fel, hogy $2\gamma > \text{ord}_{p_i}(s_3)$. Ekkor $p_i \mid P$, ahonnan (22) első és második egyenlete szerint $p_i \mid a^2x^2$ és $p_i \mid c^2x^2$. Innen $p_i \nmid x$ alapján $p_i \mid a$, $p_i \mid c$ adódik, tehát a és c értelmezése alapján $p_i \mid n_1$, $p_i \mid m_1$, ami ellentmond $\text{lko}(m_1, n_1) = 1$ -nek.

(iii/1) Legyen $\alpha' \in \mathbb{N}$ olyan, hogy $2^{\alpha'} \mid x, y$. Ekkor (22) első egyenlete szerint $2^{2\alpha'} \mid s_1P$.

Indirekt tegyük fel, hogy $2\alpha' > \text{ord}_2(s_1) + 3$ (és így még $\alpha' > 1$ is teljesül, tehát $2^2 \mid x, y$). Ekkor $2^4 \mid P$, ahonnan (22) második egyenlete és $2^2 \mid x$ szerint $2^4 \mid mz^2$. Azonban $\text{lko}(x, y, z) \leq 2$ és $2^2 \mid x, y$ alapján $\text{ord}_2(z) \leq 1$, ezért $2^2 \nmid m$, ami ellentmond m négyzetmentességének.

(iii/2) Legyen $\beta' \in \mathbb{N}$ olyan, hogy $2^{\beta'} \mid x, z$. Ekkor (22) második egyenletéből $2^{2\beta'} \mid s_2P$.

Indirekt tegyük fel, hogy $2\beta' > \text{ord}_2(s_2) + 3$ (és így $\beta' > 1$ is igaz, vagyis $2^2 \mid x, z$). Ekkor $2^4 \mid P$, amiből (22) első egyenlete és $2^2 \mid x$ alapján $2^4 \mid ny^2$. De $\text{lko}(x, y, z) \leq 2$ és $2^2 \mid x, z$, ezért $\text{ord}_2(y) \leq 1$, tehát $2^2 \nmid n$, ami ellentmond n négyzetmentességének.

(iii/3) Legyen $\gamma' \in \mathbb{N}$ olyan, hogy $2^{\gamma'} \mid y, z$. Ekkor (22) harmadik egyenletéből kapjuk, hogy $2^{2\gamma'} \mid s_3P$.

Indirekt tegyük fel, hogy $2\gamma' > \text{ord}_2(s_3) + 2$ (és így $\gamma' > 1$, azaz $2^2 \mid y, z$). Ekkor $2^3 \mid P$, így (22) első, második egyenletéből és $2^2 \mid y, z$ -ből $2^3 \mid a^2x^2$ és $2^3 \mid c^2x^2$. Mivel $\text{lko}(x, y, z) \leq 2$ és $2^2 \mid y, z$ miatt $\text{ord}_2(x) \leq 1$, ezért $2 \mid a^2$, $2 \mid c^2$, tehát $2 \mid a$, $2 \mid c$, ahonnan a és c értelmezése szerint $2 \mid n_1$, $2 \mid m_1$, ami pedig ellentmond $\text{lko}(m_1, n_1) = 1$ -nek. $\square$

Legyen $x, y, z \in \mathbb{Z}$ egy tetszőlegesen rögzített megoldása (22)-nek. Ekkor $i = 1, 2, 3$ esetén legyen

i	α_i	β_i	φ_{i1}	φ_{i2}	D_{1i}	D_{2i}
1	a	$\sqrt{n}$	$ax - \sqrt{n}y$	$ax + \sqrt{n}y$	0	3
2	c	$\sqrt{m}$	$cx - \sqrt{m}z$	$cx + \sqrt{m}z$	1	3
3	f	$\sqrt{m_1n_1}$	$fz - \sqrt{m_1n_1}y$	$fz + \sqrt{m_1n_1}y$	0	2

Közismert, hogy ha $p \in \mathbb{Z}$ prímszám, akkor a p által generált ideál egy másodfokú algebrai számtestben háromféleképpen bomolhat fel prímeálók szorzatára. Ennek megfelelően választjuk szét az eseteket a következő állításban.

4.4.2. LEMMA

(i) Legyen $p_j \in \{p_1, \dots, p_s\} \setminus \{2\}$.

Ha $p_j\mathbb{Z}_{M_i}$ prímeál M_i -ben ($i = 1, 2, 3$), akkor

$$a_j \leq 2 \max(\text{ord}_{p_j}(2\alpha_i), \text{ord}_{p_j}(2\beta_i)) + D_{1i}.$$

(ii) Legyen $p_j = 2$.

Ha $2\mathbb{Z}_{M_i}$ prímeál M_i -ben ($i = 1, 2, 3$), akkor

$$a_j \leq 2 \max(\text{ord}_2(2\alpha_i), \text{ord}_2(2\beta_i)) + D_{2i}.$$

(iii) Legyen $p_j \in \{p_1, \dots, p_s\} \setminus \{2\}$.

Ha $p_j\mathbb{Z}_{M_i} = \wp^2$ valamilyen $\wp$ prímeálra M_i -ben ($i = 1, 2, 3$), akkor

$$a_j \leq \max(\text{ord}_\wp(2\alpha_i), \text{ord}_\wp(2\beta_i)) + D_{1i}.$$

(iv) Legyen $p_j = 2$.

Ha $2\mathbb{Z}_{M_i} = \wp^2$ valamilyen $\wp$ prímeállal M_i -ben ($i = 1, 2, 3$), akkor

$$a_j \leq \max(\text{ord}_\wp(2\alpha_i), \text{ord}_\wp(2\beta_i)) + D_{2i}.$$

(v) Legyen $p_j \in \{p_1, \dots, p_s\} \setminus \{2\}$.

Ha $p_j\mathbb{Z}_{M_i} = \wp \cdot \overline{\wp}$ valamilyen $\wp$ prímeálra M_i -ben ($i = 1, 2, 3$) és $\wp^k \mid \varphi_{i1}$, $\overline{\wp}^k \mid \varphi_{i1}$, akkor

$$k \leq \max(\text{ord}_{p_j}(2\alpha_i), \text{ord}_{p_j}(2\beta_i)) + \frac{\text{ord}_{p_j}(s_i) + D_{1i}}{2},$$

ahol itt $\sigma \in \mathbb{Z}_{M_i}$ esetén $\text{ord}_{p_j}(\sigma) = \min(\text{ord}_\wp(\sigma), \text{ord}_{\overline{\wp}}(\sigma))$.

(vi) Legyen $p_j = 2$.

Ha M_i -ben $2\mathbb{Z}_{M_i} = \wp \cdot \overline{\wp}$ valamilyen $\wp$ prímeállal ($i = 1, 2, 3$) és $\wp^k \mid \varphi_{i1}$, $\overline{\wp}^k \mid \varphi_{i1}$, akkor

$$k \leq \max(\text{ord}_2(2\alpha_i), \text{ord}_2(2\beta_i)) + \frac{\text{ord}_2(s_i) + D_{2i}}{2},$$

ahol itt $\sigma \in \mathbb{Z}_{M_i}$ esetén $\text{ord}_2(\sigma) = \min(\text{ord}_\wp(\sigma), \text{ord}_{\overline{\wp}}(\sigma))$.

BIZONYÍTÁS (i) Tegyük fel, hogy $p_j\mathbb{Z}_{M_1}$ prímeál M_1 -ben és legyen $\overline{a_j} = a_j + \text{ord}_{p_j}(s_1)$.

Ekkor (22) első egyenlete alapján $\overline{p_j^{a_j}} \parallel (ax)^2 - ny^2 = \varphi_{11} \cdot \varphi_{12}$. Mivel M_1 -ben a φ_{11} és φ_{12} algebrai egész elemek egymás konjugáltjai, ezért valamely $b_j \in \mathbb{Z}$ nemnegatív számra $p_j^{b_j} \mid \varphi_{11}$ pontosan akkor teljesül, ha $p_j^{b_j} \mid \varphi_{12}$. Ha b_j -t a legnagyobb lehetséges értéknek

választjuk, akkor a fentieket egybevetve $\bar{a}_j = 2b_j$ adódik. Továbbá $p_j^{b_j} \mid \varphi_{11} + \varphi_{12} = 2ax$ és $p_j^{b_j} \mid \varphi_{12} - \varphi_{11} = 2\sqrt{n}y$, ami szerint $b_j \leq \text{ord}_{p_j}(2a) + \text{ord}_{p_j}(x)$ és $b_j \leq \text{ord}_{p_j}(2\sqrt{n}) + \text{ord}_{p_j}(y)$, a 4.4.1. lemma alapján pedig $\min(\text{ord}_{p_j}(x), \text{ord}_{p_j}(y)) \leq \text{ord}_{p_j}(s_1)/2$. Ezekből $b_j \leq \max(\text{ord}_{p_j}(2a), \text{ord}_{p_j}(2\sqrt{n})) + \text{ord}_{p_j}(s_1)/2$, ahonnan $2b_j = \bar{a}_j = a_j + \text{ord}_{p_j}(s_1)$ -et felhasználva éppen a kívánt állítás adódik.

(iii) Tegyük fel, hogy $p_j\mathbb{Z}_{M_1} = \wp^2$, ahol $\wp$ prímeál M_1 -ben. Legyen ismét $\bar{a}_j = a_j + \text{ord}_{p_j}(s_1)$.

Most is érvényes $p_j^{\bar{a}_j} \parallel (ax)^2 - ny^2 = \varphi_{11} \cdot \varphi_{12}$ és hogy tetszőleges $b_j \in \mathbb{Z}$ nemnegatív számra $\wp^{b_j} \mid \varphi_{11}$ akkor és csak akkor áll fenn, ha $\wp^{b_j} \mid \varphi_{12}$, mivel $\wp$ ilyenkor egyenlő saját konjugáltjával. Tekintsük most is a lehetséges legnagyobb b_j -t, melyre az előbbi oszthatóságok teljesülnek. A fentiek egybevetésével kapjuk, hogy $\bar{a}_j = b_j$, továbbá $\wp^{b_j} \mid 2ax$ és $\wp^{b_j} \mid 2\sqrt{n}y$, ezért $b_j \leq \text{ord}_{\wp}(2a) + \text{ord}_{\wp}(x)$ és $b_j \leq \text{ord}_{\wp}(2\sqrt{n}) + \text{ord}_{\wp}(y)$. Másrészt a 4.4.1. lemma szerint $\min(\text{ord}_{\wp}(x), \text{ord}_{\wp}(y)) = 2 \min(\text{ord}_{p_j}(x), \text{ord}_{p_j}(y)) \leq \text{ord}_{p_j}(s_1)$. Ezekből $b_j \leq \max(\text{ord}_{\wp}(2a), \text{ord}_{\wp}(2\sqrt{n})) + \text{ord}_{p_j}(s_1)$, ahonnan $b_j = \bar{a}_j = a_j + \text{ord}_{p_j}(s_1)$ -et felhasználva kapjuk az állítást.

(v) Tegyük fel, hogy $p_j\mathbb{Z}_{M_1} = \wp \cdot \bar{\wp}$, ahol $\wp$ prímeál M_1 -ben. A feltétel szerint $\wp^k \mid \varphi_{11}$ és $\bar{\wp}^k \mid \varphi_{11}$, ezért konjugálás után $\wp^k \mid \varphi_{12}$ és $\bar{\wp}^k \mid \varphi_{12}$ adódik. Ekkor az előző esetekhez hasonlóan kapjuk, hogy $\wp^k \mid 2ax$ és $\wp^k \mid 2\sqrt{n}y$, ezért $k \leq \text{ord}_{\wp}(2a) + \text{ord}_{\wp}(x)$ és $k \leq \text{ord}_{\wp}(2\sqrt{n}) + \text{ord}_{\wp}(y)$. A 4.4.1. lemma szerint $\min(\text{ord}_{\wp}(x), \text{ord}_{\wp}(y)) = \min(\text{ord}_{p_j}(x), \text{ord}_{p_j}(y)) \leq \text{ord}_{p_j}(s_1)/2$, így $k \leq \max(\text{ord}_{\wp}(2a), \text{ord}_{\wp}(2\sqrt{n})) + \text{ord}_{p_j}(s_1)/2$. Hasonlóan $k \leq \max(\text{ord}_{\bar{\wp}}(2a), \text{ord}_{\bar{\wp}}(2\sqrt{n})) + \text{ord}_{p_j}(s_1)/2$ is teljesül. Kihasználva, hogy $\text{ord}_{\wp}(2a) = \text{ord}_{\bar{\wp}}(2a) = \text{ord}_{p_j}(2a)$ és hogy tetszőleges $A, B, C \in \mathbb{R}$ számok esetén érvényes $\min(\max(A, B), \max(A, C)) = \max(A, \min(B, C))$, kapjuk az állítást.

A lemma mindegyik része hasonlóan igazolható M_2 és M_3 esetén. A (ii), (iv), (vi) részek bizonyítása pedig ugyanúgy végezhető el, mint rendre az (i), (iii), (v) részeké. $\square$

A 4.4.2. lemma (i)-(iv) részének köszönhetően, ha egy $p_j \in \{p_1, \dots, p_s\}$ prím esetén a p_j által generált ideál prímeál vagy egy prímeál négyzete K valamelyik másodfokú résztestében, akkor ezen prím a_j kitevőjére egy igen kis felső korlát nyerhető. Ez alapján ha a (11) jobb oldalán szereplő összes prím ilyen típusú, akkor csak véges sok, viszonylag kevés lehetséges F_1, F_2, F_3

érték adódik. Ezekre tekintve a (13) egyenletrendszert, innentől kezdve (11) megoldásának befejezéséhez a teljesen valós esetben *Gaál I.*, *Pethő A.*, *M. Pohst* [21] szimultán Pell-egyenletekre vezető, míg teljesen komplex esetben a 3.4. részben említett, definitséget felhasználó módszert követhetjük.

Említsük még meg, hogy ha a bikvadratikus számtestünk az 1., a 2. vagy az 5. esethez tartozik, akkor m és n szerepe szimmetrikus, sőt ezekben az esetekben a (15) S-egység egyenlet is lényegében ugyanaz marad, ha m és n értékét felcseréljük. A 4.4.2. lemma azonban m és n felcserélésekor adhat különböző felső becsléseket a kitevőkre, ezért érdemes azt kipróbálni mindkét módon, majd a megoldást a választással folytatni, melynél kevesebb lehetséges kitevő jön számításba.

Viszont ha van olyan prím $p_1, \dots, p_s$ között, amely által generált ideál két különböző prímideál szorzatára bomlik a bikvadratikus számtest mindhárom másodfokú résztestében, akkor egy további, K feletti S-egység egyenletet is meg kell még oldanunk. A fejezet hátralevő részében ezzel az esettel foglalkozunk.

4.5. Az S-egység egyenlet a negyedfokú test felett

Ebben a részben a (14) azonosság alapján egy S-egység egyenletet nyerünk a bikvadratikus számtestünk felett. Megjegyezzük, hogy *Győry K.* [27] is S-egység egyenletekre vezette vissza a p -adikus index forma egyenlet megoldását. Mi azonban a további részletek kidolgozásakor az eljárás hatékonyabbá tétele érdekében kihasználjuk az általunk vizsgált test sajátosságait, valamint szükségünk lesz a részletes számolásra azért is, hogy előkészítsük a redukciós eljárás alkalmazását. A leírást a teljesen valós bikvadratikus számtestek esetén adjuk meg, a teljesen komplex esetben néhány képletben kellene kisebb változtatásokat elvégezni.

A továbbiakhoz jelöljük h_i -vel M_i ideálosztályszámát, ε_i -vel pedig M_i egy alapegységét ($i = 1, 2, 3$). Jelölje továbbá $h = \text{lkk}(h_1, h_2, h_3)$ az ideálosztályszámok legkisebb közös többszörösét.

Legyen I_{i1}, I_{i2}, I_{i3} a következő módon definiált osztályozása $\{1, \dots, s\}$ -nek ($i = 1, 2, 3$):

I. $j \in I_{i1}$, ha $p_j \mathbb{Z}_{M_i}$ prímideál M_i -ben.

II. $j \in I_{i2}$, ha $p_j \mathbb{Z}_{M_i} = \wp_{ji}^2$ egy $\wp_{ji}$ prímeál négyzete M_i -ben.

III. $j \in I_{i3}$, ha $p_j \mathbb{Z}_{M_i} = \wp_{ji1} \cdot \wp_{ji2}$ a különböző $\wp_{ji1}$, $\wp_{ji2}$ prímeálok szorzata M_i -ben.

(22) szerint tudjuk, hogy

$$\varphi_{i1} \cdot \varphi_{i2} = \pm s_i \cdot p_1^{a_1} \cdot \dots \cdot p_s^{a_s} \quad (i = 1, 2, 3).$$

Jegyezzük meg, hogy az előző rész szerint ha $j \in \bigcup_{i=1}^3 (I_{i1} \cup I_{i2})$, akkor a_j -re kis felső korlát adható, ezért a hozzá tartozó tényező konstansként is kezelhető, ami jelentősen csökkenti az S-egység egyenlet ismeretleneinek számát. Azonban ha az a_j -re nyert korlát mégsem elég kicsi, akkor a túl sok eset vizsgálatának elkerülése végett akár továbbra is tekinthetjük ismeretlennek.

I. Ha $j \in I_{i1}$, akkor p_j -nek ugyanolyan kitevős hatványa osztja φ_{i1} -et és φ_{i2} -t, ezért $\text{ord}_{p_j}(\varphi_{i1}\varphi_{i2}) = \text{ord}_{p_j}(s_i) + a_j$ biztosan páros. (Ez a gyakorlati megvalósításnál felhasználható arra is, hogy kizárjuk a_j -nek vagy a páros, vagy a páratlan értékeit.) Legyen $c_{ji} \in \mathbb{Z}$ a következőképpen értelmezve:

$$a_j + \text{ord}_{p_j}(s_i) = 2 \cdot \left\lfloor \frac{a_j}{2} \right\rfloor + 2c_{ji}$$

Ekkor φ_{i1} prímeálfelbontásában $p_j \mathbb{Z}_{M_i}$ az $\left\lfloor \frac{a_j}{2} \right\rfloor + c_{ji}$ kitevőjű hatványon szerepel.

II. Ha $j \in I_{i2}$, akkor $\wp_{ji}$ -nek ugyanolyan kitevős hatványa osztja φ_{i1} -et és φ_{i2} -t, ez a kitevő pedig éppen $\text{ord}_{p_j}(\varphi_{i1}\varphi_{i2}) = a_j + \text{ord}_{p_j}(s_i)$. Legyen most c_{ji} a következő egyenlőséggel definiálva:

$$a_j + \text{ord}_{p_j}(s_i) = 2 \cdot \left\lfloor \frac{a_j}{2} \right\rfloor + c_{ji}$$

Ekkor φ_{i1} prímeálfelbontásában tényezőként

$$\wp_{ji}^{a_j + \text{ord}_{p_j}(s_i)} = (p_j \mathbb{Z}_{M_i})^{\left\lfloor \frac{a_j}{2} \right\rfloor} \cdot \wp_{ji}^{c_{ji}}$$

szerepel.

III. Legyen $j \in I_{i3}$. Ekkor a $p_j \mathbb{Z}_{M_i}$ előállításában szereplő $\wp_{ji1}$, $\wp_{ji2}$ különböző, egymással relatív prím és konjugált M_i -beli prímeálokhoz

léteznek olyan $\pi_{ji1}, \pi_{ji2} \in \mathbb{Z}_{M_i}$ elemek, hogy $\wp_{ji1}^h = \pi_{ji1}\mathbb{Z}_{M_i}$ és $\wp_{ji2}^h = \pi_{ji2}\mathbb{Z}_{M_i}$.

Ha $\wp_{ji1}$ -nek egy bizonyos hatványa osztja φ_{i1} -et, akkor $\wp_{ji2}$ -nek ugyanolyan kitevőjű hatványa osztja φ_{i2} -t és ugyanez igaz $\wp_{ji1}$ és $\wp_{ji2}$ felcserélésével. A 4.4.2. lemma (v) és (vi) része szerint φ_{i1} -et oszthatja $\wp_{ji1}$ és $\wp_{ji2}$ közül mindkettő, de legfeljebb egy kis kitevős hatványon, legyen ez a kitevő $b_{ji} \in \mathbb{Z}$.

Ezek szerint φ_{i1} prímeideálfelbontásában

vagy $\wp_{ji1}^{b_{ji}+l_{ji}} \cdot \wp_{ji2}^{b_{ji}} = (p_j\mathbb{Z}_{M_i})^{b_{ji}} \cdot \wp_{ji1}^{l_{ji}}$, vagy $\wp_{ji1}^{b_{ji}} \cdot \wp_{ji2}^{b_{ji}+l_{ji}} = (p_j\mathbb{Z}_{M_i})^{b_{ji}} \cdot \wp_{ji2}^{l_{ji}}$ szerepel, ahol $a_j + \text{ord}_{p_j}(s_i) = 2b_{ji} + l_{ji}$ teljesül.

Legyen ekkor $c_{ji} \in \mathbb{Z}$ a következőképpen értelmezve:

$$l_{ji} = h \cdot \left\lfloor \frac{a_j}{h} \right\rfloor + c_{ji}$$

Ekkor a φ_{i1} felbontásában szereplő megfelelő tényező

vagy $(p_j\mathbb{Z}_{M_i})^{b_{ji}} \cdot (\pi_{ji1}\mathbb{Z}_{M_i})^{\left\lfloor \frac{a_j}{h} \right\rfloor} \cdot \wp_{ji1}^{c_{ji}}$, vagy $(p_j\mathbb{Z}_{M_i})^{b_{ji}} \cdot (\pi_{ji2}\mathbb{Z}_{M_i})^{\left\lfloor \frac{a_j}{h} \right\rfloor} \cdot \wp_{ji2}^{c_{ji}}$.

Az

$$s'_i = s_i \cdot \prod_{j=1}^s p_j^{-\text{ord}_{p_j}(s_i)} \quad (i = 1, 2, 3)$$

jelölés bevezetése után, a fentieket összevetve azt kapjuk, hogy φ_{i1} felbontása

$$\begin{aligned} & \alpha_i \cdot \prod_{j \in I_{i1}} (p_j\mathbb{Z}_{M_i})^{\left\lfloor \frac{a_j}{2} \right\rfloor + c_{ji}} \cdot \prod_{j \in I_{i2}} \left((p_j\mathbb{Z}_{M_i})^{\left\lfloor \frac{a_j}{2} \right\rfloor} \cdot \wp_{ji}^{c_{ji}} \right) \cdot \\ & \cdot \prod_{j \in I_{i3}} \left((p_j\mathbb{Z}_{M_i})^{b_{ji}} \cdot (\pi_{jik_{ji}}\mathbb{Z}_{M_i})^{\left\lfloor \frac{a_j}{h} \right\rfloor} \cdot \wp_{jik_{ji}}^{c_{ji}} \right), \end{aligned}$$

ahol α_i egy s'_i normájú ideál és $j \in I_{i3}$ esetén $k_{ji} = 1$ vagy 2 . Az

$$\alpha_i \cdot \prod_{j \in I_{i1}} (p_j\mathbb{Z}_{M_i})^{c_{ji}} \cdot \prod_{j \in I_{i2}} \wp_{ji}^{c_{ji}} \cdot \prod_{j \in I_{i3}} \left((p_j\mathbb{Z}_{M_i})^{b_{ji}} \cdot \wp_{jik_{ji}}^{c_{ji}} \right)$$

ideál főideál, melynek egy $\gamma_i \in \mathbb{Z}_{M_i}$ generátora egységtényező erejéig kiszámítható. Ezért azt kapjuk, hogy valamilyen $e_i \in \mathbb{Z}$ -vel

$$\varphi_{i1} = \pm \gamma_i \cdot \varepsilon_i^{e_i} \cdot \prod_{j \in I_{i1} \cup I_{i2}} p_j^{\left\lfloor \frac{a_j}{2} \right\rfloor} \cdot \prod_{j \in I_{i3}} \pi_{jik_{ji}}^{\left\lfloor \frac{a_j}{h} \right\rfloor}. \quad (23)$$

Jelöléseinkkel a (14) azonosság a

$$tc \cdot \varphi_{11} - ta \cdot \varphi_{21} = \sqrt{m} \cdot \varphi_{31} \quad (24)$$

alakot ölti.

Ha valamely p_j prím esetén a p_j által generált ideál mindhárom másodfokú résztestben prímeál vagy prímeál négyzete, azaz $j \in I_0 = \bigcap_{i=1}^3 (I_{i1} \cup I_{i2})$, akkor (24)-ben a (23) felhasználása után adódó $p_j^{\lfloor \frac{a_j}{2} \rfloor}$ tényezők kiesnek. A $j \in \left(\bigcup_{i=1}^3 (I_{i1} \cup I_{i2}) \right) \setminus I_0$ indexekhez tartozó tényezők pedig a korábban írtak szerint konstansként kezelhetők.

Legyen $I = I_{13} \cap I_{23} \cap I_{33}$. Ekkor a fentiek értelmében φ_{i1} -et a

$$\varphi_{i1} = \pm \delta_i \cdot \varepsilon_i^{e_i} \cdot \prod_{j \in I} \pi_{jik_{ji}}^{d_j}$$

alakban állíthatjuk elő ($i = 1, 2, 3$), ahol $\delta_i \in \mathbb{Z}_{M_i}$, aminek néhány lehetséges értéke kiszámolható, továbbá $k_{ji} = 1$ vagy 2 , $d_j = \lfloor \frac{a_j}{h} \rfloor$. Ha meg tudjuk határozni d_j lehetséges értékeit, akkor azokból már ki tudjuk számolni az a_j által felvehető értékeket is $j \in I$ esetén.

A fentiek alapján (24) átírható

$$\pm tc \cdot \delta_1 \varepsilon_1^{e_1} \prod_{j \in I} \pi_{j1k_{j1}}^{d_j} \pm ta \cdot \delta_2 \varepsilon_2^{e_2} \prod_{j \in I} \pi_{j2k_{j2}}^{d_j} = \pm \sqrt{m} \cdot \delta_3 \varepsilon_3^{e_3} \prod_{j \in I} \pi_{j3k_{j3}}^{d_j}$$

alakba, amiből

$$\pm \rho_1 \varepsilon_1^{e_1} \varepsilon_3^{-e_3} \prod_{j \in I} \left(\frac{\pi_{j1k_{j1}}}{\pi_{j3k_{j3}}} \right)^{d_j} \pm \rho_2 \varepsilon_2^{e_2} \varepsilon_3^{-e_3} \prod_{j \in I} \left(\frac{\pi_{j2k_{j2}}}{\pi_{j3k_{j3}}} \right)^{d_j} = 1 \quad (25)$$

adódik, ahol

$$\rho_1 = \frac{tc \cdot \delta_1}{\sqrt{m} \cdot \delta_3}, \quad \rho_2 = \frac{ta \cdot \delta_2}{\sqrt{m} \cdot \delta_3}.$$

Legyen $E = \max(|e_1|, |e_2|, |e_3|)$, $E_1 = \max(|e_1|, |e_3|)$, $E_2 = \max(|e_2|, |e_3|)$, $D = \max_{j \in I} d_j$, $H = \max(E, D)$, $H_1 = \max(E_1, D)$, $H_2 = \max(E_2, D)$.

Ezek után a (25) K feletti S-egység egyenletet kívánjuk megoldani.

4.6. A K feletti S-egység egyenlet megoldása: felső korlátok

Ebben a részben a (25) K feletti S-egység egyenlet megoldása érdekében először D -re, majd pedig H -ra vezetünk le felső korlátot.

Ha $j \in I$ rögzített, akkor $i = 1, 2, 3$ esetén $h = \text{ord}_{p_j}(p_j^h) = \text{ord}_{p_j}(\pi_{ji1}) + \text{ord}_{p_j}(\pi_{ji2})$ teljesül a relatív prím π_{ji1} és π_{ji2} -re. Ezért $i = 1, 2, 3$, $k = 1, 2$ esetén $\text{ord}_{p_j}(\pi_{jik}) = 0$ vagy h , méghozzá $k = 1$ esetén h , $k = 2$ esetén 0 , vagy fordítva. Továbbá π_{ji1} és π_{ji2} választhatók úgy, hogy egymás konjugáltjai legyenek M_i -ben. Ezek szerint létezik olyan $\gamma \mapsto \gamma^*$ ($\gamma \in K$) konjugálás K -n, hogy $\text{ord}_{p_j}(\pi_{j1k_{j1}}^*) = h$ és $\text{ord}_{p_j}(\pi_{j3k_{j3}}^*) = 0$ álljon fenn.

Alkalmazzuk ezt a konjugálást a (25) egyenletre, de az egyszerűség kedvéért a jelölésből a továbbiakban elhagyjuk a $*$ -ot. Jegyezzük meg, hogy ε_i , továbbá $j' \neq j$, $k = 1, 2$ esetén $\pi_{j'ik}$ p_j -adikus egységek. Ekkor (25) első tagjának p_j -adikus rendje $hd_j + \text{ord}_{p_j}(\rho_1)$, ami pozitív, ha d_j nem túl kicsi. Ellenkező esetben d_j -re máris egy igen éles felső korlátot nyertünk.

Ha ez a kifejezés pozitív, akkor azt kapjuk, hogy

$$0 < hd_j + \text{ord}_{p_j}(\rho_1) = \text{ord}_{p_j} \left(\pm 1 \pm \rho_2 \varepsilon_2^{e_2} \varepsilon_3^{-e_3} \cdot \prod_{j \in I} \left(\frac{\pi_{j2k_{j2}}}{\pi_{j3k_{j3}}} \right)^{d_j} \right). \quad (26)$$

A (25) egyenlet bal oldalának tagjait rendre A -val és B -vel jelölve ekkor $\text{ord}_{p_j}(A) > 0$ miatt $\text{ord}_{p_j}(B) = \text{ord}_{p_j}(1 - A) \geq \min(\text{ord}_{p_j}(1), \text{ord}_{p_j}(A)) = \min(0, \text{ord}_{p_j}(A)) = 0$. Ha $\text{ord}_{p_j}(B) > 0$ lenne, akkor $0 = \text{ord}_{p_j}(1) = \text{ord}_{p_j}(A + B) \geq \min(\text{ord}_{p_j}(A), \text{ord}_{p_j}(B)) > 0$ miatt ellentmondáshoz jutnánk, ezért $\text{ord}_{p_j}(B) = 0$, azaz

$$0 = \text{ord}_{p_j} \left(\rho_2 \varepsilon_2^{e_2} \varepsilon_3^{-e_3} \cdot \prod_{j \in I} \left(\frac{\pi_{j2k_{j2}}}{\pi_{j3k_{j3}}} \right)^{d_j} \right) = \text{ord}_{p_j}(\rho_2) + d_j \cdot \text{ord}_{p_j} \left(\frac{\pi_{j2k_{j2}}}{\pi_{j3k_{j3}}} \right).$$

Ha $\text{ord}_{p_j} \left(\frac{\pi_{j2k_{j2}}}{\pi_{j3k_{j3}}} \right) \neq 0$, akkor d_j és így a_j az előbbi egyenlőségből kiszámolható. Azonban ha $\text{ord}_{p_j} \left(\frac{\pi_{j2k_{j2}}}{\pi_{j3k_{j3}}} \right) = 0$, akkor $\text{ord}_{p_j}(\rho_2) = 0$, tehát a (26)-ban szereplő összes tényező p_j -adikus egység. Ezért alkalmazható rá K . Yu [54] tétele, ami alapján azt kapjuk, hogy egy nagy C'_2 konstanssal

$$hd_j + \text{ord}_{p_j}(\rho_1) < C'_2 \log H_2$$

Ezt az összes $j \in I$ -re megismételve, valamilyen C_2 konstanssal az adódik, hogy

$$D < C_2 \log H_2. \quad (27)$$

Hasonló gondolatmenettel kapjuk valamilyen C_3 konstanssal, hogy

$$D < C_3 \log H_1. \quad (28)$$

Legyen $\eta_1 = \varepsilon_1^{e_1} \varepsilon_3^{-e_3}$. Ekkor $i = 1, 2, 3, 4$ -re $\log |\eta_1^{(i)}| = e_1 \log |\varepsilon_1^{(i)}| - e_3 \log |\varepsilon_3^{(i)}|$. Az ezek által meghatározott egyenletrendszerből valamilyen c_1 konstanssal azt kapjuk, hogy $c_1 E_1 < \max_i |\log |\eta_1^{(i)}||$. Tegyük fel, hogy a jobb oldalon szereplő kifejezés a maximumértéket i_0 esetén veszi fel.

Ha $\log |\eta_1^{(i_0)}| \leq 0$, akkor $-c_1 E_1 > \log |\eta_1^{(i_0)}|$. Ha pedig $\log |\eta_1^{(i_0)}| > 0$, akkor $c_1 E_1 < \log |\eta_1^{(i_0)}|$. Kihasználva, hogy $\sum_{i=1}^4 \log |\eta_1^{(i)}| = 0$ (mivel η_1 egység, így normája 1 abszolút értékű) teljesül, létezik olyan i' , amelyre $\log |\eta_1^{(i')}| < 0$ és $|\log |\eta_1^{(i')}|| \geq \frac{|\log |\eta_1^{(i_0)}||}{3}$, ezért $-\frac{c_1}{3} E_1 > \log |\eta_1^{(i')}|$.

A fenti megfontolásokat elvégezhetjük $\eta_2 = \varepsilon_2^{e_2} \varepsilon_3^{-e_3}$ -ra is. Azt kapjuk tehát, hogy létezik η_1 -nek olyan η_1^* , η_2 -nek olyan η_2^* konjugáltja, hogy valamilyen c_3 konstanssal $|\eta_1^*| < \exp(-c_3 \cdot E_1)$ és $|\eta_2^*| < \exp(-c_3 \cdot E_2)$.

Ekkor azt kapjuk, hogy valamilyen c_4 és c_5 konstansokkal

$$\left| \rho_1^* \eta_1^* \prod_{j \in I} \left(\frac{\pi_{j1k_{j1}}^*}{\pi_{j3k_{j3}}^*} \right)^{d_j} \right| < c_4 \cdot \exp(-c_3 \cdot E_1) \cdot c_5^D \quad (29)$$

és

$$\left| \rho_2^{**} \eta_2^{**} \prod_{j \in I} \left(\frac{\pi_{j2k_{j2}}^{**}}{\pi_{j3k_{j3}}^{**}} \right)^{d_j} \right| < c_4 \cdot \exp(-c_3 \cdot E_2) \cdot c_5^D. \quad (30)$$

A c_5 -öt válasszuk úgy, hogy $c_5 > \max(e^{c_3/2}, 1)$ teljesüljön.

Legyen $c_6 = \frac{c_3}{2 \log c_5}$. Ekkor c_5 megválasztása miatt $0 < c_6 < 1$.

Ha $c_6 E_1 \leq D$, akkor (28) alapján

$$H_1 = \max(D, E_1) \leq \max(D, D/c_6) = \frac{1}{c_6} D < \frac{1}{c_6} C_3 \cdot \log H_1 \leq \frac{1}{c_6} C_3 \cdot \log H. \quad (31)$$

Hasonlóan kapjuk $c_6 E_2 \leq D$ esetén (27) segítségével, hogy

$$H_2 < \frac{1}{c_6} C_2 \cdot \log H.$$

Ha azonban $D < c_6 E_1$, akkor $D \log c_5 < \frac{c_3}{2} E_1$ és $H_1 = \max(D, E_1) = E_1$, ezért (29) jobb oldalára

$$\begin{aligned} c_4 \cdot \exp(-c_3 \cdot E_1) \cdot c_5^D &= c_4 \cdot \exp(-c_3 \cdot E_1 + D \cdot \log c_5) < \\ c_4 \cdot \exp\left(-\frac{c_3}{2} \cdot E_1\right) &= c_4 \cdot \exp\left(-\frac{c_3}{2} \cdot H_1\right). \end{aligned} \quad (32)$$

Ha H_1 elég nagy, akkor (kihasználva, hogy $|\delta - 1| \leq \frac{1}{2}$ esetén $|\log \delta| \leq 2|\delta - 1|$) azt kapjuk (25)-ből, (29)-ből és (32)-ből, hogy

$$\begin{aligned} &\left| \log |\rho_2^*| + e_2 \log |\varepsilon_2^*| - e_3 \log |\varepsilon_3^*| + \sum_{j \in I} d_j \log \left| \frac{\pi_{j2k_{j2}}^*}{\pi_{j3k_{j3}}^*} \right| \right| \\ &< 2c_4 \cdot \exp\left(-\frac{c_3}{2} \cdot H_1\right). \end{aligned} \quad (33)$$

A. Baker és G. Wüstholz [2] (lsd. még [50]) logaritmikus lineáris formákra vonatkozó becslését használva a (33) bal oldalán szereplő logaritmikus formára az

$$\exp(-C_3 \log H_2) \geq \exp(-C_3 \log H)$$

alsó korlátot kapjuk.

Ezt a kapott felső korláttal egybevetve

$$\exp(-C_3 \log H) < 2c_4 \cdot \exp\left(-\frac{c_3}{2} \cdot H_1\right)$$

adódik, amiből

$$H_1 < \frac{2}{c_3} (\log(2c_4) + C_3 \log H).$$

Hasonló módon ha $D < c_6 E_2$, akkor felhasználva a (30)-ból kapható

$$\begin{aligned} &\left| \log |\rho_1^{**}| + e_1 \log |\varepsilon_1^{**}| - e_3 \log |\varepsilon_3^{**}| + \sum_{j \in I} d_j \log \left| \frac{\pi_{j1k_{j1}}^{**}}{\pi_{j3k_{j3}}^{**}} \right| \right| \\ &< 2c_4 \cdot \exp\left(-\frac{c_3}{2} \cdot H_2\right) \end{aligned} \quad (34)$$

egyenlőtlenséget hasonló felső becslés adódik H_2 -re is.

Ez azt jelenti, hogy minden esetet figyelve alkalmas C'_4, C''_4 konstansokkal $H_1 < C'_4 \log H$, $H_2 < C''_4 \log H$ teljesül, azaz $C_4 = \max(C'_4, C''_4)$ -vel $H < C_4 \log H$, ami egy felső korlátot eredményez H -ra. Jelöljük ezt a korlátot H_0 -lal.

4.7. A K feletti S-egység egyenlet megoldása: redukció

A következőkben a 4.6. részben kapott H_0 felső korlátot fogjuk redukálni.

A (26) egyenlőség alapján

$$\begin{aligned} & hd_j + \text{ord}_{p_j}(\rho_1) \\ &= \text{ord}_{p_j} \left(\log_{p_j} \rho_2 + e_2 \log_{p_j} \varepsilon_2 - e_3 \log_{p_j} \varepsilon_3 + \sum_{j \in I} d_j \log_{p_j} \left(\frac{\pi_j 2^{k_{j2}}}{\pi_j 3^{k_{j3}}} \right) \right) \end{aligned}$$

adódik. Felhasználva, hogy $D \leq H < H_0$, alkalmazzuk minden $j \in I$ esetén a 4.3.1. lemmát. Ezzel D -re egy D_R redukált korlátot kapunk, amely sokkal kisebb, mint H_0 .

A redukciónál is ugyanúgy szét kell választanunk az eseteket, mint tettük azt a felső korlát meghatározásakor. Ha $c_6 E_1 \leq D$, akkor (31)-hez hasonlóan azt kapjuk, hogy D_R/c_6 felső korlát H_1 -re. Hasonlóan $c_6 E_2 \leq D$ esetén D_R/c_6 felső korlát H_2 -re.

A további esetekben a redukció elvégzéséhez szükségünk lesz a következő lemmára, mely megtalálható [11]-ben (Lemma 2.2.2.). Itt egy számunkra szükséges kis módosítással közöljük, melynek a bizonyítása szóról-szóra megegyezik az eredetiével.

4.7.1. LEMMA *Tekintsük az*

$$|x_1 \vartheta_1 + \dots + x_n \vartheta_n| < d_1 \exp(-d_2 Y - d_3)$$

egyenlőtlenséget, ahol $\vartheta_1, \dots, \vartheta_n$ adott komplex számok, melyek lineárisan függetlenek $\mathbb{Q}$ felett, d_1, d_2, d_3 adott pozitív konstansok, $x_1, \dots, x_n \in \mathbb{Z}$, $Y > 0$ és $X = \max(|x_1|, \dots, |x_n|)$. Legyen S egy adott konstans és $\mathcal{L}$ a

következő $(n+2) \times n$ -es mátrix oszlopvektorai által kifeszített rács

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \\ S\Re(\vartheta_1) & S\Re(\vartheta_2) & \dots & S\Re(\vartheta_n) \\ S\Im(\vartheta_1) & S\Im(\vartheta_2) & \dots & S\Im(\vartheta_n) \end{pmatrix}.$$

(Jegyezzük meg, hogy ha $\vartheta_1, \dots, \vartheta_n \in \mathbb{R}$, akkor a mátrix utolsó sora elhagyható.) Jelöljük b_1 -gyel a rács LLL-redukált bázisának első vektorát.

Ha $X \leq X_0$ és $\|b_1\| \geq \sqrt{(n+1)2^{n-1}} \cdot X_0$, akkor

$$Y \leq \frac{\log S + \log d_1 - d_3 - \log X_0}{d_2}.$$

A lemma alkalmazásakor az S konstans úgy kell megválasztani, hogy a lemma jelölései mellett X_0^n nagyságrendű legyen.

Ha $D < c_6 E_1$, akkor a $H_2 < H_0$ egyenlőtlenséget kihasználva és a lemmát (33)-ra alkalmazva kapunk egy új felső korlátot H_1 -re. Hasonlóan $D < c_6 E_2$ esetén $H_1 < H_0$ alapján a lemmát (34)-re alkalmazva kapunk egy felső korlátot H_2 -re.

A fentiek azt jelentik, hogy minden eshetőség mellett kapunk egy új felső korlátot H_1 -re és H_2 -re, ami alapján H -ra is adódik egy új, redukált korlát.

Ekkor a H -ra kapott új felső korlátot H_0 helyére írva a redukciót megismételjük mindaddig, amíg ezzel H_0 -at csökkenteni tudjuk.

A redukció során a felső korlát rendszerint 3-5 lépésben csökkenthető, a redukció pedig elég hatékony, hiszen az első lépésben a felső korlátot annak logaritmusaival egyező nagyságrendű új korlátra redukálja.

Ezek után az így nyert végső korlát alatti értékeket végigvizsgáljuk, hogy melyek eredményeznek valójában megoldást az eredeti egyenletünkre.

4.8. Az algoritmus

Mielőtt ismertetnénk a módszerünkkel megoldott néhány példát, röviden áttekintjük az előző részekben részletesen tárgyalt eljárás fő lépéseit.

input: Egy K bikvadratikus számtest és $p_1, \dots, p_s$ különböző prímszámok.

output: A bikvadratikus számtest megfelelő egész bázisához tartozó index formával felírt (11) p -adikus index forma egyenlet összes megoldása.

1. Megoldjuk a (20) $\mathbb{Z}$ feletti S -egység egyenletet a 4.3. részben leírtak szerint. Először a p -adikus logaritmusok lineáris formáira vonatkozó becslést használva nyerünk egy nagy felső korlátot az ismeretlen kitevőkre (példáinkban ez a korlát $10^{18} - 10^{28}$ nagyságrendű). Ezután redukciós eljárással redukáljuk ezt a felső korlátot (példáinkban a redukció után adódó korlát 5 és 23 közti volt).
2. Meghatározzuk a (16) előállításnak megfelelően az F_1, F_2, F_3 -ban szereplő $p_1^{a_1} \cdot \dots \cdot p_s^{a_s}$ közös tényezőt. Ez azáltal tehető meg, hogy a 4.4. részben ismertetett állítások szerint az esetek jelentős részében az $a_1, \dots, a_s$ kitevők csak kicsi értékeket vehetnek fel. A kivételes eset akkor áll elő, ha a p_i prímek közt van olyan, mely K mindegyik másodfokú résztestében két különböző prímideál szorzatára esik szét.
3. Ha valamelyik p_i prímszám K mindegyik másodfokú résztestében két különböző prímideál szorzatára esik szét, akkor az $a_1, \dots, a_s$ kitevők meghatározásához a 4.5., 4.6. és 4.7. részek alapján meg kell még oldanunk egy S -egység egyenletet K felett is (példáink közül a harmadik tartozik ebbe az esetbe). Ehhez először p -adikus és komplex logaritmusok lineáris formáira vonatkozó becsléseket használunk (ezzel példánkban a fellépő kitevőkre 10^{32} adódik felső korlátként), majd a p -adikus és a komplex becsléssel adódó felső korlátokat redukciós eljárások ismételt alkalmazásával tudjuk csökkenteni (példánkban 28 lett a redukált korlát).
4. Az összes így nyert F_1, F_2, F_3 értékre megoldjuk a (13) egyenletrendszert, méghozzá teljesen valós esetben szimultán Pell-egyenletek megoldására visszavezetve, teljesen komplex esetben pedig a definit bal oldalú egyenletből kiindulva. Végül az így nyert x, y, z értékekből meghatározzuk az eredeti egyenlet megoldásait.

4.9. Első példa: egy teljesen komplex bikvadratikus test

Tekintsük a $K = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$ testet. Jelöléseink mellett most $m = m_1 = 3$, $n = n_1 = -1$, $l = 1$, K pedig az 5. esethez tartozó teljesen komplex bikvadratikus számtest.

Jelölje $I(x_2, x_3, x_4)$ az 5. esethez tartozó megfelelő index formát, a (11) jobb oldalán szereplő prímekek pedig legyenek $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$.

Ekkor az

$$I(x_2, x_3, x_4) = \pm 2^{t_1} \cdot 3^{t_2} \cdot 5^{t_3} \cdot 7^{t_4} \quad (35)$$

$$x_2, x_3, x_4 \in \mathbb{Z}, \text{ lno}(x_2, x_3, x_4) = 1, \quad 0 \leq t_1, t_2, t_3, t_4 \in \mathbb{Z}$$

egyenletet fogjuk megoldani.

Esetünkben az index forma tényezőinek F_1, F_2, F_3 abszolút értékére (15) szerint

$$\pm 3F_1 \pm F_2 = \pm 4F_3 \quad (36)$$

áll fenn, ahonnan

$$F_1 = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 7^{\alpha_4}, F_2 = 2^{\beta_1} \cdot 3^{\beta_2} \cdot 5^{\beta_3} \cdot 7^{\beta_4}, F_3 = 2^{\gamma_1} \cdot 3^{\gamma_2} \cdot 5^{\gamma_3} \cdot 7^{\gamma_4}$$

jelölésekkel

$$\pm 2^{\alpha_1} \cdot 3^{\alpha_2+1} \cdot 5^{\alpha_3} \cdot 7^{\alpha_4} \pm 2^{\beta_1} \cdot 3^{\beta_2} \cdot 5^{\beta_3} \cdot 7^{\beta_4} = \pm 2^{\gamma_1+2} \cdot 3^{\gamma_2} \cdot 5^{\gamma_3} \cdot 7^{\gamma_4}$$

adódik.

A primitív megoldások keresésekor $K. Yu$ [54] tételét alkalmazva a kitevők felső korlátjaként 10^{23} kapható (2 kitevőire 10^{23} , 3,5,7 kitevőire 10^{21}). Ezt a 4.3.1. lemma segítségével a következőképpen lehet redukálni:

lépés	$H <$	$\ b_1\ >$	μ	új korlát
<i>I.</i>	10^{23}	$0,347 \cdot 10^{24}$	240	241
<i>II.</i>	241	835	30	31
<i>III.</i>	31	108	24	25
<i>IV.</i>	25	87	21	22
<i>V.</i>	$22, p = 2$	77	20	21
<i>V.</i>	$22, p = 3$	77	13	13
<i>V.</i>	$22, p = 5$	77	9	9
<i>V.</i>	$22, p = 7$	77	9	9

A (36) $\mathbb{Z}$ feletti S-egység egyenletnek 375 darab f_1, f_2, f_3 primitív megoldása adódik. Az összes megoldás ezekből $F_1 = f_1 \cdot 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4}$, $F_2 = f_2 \cdot 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4}$, $F_3 = f_3 \cdot 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4}$ ($0 \leq a_1, a_2, a_3, a_4 \in \mathbb{Z}$) alakban áll elő.

K másodfokú résztestei $M_1 = \mathbb{Q}(\sqrt{-1})$, $M_2 = \mathbb{Q}(\sqrt{3})$, $M_3 = \mathbb{Q}(\sqrt{-3})$. A 2 által generált ideál egy prímeál négyzete M_1 , M_2 -ben és prímeál M_3 -ban, a 3 által generált ideál prímeál M_1 -ben és prímeál négyzete M_2 , M_3 -ban, az 5 által generált ideál prímeál M_2 -ben és M_3 -ban, a 7 által generált ideál pedig prímeál M_1 -ben és M_2 -ben. Ekkor a 4.4.2. lemma segítségével $a_1 \leq 4$, $a_2 = a_3 = a_4 = 0$ adódik. Az így szóba jövő $375 \cdot 5 = 1875$ darab F_1, F_2, F_3 értéket a 3.4. részben leírt, az index forma valamelyik tényezőjének definittségét kihasználó módszerrel vizsgálhatjuk végig.

Végül az adódik, hogy (35)-nek a következő 276 darab megoldása van. (Jegyezzük meg, hogy ha (x_2, x_3, x_4) megoldást szolgáltat, akkor ugyanazzal a jobb oldallal $(-x_2, -x_3, -x_4)$ is, ezért közülük csak az egyiket soroljuk fel.)

x_2	x_3	x_4	index	felbontás
0	1	0	1	1
-1	1	0	1	1
-1	2	1	1	1
1	-2	1	1	1
0	1	1	4	2^2
1	-1	1	4	2^2
-1	1	1	4	2^2
0	-1	1	4	2^2
0	2	1	20	$2^2 \cdot 3^1$
2	-2	1	20	$2^2 \cdot 3^1$
-2	2	1	20	$2^2 \cdot 3^1$
0	-2	1	20	$2^2 \cdot 3^1$
-1	3	0	27	3^3
-2	3	0	27	3^3
-1	2	2	32	2^5
1	-2	2	32	2^5
-1	3	1	36	$2^2 \cdot 3^2$
2	-3	1	36	$2^2 \cdot 3^2$
-2	3	1	36	$2^2 \cdot 3^2$
1	-3	1	36	$2^2 \cdot 3^2$
1	0	1	45	$3^2 \cdot 5^1$
-1	0	1	45	$3^2 \cdot 5^1$
-1	3	2	45	$3^2 \cdot 5^1$
2	-3	2	45	$3^2 \cdot 5^1$
-2	3	2	45	$3^2 \cdot 5^1$
1	-3	2	45	$3^2 \cdot 5^1$
1	1	0	63	$3^2 \cdot 7^1$
-2	1	0	63	$3^2 \cdot 7^1$
1	1	1	140	$2^2 \cdot 5^1 \cdot 7^1$
2	-1	1	140	$2^2 \cdot 5^1 \cdot 7^1$
-2	1	1	140	$2^2 \cdot 5^1 \cdot 7^1$
-1	-1	1	140	$2^2 \cdot 5^1 \cdot 7^1$
-2	5	3	140	$2^2 \cdot 5^1 \cdot 7^1$
3	-5	3	140	$2^2 \cdot 5^1 \cdot 7^1$
-3	5	3	140	$2^2 \cdot 5^1 \cdot 7^1$
2	-5	3	140	$2^2 \cdot 5^1 \cdot 7^1$

x_2	x_3	x_4	index	felbontás
-2	5	0	175	$5^2 \cdot 7^1$
-3	5	0	175	$5^2 \cdot 7^1$
-1	4	2	224	$2^5 \cdot 7^1$
3	-4	2	224	$2^5 \cdot 7^1$
-3	4	2	224	$2^5 \cdot 7^1$
1	-4	2	224	$2^5 \cdot 7^1$
1	0	2	288	$2^5 \cdot 3^2$
-1	0	2	288	$2^5 \cdot 3^2$
-1	4	0	448	$2^6 \cdot 7^1$
-3	4	0	448	$2^6 \cdot 7^1$
-1	3	3	540	$2^2 \cdot 3^3 \cdot 5^1$
2	-3	3	540	$2^2 \cdot 3^3 \cdot 5^1$
-2	3	3	540	$2^2 \cdot 3^3 \cdot 5^1$
1	-3	3	540	$2^2 \cdot 3^3 \cdot 5^1$
0	3	1	540	$2^2 \cdot 3^3 \cdot 5^1$
3	-3	1	540	$2^2 \cdot 3^3 \cdot 5^1$
-3	3	1	540	$2^2 \cdot 3^3 \cdot 5^1$
0	-3	1	540	$2^2 \cdot 3^3 \cdot 5^1$
-3	6	2	864	$2^5 \cdot 3^3$
3	-6	2	864	$2^5 \cdot 3^3$
-4	9	0	1701	$3^5 \cdot 7^1$
-5	9	0	1701	$3^5 \cdot 7^1$
-3	6	4	1728	$2^6 \cdot 3^3$
3	-6	4	1728	$2^6 \cdot 3^3$
1	0	4	2880	$2^6 \cdot 3^2 \cdot 5^1$
-1	0	4	2880	$2^6 \cdot 3^2 \cdot 5^1$
-1	4	4	4480	$2^7 \cdot 5^1 \cdot 7^1$
3	-4	4	4480	$2^7 \cdot 5^1 \cdot 7^1$
-3	4	4	4480	$2^7 \cdot 5^1 \cdot 7^1$
1	-4	4	4480	$2^7 \cdot 5^1 \cdot 7^1$
1	3	0	4725	$3^3 \cdot 5^2 \cdot 7^1$
-4	3	0	4725	$3^3 \cdot 5^2 \cdot 7^1$
-1	6	3	4725	$3^3 \cdot 5^2 \cdot 7^1$
5	-6	3	4725	$3^3 \cdot 5^2 \cdot 7^1$
-5	6	3	4725	$3^3 \cdot 5^2 \cdot 7^1$
1	-6	3	4725	$3^3 \cdot 5^2 \cdot 7^1$

x_2	x_3	x_4	index	felbontás
-6	12	7	5292	$2^2 \cdot 3^3 \cdot 7^2$
6	-12	7	5292	$2^2 \cdot 3^3 \cdot 7^2$
-5	10	6	7200	$2^5 \cdot 3^2 \cdot 5^2$
5	-10	6	7200	$2^5 \cdot 3^2 \cdot 5^2$
-1	6	4	8064	$2^7 \cdot 3^2 \cdot 7^1$
5	-6	4	8064	$2^7 \cdot 3^2 \cdot 7^1$
-5	6	4	8064	$2^7 \cdot 3^2 \cdot 7^1$
1	-6	4	8064	$2^7 \cdot 3^2 \cdot 7^1$
2	0	3	8100	$2^2 \cdot 3^4 \cdot 5^2$
-2	0	3	8100	$2^2 \cdot 3^4 \cdot 5^2$
-1	6	2	10080	$2^5 \cdot 3^2 \cdot 5^1 \cdot 7^1$
5	-6	2	10080	$2^5 \cdot 3^2 \cdot 5^1 \cdot 7^1$
-5	6	2	10080	$2^5 \cdot 3^2 \cdot 5^1 \cdot 7^1$
1	-6	2	10080	$2^5 \cdot 3^2 \cdot 5^1 \cdot 7^1$
-4	9	3	11340	$2^2 \cdot 3^4 \cdot 5^1 \cdot 7^1$
5	-9	3	11340	$2^2 \cdot 3^4 \cdot 5^1 \cdot 7^1$
-5	9	3	11340	$2^2 \cdot 3^4 \cdot 5^1 \cdot 7^1$
4	-9	3	11340	$2^2 \cdot 3^4 \cdot 5^1 \cdot 7^1$
-1	6	0	12096	$2^6 \cdot 3^3 \cdot 7^1$
-5	6	0	12096	$2^6 \cdot 3^3 \cdot 7^1$
3	2	0	12544	$2^8 \cdot 7^2$
-5	2	0	12544	$2^8 \cdot 7^2$
-7	14	8	12544	$2^8 \cdot 7^2$
7	-14	8	12544	$2^8 \cdot 7^2$
1	0	6	12960	$2^5 \cdot 3^4 \cdot 5^1$
-1	0	6	12960	$2^5 \cdot 3^4 \cdot 5^1$
3	0	2	12960	$2^5 \cdot 3^4 \cdot 5^1$
-3	0	2	12960	$2^5 \cdot 3^4 \cdot 5^1$
-9	18	10	194400	$2^5 \cdot 3^5 \cdot 5^2$
9	-18	10	194400	$2^5 \cdot 3^5 \cdot 5^2$
3	9	5	283500	$2^2 \cdot 3^4 \cdot 5^3 \cdot 7^1$
12	-9	5	283500	$2^2 \cdot 3^4 \cdot 5^3 \cdot 7^1$
-12	9	5	283500	$2^2 \cdot 3^4 \cdot 5^3 \cdot 7^1$
-3	-9	5	283500	$2^2 \cdot 3^4 \cdot 5^3 \cdot 7^1$

x_2	x_3	x_4	index	felbontás
-3	12	8	302400	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7^1$
9	-12	8	302400	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7^1$
-9	12	8	302400	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7^1$
3	-12	8	302400	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7^1$
-11	24	0	338688	$2^8 \cdot 3^3 \cdot 7^2$
-13	24	0	338688	$2^8 \cdot 3^3 \cdot 7^2$
1	0	14	352800	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7^2$
-1	0	14	352800	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7^2$
7	0	2	352800	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7^2$
-7	0	2	352800	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7^2$
-11	24	14	352800	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7^2$
13	-24	14	352800	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7^2$
-13	24	14	352800	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7^2$
11	-24	14	352800	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7^2$
3	0	8	518400	$2^8 \cdot 3^4 \cdot 5^2$
-3	0	8	518400	$2^8 \cdot 3^4 \cdot 5^2$
2	9	9	5953500	$2^2 \cdot 3^5 \cdot 5^3 \cdot 7^2$
11	-9	9	5953500	$2^2 \cdot 3^5 \cdot 5^3 \cdot 7^2$
-11	9	9	5953500	$2^2 \cdot 3^5 \cdot 5^3 \cdot 7^2$
-2	-9	9	5953500	$2^2 \cdot 3^5 \cdot 5^3 \cdot 7^2$
21	14	8	30732800	$2^9 \cdot 5^2 \cdot 7^4$
35	-14	8	30732800	$2^9 \cdot 5^2 \cdot 7^4$
-35	14	8	30732800	$2^9 \cdot 5^2 \cdot 7^4$
-21	-14	8	30732800	$2^9 \cdot 5^2 \cdot 7^4$
12	0	7	39690000	$2^4 \cdot 3^4 \cdot 5^4 \cdot 7^2$
-12	0	7	39690000	$2^4 \cdot 3^4 \cdot 5^4 \cdot 7^2$
-1	20	0	44452800	$2^6 \cdot 3^4 \cdot 5^2 \cdot 7^3$
-19	20	0	44452800	$2^6 \cdot 3^4 \cdot 5^2 \cdot 7^3$
-17	54	0	1200225600	$2^6 \cdot 3^7 \cdot 5^2 \cdot 7^3$
-37	54	0	1200225600	$2^6 \cdot 3^7 \cdot 5^2 \cdot 7^3$
7	0	48	2540160000	$2^{10} \cdot 3^4 \cdot 5^4 \cdot 7^2$
-7	0	48	2540160000	$2^{10} \cdot 3^4 \cdot 5^4 \cdot 7^2$

4.10. Második példa: egy teljesen valós bikvadratikus test

Következő példaként vegyük a $K = \mathbb{Q}(\sqrt{5}, \sqrt{2})$ teljesen valós bikvadratikus számtestet. Korábbi jelöléseink szerint $m = m_1 = 5$, $n = n_1 = 2$, $l = 1$ és K a 3. esethez tartozik.

Ha a megfelelő index forma $I(x_2, x_3, x_4)$, a (11) jobb oldalán álló prímszámok pedig $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, akkor az

$$I(x_2, x_3, x_4) = \pm 2^{t_1} \cdot 3^{t_2} \cdot 5^{t_3} \quad (37)$$

$$x_2, x_3, x_4 \in \mathbb{Z}, \text{ lko}(x_2, x_3, x_4) = 1, \quad 0 \leq t_1, t_2, t_3 \in \mathbb{Z}$$

egyenletet kapjuk.

(15) szerint ennél a példánál $I(x_2, x_3, x_4)$ tényezőinek F_1, F_2, F_3 abszolút értékére

$$\pm 5F_1 \pm 8F_2 = \pm F_3 \quad (38)$$

teljesül, amiből az

$$F_1 = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3}, F_2 = 2^{\beta_1} \cdot 3^{\beta_2} \cdot 5^{\beta_3}, F_3 = 2^{\gamma_1} \cdot 3^{\gamma_2} \cdot 5^{\gamma_3}$$

jelölésekkel a

$$\pm 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3+1} \pm 2^{\beta_1+3} \cdot 3^{\beta_2} \cdot 5^{\beta_3} = \pm 2^{\gamma_1} \cdot 3^{\gamma_2} \cdot 5^{\gamma_3}$$

egyenletet kapjuk.

A primitív megoldások keresésekor K . Yu [54] tétele alapján a kitevőkre 10^{18} adódik felső korlátként (2 kitevőre 10^{18} , 3 és 5 kitevőre 10^{17}), amit a 4.3.1. lemma segítségével a következőképpen redukálhatunk:

lépés	$H <$	$\ b_1\ >$	μ	új korlát
<i>I.</i>	10^{18}	$0, 2 \cdot 10^{19}$	125	126
<i>II.</i>	126	252	17	18
<i>III.</i>	$18, p = 2$	36	11	12
<i>III.</i>	$18, p = 3$	36	8	8
<i>III.</i>	$18, p = 5$	36	5	5

Ez alapján a (38) $\mathbb{Z}$ feletti S-egység egyenletnek 99 darab f_1, f_2, f_3 primitív megoldása adódik. Az összes megoldás ezekből $F_1 = f_1 \cdot 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$, $F_2 = f_2 \cdot 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$, $F_3 = f_3 \cdot 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$ alakban áll elő, ahol $0 \leq a_1, a_2, a_3 \in \mathbb{Z}$.

K másodfokú résztestei $M_1 = \mathbb{Q}(\sqrt{2})$, $M_2 = \mathbb{Q}(\sqrt{5})$, $M_3 = \mathbb{Q}(\sqrt{10})$. Ekkor a 2 által generált ideál egy prímeál négyzete M_1 , M_3 -ban és prímeál M_2 -ben, a 3 által generált ideál prímeál M_1 , M_2 -ben, míg az 5 által generált ideál prímeál M_1 -ben és prímeál négyzete M_2 , M_3 -ban. Ezért a 4.4.2. lemma alapján $a_1 \leq 5$, $a_2 = a_3 = 0$ kapható. A lehetséges $99 \cdot 6 = 594$ darab F_1, F_2, F_3 értéket Gaál I., Pethő A. és M. Pohst [21] módszerével, szimultán Pell-egyenleteket megoldva nézzük végig.

A (37) egyenletnek összesen 280 darab megoldása adódik, melyek a következők (akárcsak az előző példánál ha (x_2, x_3, x_4) megoldást szolgáltat, akkor ugyanazzal a jobb oldallal $(-x_2, -x_3, -x_4)$ is, ezért csak az egyiket soroljuk fel):

x_2	x_3	x_4	index	felbontás
1	-1	1	3	3^1
-1	-1	1	3	3^1
1	0	1	3	3^1
-1	0	1	3	3^1
7	-8	5	3	3^1
7	3	5	3	3^1
-7	3	5	3	3^1
-7	-8	5	3	3^1
-1	1	0	3	3^1
1	1	0	3	3^1
2	1	1	4	2^2
0	-1	1	4	2^2
0	0	1	4	2^2
-2	-2	1	4	2^2
2	-2	1	4	2^2
-2	1	1	4	2^2
0	-2	1	36	$2^2 \cdot 3^2$
2	0	1	36	$2^2 \cdot 3^2$
2	-1	1	36	$2^2 \cdot 3^2$
-2	0	1	36	$2^2 \cdot 3^2$
-2	-1	1	36	$2^2 \cdot 3^2$
0	1	1	36	$2^2 \cdot 3^2$
4	2	3	36	$2^2 \cdot 3^2$
-4	2	3	36	$2^2 \cdot 3^2$
4	-5	3	36	$2^2 \cdot 3^2$
-4	-5	3	36	$2^2 \cdot 3^2$
2	1	2	48	$2^4 \cdot 3^1$
-2	1	0	48	$2^4 \cdot 3^1$
2	1	0	48	$2^4 \cdot 3^1$
-2	-3	2	48	$2^4 \cdot 3^1$
-2	1	2	48	$2^4 \cdot 3^1$
2	-3	2	48	$2^4 \cdot 3^1$
-3	-4	2	108	$2^2 \cdot 3^3$
-3	2	2	108	$2^2 \cdot 3^3$
3	-4	2	108	$2^2 \cdot 3^3$
3	2	2	108	$2^2 \cdot 3^3$
1	2	0	108	$2^2 \cdot 3^3$
-1	2	0	108	$2^2 \cdot 3^3$

x_2	x_3	x_4	index	felbontás
-3	-4	3	225	$3^2 \cdot 5^2$
3	1	3	225	$3^2 \cdot 5^2$
-3	1	3	225	$3^2 \cdot 5^2$
3	-4	3	225	$3^2 \cdot 5^2$
3	-1	2	225	$3^2 \cdot 5^2$
-3	-1	2	225	$3^2 \cdot 5^2$
1	2	1	225	$3^2 \cdot 5^2$
1	-3	1	225	$3^2 \cdot 5^2$
-1	2	1	225	$3^2 \cdot 5^2$
-1	-3	1	225	$3^2 \cdot 5^2$
41	-47	29	225	$3^2 \cdot 5^2$
41	18	29	225	$3^2 \cdot 5^2$
-41	18	29	225	$3^2 \cdot 5^2$
-41	-47	29	225	$3^2 \cdot 5^2$
0	1	2	256	2^8
0	-3	2	256	2^8
48	21	34	256	2^8
-48	-55	34	256	2^8
-48	21	34	256	2^8
48	-55	34	256	2^8
-4	-4	3	300	$2^2 \cdot 3^1 \cdot 5^2$
2	2	1	300	$2^2 \cdot 3^1 \cdot 5^2$
-2	-3	1	300	$2^2 \cdot 3^1 \cdot 5^2$
-2	2	1	300	$2^2 \cdot 3^1 \cdot 5^2$
2	-3	1	300	$2^2 \cdot 3^1 \cdot 5^2$
4	1	3	300	$2^2 \cdot 3^1 \cdot 5^2$
4	-4	3	300	$2^2 \cdot 3^1 \cdot 5^2$
-4	1	3	300	$2^2 \cdot 3^1 \cdot 5^2$
-4	1	2	384	$2^7 \cdot 3^1$
4	-3	2	384	$2^7 \cdot 3^1$
4	1	2	384	$2^7 \cdot 3^1$
-4	-3	2	384	$2^7 \cdot 3^1$
6	3	4	400	$2^4 \cdot 5^2$
-6	3	4	400	$2^4 \cdot 5^2$
-6	-7	4	400	$2^4 \cdot 5^2$
6	-7	4	400	$2^4 \cdot 5^2$
-2	-1	2	400	$2^4 \cdot 5^2$
2	-1	2	400	$2^4 \cdot 5^2$

x_2	x_3	x_4	index	felbontás
0	2	1	500	$2^2 \cdot 5^3$
0	-3	1	500	$2^2 \cdot 5^3$
-10	4	7	500	$2^2 \cdot 5^3$
10	-11	7	500	$2^2 \cdot 5^3$
10	4	7	500	$2^2 \cdot 5^3$
-10	-11	7	500	$2^2 \cdot 5^3$
4	3	0	1152	$2^7 \cdot 3^2$
-4	3	0	1152	$2^7 \cdot 3^2$
-4	1	0	1152	$2^7 \cdot 3^2$
4	1	0	1152	$2^7 \cdot 3^2$
-12	-13	8	1152	$2^7 \cdot 3^2$
-12	5	8	1152	$2^7 \cdot 3^2$
12	-13	8	1152	$2^7 \cdot 3^2$
12	5	8	1152	$2^7 \cdot 3^2$
5	4	0	1200	$2^4 \cdot 3^1 \cdot 5^2$
-5	4	0	1200	$2^4 \cdot 3^1 \cdot 5^2$
-8	-9	6	2304	$2^8 \cdot 3^2$
-8	3	6	2304	$2^8 \cdot 3^2$
8	-9	6	2304	$2^8 \cdot 3^2$
8	3	6	2304	$2^8 \cdot 3^2$
-4	-1	2	3200	$2^7 \cdot 5^2$
4	-1	2	3200	$2^7 \cdot 5^2$
0	-4	3	4500	$2^2 \cdot 3^2 \cdot 5^3$
0	1	3	4500	$2^2 \cdot 3^2 \cdot 5^3$
-4	3	4	9600	$2^7 \cdot 3^1 \cdot 5^2$
-4	-7	4	9600	$2^7 \cdot 3^1 \cdot 5^2$
4	3	4	9600	$2^7 \cdot 3^1 \cdot 5^2$
4	-7	4	9600	$2^7 \cdot 3^1 \cdot 5^2$
6	5	0	18000	$2^4 \cdot 3^2 \cdot 5^3$
-6	5	0	18000	$2^4 \cdot 3^2 \cdot 5^3$
-14	5	10	18000	$2^4 \cdot 3^2 \cdot 5^3$
-14	-15	10	18000	$2^4 \cdot 3^2 \cdot 5^3$
14	5	10	18000	$2^4 \cdot 3^2 \cdot 5^3$
14	-15	10	18000	$2^4 \cdot 3^2 \cdot 5^3$
2	5	0	18000	$2^4 \cdot 3^2 \cdot 5^3$
-2	5	0	18000	$2^4 \cdot 3^2 \cdot 5^3$

x_2	x_3	x_4	index	felbontás
8	3	4	19200	$2^8 \cdot 3^1 \cdot 5^2$
8	-7	4	19200	$2^8 \cdot 3^1 \cdot 5^2$
-8	-7	4	19200	$2^8 \cdot 3^1 \cdot 5^2$
-8	3	4	19200	$2^8 \cdot 3^1 \cdot 5^2$
0	3	4	32000	$2^8 \cdot 5^3$
0	-7	4	32000	$2^8 \cdot 5^3$
4	5	0	48000	$2^7 \cdot 3^1 \cdot 5^3$
-4	5	0	48000	$2^7 \cdot 3^1 \cdot 5^3$
0	-13	8	82944	$2^{10} \cdot 3^4$
0	5	8	82944	$2^{10} \cdot 3^4$
24	-29	18	115200	$2^9 \cdot 3^2 \cdot 5^2$
24	11	18	115200	$2^9 \cdot 3^2 \cdot 5^2$
-24	-29	18	115200	$2^9 \cdot 3^2 \cdot 5^2$
-24	11	18	115200	$2^9 \cdot 3^2 \cdot 5^2$
8	-3	6	115200	$2^9 \cdot 3^2 \cdot 5^2$
-8	-3	6	115200	$2^9 \cdot 3^2 \cdot 5^2$
8	5	0	192000	$2^9 \cdot 3^1 \cdot 5^3$
-8	5	0	192000	$2^9 \cdot 3^1 \cdot 5^3$
-28	15	20	2160000	$2^7 \cdot 3^3 \cdot 5^4$
28	-35	20	2160000	$2^7 \cdot 3^3 \cdot 5^4$
28	15	20	2160000	$2^7 \cdot 3^3 \cdot 5^4$
-28	-35	20	2160000	$2^7 \cdot 3^3 \cdot 5^4$
-16	5	0	6912000	$2^{11} \cdot 3^3 \cdot 5^3$
16	5	0	6912000	$2^{11} \cdot 3^3 \cdot 5^3$
0	-29	18	10368000	$2^{10} \cdot 3^4 \cdot 5^3$
0	11	18	10368000	$2^{10} \cdot 3^4 \cdot 5^3$
32	25	0	76800000	$2^{13} \cdot 3^1 \cdot 5^5$
-32	25	0	76800000	$2^{13} \cdot 3^1 \cdot 5^5$

4.11. Harmadik példa: egy teljesen valós bikvadratikus test, amikor bonyolultabb a megoldás

Utolsó példaként tekintsük a $K = \mathbb{Q}(\sqrt{19}, \sqrt{7})$ teljesen valós bikvadratikus számtestet. Korábbi jelöléseinkkel ennél a példánál $m = m_1 = 19$, $n = n_1 = 7$, $l = 1$, a test pedig az 5. esethez tartozik.

Legyen a megfelelő, 5. esetbeli index forma $I(x_2, x_3, x_4)$, a (11) jobb oldalán álló prímek pedig legyenek $p_1 = 2$, $p_2 = 3$. Ekkor

$$I(x_2, x_3, x_4) = \pm 2^{t_1} \cdot 3^{t_2} \quad (39)$$

$$x_2, x_3, x_4 \in \mathbb{Z}, \text{ lno}(x_2, x_3, x_4) = 1, \quad 0 \leq t_1, t_2 \in \mathbb{Z}$$

lesz a megoldandó egyenletünk.

Az index forma tényezőinek F_1, F_2, F_3 abszolút értékeire (15) szerint

$$\pm 19F_1 \pm 7F_2 = \pm 4F_3 \quad (40)$$

áll fenn, amiből az

$$F_1 = 2^{\alpha_1} \cdot 3^{\alpha_2}, F_2 = 2^{\beta_1} \cdot 3^{\beta_2}, F_3 = 2^{\gamma_1} \cdot 3^{\gamma_2}$$

jelölésekkel a

$$\pm 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 7^{\alpha_3} \cdot 19^{\alpha_4} \pm 2^{\beta_1} \cdot 3^{\beta_2} \cdot 7^{\beta_3} \cdot 19^{\beta_4} = \pm 2^{\gamma_1+2} \cdot 3^{\gamma_2} \cdot 7^{\gamma_3} \cdot 19^{\gamma_4}$$

egyenletet kapjuk. Itt a (39) egyenletben szereplő prímekhez hozzávettük a (40) együtthatóiban előforduló prímszámokat, a 7-et és a 19-et is, odafigyelve arra, hogy végül majd csak azokat a megoldásokat kell figyelembe vennünk, melyeknél $\alpha_4 = \beta_3 = 1$ és $\alpha_3 = \beta_4 = \gamma_3 = \gamma_4 = 0$.

K . Yu [54] tétele szerint a kitevőkre 10^{28} adódik felső korlátként (a 2 kitevőire 10^{28} , a 3 kitevőire 10^{26}). Ezt a korlátot a 4.3.1. lemma felhasználásával a következőképpen lehet redukálni:

lépés	$H <$	$\ b_1\ >$	μ	új korlát
<i>I.</i>	10^{28}	$0,347 \cdot 10^{29}$	300	301
<i>II.</i>	301	1043	34	35
<i>III.</i>	35	122	23	24
<i>IV.</i>	$24, p = 2$	84	22	23
<i>IV.</i>	$24, p = 3$	84	16	16

Ez alapján a (40) $\mathbb{Z}$ feletti S-egység egyenletnek csak a következő hat primitív megoldása adódik:

$$(f_1, f_2, f_3) = (1, 1, 3), (3, 1, 16), (2, 6, 1), (4, 16, 9), (12, 32, 1), (4, 128, 243).$$

Az $x = x_4, y = 2x_2 + x_3, z = x_3$ jelölésekkel (22) a következő alakot ölti:

$$\begin{aligned} (7x)^2 - 7y^2 &= \pm 7 \cdot f_1 \cdot 2^{a_1} \cdot 3^{a_2} \\ (19x)^2 - 19z^2 &= \pm 19 \cdot f_2 \cdot 2^{a_1} \cdot 3^{a_2} \\ (7z)^2 - 133y^2 &= \pm 28 \cdot f_3 \cdot 2^{a_1} \cdot 3^{a_2} \end{aligned}$$

K másodfokú résztesteire vonatkozóan a következőket tudjuk: $M_1 = \mathbb{Q}(\sqrt{7})$ -ben az ideálosztályszám 1, $\varepsilon_1 = 8 + 3\sqrt{7}$ alapegység, továbbá $2 = \pi_{11}^2 \cdot (8 - 3\sqrt{7})$, ahol $\pi_{11} = 3 + \sqrt{7}$ prímelem, a másik tényező egység, illetve $3 = -\pi_{211} \cdot \pi_{212}$, ahol $\pi_{211} = 2 - \sqrt{7}$ és $\pi_{212} = 2 + \sqrt{7}$ prímelemek.

$M_2 = \mathbb{Q}(\sqrt{19})$ -ben az ideálosztályszám 1, $\varepsilon_2 = 170 + 39\sqrt{19}$ alapegység, továbbá $2 = \pi_{12}^2 \cdot (170 - 39\sqrt{19})$, ahol $\pi_{12} = 13 + 3\sqrt{19}$ prímelem, a másik tényező egység, illetve $3 = -\pi_{221} \cdot \pi_{222}$, ahol $\pi_{221} = 4 + \sqrt{19}$ és $\pi_{222} = 4 - \sqrt{19}$ prímelemek.

$M_3 = \mathbb{Q}(\sqrt{133})$ -ban az ideálosztályszám 1, $\varepsilon_3 = \frac{173-15\sqrt{133}}{2}$ alapegység, továbbá 2 prímelem, illetve $3 = -\pi_{231} \cdot \pi_{232}$, ahol $\pi_{231} = \frac{11-\sqrt{133}}{2}$ és $\pi_{232} = \frac{11+\sqrt{133}}{2}$ prímelemek.

Korábbi jelöléseinkkel $\text{ord}_2(s_3) = 2$ vagy 6, azaz bármely (f_1, f_2, f_3) hármas esetén páros. Mivel M_3 -ban 2 prímelem, ezért korábbi megjegyzésünk alapján $\text{ord}_2(s_3) + a_1$ páros, következésképpen a_1 csak páros lehet. A 4.4.2. lemma szerint $a_1 \leq 5$ adódik, így a fentiek szerint csak $a_1 = 0, 2, 4$ jöhet szóba.

A 3 viszont mindhárom másodfokú résztestben két különböző prímelem szorzata, ezért most meg kell oldanunk egy K feletti S-egység egyenletet is.

Azt kapjuk, hogy

$$7x - \sqrt{7}y = \pm \varepsilon_1^{e_1} \cdot \gamma_1 \cdot 2^{a_1/2} \cdot \pi_{21k_{21}}^{a_2} \quad (41)$$

$$19x - \sqrt{19}z = \pm \varepsilon_2^{e_2} \cdot \gamma_2 \cdot 2^{a_1/2} \cdot \pi_{22k_{22}}^{a_2} \quad (42)$$

$$7z - \sqrt{133}y = \pm \varepsilon_3^{e_3} \cdot \gamma_3 \cdot 2^{a_1/2} \cdot \pi_{23k_{23}}^{a_2} \quad (43)$$

ahol $k_{21}, k_{22}, k_{23} \in \{1, 2\}$ és $\gamma_1, \gamma_2, \gamma_3$ normája rendre $\pm 7f_1, \pm 19f_2, \pm 28f_3$.

Ismét a 4.4.2. lemmát alkalmazva az adódik, hogy a szóba jövő f_1, f_2, f_3 értékek közül a harmadik hármasnál π_{221} és π_{222} is oszthatja (42) bal oldalát legfeljebb első hatványon, illetve rendre a negyedik és hatodik hármasnál π_{231} és π_{232} is oszthatja (43) bal oldalát rendre legfeljebb első és legfeljebb második hatványon.

Eszerint a megfelelő esetekben akkor, amikor γ_2 illetve γ_3 nem osztható 3-mal (illetve 9-cel), akkor (42)-ben a lehetséges γ_2 értékek helyett a $3\gamma_2$, (43)-ban γ_3 helyett a $3\gamma_3$ (illetve $9\gamma_3$) értékeket is külön meg kell vizsgálni, még hozzá (42), (43)-ban a_2 helyett $a_2 - 2$ (illetve $a_2 - 4$) kitevőt használva. A hátralevő részben az egyszerűség kedvéért az eredetileg felírt (41), (42), (43) egyenletekkel dolgozunk.

Esetünkben a (14) egyenletből nyert (25) egyenlet a következő alakot ölti (a 2-eshez tartozó tényezők kiesnek):

$$\pm 19\varepsilon_1^{e_1} \cdot \gamma_1 \cdot \pi_{21k_{21}}^{a_2} \pm 7\varepsilon_2^{e_2} \cdot \gamma_2 \cdot \pi_{22k_{22}}^{a_2} = \pm \sqrt{19}\varepsilon_3^{e_3} \cdot \gamma_3 \cdot \pi_{23k_{23}}^{a_2},$$

azaz

$$\pm \left(\sqrt{19} \frac{\gamma_1}{\gamma_3} \right) \varepsilon_1^{e_1} \cdot \varepsilon_3^{-e_3} \cdot \left(\frac{\pi_{21k_{21}}}{\pi_{23k_{23}}} \right)^{a_2} \pm \left(\frac{7}{\sqrt{19}} \frac{\gamma_2}{\gamma_3} \right) \varepsilon_2^{e_2} \cdot \varepsilon_3^{-e_3} \cdot \left(\frac{\pi_{22k_{22}}}{\pi_{23k_{23}}} \right)^{a_2} = 1$$

(Az összes lehetséges $\gamma_1, \gamma_2, \gamma_3$ értékkel vennünk kell ezt az egyenletet.)

Megfelelő konjugálással elérhetjük, hogy

$$\text{ord}_3 \left(\frac{\pi_{21k_{21}}}{\pi_{23k_{23}}} \right) = 1.$$

Ekkor az általános esetről leírtaknak megfelelően kapjuk, hogy ha a_2 nem túl kis szám, akkor

$$\text{ord}_3 \left(\frac{7}{\sqrt{19}} \frac{\gamma_2}{\gamma_3} \right) = 0, \quad \text{ord}_3 \left(\frac{\pi_{22k_{22}}}{\pi_{23k_{23}}} \right) = 0.$$

Ezek után *K. Yu* [54] tételét alkalmazva azt kapjuk, hogy

$$a_2 < 0,65 \cdot 10^{28} \log H_1, \quad a_2 < 0,65 \cdot 10^{28} \log H_2.$$

Az $a_2 < 0,807E_i$, $a_2 \geq 0,807E_i$ ($i = 1, 2$) eseteket külön-külön vizsgálva $H < 10^{32}$ adódik.

Ezt a korlátot fogjuk a leírt eljárásokat alkalmazva redukálni. A következő táblázat a redukció lépéseinek főbb értékeit foglalja össze, a „p-adikus μ ” és a „Digits” a p-adikus, illetve a 4.7.1. lemmának megfelelő redukció pontosságára utalnak.

lépés	$H <$	p – adikus μ	Digits	új korlát H -ra
<i>I.</i>	10^{32}	400	200	445
<i>II.</i>	445	32	50	36
<i>III.</i>	36	25	30	28

Végül az összes előforduló esetre érvényes $a_2 \leq 28$, $e_1, e_2, e_3 \in [-28, 28]$ korlátokat kapjuk eredményül, illetve korábbról tudjuk, hogy $a_1 \in \{0, 2, 4\}$. Behelyettesítve az összes lehetséges kitevőt a (41), (42), (43) egyenletek jobb oldalaiba, kiszámítjuk a hozzájuk tartozó x, y, z értékeket, melyekből nyerjük x_2, x_3, x_4 -et, majd ellenőrizzük, hogy $\text{Inko}(x_2, x_3, x_4) = 1$ teljesül-e és hogy a megfelelő K -beli elemek indexének valóban csak 2 és 3 a prímosztói.

A (39) egyenletnek 104 darab megoldása adódik, melyeket a következő táblázat tartalmaz. (Mint az eddigi példákban, ha (x_2, x_3, x_4) megoldást szolgáltat, akkor ugyanazzal a jobb oldallal $(-x_2, -x_3, -x_4)$ is, de közülük csak az egyiket soroljuk fel.)

x_2	x_3	x_4	index	felbontás
0	1	0	3	3^1
-1	1	0	3	3^1
1	-5	1	12	$2^2 \cdot 3^1$
-4	5	1	12	$2^2 \cdot 3^1$
4	-5	1	12	$2^2 \cdot 3^1$
-1	5	1	12	$2^2 \cdot 3^1$
-3	4	1	81	3^4
1	-4	1	81	3^4
-1	4	1	81	3^4
3	-4	1	81	3^4
12	-61	14	81	3^4
-49	61	14	81	3^4
49	-61	14	81	3^4
-12	61	14	81	3^4
0	-1	1	324	$2^2 \cdot 3^4$
-1	1	1	324	$2^2 \cdot 3^4$
1	-1	1	324	$2^2 \cdot 3^4$
0	1	1	324	$2^2 \cdot 3^4$
-1	4	0	576	$2^6 \cdot 3^2$
-3	4	0	576	$2^6 \cdot 3^2$
0	4	1	1296	$2^4 \cdot 3^4$
4	-4	1	1296	$2^4 \cdot 3^4$
-4	4	1	1296	$2^4 \cdot 3^4$
0	-4	1	1296	$2^4 \cdot 3^4$
13	-16	4	15552	$2^6 \cdot 3^5$
-3	16	4	15552	$2^6 \cdot 3^5$
3	-16	4	15552	$2^6 \cdot 3^5$
-13	16	4	15552	$2^6 \cdot 3^5$

x_2	x_3	x_4	index	felbontás
3	-7	2	59049	3^{10}
-4	7	2	59049	3^{10}
4	-7	2	59049	3^{10}
-3	7	2	59049	3^{10}
3	-4	4	279936	$2^7 \cdot 3^7$
-1	4	4	279936	$2^7 \cdot 3^7$
1	-4	4	279936	$2^7 \cdot 3^7$
-3	4	4	279936	$2^7 \cdot 3^7$
-15	8	8	90699264	$2^9 \cdot 3^{11}$
-7	-8	8	90699264	$2^9 \cdot 3^{11}$
7	8	8	90699264	$2^9 \cdot 3^{11}$
15	-8	8	90699264	$2^9 \cdot 3^{11}$
-24	29	11	172186884	$2^2 \cdot 3^{16}$
5	-29	11	172186884	$2^2 \cdot 3^{16}$
-5	29	11	172186884	$2^2 \cdot 3^{16}$
24	-29	11	172186884	$2^2 \cdot 3^{16}$
147	-748	172	204073344	$2^7 \cdot 3^{13}$
-601	748	172	204073344	$2^7 \cdot 3^{13}$
601	-748	172	204073344	$2^7 \cdot 3^{13}$
-147	748	172	204073344	$2^7 \cdot 3^{13}$
60	-32	13	502096953744	$2^4 \cdot 3^{22}$
28	32	13	502096953744	$2^4 \cdot 3^{22}$
-28	-32	13	502096953744	$2^4 \cdot 3^{22}$
-60	32	13	502096953744	$2^4 \cdot 3^{22}$

4.12. A példák számításigénye

A példák kiszámításához a Maple programcsomagot használtuk. A $\mathbb{Z}$ feletti S-egység egyenlet megoldása mindössze néhány percet vett igénybe. Az első és a második példa esetén (ezek azok a példák, melyeknél elég volt a $\mathbb{Z}$ feletti S-egység egyenletet megoldani) a további számítások elvégzése is gyors volt, így ezekben az esetekben algoritmusunk különösen hatékornak tekinthető.

A harmadik példa olyan, ahol a bikvadratikus számtest felett is meg kellett oldani egy S-egység egyenletet. Ennek megoldása több órát vett igénybe, mely egyrészt a redukciónál nagy pontossággal kiszámítandó p-adikus logaritmusok kiszámítása, másrészt a redukált korlátok alatti értékek leszámmlálása és tesztelése miatt volt ilyen hosszadalmas. Megjegyezzük azonban, hogy az algebrai számok p-adikus logaritmusával való számolás hatékony megvalósításával (ami a Maple-ből hiányzik) és esetlegesen szitamódszerek alkalmazásával eljárásunk még gyorsabbá tehető.

5. Multikvadratikus számtestek monogenitása

5.1. Multikvadratikus számtestek

A bikvadratikus számtestek természetes általánosításai a multikvadratikus számtestek. Legyen $n \in \mathbb{N}$, továbbá $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ páronként különböző négyzetmentes egész számok. Ekkor a $\mathbb{Q}(\sqrt{k_1}, \dots, \sqrt{k_n})$ testet **multikvadratikus számtestnek** hívjuk. ($n = 2$ esetén kapjuk vissza a bikvadratikus számtesteket.)

Multikvadratikus számtestekben nem ismert olyan egyszerűen megadott egész bázis, mint bikvadratikus számtestek esetén a *K. S. Williams* [53] által leírt egész bázis, bár vannak ezzel kapcsolatos eredmények (*B. Schmal* [48]).

Részben ez az oka annak, hogy a bikvadratikus számtestekkel ellentétben multikvadratikus számtestekben $n \geq 3$ esetén index forma egyenletekkel és a monogenitás problémájával kapcsolatban a közelmúltig nem születtek eredmények.

Ebben a fejezetben először $n = 3$ esetén mutatjuk meg, hogy nem létezik hatvány egész bázis abban az esetben, amikor a $\mathbb{Q}(\sqrt{k_j})$ résztestek közül legalább az egyik imaginárius másodfokú számtest és a résztestek diszkriminánsai bizonyos feltételekből következően páronként relatív prímek. Majd tetszőleges n esetén igazolunk hasonló állításokat, még hozzá páratlan diszkrimináns esetén $\mathbb{Z}_K$ -ban, illetve megkötések nélkül a $\mathbb{Z}[\sqrt{k_1}, \dots, \sqrt{k_n}]$ rendben.

Újabban *Y. Motoda* és *T. Nakahara* [42] érték el multikvadratikus számtestek monogenitására vonatkozó további eredményeket.

5.2. Három másodfokú számtest kompozitumának monogenitása

Ebben a részben három másodfokú résztestének kompozitumaként előálló nyolcadfokú számtestekben foglalkozunk a monogenitás problémájával, melyeknél feltesszük, hogy valamelyik másodfokú résztest képzetes és további feltételek biztosítják, hogy a másodfokú testek diszkriminánsai páronként relatív prímek.

A tétel bizonyításában használni fogjuk az alábbi, algebrai számtestek

kompozitumának egész bázisáról és diszkriminánsáról szóló állítást.

5.2.1. LEMMA ([44]-ben Theorem 4.26.)

Legyen az m -edfokú K algebrai számtest egy egész bázisa $(\xi_1 = 1, \xi_2, \dots, \xi_m)$, diszkriminánsa D_K és az n -edfokú L algebrai számtest egy egész bázisa $(\eta_1 = 1, \eta_2, \dots, \eta_n)$, diszkriminánsa D_L . Jelölje N a K és L testek kompozitumát, továbbá tegyük fel, hogy $\text{luko}(D_K, D_L) = 1$. Ekkor az N algebrai számtest fokszáma $m \cdot n$, N egy egész bázisa

$$(\xi_i \eta_j \mid i = 1, \dots, m ; j = 1, \dots, n),$$

N diszkriminánsa pedig

$$D_N = D_K^n \cdot D_L^m.$$

5.2.2. TÉTEL (Nyul G. [46], Theorem 3.)

Legyenek $k, l, m \in \mathbb{Z} \setminus \{0, 1\}$ páronként relatív prímek, négyzetmentesek, $k < 0$ és $l \equiv m \equiv 1 \pmod{4}$. Ekkor az $N = \mathbb{Q}(\sqrt{k}, \sqrt{l}, \sqrt{m})$ nyolcadfokú számtestben nincs hatvány egész bázis.

BIZONYÍTÁS

Legyen $K = \mathbb{Q}(\sqrt{k})$, $L = \mathbb{Q}(\sqrt{l})$, $M = \mathbb{Q}(\sqrt{m})$. Közismert, hogy ekkor az $l \equiv m \equiv 1 \pmod{4}$ feltételt figyelembe véve K , L , M -ben rendre $(1, \omega_1)$, $(1, \omega_2)$, $(1, \omega_3)$ egész bázis, ahol

$$\omega_1 = \begin{cases} \frac{1+\sqrt{k}}{2} & \text{ha } k \equiv 1 \pmod{4} \\ \sqrt{k} & \text{ha } k \equiv 2 \text{ vagy } 3 \pmod{4} \end{cases}, \quad \omega_2 = \frac{1+\sqrt{l}}{2}, \quad \omega_3 = \frac{1+\sqrt{m}}{2},$$

K , L , M diszkriminánsa pedig rendre

$$D_K = \begin{cases} k & \text{ha } k \equiv 1 \pmod{4} \\ 4k & \text{ha } k \equiv 2 \text{ vagy } 3 \pmod{4} \end{cases}, \quad D_L = l, \quad D_M = m.$$

Feltételeink értelmében D_K , D_L , D_M páronként relatív prímek, így az 5.2.1. lemmát alkalmazva azt kapjuk, hogy N nyolcadfokú számtest és

$$(1, \omega_1, \omega_2, \omega_3, \omega_1 \omega_2, \omega_1 \omega_3, \omega_2 \omega_3, \omega_1 \omega_2 \omega_3) \quad (44)$$

egész bázisa N -nek.

Legyen $\{(\varepsilon_1^{(j)}, \varepsilon_2^{(j)}, \varepsilon_3^{(j)}) \mid j = 1, \dots, 8\}$ antilexikografikusan rendezve az összes olyan vektor halmaza, melynek minden koordinátája ± 1 .

Négy esetet különböztetünk meg.

1. *eset*: ha $k \equiv 2$ vagy $3 \pmod{4}$, de $k \neq -1$.

Ebben az esetben az 5.2.1. lemma alapján N diszkriminánsa $D_N = 256k^4l^4m^4$. Készítsük el a (44) egész bázishoz tartozó lineáris formákat:

$$\begin{aligned} l^{(j)}(\underline{x}) = & x_1 + x_2\varepsilon_1^{(j)}\sqrt{k} + x_3\frac{1+\varepsilon_2^{(j)}\sqrt{l}}{2} + x_4\frac{1+\varepsilon_3^{(j)}\sqrt{m}}{2} + x_5\varepsilon_1^{(j)}\sqrt{k}\frac{1+\varepsilon_2^{(j)}\sqrt{l}}{2} \\ & + x_6\varepsilon_1^{(j)}\sqrt{k}\frac{1+\varepsilon_3^{(j)}\sqrt{m}}{2} + x_7\frac{1+\varepsilon_2^{(j)}\sqrt{l}+\varepsilon_3^{(j)}\sqrt{m}+\varepsilon_2^{(j)}\varepsilon_3^{(j)}\sqrt{lm}}{4} \\ & + x_8\varepsilon_1^{(j)}\sqrt{k}\frac{1+\varepsilon_2^{(j)}\sqrt{l}+\varepsilon_3^{(j)}\sqrt{m}+\varepsilon_2^{(j)}\varepsilon_3^{(j)}\sqrt{lm}}{4} \\ & (j = 1, \dots, 8) \end{aligned}$$

Mint látni fogjuk, a 28 darab $l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$ ($1 \leq i < j \leq 8$) alakú különbséget hét darab négyes csoportba tudjuk sorolni (a.-g.) olyan módon, hogy bármely négy, egy csoportba tartozó különbség szorzata egész szám legyen, ha $x_2, \dots, x_8 \in \mathbb{Z}$, amit a továbbiakban feltételezni is fogunk. Vezessük még be a következő jelöléseket is különböző $e, f, i, j \in \{2, \dots, 8\}$ indexek esetén:

$$A_{efij} = 2x_e + 2x_f\sqrt{k} + x_i + x_j\sqrt{k}$$

$$\overline{A}_{efij} = 2x_e - 2x_f\sqrt{k} + x_i - x_j\sqrt{k}$$

$$A_{ij} = x_i + x_j\sqrt{k}$$

$$\overline{A}_{ij} = x_i - x_j\sqrt{k}$$

a.) Teljesül, hogy $m^2 \cdot F_1(\underline{x}) =$

$$\left(l^{(1)}(\underline{x}) - l^{(2)}(\underline{x})\right) \left(l^{(3)}(\underline{x}) - l^{(4)}(\underline{x})\right) \left(l^{(5)}(\underline{x}) - l^{(6)}(\underline{x})\right) \left(l^{(7)}(\underline{x}) - l^{(8)}(\underline{x})\right)$$

ahol

$$F_1(\underline{x}) = \frac{1}{4} \left(A_{4678}^2 - l \cdot A_{78}^2 \right) \cdot \frac{1}{4} \left(\overline{A}_{4678}^2 - l \cdot \overline{A}_{78}^2 \right).$$

Az $A_{4678} = 2A_{46} + A_{78}$ és $\overline{A}_{4678} = 2\overline{A}_{46} + \overline{A}_{78}$ azonosságok figyelembe vételével

$$F_1(\underline{x}) = \left(A_{46}^2 + A_{46}A_{78} + \frac{1-l}{4}A_{78}^2 \right) \cdot \left(\overline{A}_{46}^2 + \overline{A}_{46}\overline{A}_{78} + \frac{1-l}{4}\overline{A}_{78}^2 \right).$$

Innen $l \equiv 1 \pmod{4}$ miatt adódik, hogy $F_1(\underline{x})$ mindkét tényezője eleme $\mathbb{Z}_K$ -nak és egymás konjugáltjai, amiből adódik, hogy $F_1(\underline{x})$ racionális egész értékű.

b.) Fennáll továbbá, hogy $l^2 \cdot F_2(\underline{x}) =$

$$\left(l^{(1)}(\underline{x}) - l^{(3)}(\underline{x}) \right) \left(l^{(2)}(\underline{x}) - l^{(4)}(\underline{x}) \right) \left(l^{(5)}(\underline{x}) - l^{(7)}(\underline{x}) \right) \left(l^{(6)}(\underline{x}) - l^{(8)}(\underline{x}) \right)$$

ahol

$$F_2(\underline{x}) = \frac{1}{4} \left(A_{3578}^2 - m \cdot A_{78}^2 \right) \cdot \frac{1}{4} \left(\overline{A}_{3578}^2 - m \cdot \overline{A}_{78}^2 \right).$$

Ekkor $m \equiv 1 \pmod{4}$ -ből az előzőekhez hasonlóan kapjuk, hogy $F_2(\underline{x})$ mindkét tényezője eleme $\mathbb{Z}_K$ -nak, továbbá egymás konjugáltjai, így szorzatuk, $F_2(\underline{x})$ racionális egész.

c.) Belátható az is, hogy $16k^2 \cdot F_3(\underline{x}) =$

$$\left(l^{(1)}(\underline{x}) - l^{(5)}(\underline{x}) \right) \left(l^{(2)}(\underline{x}) - l^{(6)}(\underline{x}) \right) \left(l^{(3)}(\underline{x}) - l^{(7)}(\underline{x}) \right) \left(l^{(4)}(\underline{x}) - l^{(8)}(\underline{x}) \right)$$

ahol $F_3(\underline{x})$ racionális egész szám.

d.) Legyen $F_4(\underline{x}) =$

$$\left(l^{(1)}(\underline{x}) - l^{(4)}(\underline{x}) \right) \left(l^{(2)}(\underline{x}) - l^{(3)}(\underline{x}) \right) \left(l^{(5)}(\underline{x}) - l^{(8)}(\underline{x}) \right) \left(l^{(6)}(\underline{x}) - l^{(7)}(\underline{x}) \right) =$$

$$\frac{1}{4} \left(l \cdot A_{3578}^2 - m \cdot A_{4678}^2 \right) \cdot \frac{1}{4} \left(l \cdot \overline{A}_{3578}^2 - m \cdot \overline{A}_{4678}^2 \right)$$

Itt $l \equiv m \pmod{4}$ alapján kapjuk, hogy mindkét tényező $\mathbb{Z}_K$ -beli és egymás konjugáltjai, tehát $F_4(\underline{x})$ is $\mathbb{Z}$ -beli.

e.) Hasonlóan $F_5(\underline{x}) =$

$$\left(l^{(1)}(\underline{x}) - l^{(6)}(\underline{x}) \right) \left(l^{(2)}(\underline{x}) - l^{(5)}(\underline{x}) \right) \left(l^{(3)}(\underline{x}) - l^{(8)}(\underline{x}) \right) \left(l^{(4)}(\underline{x}) - l^{(7)}(\underline{x}) \right)$$

is racionális egész.

f.) Az $F_6(\underline{x}) =$

$$\left(l^{(1)}(\underline{x}) - l^{(7)}(\underline{x})\right) \left(l^{(2)}(\underline{x}) - l^{(8)}(\underline{x})\right) \left(l^{(3)}(\underline{x}) - l^{(5)}(\underline{x})\right) \left(l^{(4)}(\underline{x}) - l^{(6)}(\underline{x})\right)$$

is eleme $\mathbb{Z}$ -nek.

g.) Legyen végül $F_7(\underline{x}) =$

$$\left(l^{(1)}(\underline{x}) - l^{(8)}(\underline{x})\right) \left(l^{(2)}(\underline{x}) - l^{(7)}(\underline{x})\right) \left(l^{(3)}(\underline{x}) - l^{(6)}(\underline{x})\right) \left(l^{(4)}(\underline{x}) - l^{(5)}(\underline{x})\right).$$

Leírva ezt a négy különbséget észrevehetjük, hogy azok egymás konjugáltjai K felett, ezért szorzatuk, $F_7(\underline{x})$ $\mathbb{Z}_K$ -beli értéket vesz fel. De ha az első tényezőt az utolsóval, a másodikat pedig a harmadikkal szorozzuk össze, akkor azt kapjuk, hogy $F_7(\underline{x}) =$

$$\left[k \left(2x_2 + x_5 + x_6 + x_8 \frac{1 + \sqrt{lm}}{2} \right)^2 - \left(x_3 \sqrt{l} + x_4 \sqrt{m} + x_7 \frac{\sqrt{l} + \sqrt{m}}{2} \right)^2 \right] \cdot \left[k \left(2x_2 + x_5 + x_6 + x_8 \frac{1 - \sqrt{lm}}{2} \right)^2 - \left(x_3 \sqrt{l} - x_4 \sqrt{m} + x_7 \frac{\sqrt{l} - \sqrt{m}}{2} \right)^2 \right]$$

Látható, hogy ebben a kifejezésben a szorzást elvégezve nem marad $\sqrt{k}$ -től függő tag, ami azt jelenti, hogy $F_7(\underline{x})$ racionális egész értékű.

Ezeket felhasználva az index forma definíciója alapján kapjuk a (44) egész bázishoz tartozó index formát:

$$\left(16k^2 l^2 m^2 \prod_{j=1}^7 F_j(\underline{x}) \right)^2 = (I(x_2, \dots, x_8))^2 \cdot D_N,$$

$$I(x_2, \dots, x_8) = \prod_{j=1}^7 F_j(\underline{x}).$$

A fentiekben azt kaptuk, hogy ha $x_2, \dots, x_8 \in \mathbb{Z}$, akkor $F_j(\underline{x}) \in \mathbb{Z}$ ($j = 1, \dots, 7$), ezért ha ezzel az index formával teljesül az $I(x_2, \dots, x_8) = \pm 1$ ($x_2, \dots, x_8 \in \mathbb{Z}$) index forma egyenlet, akkor $F_j(\underline{x}) = \pm 1$ ($j = 1, \dots, 7$) is fennáll.

Ez azt jelenti, hogy például $F_1(\underline{x}) = \pm 1$. Viszont láttuk, hogy $F_1(\underline{x})$ két K -beli algebrai egész szorzata, az 1. esetben pedig csak ± 1 egységek $\mathbb{Z}_K$ -ban, tehát

$$\frac{1}{4} \left(A_{4678}^2 - l \cdot A_{78}^2 \right) = \pm 1.$$

Hasonlóan $F_2(\underline{x}) = \pm 1$ és $F_4(\underline{x}) = \pm 1$ -ből azt kapjuk, hogy

$$\frac{1}{4} \left(A_{3578}^2 - m \cdot A_{78}^2 \right) = \pm 1,$$

$$\frac{1}{4} \left(l \cdot A_{3578}^2 - m \cdot A_{4678}^2 \right) = \pm 1.$$

A rövidebb írásmód érdekében legyen $x = A_{78}^2$, $y = A_{3578}^2$, $z = A_{4678}^2$. Ezekkel a jelölésekkel az alábbi egyenletrendszer teljesül (az előjelek függetlenek egymástól):

$$\begin{aligned} y - mx &= \pm 4 \\ z - lx &= \pm 4 \\ ly - mz &= \pm 4 \end{aligned} \tag{45}$$

Az első két egyenletből kapott $y = mx \pm 4$ és $z = lx \pm 4$ értékeket behelyettesítve a harmadik egyenletbe $l(mx \pm 4) - m(lx \pm 4) = \pm 4$, ahonnan $\pm l \pm m = \pm 1$. Ez viszont ellentmond az $l \equiv m \pmod{4}$ feltételnek.

2. eset: ha $k = -1$.

Ebben az esetben a bizonyítás eleje szó szerint megegyezik az 1. esetbeli bizonyítással. A 2. esetben azonban $\mathbb{Z}_K = \mathbb{Z}_{\mathbb{Q}(\sqrt{-1})}$ egységei i^α ($\alpha = 0, 1, 2, 3$). Ekkor az 1. eset jelöléseit használva a (45) egyenletrendszer helyett az

$$\begin{aligned} y - mx &= 4i^{\alpha_1} \\ z - lx &= 4i^{\alpha_2} \\ ly - mz &= 4i^{\alpha_3} \end{aligned}$$

egyenletrendszert kapjuk, ahol $\alpha_1, \alpha_2, \alpha_3 \in \{0, 1, 2, 3\}$.

Behelyettesítések után $l(mx + 4i^{\alpha_1}) - m(lx + 4i^{\alpha_2}) = 4i^{\alpha_3}$, azaz $li^{\alpha_1} - mi^{\alpha_2} = i^{\alpha_3}$.

Ekkor $1 = |i^{\alpha_3}| = |li^{\alpha_1} - mi^{\alpha_2}| \geq ||li^{\alpha_1}| - |mi^{\alpha_2}|| = ||l| - |m|| \geq 2$, ahol az utolsó egyenlőtlenség az l -re és m -re tett feltételekből adódik. Ezzel ismét ellentmondáshoz jutottunk.

3. eset: ha $k \equiv 1 \pmod{4}$, de $k \neq -3$.

4. eset: ha $k = -3$.

Ezekben az esetekben a bizonyítás hasonlóan végezhető el, mint az 1. és a 2. esetben.

Az összes esetben megmutattuk, hogy az index forma egyenlet ± 1 jobb oldallal nem megoldható, tehát N -ben nincs hatvány egész bázis. $\square$

5.3. Testindex multikvadratikus számtestekben

Ebben a részben a páratlan diszkriminánsú multikvadratikus számtestek esetén mutatjuk meg, hogy nincs bennük hatvány egész bázis. Ez abból fog következni, hogy belátjuk, hogy ezeknek a testeknek a testindexe páros.

5.3.1. TÉTEL (Nyul G. [46], Theorem 1.)

Legyenek $n \in \mathbb{N}$, $n \geq 3$ és $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ páronként különböző négyzetmentes számok úgy, hogy $K = \mathbb{Q}(\sqrt{k_1}, \dots, \sqrt{k_n})$ egy 2^n -edfokú algebrai számtest és D_K páratlan. Ekkor K testindexe páros, következésképpen K -ban nincs hatvány egész bázis.

BIZONYÍTÁS Mivel $2 \nmid D_K$, ezért $2\mathbb{Z}_K = \wp_1 \cdot \dots \cdot \wp_g$ páronként különböző prímeállok szorzata. Mivel K normális bővítése $\mathbb{Q}$ -nak, ezért a $\wp_j$ prímeállok foka egyenlő, legyen ez a közös fok f . K Galois-csoportja n darab másodrendű ciklikus csoport direkt szorzata, így [44] Theorem 8.2.-ből adódik, hogy $f = 1$ vagy $f = 2$. Továbbá $n \geq 3$ miatt ezekből azt kapjuk, hogy $g = \frac{2^n}{f} \geq 4$.

R. Dedekind tétele (lásd például [44] Theorem 4.34.) azt állítja, hogy egy p prímszám pontosan akkor osztja a K algebrai számtest i_K testindexét, ha van olyan f természetes szám, hogy $p\mathbb{Z}_K$ prímeálfaktorizációjában az f fokú prímeáltrevezők száma nagyobb, mint a $GF(p)$ feletti f fokszámú irreducibilis főpolinomok száma.

$GF(2)$ felett pontosan két darab elsőfokú (az x és $x + 1$) és pontosan egy darab másodfokú (az $x^2 + x + 1$) irreducibilis polinom létezik, ezért esetünkben *R. Dedekind* tétele alapján az adódik, hogy i_K páros. $\square$

MEGJEGYZÉS Az 5.2.2. tétel feltételeit és jelöléseit használva a bizonyítás 3. és 4. esetében (amikor $k \equiv 1 \pmod{4}$) N diszkriminánsa $D_N = k^4 l^4 m^4$, ami $k \equiv l \equiv m \equiv 1 \pmod{4}$ miatt páratlan. Így alkalmazva az 5.3.1. tételt az $N = \mathbb{Q}(\sqrt{k}, \sqrt{l}, \sqrt{m})$ nyolcadfokú testre azt kapjuk, hogy i_N páros, tehát N -ben nincs hatvány egész bázis. Ezek szerint az 5.2.2. tétel állítása a 3. és a 4. esetben az 5.3.1. tételből is következik.

5.4. Monogenitás multikvadratikus számtestek egy rendjében

A most következő eredmény tetszőleges multikvadratikus számtest esetén teljesülni fog. A monogenitást azonban a maximális rend helyett a $\mathbb{Z}[\sqrt{k_1}, \dots, \sqrt{k_n}]$ rendben vizsgáljuk. Azt fogjuk igazolni, hogy ebben a rendben minden elem indexe osztható 2-nek egy nagy kitevős hatványával, amiből $n \geq 2$ esetén az is adódik, hogy ebben a rendben nincs hatvány egész bázis.

A monogenitásról szóló tétel ismertetése előtt meghatározzuk a rend diszkriminánsát, hogy majd vizsgálni tudjuk az index formát.

5.4.1. LEMMA (Nyul G. [46], Lemma 1.)

Ha $n \in \mathbb{N}$, $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ páronként különböző négyzetmentes egész számok és $\mathbb{Q}(\sqrt{k_1}, \dots, \sqrt{k_n})$ egy 2^n -edfokú algebrai számtest, akkor az $\mathcal{O} = \mathbb{Z}[\sqrt{k_1}, \dots, \sqrt{k_n}]$ rend diszkriminánsa $D_{\mathcal{O}} = (k_1 \cdot \dots \cdot k_n)^{2^{n-1}} \cdot 2^{n \cdot 2^n}$.

BIZONYÍTÁS Vegyük $\mathcal{O}$ -ban az

$$\left(1, \sqrt{k_1}, \dots, \sqrt{k_n}, \sqrt{k_1 k_2}, \dots, \sqrt{k_{n-1} k_n}, \dots, \sqrt{k_1 \cdot \dots \cdot k_n}\right) \quad (46)$$

egész bázist. Legyen $\{(\varepsilon_n^{(j)}, \dots, \varepsilon_1^{(j)}) \mid j = 1, \dots, 2^n\}$ azon vektorok anti-lexikografikus módon rendezett halmaza, melyeknek minden koordinátája ± 1 -gyel egyenlő. Ekkor $D_{\mathcal{O}}$ egyenlő annak a $2^n \times 2^n$ -es determinánsnak a négyzetével, melynek j -edik sora ($j = 1, \dots, 2^n$)

$$\begin{pmatrix} 1, \varepsilon_1^{(j)} \sqrt{k_1}, \dots, \varepsilon_n^{(j)} \sqrt{k_n}, \\ \varepsilon_1^{(j)} \varepsilon_2^{(j)} \sqrt{k_1 k_2}, \dots, \varepsilon_{n-1}^{(j)} \varepsilon_n^{(j)} \sqrt{k_{n-1} k_n}, \dots, \varepsilon_1^{(j)} \cdot \dots \cdot \varepsilon_n^{(j)} \sqrt{k_1 \cdot \dots \cdot k_n} \end{pmatrix}$$

Emeljük ki ezen determináns oszlopaiból a $\sqrt{k_1}, \dots, \sqrt{k_n}$ -ek alkotta közös tényezőket. Jelöljük D_n -nel a kiemelés után visszamaradó mátrixot. Bármely $j \in \{1, \dots, n\}$ esetén pontosan $\binom{n-1}{l}$ olyan oszlopa van a determinánsnak, melyből $\sqrt{k_j}$ egy $l+1$ tényezős szorzat egyik tényezőjeként lett kiemelve ($l = 0, \dots, n-1$), ezért

$$D_{\mathcal{O}} = \left(\left(\sqrt{k_1 \cdot \dots \cdot k_n} \right)^{\binom{n-1}{0} + \binom{n-1}{1} + \dots + \binom{n-1}{n-1}} \right)^2 \cdot |D_n|^2 = (k_1 \cdot \dots \cdot k_n)^{2^{n-1}} \cdot |D_n|^2.$$

A lemma igazolásához már csak azt kell megmutatnunk, hogy $|D_n|^2 = 2^{n \cdot 2^n}$ teljesül minden $n \in \mathbb{N}$ esetén. Ezt teljes indukcióval látjuk be.

$n = 1$ esetén az állítás igaz, mert

$$|D_1|^2 = \left| \begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right|^2 = 4 = 2^{1 \cdot 2^1}.$$

Tegyük fel, hogy $|D_n|^2 = 2^{n \cdot 2^n}$ teljesül valamely $n \geq 1$ esetén. Ezek után a $|D_{n+1}|$ determinánsban cseréljük fel az oszlopok sorrendjét úgy, hogy az első 2^n darab oszlop legyen az $1, \sqrt{k_1}, \dots, \sqrt{k_n}, \sqrt{k_1 k_2}, \dots, \sqrt{k_{n-1} k_n}, \dots, \sqrt{k_1 \cdot \dots \cdot k_n}$ -hez, az utolsó 2^n darab pedig a $\sqrt{k_{n+1}}, \sqrt{k_1 k_{n+1}}, \dots, \sqrt{k_n k_{n+1}}, \sqrt{k_1 k_2 k_{n+1}}, \dots, \sqrt{k_{n-1} k_n k_{n+1}}, \dots, \sqrt{k_1 \cdot \dots \cdot k_n k_{n+1}}$ -hez tartozó oszlop. A cserék után azt kapjuk, hogy

$$|D_{n+1}|^2 = \left| \begin{array}{cc} D_n & D_n \\ D_n & -D_n \end{array} \right|^2.$$

A j -edik sort kivonva a $(2^n + j)$ -edik sorból ($1 \leq j \leq 2^n$), majd a Laplace-féle kifejtési tételt, végül pedig az indukciós feltevést alkalmazva azt kapjuk, hogy

$$|D_{n+1}|^2 = \left| \begin{array}{cc} D_n & D_n \\ 0 & -2D_n \end{array} \right|^2 = (2^{2^n} \cdot |D_n|^2)^2 = (2^{2^n} \cdot 2^{n \cdot 2^n})^2 = 2^{(n+1) \cdot 2^{n+1}}.$$

□

5.4.2. TÉTEL (Nyul G. [46], Theorem 2.)

Az 5.4.1. lemma jelölései és feltételei mellett az $\mathcal{O}$ rendben minden elem indexe osztható $2^{2^{n-1}(2^n - n - 1)}$ -gyel.

BIZONYÍTÁS A bizonyítás során megtartjuk az 5.4.1. lemma bizonyításának a jelöléseit.

Számítsuk ki $\mathcal{O}$ -nak a (46) egész bázisához tartozó index formát. A szükséges lineáris formák:

$$l^{(j)}(\underline{x}) = x_1 + \varepsilon_1^{(j)} \sqrt{k_1} x_2 + \dots + \varepsilon_n^{(j)} \sqrt{k_n} x_{n+1} + \varepsilon_1^{(j)} \varepsilon_2^{(j)} \sqrt{k_1 k_2} x_{n+2} + \dots + \varepsilon_1^{(j)} \dots \varepsilon_n^{(j)} \sqrt{k_1 \dots k_n} x_{2^n} \quad (j = 1, \dots, 2^n).$$

Az index forma definíciója alapján

$$\left(\prod_{1 \leq i < j \leq 2^n} (l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})) \right)^2 = (I(x_2, \dots, x_{2^n}))^2 \cdot D_{\mathcal{O}}. \quad (47)$$

Világos, hogy az $l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$ ($1 \leq i < j \leq 2^n$) különbségekben a lineáris forma minden tagja vagy kiesik, vagy 2 együtthatóval szerepel. Ezért minden $l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$ különbségből kiemelhetünk 2-t, összesen tehát 2-t a $\binom{2^n}{2} = 2^{n-1}(2^n - 1)$ -edik hatványon tudjuk kiemelni. Továbbá $\sqrt{k_m}$ ($m = 1, \dots, n$) is kiemelhető $l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$ -ből, ha $\varepsilon_m^{(i)} = -\varepsilon_m^{(j)}$ és $1 \leq h \leq n$, $h \neq m$ esetén $\varepsilon_h^{(i)} = \varepsilon_h^{(j)}$. Ez 2^{n-1} darab esetben következik be (ennyi lehetséges értéke lehet $\varepsilon_h^{(i)} = \varepsilon_h^{(j)}$ -nek, $1 \leq h \leq n, h \neq m$), ezért $(\sqrt{k_m})^{2^{n-1}}$ is kiemelhető a lineáris formák különbségeinek szorzatából ($m = 1, \dots, n$). Összefoglalva tehát

$$\prod_{1 \leq i < j \leq 2^n} (l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})) = 2^{2^{n-1}(2^n-1)} \cdot (\sqrt{k_1 \dots k_n})^{2^{n-1}} \cdot I_0(x_2, \dots, x_{2^n}), \quad (48)$$

ahol $I_0(x_2, \dots, x_{2^n})$ egész együtthatós polinom.

Végül (47), (48) és az 5.4.1. lemma alapján az adódik, hogy

$$I(x_2, \dots, x_{2^n}) = 2^{2^{n-1}(2^n-n-1)} \cdot I_0(x_2, \dots, x_{2^n}),$$

ahol $x_2, \dots, x_{2^n} \in \mathbb{Z}$ esetén $I_0(x_2, \dots, x_{2^n})$ egész értékeket vesz fel, amivel az állítást igazoltuk. $\square$

Mivel $n \geq 2$ esetén $2^{n-1}(2^n - n - 1) > 1$, így adódik az alábbi következmény.

5.4.3. KÖVETKEZMÉNY Az 5.4.1. lemma jelölései és feltételei mellett, $n \geq 2$ esetén az $\mathcal{O}$ rendben nincs hatvány egész bázis.

6. Algebrai számtestek testindexe

6.1. Testindex

Egy K algebrai számtest i_K testindexe alatt a $\mathbb{Z}_K$ -beli primitív elemek indexeinek legnagyobb közös osztóját értjük. Az alábbiakban először összefoglaljuk az algebrai számtestek testindexével kapcsolatos legfontosabb eredményeket. Ezután bizonyos ismert számtestcsaládok, a Kishi-féle harmadfokú és a legegyszerűbb negyedfokú testek esetén határozzuk meg a testindex értékét.

M. Bauer [3] igazolta, hogy ha p prímszám és $p < n$, akkor létezik olyan n -edfokú algebrai számtest, melyben $p \mid i_K$. Ennek egyfajta megfordítását állítja *E. von Žyliński* [55] tétele, mely szerint ha egy p prímszám osztója K testindexének, akkor $p < [K : \mathbb{Q}]$.

Tegyük fel, hogy ismert egy n -edfokú K algebrai számtest valamely egész bázisához tartozó $I(x_2, \dots, x_n)$ index forma. Ekkor *E. von Žyliński* előbbi állítása, valamint a bevezetőben említett

$$i_K = \text{lko} \{I(x_2, \dots, x_n) \mid x_2, \dots, x_n \in \mathbb{Z}\}$$

formula lehetővé teszi, hogy csupán moduláris számolások segítségével meghatározzuk K testindexét. Ráadásul számtestek családjai esetén ezzel a módszerrel a testindexet a paraméterek értékétől függően is le tudjuk írni.

H. T. Engstrom [7] megmutatta, hogy legfeljebb hetedfokú algebrai számtestek esetén $\text{ord}_p(i_K)$ a p prímszám K -beli prímeálfaktorizációjától függ és példát adott arra is, hogy ez magasabb fokszám esetén már nem teljesül. Eredményéből következik, hogy harmadfokú K számtest esetén $i_K \in \{1, 2\}$, valamint negyedfokú K -ra $i_K \in \{1, 2, 3, 4, 6, 12\}$.

Megmutatható, hogy léteznek 1 illetve 2 testindexű harmadfokú algebrai számtestek is.

A $K = \mathbb{Q}(\sqrt[3]{m})$ tiszta harmadfokú számtestek ($m \in \mathbb{Z} \setminus \{-1, 0, 1\}$ köbmentes) esetén ismert egy egész bázis és a diszkrimináns leírása (ld. például [39] 38. oldal, [44] Theorem 2.19.). A megfelelő index forma meghatározása és vizsgálata után kapható, hogy mindegyik tiszta harmadfokú számtest testindexe 1. (Ezt a számolást egy esetben *W. Narkiewicz* [44] (65. oldal) elvégezte, ezzel adva példát olyan nem monogén

algebrai számtestre, melyben $i_K = 1$.)

T. Funakura [8] meghatározta a $K = \mathbb{Q}(\sqrt[4]{m})$ tiszta negyedfokú számtestek ($m \in \mathbb{Z} \setminus \{0, 1\}$ negyedik hatvány mentes) testindexét:

$$i_K = \begin{cases} 2 & \text{ha } m \equiv 1 \pmod{16} \\ 1 & \text{amúgy} \end{cases}$$

T. Nakahara [43] megmutatta, hogy bikvadratikus számtest testindexe az 1, 2, 3, 4, 6, 12 értékek mindegyike lehet. Erre vonatkozóan a fent ismertetett moduláris módszer segítségével *Gaál I.*, *Pethő A.* és *M. Pohst* [16] új bizonyítást adtak, a bikvadratikus számtest paramétereitől függően pedig leírták a testindex értékét.

Hasonló eredményt ért el *B. K. Spearman* és *K. S. Williams* [51], akik megmutatták, hogy 12 minden osztója lehet ciklikus negyedfokú számtest testindexe.

6.2. Kishi-féle harmadfokú testek

Legyen α gyöke a $t^3 - a(a^2 + a + 3)(a^2 + 2)t^2 - (a^3 + 2a^2 + 3a + 3)t - 1 \in \mathbb{Z}[t]$ polinomnak, ahol $a \in \mathbb{Z}$. Ez a polinom irreducibilis $\mathbb{Q}$ felett, diszkriminánsa $(a^2 + 1)^2(a^2 + 3)^2(a^4 + a^3 + 4a^2 + 3)^2$. Ebből következik, hogy a $K = K_a = \mathbb{Q}(\alpha)$ **Kishi-féle harmadfokú testek** teljesen valós, ciklikus harmadfokú számtestek.

Ezekről a testekről *Y. Kishi* [36] az alábbiakat mutatta meg. Legyen

$$\delta_1 = \begin{cases} 0 & \text{ha } 2 \mid a \\ 1 & \text{ha } 2 \nmid a \end{cases}, \quad \delta_2 = \begin{cases} 0 & \text{ha } a \equiv 2 \pmod{3} \\ 1 & \text{ha } a \not\equiv 2 \pmod{3} \end{cases},$$

továbbá

$$B = \frac{(a^2 + 3)(a^4 + a^3 + 4a^2 + 3)}{4^{\delta_1} \cdot 9^{\delta_2}}.$$

Ha B négyzetmentes és $a \notin \{-2, -1, 1\}$, akkor a K -t meghatározó polinom bármely két különböző gyöke alapegységrendszert alkot K -ban.

A továbbiakhoz a Kishi-féle harmadfokú testeket az a paramétertől függően a következő hat esetben soroljuk:

1. eset: $a \equiv 0, 2 \pmod{6}$ vagy $a \equiv 4, 10 \pmod{18}$
2. eset: $a \equiv 34, 52 \pmod{54}$

3. eset: $a \equiv 3, 5 \pmod{6}$ vagy $a \equiv 1, 13 \pmod{18}$
4. eset: $a \equiv 7, 25 \pmod{54}$
5. eset: $a \equiv 16 \pmod{54}$
6. eset: $a \equiv 43 \pmod{54}$

Y. Kishi [36] mindegyik esetben megadta K diszkriminánsát.

6.2.1. LEMMA (*Y. Kishi* [36], Corollary 1.4.)

Ha B négyzetmentes, akkor a Kishi-féle harmadfokú K test diszkriminánsa

$$D_K = \frac{(a^2 + 3)^2(a^4 + a^3 + 4a^2 + 3)^2}{b^2},$$

ahol b értéke az esetek fenti sorrendjében rendre 1, 3, 4, 12, 27, 108.

A továbbiakban meghatározzuk a Kishi-féle harmadfokú testek egy egész bázisát, majd az ehhez tartozó index forma kiszámítása után belátjuk, hogy ezen számtestcsalád minden elemének testindexe 1.

6.2.2. TÉTEL

Ha B négyzetmentes, akkor a $K = \mathbb{Q}(\alpha)$ Kishi-féle harmadfokú test egy egész bázisa $(\omega_1 = 1, \omega_2, \omega_3) =$

1. eset: $\left(1, \alpha, \frac{-a + (-a + 1)\alpha + \alpha^2}{a^2 + 1}\right)$
2. eset: $\left(1, \alpha, \frac{a^2 - a + 1 + (2a^2 - a + 3)\alpha + \alpha^2}{3(a^2 + 1)}\right)$
3. eset: $\left(1, \frac{1 + \alpha}{2}, \frac{-a + (-a + 1)\alpha + \alpha^2}{2(a^2 + 1)}\right)$
4. eset: $\left(1, \frac{1 + \alpha}{2}, \frac{4a^2 - a + 4 + (2a^2 - a + 3)\alpha + \alpha^2}{6(a^2 + 1)}\right)$
5. eset: $\left(1, \frac{2 + \alpha}{3}, \frac{4a^2 - a + 4 + (2a^2 - a + 3)\alpha + \alpha^2}{9(a^2 + 1)}\right)$
6. eset: $\left(1, \frac{5 + \alpha}{6}, \frac{4a^2 - a + 4 + (2a^2 - a + 3)\alpha + \alpha^2}{18(a^2 + 1)}\right)$

BIZONYÍTÁS Az egyszerűség kedvéért csak az 1. esetben bizonyítunk. Ebben az esetben egyrészt $\omega_1, \omega_2 \in \mathbb{Z}_K$ nyilvánvaló, továbbá meghatározható ω_3 definiáló polinomja:

$$\begin{aligned} & x^3 + (-a^8 - 2a^7 - 10a^6 - 12a^5 - 30a^4 - 20a^3 - 30a^2 - 9a - 6)x^2 \\ & + (-2a^7 - 4a^6 - 17a^5 - 18a^4 - 37a^3 - 15a^2 - 18a + 3)x \\ & + (-a^6 - 2a^5 - 7a^4 - 6a^3 - 9a^2 + 1), \end{aligned}$$

ezért $\omega_3 \in \mathbb{Z}_K$ is teljesül. Másrészt kiszámolható, hogy

$$D(\omega_1, \omega_2, \omega_3) = (a^2 + 3)^2(a^4 + a^3 + 4a^2 + 3)^2,$$

ami a 6.2.1. lemma szerint D_K -val egyenlő. Ezekből már következik az állítás. $\square$

6.2.3. TÉTEL

Ha B négyzetmentes, akkor a K Kishi-féle harmadfokú test testindexe 1.

BIZONYÍTÁS *E. von Žylin'ski* [55] tétele alapján elég azt belátni, hogy K tartalmaz páratlan indexű primitív algebrai egész elemet.

A 6.2.1. lemma jelölései mellett $I(\alpha) = b(a^2 + 1)$, ami az 1., 2. és 5. esetben páratlan, így ezekben az esetekben teljesül az állítás.

Mindegyik esetben (akár a már igazolt három esetben is) célt érhetünk úgy is, hogy kiszámítjuk a 6.2.2. tételben megadott egész bázishoz tartozó index formát, majd alkalmazzuk a moduláris módszert.

Ezt a bizonyítást a 3. esetben ismertetjük. A megadott egész bázishoz tartozó index forma

$$\begin{aligned} I(x_2, x_3) = & \left(-\frac{1}{2}a^2 - \frac{1}{2}\right)x_2^3 + \left(-a^5 - a^4 - 5a^3 - 2a^2 - \frac{9}{2}a - \frac{3}{2}\right)x_2^2x_3 \\ & + \left(-\frac{1}{2}a^8 - a^7 - 5a^6 - 6a^5 - \frac{27}{2}a^4 - 10a^3 - \frac{21}{2}a^2 - \frac{15}{2}a\right)x_2x_3^2 \\ & + \left(\frac{1}{2}a^7 + \frac{1}{2}a^6 + \frac{7}{2}a^5 + a^4 + \frac{13}{2}a^3 - a^2 + \frac{9}{2}a + \frac{3}{2}\right)x_3^3. \end{aligned}$$

Ha például x_2 páratlan és x_3 páros, akkor $I(x_2, x_3) \equiv 1 \pmod{2}$, ami igazolja állításunkat. $\square$

6.3. Legegyszerűbb negyedfokú testek

Legyen $a \in \mathbb{Z} \setminus \{0\}$ és tegyük fel, hogy $a^2 + 16$ nem osztható 1-nél nagyobb páratlan négyzetszámmal. Legyen α gyöke a $t^4 - at^3 - 6t^2 + at + 1 \in \mathbb{Z}[t]$ polinomnak. Feltételeink mellett ez a polinom irreducibilis $\mathbb{Q}$ felett, diszkriminánsa pedig $4(a^2 + 16)^3$. Ekkor a $K = K_a = \mathbb{Q}(\alpha)$ testeket a **legegyszerűbb negyedfokú testek** családjának nevezzük.

A legegyszerűbb negyedfokú testek teljesen valós, ciklikus számtestek. *M.-N. Gras* [24] megmutatta, hogy a legegyszerűbb negyedfokú testek családja végtelen sok testből áll. Továbbá *H. K. Kim* és *J. S. Kim* [35], valamint *A. J. Lazarus* [37] eredményei alapján ismerjük ezen testek egy egész bázisát és diszkriminánsát.

6.3.1. LEMMA ([35], Theorem 2.3.; [37], Table 4.1.)

A legegyszerűbb negyedfokú $K = \mathbb{Q}(\alpha)$ test egy egész bázisa

$$\begin{aligned} & \left(1, \alpha, \alpha^2, \frac{1+\alpha^3}{2}\right) \quad \text{ha } a \equiv 1 \pmod{2} \\ & \left(1, \alpha, \frac{1+\alpha^2}{2}, \frac{\alpha+\alpha^3}{2}\right) \quad \text{ha } a \equiv 2 \pmod{4} \\ & \left(1, \alpha, \frac{1+\alpha^2}{2}, \frac{1+\alpha+\alpha^2+\alpha^3}{4}\right) \quad \text{ha } a \equiv 4 \pmod{8} \\ & \left(1, \alpha, \frac{1+2\alpha-\alpha^2}{4}, \frac{1+\alpha+\alpha^2+\alpha^3}{4}\right) \quad \text{ha } a \equiv 0 \pmod{8} \end{aligned}$$

és K diszkriminánsa

$$D_K = \begin{cases} (a^2+16)^3 & \text{ha } a \equiv 1 \pmod{2} \\ \frac{(a^2+16)^3}{4} & \text{ha } a \equiv 2 \pmod{4} \\ \frac{(a^2+16)^3}{16} & \text{ha } a \equiv 4 \pmod{8} \\ \frac{(a^2+16)^3}{64} & \text{ha } a \equiv 0 \pmod{8} \end{cases}.$$

G. Lettl és *Pethő A.* [38] leírták a hatvány egész bázisokat a legegyszerűbb negyedfokú testek $\mathbb{Z}[\alpha]$ rendjében. *Olajos P.* [47] bebizonyította, hogy egy legegyszerűbb negyedfokú test akkor és csak akkor monogén, ha $a = \pm 2$ vagy $a = \pm 4$, továbbá ezekben az esetekben megadta a hatvány egész bázisok generátorait.

Igazolni fogjuk, hogy a legegyszerűbb negyedfokú testek testindexe a paritásától függően 1 vagy 2.

6.3.2. TÉTEL *A K legegyszerűbb negyedfokú test testindexe*

$$i_K = \begin{cases} 1 & \text{ha } a \equiv 0 \pmod{2} \\ 2 & \text{ha } a \equiv 1 \pmod{2}. \end{cases}$$

BIZONYÍTÁS

1. eset: ha $a \equiv 0 \pmod{2}$.

Mivel $a \equiv 2 \pmod{4}$, $a \equiv 4 \pmod{8}$, $a \equiv 0 \pmod{8}$ esetén rendre $I(\alpha) = 4$, $I(\alpha) = 8$, $I(\alpha) = 16$, ezért $i_K \mid 16$.

Másrészt a 6.3.1. lemma szerint rendre $16 \mid D_K$, $2048 \mid D_K$, $64 \mid D_K$. *B. K. Spearman* és *K. S. Williams* [51] (Lemma 1.3.1.) fent említett eredményük bizonyítása során belátták, hogy ha egy K ciklikus negyedfokú számtest diszkriminánsa páros, akkor testindexe páratlan, ezért esetünkben $i_K = 1$.

2. eset: ha $a \equiv 1 \pmod{2}$.

Ebben az esetben $I(\alpha) = 2$, ezért elég azt belátni, hogy minden $\mathbb{Z}_K$ -beli primitív elem indexe páros.

A 2.1. résznek megfelelően bármely $\theta \in \mathbb{Z}_K$ primitív elem felírható

$$\theta = \frac{s + x\alpha + y\alpha^2 + z\alpha^3}{d} \quad (s, x, y, z \in \mathbb{Z})$$

alakban, ahol esetünkben a 6.3.1. lemma alapján $d = 2$ és $2 \mid x, y$. Mivel most $\frac{d^6 A}{I(\alpha)} = 32A$, ezért a 2.1.1. tételt alkalmazva elég azt megmutatni, hogy $64 \mid F(u, v)$ teljesül minden olyan $x, y, z \in \mathbb{Z}$ esetén, amikor $2 \mid x, y$ és ahol

$$\begin{aligned} Q_1(x, y, z) &= x^2 + axy - 6y^2 + (a^2 + 12)xz - 5ayz + (a^2 + 37)z^2 = u, \\ Q_2(x, y, z) &= y^2 - xz + ayz - 6z^2 = v, \\ F(u, v) &= u^3 + 6u^2v + (-a^2 - 4)uv^2 + (-24 - 2a^2)v^3. \end{aligned}$$

Ez pedig könnyen ellenőrizhető, ha végignézzük a, x, y, z összes lehetséges értékét modulo 64. (A számolás például Maple segítségével gyorsan végrehajtható.) $\square$

Jegyezzük meg, hogy tételünkből páratlan a esetén következik, hogy a legegyszerűbb negyedfokú test nem monogén, amivel *Olajos P.* [47] tételének egy részére új bizonyítást nyertünk.

Összefoglaló

Az algebrai számelmélet egyik klasszikus problémája annak eldöntése, hogy egy n -edfokú K algebrai számtestben létezik-e hatvány egész bázis, azaz $(1, \alpha, \dots, \alpha^{n-1})$ alakú egész bázis. A K számtestet akkor nevezzük monogénnek, ha van benne hatvány egész bázis. Az értekezésben algebrai számtestek monogenitását és ezzel rokon kérdéseket vizsgálunk.

A bevezető fejezetben a monogenitással kapcsolatos alapvető fogalmakat és eredményeket foglaljuk össze. Egy $\alpha \in \mathbb{Z}_K$ primitív elem indexén $I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+)$ -t értjük. Az α elem akkor és csak akkor generál hatvány egész bázist K -ban, ha $I(\alpha) = 1$. Adott indexű primitív $\mathbb{Z}_K$ -beli elemek és így a hatvány egész bázisok keresése ekvivalens index forma egyenletek megoldásával.

Győry K. [26] effektív módon bebizonyította, hogy az index forma egyenleteknek csak véges sok megoldásuk van, következésképpen $\mathbb{Z}$ -ekvivalenciától eltekintve csak véges sok adott indexű primitív $\mathbb{Z}_K$ -beli elem létezik. Ezután is fontos feladat maradt azonban hatékony algoritmust keresni az index forma egyenlet megoldására, adott indexű primitív elemek meghatározására. Lehetséges továbbá ezeknek a problémáknak algebrai számtestek egy végtelen parametrikus családjában történő vizsgálata, amikor a megoldást a család összes teste esetén egyszerre keressük.

Legyenek $p_1, \dots, p_s$ különböző rögzített prímszámok. Ilyenkor kereshetők azok a K -beli primitív algebrai egészek, melyeknek indexe csak az adott prímekkel osztható, ami pedig az index forma egyenlet p -adikus változatának megoldásával ekvivalens. Ennek megoldásaira szintén *Győry K.* [27] adott effektív felső korlátot.

Végül definiálható egy K algebrai számtest m_K minimális indexe, illetve i_K testindexe, mint a K -beli primitív algebrai egészek indexeinek minimuma, illetve legnagyobb közös osztója.

A 2. fejezetben vegyes szignatúrájú diéder negyedfokú számtestek monogenitását vizsgáljuk. *A. C. Kable* [33] megmutatta, hogy adott

M valós másodfokú számtest esetén csak véges sok olyan K monogén, vegyes szignatúrájú diéder negyedfokú számtest létezik, aminek másodfokú részteste M , a szóba jöhető K testek diszkriminánsának abszolút értékére pedig D_M -től függő felső korlátot adott. Ezt az eredményt kombináljuk *Gaál I.*, *Pethő A.* és *M. Pohst* [19], [22] módszerével, ami az index forma egyenletet Thue-egyenletekre visszavezetve ad hatékony algoritmust negyedfokú számtestekben adott indexű primitív algebrai egész elemek megkeresésére. Egy olyan gyors algoritmust adunk, ami adott M esetén megadja az összes megfelelő K negyedfokú számtestet, egyúttal ezekben meghatározza az összes hatvány egész bázis generátort. Algoritmusunkat például a $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$ másodfokú számtestekre alkalmaztuk, melyekre nyert numerikus eredményeket a fejezet végén ismertetjük.

A 3. és a 4. fejezetben bikvadratikus számtestekkel foglalkozunk. Így nevezzük azokat a negyedfokú algebrai számtesteket, melyek Galois-csoportja Klein-csoport vagy ekvivalens módon azokat, amik különböző négyzetmentes $m, n \in \mathbb{Z} \setminus \{0, 1\}$ számokkal $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ alakba írhatók. Bikvadratikus számtestek monogenitásával sokan foglalkoztak. Az ismert eredmények közül kiemeljük, hogy *K. S. Williams* [53] leírta a bikvadratikus számtestek egy egész bázisát, valamint diszkriminánsát. *Gaál I.*, *Pethő A.* és *M. Pohst* [16] kiszámították az ehhez az egész bázishoz tartozó index formát és a bikvadratikus számtestek testindexét. Ugyancsak ők [21] szimultán Pell-egyenletekre vezető hatékony eljárást adtak a teljesen valós bikvadratikus számtestek esetén az index forma egyenlet megoldására. Ennek illusztrálására az összes 10^6 -nál kisebb diszkriminánsú, teljesen valós bikvadratikus számtest esetén kiszámították a minimális indexet és meghatározták az összes ilyen indexű elemet.

A 3. fejezet célja az, hogy a teljesen komplex eset vizsgálatával teljessé tegyük a monogenitás vizsgálatát bikvadratikus számtestekben. Egyszerűen ellenőrizhető szükséges és elégséges feltételt adunk hatvány egész bázis létezésére és leírjuk az összes hatvány egész bázist generáló elemet. Kiderül, hogy a generátoroknak az egész bázisra vonatkozó együtthatói konstans vektorok egy kis elemszámú halmazából kerülhetnek ki. A bizonyítás fontos eleme, hogy bikvadratikus számtestek esetén az index forma három kvadratikus forma szorzatára bomlik, a teljesen komplex bikvadratikus számtestekben pedig ezen tényezők között van definit kvadratikus forma. Ezt az észrevételt felhasználva tetszőleges jobb oldalú index forma egyenletet

meg lehet oldani. Ezt alkalmazva a teljesen valós esetről említettethez hasonló táblázatot készítünk, melyben összefoglaljuk a 10^4 -nél kisebb diszkriminánsú teljesen komplex bikvadratikus számtesteket, kiszámolva testindexüket, minimális indexüket és a minimális indexszel rendelkező összes elemet.

A 4. fejezetben célunk hatékony algoritmust adni a p -adikus index forma egyenlet megoldására bikvadratikus számtestek esetén. Egy példától eltekintve p -adikus index forma egyenletet numerikusan eddig még nem oldottak meg. Egyenletünket először egy $\mathbb{Z}$ feletti S -egység egyenletre vezetjük vissza. Megmutatjuk, hogy az esetek jelentős részében ennek megoldásával lényegében már célt érhetünk. Kiderül azonban, hogy ha az egyenlet jobb oldalán szereplő prímekek valamelyike két különböző prímeideál szorzatára bomlik fel a bikvadratikus számtest mindhárom résztestében, akkor még meg kell oldani egy S -egység egyenletet a negyedfokú test felett is. Az S -egység egyenletek megoldásához p -adikus és komplex logaritmusok lineáris formáira vonatkozó becsléseket és különböző redukciós eljárásokat alkalmazunk. Az algoritmus illusztrálásaként három konkrét egyenletet is megoldunk.

A bikvadratikus számtestek általánosításaként kapjuk a $\mathbb{Q}(\sqrt{k_1}, \dots, \sqrt{k_n})$ multikvadratikus számtesteket, ahol $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ különböző négyzetmentes számok. Ezek monogenitásával kapcsolatban az 5. fejezetben szereplők az első eredmények, újabban *Y. Motoda* és *T. Nakahara* [42] érték el további eredményeket. A testről mindig feltesszük vagy más feltételekből következik, hogy a számtest fokszáma 2^n . Belátjuk, hogy ha $n = 3$, k_1, k_2, k_3 páronként relatív prímekek, $k_1 < 0$ és $k_2 \equiv k_3 \equiv 1 \pmod{4}$, akkor a multikvadratikus számtest nem monogén. Ezután tetszőleges n esetén igazoljuk, hogy páratlan diszkrimináns mellett a testindex páros, míg további megkötés nélkül az $\mathcal{O} = \mathbb{Z}[\sqrt{k_1}, \dots, \sqrt{k_n}]$ rend minden elemének indexe osztható 2-nek egy nagy kitevős hatványával. Ezekből az is következik, hogy a feltételek megtartása mellett rendre a maximális rendben illetve $\mathcal{O}$ -ban nincs hatvány egész bázis.

Az utolsó fejezetben algebrai számtestek két parametrikus családjára esetén határozzuk meg a testindexet. Először a *Y. Kishi* [36] által vizsgált harmadfokú testeket vizsgáljuk. Így nevezzük a $t^3 - a(a^2 + a + 3)(a^2 + 2)t^2 - (a^3 + 2a^2 + 3a + 3)t - 1 \in \mathbb{Z}[t]$ polinomok felbontási testét, ahol

$a \in \mathbb{Z}$ olyan egész szám, amire egy jól meghatározott, a -tól függő egész szám négyzetmentes. A Kishi-féle harmadfokú testeknek megadjuk egy egész bázisát, majd kiszámítjuk az ehhez tartozó index formát, aminek vizsgálatával bebizonyítjuk, hogy a testindex minden ilyen test esetén 1. Ezután a legegyszerűbb negyedfokú testek családját tekintjük, amiket a $t^4 - at^3 - 6t^2 + at + 1 \in \mathbb{Z}[t]$ polinom felbontási testeként definiálunk, ahol $a \in \mathbb{Z} \setminus \{0\}$ olyan, hogy $a^2 + 16$ -nak az 1-en kívül nincs páratlan négyzetszám osztója. Ezekről a 2. fejezetben már használt módszert alkalmazva azt igazoljuk, hogy testindexük rendre 1 vagy 2 attól függően, hogy a páros vagy páratlan.

Summary

It is a classical problem of algebraic number theory to decide if a number field K of degree n admits power integral bases, that is integral bases of the form $(1, \alpha, \dots, \alpha^{n-1})$. The field K is called monogeneous if there exist power integral bases in K . In our thesis we investigate monogeneity of algebraic number fields and related topics.

In the first chapter we summarize the basic definitions and results about monogeneity. The index of a primitive element $\alpha \in \mathbb{Z}_K$ is defined by $I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+)$. This α generates a power integral basis in K if and only if $I(\alpha) = 1$. Finding primitive elements of $\mathbb{Z}_K$ with given index, and so computing power integral bases is equivalent to solving index form equations.

K. Győry [26] proved that index form equations have only finitely many solutions and effective upper bounds can be given for the absolute values of the solutions. It follows that apart from $\mathbb{Z}$ -equivalence there are only finitely many primitive elements in $\mathbb{Z}_K$ with given index. But it remained an important problem to give efficient algorithms for solving index form equations and for finding primitive elements of given index. We can look at this question in an infinite family of algebraic number fields, which means to find the solutions in each field of the family at the same time.

Let $p_1, \dots, p_s$ be distinct given primes. Now we can search for the primitive algebraic integers in K of index divisible by the fixed primes only, that is equivalent to solving the p -adic version of the index form equation. *K. Győry* [27] gave an effective upper bound for the solutions of this equation.

Finally we can define the minimal index m_K and the field index i_K of the field K as the minimum and greatest common divisor of the indices of all primitive algebraic integer elements in K .

In the second chapter we study the monogeneity of dihedral quartic fields with mixed signature. *A. C. Kable* [33] proved that for a given real quadratic number field M there exist only finitely many monogeneous mixed dihedral quartic field K containing M as a subfield and gave an upper bound for the

absolute value of D_K depending on D_M . We combine this result with the method of *I. Gaál, A. Pethő and M. Pohst* [19], [22], which gives an efficient algorithm for solving index form equations in quartic fields by reducing them to Thue equations. We present a fast algorithm for determining all such quartic fields K if M is given. We also determine all generators of power integral bases in these fields. To illustrate our algorithm we performed computations for $M = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5})$.

In Chapter 3 and Chapter 4 we study biquadratic number fields. These are the quartic fields having Klein group as Galois group or equivalently the fields of type $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ where $m, n \in \mathbb{Z} \setminus \{0, 1\}$ are distinct square-free integers. The monogeneity of biquadratic number fields were considered by several authors. *K. S. Williams* [53] described an integral basis and the discriminant of these fields. *I. Gaál, A. Pethő and M. Pohst* [16] formulated the corresponding index forms and characterized the field indices. They [21] also gave an efficient algorithm for solving index form equations in totally real biquadratic fields by solving simultaneous Pellian equations. Using this method they determined the minimal indices and all elements with minimal index in the totally real biquadratic fields having discriminant less than 10^6 .

To complete the above theory of power integral bases in biquadratic number fields, our purpose in the third chapter is to give necessary and sufficient conditions for the monogeneity in totally complex biquadratic fields which can be easily checked. We also describe all generators of power integral bases in totally complex biquadratic fields. It turns out, that surprisingly the coordinates of the generators are contained in a finite set of constant vectors. It is important in our proof that the index form splits into three quadratic factors in biquadratic fields, moreover in the totally complex case there is a definite quadratic form among these factors. Using this we can solve index form equations with arbitrary number on the right hand side. This way we can present a list of all totally complex biquadratic fields up to discriminant 10^4 computing the field indices, the minimal indices and elements with minimal index.

In the fourth chapter our purpose is to give an efficient algorithm for solving the p-adic analogue of the index form equation in biquadratic fields. Except from an example no p-adic index form equations have been solved so far. First we have to solve an S-unit equation over $\mathbb{Z}$. We show that in

most of the cases this is enough to solve our equation completely. But if there is a prime on the right hand side of our equation which splits into the product of two distinct prime ideals in all the three quadratic subfields of our biquadratic field, then we have to proceed by solving an S-unit equation over the quartic field. Our procedure involves estimates for linear forms of p-adic and complex logarithms and certain reduction procedures. To illustrate our algorithm we solve three concrete equations.

As the generalization of biquadratic number fields we get multiquadratic fields $\mathbb{Q}(\sqrt{k_1}, \dots, \sqrt{k_n})$ where $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ are distinct square-free integers. In higher degree multiquadratic fields the problem of monogeneity was not investigated yet, the results of Chapter 5 are the first known ones. Recently *Y. Motoda és T. Nakahara* [42] presented some other results. In the following we assume or it follows from other assumptions that the multiquadratic field is of degree 2^n . Our first result states that if $n = 3$, k_1, k_2, k_3 are pairwise coprime, $k_1 < 0$ and $k_2 \equiv k_3 \equiv 1 \pmod{4}$, then the field is not monogeneous. For arbitrary n we prove that a multiquadratic field with odd discriminant have even field index and without any additional assumptions the index of any element of the order $\mathcal{O} = \mathbb{Z}[\sqrt{k_1}, \dots, \sqrt{k_n}]$ is divisible by a high power of 2. Consequently with these assumptions the maximal order and $\mathcal{O}$ admits no power integral bases.

In the final chapter we compute the field indices in two parametric family of algebraic number fields. First we present the cubic fields of *Y. Kishi* [36]. These are the fields defined as the splitting fields of the polynomials $t^3 - a(a^2 + a + 3)(a^2 + 2)t^2 - (a^3 + 2a^2 + 3a + 3)t - 1 \in \mathbb{Z}[t]$, where $a \in \mathbb{Z}$ such that a certain integer depending on a is square-free. We describe an integral basis of the cubic fields of Kishi, compute the corresponding index form and using it we have that the field index of these fields is 1. Next we consider the family of simplest quartic fields, that is the splitting fields of the polynomials $t^4 - at^3 - 6t^2 + at + 1 \in \mathbb{Z}[t]$, where $a \in \mathbb{Z} \setminus \{0\}$ and $a^2 + 16$ is not divisible by any odd squares other than 1. By the method also used in Chapter 2 we prove that the field index of a simplest quartic field is 1 or 2 depending on the parity of a .

Irodalom

- [1] A. Baker and H. Davenport, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$* , Quart. J. Math. Oxford, **20** (1969), 129–137.
- [2] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math., **442** (1993), 19–62.
- [3] M. Bauer, *Über den ausserwesentlichen Diskriminantenteiler algebraischer Körper*, Math. Ann., **64** (1907), 573.
- [4] Y. Bilu, I. Gaál and K. Győry, *Index form equations in sextic fields: a hard computation*, Acta Arith., **115** (2004), 85–96.
- [5] Y. Bilu and G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory, **60** (1996), 373–392.
- [6] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörmig and K. Wildanger, *KANT V4*, J. Symbolic Comp., **24** (1997), 267–283.
- [7] H. T. Engstrom, *On the common index divisors of an algebraic field*, Trans. Amer. Math. Soc., **32** (1930), 223–237.
- [8] T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ., **26** (1984), 27–41.
- [9] I. Gaál, *Computing power integral bases in algebraic number fields*, in: Number Theory (eds. K. Győry, A. Pethő and V. T. Sós), Walter de Gruyter, 1998, 243–254.
- [10] I. Gaál, *Power integer bases in algebraic number fields*, Annales Univ. Sci. Budapest., Sectio Comp., **18** (1999) 61–87.
- [11] I. Gaál, *Diophantine Equations and Power Integral Bases*, Birkhäuser, 2002.
- [12] I. Gaál and K. Győry, *Index form equations in quintic fields*, Acta Arith., **89** (1999), 379–396.
- [13] I. Gaál, I. Járási and F. Luca, *A remark on prime divisors of lengths of sides of Heron triangles*, Experimental Math., **12** (2003), 303–310.

- [14] I. Gaál and G. Nyul, *Computing all monogeneous mixed dihedral quartic extensions of a quadratic field*, J. Théorie Nombres Bordeaux, **13** (2001), 137–142.
- [15] I. Gaál and G. Nyul, *Index form equations in biquadratic fields: the p -adic case*, Publ. Math. Debrecen, **68** (2006), 225–242.
- [16] I. Gaál, A. Pethő and M. Pohst, *On the indices of biquadratic number fields having Galois group V_4* , Arch. Math., **57** (1991), 357–361.
- [17] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in biquadratic number fields, I*, J. Number Theory, **38** (1991), 18–34.
- [18] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in biquadratic number fields, II*, J. Number Theory, **38** (1991), 35–51.
- [19] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in quartic number fields*, J. Symbolic Comp., **16** (1993), 563–584.
- [20] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in dihedral quartic number fields*, Experimental Math., **3** (1994), 245–254.
- [21] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in biquadratic number fields, III. The bicyclic biquadratic case*, J. Number Theory, **53** (1995), 100–114.
- [22] I. Gaál, A. Pethő and M. Pohst, *Simultaneous representation of integers by a pair of ternary quadratic forms – with an application to index form equations in quartic number fields*, J. Number Theory, **57** (1996), 90–104.
- [23] I. Gaál and N. Schulte *Computing all power integral bases of cubic fields*, Math. Comp., **53** (1989), 689–696.
- [24] M.-N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$* , Publ. Math. Fac. Sci. Besançon, Theor. Nombres, Année 1977-1978, Fasc. 2.

- [25] M.-N. Gras and F. Tanoé, *Corps biquadratiques monogènes*, Manuscripta Math., **86** (1995), 63–79.
- [26] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné III.*, Publ. Math. Debrecen, **23** (1976), 141–165.
- [27] K. Győry, *On polynomials with integer coefficients and given discriminant V. p -adic generalizations*, Acta Math. Acad. Sci. Hungar., **32** (1978), 175–190.
- [28] K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv., **54** (1979), 583–600.
- [29] K. Győry, *Bounds for the solutions of decomposable form equations*, Publ. Math. Debrecen, **52** (1998), 1–31.
- [30] K. Győry, *Discriminant form and index form equations*, in: Algebraic Number Theory and Diophantine Analysis (eds. F. Halter-Koch and R. F. Tichy), Walter de Gruyter, 2000, 191–214.
- [31] K. Győry, *Index form equations and their applications*, Proc. Inst. Math. NASB Belarus, **13** (2005), 83–93.
- [32] J. G. Huard, B. K. Spearman and K. S. Williams, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory, **51** (1995), 87–102.
- [33] A. C. Kable, *Power bases in dihedral quartic fields*, J. Number Theory, **76** (1999), 120–129.
- [34] L.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly, **96** (1989), 133–137.
- [35] H. K. Kim and J. S. Kim, *Computation of the different of the simplest quartic fields*, manuscript.
- [36] Y. Kishi, *A family of cyclic cubic polynomials whose roots are systems of fundamental units*, J. Number Theory, **102** (2003), 90–106.
- [37] A. J. Lazarus, *On the class number and unit index of simplest quartic fields*, Nagoya Math. J., **121** (1991), 1–13.

- [38] G. Lettl and A. Pethő, *Complete solution of a family of quartic Thue equations*, Abh. Math. Sem. Univ. Hamburg, **65** (1995), 365–383.
- [39] D. A. Marcus, *Number Fields*, Springer–Verlag, 1977.
- [40] L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.
- [41] Y. Motoda, *On integral bases of certain real monogenic biquadratic fields*, Rep. Fac. Sci. Engrg. Saga Univ. Math., **33** (2004), 9–22.
- [42] Y. Motoda and T. Nakahara, *Monogenesis of algebraic number fields whose Galois groups are 2-elementary abelian*, Proc. 2003 Nagoya Conf. „Yokoi-Chowla Conjecture and Related Problems” (eds. S. Katayama, C. Levesque and T. Nakahara), Furukawa Total Pr. Co., 2004, 91–99.
- [43] T. Nakahara, *On the indices and integral bases of non-cyclic but abelian biquadratic fields*, Arch. Math., **41** (1983), 504–508.
- [44] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Third Edition, Springer–Verlag, 2004.
- [45] G. Nyul, *Power integral bases in totally complex biquadratic number fields*, Acta Acad. Paed. Agriensis, Sectio Math., **28** (2001), 79–86.
- [46] G. Nyul, *Non-monogeneity of multiquadratic number fields*, Acta Math. Inf. Univ. Ostraviensis, **10** (2002), 85–93.
- [47] P. Olajos, *Power integral bases in the family of simplest quartic fields*, Experimental Math., **14** (2005), 129–132.
- [48] B. Schmal, *Diskriminanten, $\mathbb{Z}$ -Ganzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern*, Arch. Math., **52** (1989), 245–257.
- [49] N. P. Smart, *Solving a quartic discriminant form equation*, Publ. Math. Debrecen, **43** (1993), 29–39.
- [50] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Math. Soc., Cambridge University Press, 1998.
- [51] B. K. Spearman and K. S. Williams, *The index of a cyclic quartic field*, Monatsh. Math., **140** (2003), 19–70.

- [52] B. M. M. de Weger, Algorithms for diophantine equations, CWI Tract 65, Amsterdam, 1989.
- [53] K. S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull., **13** (1970), 519–526.
- [54] K. Yu, *Linear forms in p -adic logarithms*, Acta Arith., **53** (1989), 107–186.
- [55] E. von Žyliński, *Zur Theorie der ausserwesentlichen Diskriminantenteiler algebraischer Körper*, Math. Ann., **73** (1913), 273–274.

Publikációk

1. I. Gaál and G. Nyul, *Computing all monogeneous mixed dihedral quartic extensions of a quadratic field*, Journal de Théorie des Nombres de Bordeaux, **13** (2001), 137–142.
2. G. Nyul, *Power integral bases in totally complex biquadratic number fields*, Acta Academie Paedagogicae Agriensis, Sectio Mathematicae, **28** (2001), 79–86.
3. G. Nyul, *Non-monogenity of multiquadratic number fields*, Acta Mathematica et Informatica Universitatis Ostraviensis, **10** (2002), 85–93.
4. G. Nyul, *A divisibility problem of binomial coefficients*, Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös nominatae, Sectio Mathematica, **47** (2004), 115–121.
5. I. Gaál and G. Nyul, *Index form equations in biquadratic fields: the p -adic case*, Publicationes Mathematicae Debrecen, **68** (2006), 225–242.

Előadások

1. *Power integral bases in biquadratic number fields*, The 15th Czech and Slovak International Conference on Number Theory, 2001. szeptember 3.–8., Ostravice (Csehország).
2. *Index forma egyenletek bikvadratikus számtestekben*, Számelméleti tudományos emlékülés Kiss Péter emlékére, 2002. november 22.–23., Eger.
3. *Index form equations in biquadratic and multiquadratic number fields*, Workshop on Computational Number Theory, 2003. október 20.–24., Debrecen.
4. *Binomiális együtthatók oszthatósága*, Soproni Diofantikus Nap, 2004. október 9., Sopron.
5. *Hatvány egész bázisok másodfokú számtestek kompozitumában*, Nyíregyházi Kriptográfiai és Diofantikus Nap, 2005. április 30., Nyíregyháza.
6. *The field index of some families of number fields*, The 17th Czech and Slovak International Conference on Number Theory, 2005. szeptember 5.–10., Malenovice (Csehország).
7. *Algebrai számtestek testindexe*, Berekfürdői Diofantikus és Kriptográfiai Napok, 2006. április 22., Berekfürdő.

Monogenitási vizsgálatok algebrai számtestekben

Értekezés a doktori (PhD) fokozat megszerzése érdekében
a matematika tudományában.

Írta: Nyul Gábor okleveles matematikus

Készült a Debreceni Egyetem Matematika és Számítástudományok
Doktori Iskolája (Diofantikus és konstruktív számelmélet programja)
keretében

Témavezető: Dr. Gaál István

A doktori szigorlati bizottság:

elnök:	Dr. Bódi Béla	
tagok:	Dr. Mátyás Ferenc	
	Dr. Pethő Attila	

A doktori szigorlat időpontja: 2007. január 3.

Az értekezés bírálói:

Dr.		
Dr.		
Dr.		

A bírálóbizottság:

Dr.		
Dr.		
Dr.		
Dr.		
Dr.		

Az értekezés védésének időpontja: 200... ..