T.C.
SELÇUK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BELİRLİ VE BELİRSİZ İKİ DEĞİŞKENLİ KUADRATİK FORMLARLA TEMSİL EDİLEN ASALLAR

Nihal BİRCAN

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

Konya, 2008

ÖZET

Doktora Tezi

BELİRLİ VE BELİRSİZ İKİ DEĞİŞKENLİ
KUADRATİK FORMLARLA
TEMSİL EDİLEN
ASALLAR

Nihal BİRCAN

Selçuk Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Hasan ŞENAY

Mayıs 2008, Sayfa: 98

Jüri:

Prof. Dr. Hasan ŞENAY Prof. Dr. Dursun TAŞÇI

Prof. Dr. Hüseyin ALTINDİŞ Prof. Dr. Durmuş BOZKURT

Yrd. Doç. Dr. Ahmet CİHANGİR

Bu çalışmada, genel anlamda tamsayıların özellikle asalların temsil problemi ele alınmıştır. Özellikle, a, b, c en az biri sıfırdan farklı tamsayı olmak üzere $f(x,y)=ax^2+bxy+cy^2$ iki değişkenli kuadratik formunun temsilleri üzerinde çalışılmıştır. Bir $f(x,y)$ formu, x_0, $y_0 \in \mathbb{Z}$ olmak üzere;

$$ax_0^{\,2}+bx_0y_0+cy_0^{\,2}=m$$

oluyorsa bu form m *tamsayısını temsil eder* denir. Eğer $\gcd(x_0,y_0)=1$ ise, bu temsil primitiftir.

Verilen bir formla hangi tamsayıların temsil edilebildiği, hangi formların verilen tamsayıyı temsil ettiği, bir form bir tamsayıyı temsil ediyorsa, böyle kaç tane temsillerin olduğu ve bu temsillerin sayısı ve nasıl hesaplandığı soruları temsil probleminin dolayısıyla çalışmamızın kapsamındadır.

İdeal teorisi geliştirildikten sonra iki değişkenli kuadratik formların, kuadratik sayı cisminin sınıf grubu teorisiyle özdeş olduğu görülmüştür.

Burada, temsil problemi, kuadratik formlar, idealler ve bunlar arasındaki ilişkiler verilmiştir.

Sonuçlar kısmında ise, ilk olarak iki değişkenli kuadratik formların kompozisyonu ideal teorisi kullanılarak ispatlanmıştır. Ayrıca, çok-değişkenli $x^2 + y^2 + z^2 = t^2$ polygonal sayılarının yeni bir parametrik bir temsili *magma* programı kullanılarak ispatlanmıştır.

Anahtar Kelimeler: İki değişkenli kuadratik formlar, polygonal sayılar, idealler

ABSTRACT

Ph.D. Thesis

PRIMES
REPRESENTED BY
DEFINITE AND INDEFINITE
BINARY QUADRATIC FORMS

Nihal BİRCAN

Selçuk University
Graduate School of Natural and Applied Science
Department of Mathematics

Supervisor: Prof. Dr. Hasan ŞENAY

May 2008, Page: 98

Jury:

Prof. Dr. Hasan ŞENAY — Prof. Dr. Dursun TAŞÇI

Prof. Dr. Hüseyin ALTINDİŞ — Prof. Dr. Durmuş BOZKURT

Assist. Prof. Dr. Ahmet CİHANGİR

In this study; we studied representation problem for integers, especially prime numbers. In particular, binary quadratic forms $f(x,y)=ax^2+bxy+cy^2$ with integer coefficients a, b, c is studied. The questions 'which integers can be represented by a given form?, which form can represent a given integer?, If a form represents an integer how many representations exist? How may they all be calculated?' are in the scope of representation problem.

A form $f(x,y)$ represents an integer m, if there exists integers x_0, y_0 such that;

$$ax_0^2+bx_0y_0+cy_0^2=m.$$

The representation is primitive if $\gcd(x_0,\ y_0)=1$.

When the theory of ideals was developed, it became clear that the theory of binary quadratic forms was essentially identical with the theory of the class groups of quadratic fields.

In our study, composition of binary quadratic forms is proved by using ideal theory and a new parametric representation for $x^2+y^2+z^2=t^2$ of polygonal numbers is given.

Keywords: Binary quadratic forms, polygonal numbers, ideals

ÖNSÖZ

Selçuk Üniversitesi Fen Bilimleri Enstitüsü'ne doktora tezi olarak sunulan bu çalışma, TÜBİTAK 105T070, HD/47 no'lu proje ile desteklenmiştir.

Çalışmamın tamamlanmasında gereken her türlü yardımda bulunan, bilgi ve tavsiyeleriyle beni yönlendiren danışmanım Prof. Dr. Hasan ŞENAY'a saygı ve teşekkürlerimi sunarım.

Bir akademisyen için son derece faydalı olduğunu düşündüğüm TÜBİTAK Tr-Access Mobility (Araştırmacıların yurtiçi dolaşımı) programının düzenleyicilerine ve bu program dolayısıyla bilgi ve bilimsel vizyonumun gelişmesine büyük katkısı olan Prof. Dr. Ahmet K. FEYZİOĞLU'na teşekkürlerimi ve saygılarımı sunarım.

Berlin Teknik Üniversitesi Matematik Enstitüsü'ndeki çalışmalarım süresince bana sonsuz destek vererek bilgisini paylaşan Prof. Dr. Michael E. POHST'a en derin teşekkürlerimi sunarım.

Akademik tecrübenin bilim dalı farkı gözetmeyeceğinden hareketle, her zaman tecrübelerini paylaşan ve çalışma ortamımızı mükemmel bir paylaşım ortamı haline getirmemizde büyük katkısı olan çalışma arkadaşım Kimya Anabilim Dalı öğretim üyelerinden Yrd. Doç. Dr. Emine G. AKGEMCİ'ye teşekkürü bir borç bilirim.

Çalışmalarımın her aşamasında yardımlarını, bilgi ve önerilerini esirgemeyen S.Ü. Fen-Edebiyat Fakültesi Matematik Bölümü'ndeki ve S. Ü. Eğitim Fakültesi Matematik Eğitimi Anabilim Dalı'ndaki kıymetli hocalarıma, çalışmalarımı gerçekleştirmem için bana fırsat tanıyan Selçuk Üniversitesi yönetici ve ilgililerine, teknik anlamda her zaman destekleyen S.Ü. Eğitim Fakültesi bilgi-işleminden sorumlu uzman Kemal KAYA'ya teşekkürlerimi sunarım.

Hayatımın her aşamasında yanımda olan sevgili ailemin verdiği destek için sonsuz sevgi, saygı ve minnettarlığımı sunarım.

Nihal BİRCAN

İÇİNDEKİLER

ÖZET ..... **iii**
ABSTRACT ..... **v**
ÖNSÖZ ..... **vi**
İÇİNDEKİLER ..... **vii**
TABLOLARIN LİSTESİ ..... **ix**
SEMBOLLER ..... **x**
1. GİRİŞ **1**
2. KAYNAK ARAŞTIRMASI **7**
3. TAMSAYILARIN TEMSİL PROBLEMİ **16**
4. KUADRATİK SAYI CİSİMLERİ VE KUADRATİK FORMLAR **23**
4.1. Kuadratik Sayı Cisimleri ve Cebirsel Sayılar 23
4.1.1. Kuadratik Cismin Diskriminantı 29
4.2. Gauss Tamsayıları 32
4.3. İki Değişkenli Kuadratik Formlar 36
4.3.1. Lineer dönüşümler 37
4.3.2. İki değişkenli kuadratik formların denkliği 40
4.3.3. İki değişkenli kuadratik formların indirgenebilirliği 42
5. KUADRATİK FORMLAR VE İDEALLER **45**
5.1. İdealler 45
5.1.1. İdeallerin toplamı ve baz 47
5.1.2. İdeal bazının dönüştürülmesi 49
5.2. İki Değişkenli Kuadratik Formlar ve İdealler 51
5.2.1. Bir idealin sıralı bazı 51
5.2.2. Dar anlamda denk idealler 53
5.2.3. Kuadratik formların denklik sınıfları 55
5.2.4. Karşılık gelme prosedürü 58
5.2.5. Karşılık gelme teoremi 62
5.3. Kompozisyon ve Sınıf Grubu 67
5.4. Karakterler 79

5.4.1. Karakterlerin toplam sayısı..... 83
5.5. Cins Teorisi..... 86
6. SONUÇLAR..... 90
7. KAYNAKLAR..... 96
ÖZGEÇMİŞ..... 98

TABLOLARIN LİSTESİ

Tablo 1	İki değişkenli kuadratik formlarla temsil edilen bazı asallar	22
Tablo 2	D diskriminantının indirgenmiş formları sınıf sayısı	44
Tablo 3	Verilen indirgenmiş formların kompozisyonu	70
Tablo 4	$D \equiv 0 \pmod 4$ olduğunda $D = -4n,\ (n > 0)$ durumunda $C(D)$ sınıf grubunda mertebesi 2 olan elemanların sayısı	77
Tablo 5	Mod 5 e göre indirgenmiş kalanlar	81
Tablo 6	Mod 8 e göre indirgenmiş kalanlar	82

SEMBOLLER

$\mathbb{Z}$	:	Tamsayılar kümesi : $\{...-2,\ -1,\ 0,\ 1,\ 2,...\}$
$\mathbb{Z}^*$	:	Negatif olmayan tamsayılar kümesi: $\{\ 0,\ 1,\ 2,...\}$
$\mathbb{Z}^+$	:	Pozitif tamsayılar kümesi: $\{1,\ 2,...\}$
$\mathbb{N}$	:	Doğal sayılar kümesi
$\mathbb{Q}$	:	Rasyonel sayılar kümesi
$\mathbb{Q}^*$	:	Negatif olmayan rasyonel sayılar kümesi
$\mathbb{R}$	:	Reel sayılar kümesi
$K=\mathbb{Q}(\sqrt{d})$	:	İkinci dereceden sayı cismi
$SL(2,\mathbb{Z})$	:	Determinantı $\{+1\}$ ve elemanları tamsayı olan 2×2 matris
$GL(2,\mathbb{Z})$	:	Determinantı $\{\mp 1\}$ ve elemanları tamsayı olan 2×2 matris
$\mathfrak{O}$	:	$\mathbb{Q}(\sqrt{d})$ cismindeki kuadratik tamsayıların oluşturduğu tamlık bölgesi
$\mathfrak{O}_n$	:	$\mathbb{Q}(\sqrt{d})$ deki rasyonellerin tamamını içermeyen bazı sabit pozitif n rasyonel sayılarıyla karakterize edilen mod n e göre (değişken) bir rasyonel sayıya kongrent olan $\mathfrak{O}$ nun bir tamlık bölgesi
R	:	Birimli değişmeli halka
D	:	İki değişkenli kuadratik formun diskriminantı
d	:	Cisim diskriminantı
$N(\alpha)$	:	α nın $\mathbb{Q}$ üzerinde normu
$T(\alpha)$	:	α nın $\mathbb{Q}$ üzerinde izi
$(\mathbb{Z}/m\mathbb{Z})$	:	m modülüne göre denklik sınıfları
$(\mathbb{Z}/m\mathbb{Z})^*$	:	m modülüne göre tersleri alınabilen sayıların denklik sınıfları
$\mathbb{Z}[i]$	:	Gauss tamsayılar halkası
$[p]$	:	p tamsayısının kalan sınıfı
$\gcd(a,b)$	:	a ve b nin en büyük ortak böleni

$\mathfrak{j}, \mathfrak{a}, \mathfrak{b}$	:	İdealler
$Mat_2(\mathbb{Z})$	:	Elemanları tamsayılar olan 2×2 tipindeki matrisler
$\left(p/q\right)$	:	Legendre sembolü

1. GİRİŞ

Bu bölümde, çalışmamızda bahsedilen bazı tanımlar ve genel bilgiler verilmiştir.

Cebirsel sayılar teorisinin kapsamında olan bu konu tamsayıların ve özellikle asalların formlarla temsil edilmesi problemi olup, temelde denklemlerin çözümü ile yakından ilgilidir. Bu konuda yapılan çalışmalar ilerledikçe bunun matematiğin diğer dalları ile ilgisi anlaşılmış ve çalışmalar sonucunda üretilen algoritmalarla her geçen gün daha da ileriye gitmiştir.

Bu çalışmamızda 'Tamsayıların temsil problemi' bölümünde; temel anlamda temsil problemi ve bu problemin ileriki aşamalarında kapsadığı konular kısaca açıklanmıştır.

'Kuadratik sayı cisimleri ve kuadratik formlar bölümünde iki ve çok değişkenli kuadratik formlar tanımlanarak temel özellikleri verilmiştir. Cebirsel sayılar ve $\mathbb{Q}(\sqrt{d})$ kuadratik sayı cismi detaylı bir şekilde incelenmiştir.

'Kuadratik formlar ve idealler' bölümünde; idealler ve ideal bazı hakkında bilgiler verilip, ideallerin formlara nasıl karşılık geldiği, karşılık gelme teoremiyle açıklanmıştır.

Daha sonraki bölümlerde ise kalan sınıfını temsil ederken kullanılan karakterlerden ve bunların grup yapısından bahsedilerek bu karakterlerin cins teorisinde nasıl kullanıldığı açıklanmıştır.

Son olarak; formların kompozisyonu ile ilgili bulduğumuz sonuçlar ve kuadratik denklemlere çalışırken elde ettiğimiz diğer sonuçlar verilmiştir.

Eğer 1'den farklı bir p doğal sayısı sadece 1 ve p sayılarına bölünüyorsa, o sayıya *indirgenemez sayı* denir. Bu tanıma göre, $p>1$ ise ve her $x, y \in \mathbb{N}$ için, $p = xy$ eşitliği doğru olduğunda ya x ya da y sayısı 1 olmak zorunda ise, o zaman

p ye *indirgenemez* denir. Örneğin, 2, 3, 5, 7, 11, 13, 17, 19, 23 indirgenemez doğal sayılardır.

Eğer 1'den ve 0'dan farklı bir p pozitif tamsayısı, iki sayının çarpımını böldüğünde çarpanlardan en azından birini bölüyorsa o sayıya *asal* denir. Yani eğer $x, y \in \mathbb{N}$ için, p, xy' yi böldüğünde, p ya x'i ya da y'yi bölüyorsa p' ye asal denir. Örneğin 2, 3, 5, 7, 11, 13, 17, 19, 23 asal sayılardır.

Bu iki kavram doğal sayılarda ve tamsayılarda örtüşürler. Yani asal her doğal sayı aynı zamanda indirgenemezdir ve indirgenemez her doğal sayı asaldır. Asallarla indirgenemezler arasında doğal sayılarda ve tam sayılarda bir ayırım yoksa da, başka sayı kümelerinde bu iki kavram arasında bir ayırım vardır. Bir sayı halkasında indirgenemez ve asal kavramı her zaman aynı değildir. Kısaca örnekleyerek açıklamak gerekirse, 2, $\mathbb{Z}$'nin indirgenemezi olmasına karşın $\mathbb{Z}[\sqrt{2}]$'nin indirgenemezi değildir; 2, $\mathbb{Z}[\sqrt{2}]$ halkasında $\sqrt{2}.\sqrt{2}$ olarak indirgenebilirdir. Ayrıca,

$$7 = (3+\sqrt{2})(3-\sqrt{2})$$

eşitliğinden dolayı 7 de $\mathbb{Z}[\sqrt{2}]$ halkasında indirgenir bir sayıdır. Görüldüğü gibi $\mathbb{Z}$ de indirgenemez olan bir sayı $\mathbb{Z}[\sqrt{2}]$ halkasında indirgenebilirdir. Son olarak her asalın her halkada indirgenemez olduğunu ama her indirgenemezin her halkada bir asal olmadığını söyleyerek formların temsil problemiyle ilgili genel bilgiler verelim. (Nesin 2004)

18. yüzyılda Euler ve diğer matematikçiler bir tamsayıyı $x^2 + 2y^2$ veya $x^2 + 3y^2$ gibi formlarla temsil edebilmenin gerek ve yeter koşullarını bulmada oldukça başarılı olmuşlar ve bu formlarla hangi asalların temsil edildiğini araştırmışlardır. Bu araştırmalar matematikçileri benzer sonuçları kuadratik formlar için bulmaya yöneltmiştir. Bu bağlamda; bir kuadratik form; homojen, kuadratik iki değişkenli a, b, c katsayıları tamsayı olan $ax^2 + 2bxy + cy^2$ biçimindeki bir

ifadedir. Kuadratik formlar iki (binary form), üç (ternary form) veya herhangi sayıda değişkene sahip olabilir. (Davenport 1992)

Genel kuadratik form için kullanılan iki ayrı notasyon vardır. Birincisi $ax^2 + bxy + cy^2$, ikincisi $ax^2 + 2bxy + cy^2$ dir. İkinci durumda ortadaki katsayı çifttir. $ax^2 + 2bxy + cy^2$ notasyonundaki form $x^2 + xy + y^2$ biçimindeki formları da kapsar. Çünkü açık olarak bu formla sözgelişi $2x^2 + 2xy + 2y^2 = 2(x^2 + xy + y^2)$ formunun bütün özellikleri aynıdır. Bu notasyonların birinin diğerine üstünlüğü yoktur. Bazı sonuçlar ilk notasyonu kullandığımızda, bazı sonuçlar ise diğer notasyonu kullandığımızda daha basit olarak ortaya çıkmaktadır. Birinci durumdaki notasyon Dedekind'in formların sınıfları arasında karşılaştırmalarda daha uygun ve $a\xi^2 + b\xi + c = 0$ ın kökleri ile hesaplanan bazı cebirsel sayı kümeleri için daha avantajlıdır. $D = b^2 - 4ac$ diskriminantı birinci durum için söz konusudur. Burada $(a,\ b,\ c)$ notasyonu ikinci durum için kullanılır. 2 çarpanının kullanıldığı notasyon Legendre, Gauss ve Dirichlet tarafından; 2 çarpanının olmadığı notasyon ise Lagrange, Kronecker ve Dedekind tarafından kullanılmıştır.

Genel kuadratik $ax^2 + 2bxy + cy^2$ formlarıyla ilgili problemlerin ilki; aralarında asal x, y tamsayıları için bu formun hangi n tamsayılarını temsil ettiği problemidir. Bu problemde $x' = \alpha x + \beta y$ ve $y' = \gamma x + \delta y$ ile verilen lineer dönüşümleri göz önüne alalım. Böyle bir dönüşümde $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ katsayıları $\alpha\delta - \beta\gamma = \mp 1$ eşitliğini gerçekleyen tamsayılar olmak üzere; bu unimodüler dönüşüm bir denklik bağıntısı olduğundan $f(x, y)$ formu $f(x', y')$ formuna dönüşür. Böylece (x, y), $\mathbb{Z}\times\mathbb{Z}$ de değerler aldıkça (x', y') de $\mathbb{Z}\times\mathbb{Z}$ de değerler alacaktır. O halde; yeni form $a'x'^2 + 2b'x'y' + c'y'^2$ biçiminde olup ilk formla aynı değerleri alacaktır ki bu durumda formlara '*denktir*' denir. Böylece denklik tanımı gereği kuadratik formlarda çalışırken bir formun yerine daha basit olan dengi ile çalışmak uygun olacaktır. Yukarıda bahsettiğimiz bir sayının temsil probleminin denk formlar için değişmeyeceğini söyleyebiliriz. '$x,\ y$ aralarında asal ve $n = nx^2 + 2bxy + cy^2$ ise n tamsayısı $(a,\ b,\ c)$ formu ile *has olarak temsil edilir* denir.' Bir $(a,\ b,\ c)$

formuyla has olarak temsil edilebilen tamsayıların tam olarak $(a,\ b,\ c)$ ye denk olan formların ilk katsayısı olan tamsayılar olduğunu söyleyebiliriz.

Lagrange denk formlarla ilgili yaptığı çalışmalarda pratik ve kesin olan yöntemler bulmuştur. Bunlardan en önemlisi bütün derin araştırmalar için genel bir fikir olan sınıf sayısını keşfetmiştir. $x' = x + y$ ve $y' = y$ dönüşümleriyle $ax^2 + 2bxy + cy^2$ formunu $ax'^2 + (2b \pm 2a)x'y' + (a + c \pm 2b)y'^2$ denk formuna dönüştürmüş ve benzer dönüşümlerle ilk formu $(a + c \pm 2b)x'^2 + (2b \pm 2c)x'y' + cy'^2$ formuna dönüştürmüştür ki, bu bize katsayıların basitleştirilmesi için Euclid algoritmasına benzer bir yöntem vermiş olur. Bununla beraber basitleştirme işlemi tamamlanmadan bu yöntemin yeterince açık olmadığını söyleyebiliriz. O zaman birbirine denk olmayan formları nasıl ayırt edebileceğimiz sorusu ortaya çıkar. Bunun için bir formun değişmezlerinden (invariant) biri olan $D = b^2 - ac$ diskriminant kavramını kullanmak uygun olur.

Diskriminantları farklı olan formların denk olmadığı açıktır. Fakat aynı diskriminantlı iki formun denk olup olmaması diskriminantın değerine bağlıdır. Örneğin; $D = -1$ olan bütün formlar $x^2 + y^2$ ye denktir. Lagrange, bunu Fermat'ın son teoreminin yeni bir ispatını vermek amacıyla bu formun asal değerleri için kullandı. Buradan benzer olarak ikinci bir sonuç çıkardı ki $x^2 + 2y^2$ formunun asal değerleri $8n + 1$ ve $8n + 3$ lineer formlarına karşılık gelir. Bunu da $D = -2$ olan bütün formların $x^2 + 2y^2$ ye denk olduğunu göstererek yaptı. Öte yandan; $D = -5$ olan $x^2 + 5y^2$ ve $2x^2 + 2xy + 3y^2$ formları birbirine denk değildir. $D = -5$ in karşılık geldiği sayılar $20n + 1,\ 20n + 3,\ 20n + 7$ ve $20n + 9$ dur. Fakat bunların hepsi $x^2 + 5y^2$ formuyla temsil edilmez. Yani; $20n + 1$ ve $20n + 9$, $x^2 + 5y^2$, formunda $20n + 3$ ve $20n + 7$ ise $2x^2 + 2xy + 3y^2$ formuna karşılık gelir. (Dirichlet 1999)

Ayrıca buna ek olarak 1993 te Halter-Koch ve 1991 de Williams'ın yaptıkları çalışmaya göre $a \neq b$, A ve B $(a,b) = 1$ $(A,B) = 1$ olacak şekilde pozitif tamsayılar olmak üzere bazı x ve y tamsayıları için $(p, 2ab) = 1$ olmak üzere $p \equiv B \pmod{A}$

asalı, $ax^2 - by^2$ ile temsil edilebilirdir. Aynı şekilde bazı X ve Y tamsayıları için $(q, 2ab) = 1$ ve $q \equiv -B \pmod{A}$ olan her asal $bX^2 - aY^2$ formuyla temsil edilebilir. (Weisstein 2006)

Herhangi bir pozitif belirli (a,b,c) formu, katsayıları $|b| \le a \le c$ eşitsizlik takımını sağlıyorsa *indirgenmiş form* olarak adlandırılır. Ayrıca $D < 0$ olan (a,b,c) pozitif belirli formu indirgenmiş ise $|b| \le \sqrt{\frac{|D|}{3}}$ ve $a \le \sqrt{\frac{|D|}{3}}$ şartlarını sağlar. Burada önemle belirtilmesi gereken sonuç verilen bir forma denk olan bir ve yalnız bir indirgenmiş form olduğudur. Ayrıca; sınıf sayısının D diskriminantının indirgenmiş formlarının sayısı olduğunu da söyleyebiliriz. (Feyzioğlu 2004)

Diskriminantı verilen aynı bir D sayısı olan; birbirine denk olmayan formların sayısı sınıf sayısı olarak tanımlanır. Başka bir ifadeyle, bir D diskriminantının indirgenmiş formlarının sayısı olarak adlandırılır. Böylece yukarıda bahsedilen örneklerde $D = -1$ için sınıf sayısı 1 ve $D = -5$ için 2 dir. Lagrange'dan sonra, sınıf sayısının önemi daha net ortaya çıkmıştır. Gauss sınıf sayısını, D nin özel değerleri için hesaplamaktan öteye gidememiştir. Birçok sayısal deneylerden sonra $D \to \infty$ için sınıf sayısının sonsuza gittiğini konjektür olarak vermiştir. Bunu da ilk defa 1934 te Heilbronn ispatlamıştır ki, ispatı analitik sayılar teorisinde önemli bir adımı temsil etmektedir. (Davenport 1992)

Bir kuadratik formun diskriminantı pozitif, negatif veya sıfır olabilir. Her tamsayı, bir formun diskriminantı olamaz. Gerçekten; $b^2 - 4ac \equiv b^2 \pmod 4$ olup bu durumda herhangi bir kare mod 4 e göre 0 veya 1 e kongrüent olmalıdır. Böylece mod 4 e göre 0 veya 1 olan sayılar diskriminant olabilir.

Bir formun belirli (definite) olabilmesi için $D < 0$ olmalıdır ve formdaki katsayıların işareti ilk katsayı olan a nın işareti ile aynı olmalıdır. Eğer $a > 0$ ise *pozitif belirli* (positive definite), $a < 0$ ise *negatif belirli* (negative definite), $D > 0$ ise form *belirsizdir* (indefinite).

$(\mathbb{Z}/m\mathbb{Z})^*$ m modülüne göre tersleri alınabilen sayıların denklik sınıfları olmak üzere; f_1 ve f_2 diskriminantları D olan iki form ise ve bunlar $(\mathbb{Z}/m\mathbb{Z})^*$ da aynı değerleri temsil ediyorlarsa f_1 ve f_2 ye *aynı cinstendir* denilir.

$f(x,y) = ax^2 + bxy + cy^2$ iki değişkenli kuadratik formu a, b ve c katsayıları aralarında asal ise *pirimitif* olarak adlandırılır.

Diophantine kenarları tamsayı olan dik üçgenlerle ilgili çalışmalarında $(x^2+y^2)(x'^2+y'^2) = X^2+Y^2$, $X = xx' + yy'$ ve $Y = xy' \mp x'y$ formüllerini kullanmıştır. X ve Y, x' ve y' nün bilineer fonksiyonları olmak üzere iki değişkenli kuadratik formun genel kompozisyonu $f(x,y).f(x',y') = F(X,Y)$ şeklinde tanımlanır.

2. KAYNAK ARAŞTIRMASI

Euler (1761), $6n+1$ ve $8n+1$ formundaki her asalın sırasıyla x^2+3y^2 ve x^2+2y^2 ile temsil edildiğini yayınlayan ilk kişidir. Buna benzer teoremler 1654'te Fermat tarafından ifade edilmiştir. Lagrange (1773) kuadratik formlarla ilgili olarak birçok gerçekleri kendisinin genel teorisi olan indirgeme ve iki değişkenli kuadratik formların denkliğini kullanarak ispatlamıştır. Legendre (1798) Lagrange'ın metodlarını ve tablolarını kuadratik kalanlar için olan karşılıklı kalanlar teoreminden faydalanarak büyük ölçüde ispatlamış, fakat ispatını tam olarak bitirememiştir.

1801'de Gauss, bu teoriyi yeni fikirlerle ve çeşitli yöntemlerle genişletmiştir. Gauss'un çalışmalarının literatürde merkezi bir yeri olmuş ve metodlarından birçoğu Dirichlet tarafından sadeleştirilmiş ve bazıları da Arndt ve Mertens tarafından genişletilmiştir.

Hermite, 1851'de sürekli indirgeme ile ilgili temel teoremini geliştirmiştir. Bu; 1876 da Smith tarafından geliştirilen geometrik teori ile bağlantılı olup yine kendisi tarafından eliptik modüler fonksiyonlara uygulanmıştır. Daha sonra 1894'te Hurwitz, 1890, 1896'da Klein ve 1916, 1917'de Humbert tarafından sadeleştirilmiştir. Bu tür çalışmalar, kompleks sayıların denkliğini kullanarak 1877'de Dedekind, 1881'de Hurwitz tarafından yapılmıştır.

1874'te Selling, belirli (definite) ve belirsiz (indefinite) formların indirgemesiyle ilgili önemli teoremler vermiştir. 1880'de Poincaré sayıları $a+b\sqrt{d}$ noktalarıyla, formları latislerle temsil etme metodlarını geniş ölçüde incelemiştir. 1881 ve 1905'de transandantal aritmetik invariantları kurmuştur. 1883'de Kronecker ve 1889'da Stouff indirgemeye ve özel tip yerine koymalara göre denkliğe çalışmışlardır. Markoff'un 1879'da formların minimumlarının üst limitleri ile keşfi 1913'te Schur ve Frobenius, 1916'da Humbert tarafından geliştirilmiştir.

Euler'in asalların temsili ile ilgili yaptığı çalışmalara ek olarak Chr. Goldbach (1843), yanlışlıkla $4n+1$ biçimindeki her asalın d, n nin bir böleni olmak şartıyla dx^2+y^2 formunda olacağını ifade etmiş, fakat Euler bunun x ve y nin rasyonel olması durumunda geçerli olacağını, tamsayılar için geçerli olmayacağına dikkat çekmiştir. Yani; $89 \neq 11x^2+y^2$ eşitsizliği tamsayılar için geçerlidir. Fakat

$$89 = 11\left(\frac{5}{2}\right)^2+\left(\frac{9}{2}\right)^2 = 11\left(\frac{4}{3}\right)^2+\left(\frac{25}{3}\right)^2$$

olacaktır. Euler ve Goldbach, x ve y rasyonel olmak üzere $4dk+1$ biçimindeki asalın dx^2+y^2 formunda temsili ile ilgili çeşitli metodlar üzerinde çalışmışlardır.

Jean Bernoulli III (1773), a^2-10b^2 formundaki asalları 3000'e kadar listelemiştir.

E. Waring (1782), $N=a^2-rb^2$ olmak üzere N^{2m+1} ve N^{2m} in p^2+rq^2 formuyla (en az) $m+1$ farklı yolla gösterilebildiğini söylemiştir.

J. L. Lagrange (1773), iki değişkenli kuadratik formlarla ilgili ilk keşfini ispatlamıştır. Fakat has denklik ve has olmayan denklik arasında bir ayrım yapmamıştır. Daha önce bahsettiğimiz indirgeme ve denklik dışında yeni terimler eklememiştir.

A. M. Legendre (1798), Lagrange'ın indirgeme metodunu indirgenmiş formlarda kullanmıştır fakat detayları sadece aradaki katsayılar çift olduğu durumda vermiştir.

Gauss (1801), A'nın bir kare çarpana sahip olmaması şartıyla x^2-A nın bölenlerinin lineer formlarını bulmak için karşılıklı kalanlar teoremini uygulamıştır ve kendisini $F=ax^2+2bxy+cy^2$ formundaki ortadaki katsayı çift olan ve $(a,\ b,\ c)$ ile gösterdiği iki değişkenli kuadratik formlara kısıtlamıştır.

F. Minding (1832), a, $2b$, c nin ortak bölene sahip olmamaları şartıyla negatif determinantlı bir (a, b, c) indirgenmiş formunun x ve y nin işaretlerinin değişikliği dışında verilen bir asalı tek bir yolla temsil ettiğini ispatlamış ve $a = c$ ise ve bunların kendi içinde yer değiştirmesiyle, $a = 2b$ değilse bir temsilden x'i $x + y$ ile, y yi de $-y$ ile yer değiştirerek ikinciyi elde etmiştir.

C. G. Jacobi (1848), Dirichlet'in teoreminin; $8k+1$ asal olmak üzere $f = (4m+1)^2 + 16n^2$, $g = (4m'+1)^2 + 8n'^2$ şeklinde iki form ile temsil ediliyorsa; o zaman $m+n$ ve n' nün her ikisinin birlikte ya tek ya da çift olduğuna dikkat çekmiştir.

L. Wantzel (1848), x, y, c tamsayılar olmak üzere $c = -3,\ -2,\ -1,\ 2,\ 3,\ 5$ olan ve $x + y\sqrt{c}$ sayıları için bir en büyük ortak bölen yöntemini geliştirmiş ve böylece $p = 2$, $c = -3$, $c = 5$ ve $c = 3$ hariç bir $x^2 - cy^2$ formunu bölen asallarının yine aynı biçimde olduğunu ispatlamıştır.

P. L. Tchebychef (1848), $x^2 \pm ay^2$ nin bölenlerinin lineer formlarını tamamen belirtmiştir. Ayrıca 1851 de Euler'in asallık testi için negatif determinantlı formları kullandığına dikkat çekmektedir.

C. Hermite (1849), p, $x^2 + Ay^2$ nin herhangi bir asal böleni olmak üzere, p nin uygun seçilen bir kuvvetinin $x^2 + Ay^2$ ile temsil edilebileceğini sürekli kesirlerle elementer olarak ispatlamıştır. 1851'de reel katsayılı ve $b^2 - ac = -D$ negatif determinantlı $f = ax^2 + 2bxy + cy^2$ formunun, $2B$ sayısal olarak A ve C den küçük olmak şartıyla, $F = AX^2 + 2BXY + CY^2$ indirgenmiş formuna unimodüler dönüşümle denk olduğunu ispatlamıştır.

G. Oltramare (1855), $a^2 + kb^2$ formunun her bölenin x ve y $ax + bky = z(x^2 + ky^2)$ nin bir çözümünü oluşturmak üzere x, y ve k ile aralarında asal olmak şartıyla $x^2 + ky^2$ formuyla bir ve yalnız bir yolla ifade edilebileceğini ispatlamıştır.

G. Mainardi (1858), bir formdan diğer bir forma bütün dönüşümleri bulma problemine uygun bir dönüşüm verilmiş olması koşuluyla, daha doğrudan bir çözüm getirmiştir.

V. A. Lebesque (1859), bir asalın $x^2 + ky^2$ ile iki farklı yolla temsil edilemeyeceğini göstermiştir.

J. Liouville (1859), x, y pozitif tek tamsayılar ve q; y yi bölmeyen $24v + 3$ biçimindeki değişken bir asal olmak üzere $24\mu + 7$ tipindeki herhangi bir asalın 2 katının $x^2 + q^{4l+1}y^2$ ile tek sayıda yolla gösterilebileceğini ifade etmiştir. x, y tek ve pozitif, p de y yi bölmeyen bir değişken asal olmak üzere $20k + 3$ veya $20k + 5$ biçimindeki herhangi bir m asalı için $8m$ nin $5x^2 + p^{4l+1}y^2$ formuyla tek sayıdaki yollarla gösterilebileceğini ifade etmiş ve aynı durumun $x^2 + 5p^{4l+1}y^2$ için geçerli olduğunu eklemiştir.

L. Kronecker (1862), y tek ve bir p tek asalının $x^2 + Dy^2$, $x^2 + D'y^2$,..., ile temsil edilebilecek şekilde D, D',... farklı sayılar olmak üzere ve şayet $(a_1, b_1, c_1), (a_2, b_2, c_2)$,... $-D, -D'$,..., determinantlarının bütün indirgenmiş has primitif pozitif formlarını veriyorsa o zaman $a_i z^2 + 2b_i z + c_i \equiv 0$ (mod p) kongrüansı b_i, c_i katsayılarından biri z^2 nin katsayısı ile aynı mutlak değere sahip olmaması şartıyla, bu tür kongrüansın p farklı kökü olduğunu ispatlamıştır. Şayet $p = 4n + 3$ ise ($a = \pm 2b$ veya $a = c$ olan) $-D, -D'$,..., determinantlarından biri olan hiçbir has primitif belirsiz form yoktur. Böylece kökler p modülüne göre kalanların tam bir kümesini oluşturur.

H. J. Smith (1863), negatif diskriminantlı kuadratik formların geometrik temsilleri için Gauss'un ve Dirichlet'in sonuçlarını açıklamıştır. Göpel tarafından yapılan bazı özel durumlarda kullanılan bir metodla kuadratik formlarla temsil edilen sayılar için sürekli kesirleri kullanmıştır.

V. Simerky (1863), iki değişkenli kuadratik form teorisini açıklamıştır.

J. Liouville (1865), $k=10,\ 18,\ 22,\ 28$ veya 58 için B tek olmak üzere A^2+2kB^2 formundaki her asalı x ve y pozitif tek tamsayılar ve p, y yi bölmeyen bir asal olmak üzere $kx^2+p^{4l+1}y^2$ formuyla tek sayıda yollarla ifade etmiştir. (1866) A tek olmak üzere $4A^2+5B^2$ formundaki her m asalını; y pozitif, p tek ve y yi bölmeyen bir asal ve $m\equiv 1$ veya $9 \pmod{40}$ a uygun olarak $k=3$ veya 1 olmak üzere $2(10x+k)^2+p^{4l+1}y^2$ formuyla tek sayıda yollarla ifade etmiştir.

C. Traub (1867), $a+b\sqrt{D}$ cebirsel sayıları için en büyük ortak bölen yöntemi bulunduğunu gösterdikten sonra, $D=-1,\pm 2,\pm 3,5$ için x^2-Dy^2 ile has olarak temsil edilen asalları incelemiştir.

F. Valles (1870), $13n-1$, $13n-3$, $13n-4$ biçimindeki her asalın $\pm(x^2-13y^2)$ formlarından biriyle gösterildiğini ifade etmiş ve eğer bir asal $4n+1$ formunda ise x^2+13y^2 formuyla gösterilebileceğini söylemiştir.

P. Bachmann (1871), cebirsel dönüşümleri kullanmadan sayıların kuadratik formlarla temsil teorisini kurmuştur.

A. Korkine ve G. Zolotoreff (1873), $f_o=\sqrt{D\frac{4}{5}}(x^2-xy-y^2)$ dışındaki bütün formların, minimumlarının limitinin, tam tamına $\sqrt{D\frac{1}{2}}$ olmasına rağmen, determinantı $D>0$ olan $f_o=\sqrt{D\frac{4}{5}}(x^2-xy-y^2)$ formuna denk bütün iki değişkenli formların minimumlarının limitinin tam olarak x, y nin hepsi sıfır olmayan tamsayı değerleri için, $\sqrt{D\frac{4}{5}}$ olacağını ifade etmişler ancak ispatı Humbert tarafından yapılmıştır.

W. Göring (1874), $6m+1$ biçimindeki bir asalın x^2+3y^2 formuyla bir ve yalnız bir yolla temsil edildiğini göstermiştir.

H. Poincaré (1879), $F = am^2 + 2bmn + cn^2$ belirli formunu koordinatları $x = m\sqrt{a} + n\frac{b}{\sqrt{a}}$, $y = n\sqrt{\frac{ac - b^2}{a}}$ olan noktaların bir R latisi ile ilişkilendirmiştir. F formuna denk olan bir F' formuna düzlemde R nin noktaları ile aynı noktalara sahip olan bir R' latisi karşılık gelir. 1880'de belirli kuadratik formların alışılmış temsillerinin latislerle belirsiz formlara nasıl uygulandığını gösterdi.

A. Hurwitz (1881), Dedekind'in temel bölge teorisini geliştirerek bunu kuadratik formlara indirgemesinin basit bir geometrik teoriye yönelttiğini göstermiştir.

L. Kronecker (1885), negatif D diskriminantlı bir kuadratik formla n nin temsillerinin sayısının ortalama olarak $\pi\sqrt{-D}$ olduğunu ispatladı.

J. Vivanti (1886), pozitif kare olmayan D diskriminantlı $(a, b, -c)$ formunun a ve b pozitif, $c = a + b$ olduğunda indirgendiğini ispatlamış ve bunu sıfır form olarak adlandırmıştır. Bir sıfır form, ancak ve ancak D nin 2 dahil, $6n + 5$ biçimindeki bütün asal çarpanlarının üslerinin hepsi çift olduğunda determinantı D olan indirgenmiş sistemde oluşur.

T. Pepin (1889), (1, 0, 8) ve (1, 0, 16) ile temsil edilebilen sayıların sayısını incelemiştir. Bununla ilgili sonuçları Liouville formüllerinden çıkarmıştır. 1890 da determinantı -12 olan formlarla temsillerin sayısı üzerine bir teorem eklemiştir.

G. B. Mathews (1892), Dedekind'in kompleks sayıların indirgeme teorisini geliştirerek bunları kuadratik formların geometrik teorisine uygulamıştır.

E. Landau (1903), Kronecker'in limit formülü ile ilgili en son sonuçların diğer ispatlarını referanslarıyla birlikte vermiştir.

J. Schatunovsky (1912), $x^2 + Dy^2 \equiv 0 \pmod{p}$ nin aralarında asal çözümleri var ise, $u^2 + D \equiv 0 \pmod{p}$ nin de bir çözümünün var olduğunu ispatlamıştır.

R. Bricard, tanımladığı bir metotla her $8q \pm 1$ biçimindeki asalın $x^2 - 2y^2$ formunda olduğunu ispatlamıştır.

H. N. Wright (1914), $D = 1,...,150,800,...,848$ için negatif $-D$ diskriminantın indirgenmiş formlarını listelemiştir.

G. H. Hardy (1915), n nin, $a > 0$, $D = 4\alpha\gamma - \beta^2 > 0$ olacak şekilde $ax^2 + \beta xy + \gamma y^2$ ile temsillerinin sayısını $r(n)$ olarak ifade etmiş ve

$$R(x) = \sum_{n<x} r(n) = \frac{2\pi x}{D} + P(x)$$

olarak yazmıştır. $P(x) > Kx^{3/4}, P(x) < -Kx^{3/4}$ eşitsizliklerinin herbirinin bütün limitleri tarayan x in değerleri için gerçeklenecek şekilde bir K sabitinin varlığını ispatlamıştır. $R(x)$ i birinci mertebeden Bessel fonksiyonları cinsinden sonsuz seriler olarak net bir analitik ifadeyle vermiştir.

L. J. Mordell (1917), her ikisi birden Φ ile bölünebilen Φ_x ve Φ_y kısmi türevleri için x ve y tamsayıları bulunursa, Φ nin belirsiz (ambigous) form olduğunu ispatlamıştır.

M. Amsler (1918), indirgenmiş formlarla ilgili teoremler elde etmek amacıyla sürekli kesirleri ve Farey serilerini kullanmıştır.

J. A. Gmeiner (1919), determinantın pozitif veya negatif olması durumuna göre indirgenmiş formları bulmak için tek bir yöntem geliştirdi. (Dickson 1971)

Bir formun $-D$ diskriminantı, 3, 4, 7, 8, 11, 19, 43, 67 ve 163 değerlerini aldığında sınıf sayısının 1 olduğu biliniyordu. Heilbronn ve Linfoot 1934 te bu özelliği sağlayan en çok bir tane daha diskriminant olduğunu ispatladılar. Sayısal deneyler yukardaki sayıların haricinde onuncu bir diskriminant olmadığını gösteriyordu. Fakat tam bir ispat H. Stark tarafından 1966 da verilinceye kadar bu problem çözülmemişti. Bu konuyla ilgili değişik ispatlar aynı zamanda A. Baker,

Deuring ve Siegel tarafından yapılmıştır. 1952 de K. Hegner in ispatının geçerliliği tartışılmış ve daha sonra geçerli olduğu kabul edilmiştir. (Davenport 1992)

Ezra Brown, determinantı $-pq$ olan iki değişkenli kuadratik formları incelemiş ve p ve q , $4n+1$ biçiminde ve $(p/q)=1$ olan farklı asallar olmak üzere, $x^2 - pqy^2$ nin $(p/q)_4 = (q/p)_4 = -1$ olması durumunda -1 i; $(q/p)_4 = -(p/q)_4 = 1$ olması durumunda p yi; $(p/q)_4 = -(q/p)_4 = 1$ olması durumunda q yu temsil ettiğini ispatlamıştır. $(p/q)_4$ olması durumunda 1, p ve q dan herhangi birinin temsil edilmediğini gösteren örnekler yapmıştır. Burada $(p/q)=1$ ise $(p/q)_4 = 1$ veya -1 yazmakla p nin q nun dördüncü kuvvetten bir kalanı olmadığını belirtmiştir. (Brown 1972) Daha sonra yaptığı çalışmalarda ise d iki ya da 3 farklı asal bölene sahip olan iki değişkenli kuadratik diskriminant olmak üzere 2 nin kuvvetlerinin modülüne göre d nin sınıf sayısının kongrüans durumlarını incelemiştir. (Brown 1973)

Yoshiyuki Kitaoka, kuadratik formlarla ilgili birçok çalışma yapmıştır ve 1973 te asal diskriminantlı kuaterner, çift pozitif belirli kuadratik formlarla yaptığı incelemelerde kullandığı notasyonların ve terminolojilerin kuadratik formları daha çok cebirsel açıdan ele alan O'Meara ile benzer olduğu görülmüştür. (Kitaoka 1973)

P. Sarnak (1982), belirsiz iki değişkenli kuadratik formların sınıf sayısı ile ilgili çalışmalar yapmış ispatlarında Selberg'in formüllerinden faydalanmıştır. (Dickson 1971)

F. H. Koch, diskriminantı $-256q$ ve $-128q$ olan iki değişkenli kuadratik formların asalları temsili ile ilgili ispatlar yapmış ve P. Kaplan ve K. S. Williams'ın -768 diskriminantlı iki değişkenli kuadratik formların asalları temsili ile ilgili çalışmalarını göz önünde bulundurmuştur. (Koch 1993)

Myun-Hwan Kim ve Byeong-Kweon oh, karelerin toplamı olarak temsil edilebilen altı değişkenli pozitif belirli tam katsayılı her kuadratik formun dokuz kare

toplamı şeklinde yazılabileceğine dair C. Ko tarafından 1939 da verilen konjektürün geçerli olmadığını göstermiştir. (Kim 1997)

M. Borovoi, tamsayıların belirsiz olan üç değişkenli kuadratik formlarla temsili üzerine çalışmalar yapmıştır. (Borovoi 2000)

J. Voight, aynı asalları temsil eden pozitif belirli iki değişkenli kuadratik formları incelemiştir. (Voight 2004)

Ram Murty ve Robert Osburn, bazı pozitif belirli iki değişkenli kuadratik formlarla tamsayıların temsili ile ilgili çalışmalar yapmışlar burada N kare olmayan bir tamsayı olmak üzere $f(x,y)=x^2+Ny^2$ pozitif belirli kuadratik formunu ele almışlardır. (Murty ve Osburn 2004)

J. Buchmann ve U. Vollmer, '*Binary Quadratic Forms, An algorithmic Approach'* adlı kitaplarında iki değişkenli kuadratik formları algoritmik yaklaşımla ele almışlar ve bu konunun kriptoloji ile ilgisinden dolayı bazı kriptografik uygulamaları vermişlerdir. (Buchmann ve Vollmer 2007)

$a,b\in\mathbb{Z}^*$ ve $a\geq b$ olmak üzere a^2+ab+b^2 formu β*-temsili* olarak adlandırılmak koşuluyla en az bir β*-temsili* olan sayıya β*-sayısı* denir. (Nair 2004) Çalışmamızda iki β-sayısının çarpımının yine bir β-sayısı olduğunu, kuadratik formlar ideallere karşılık geldiğinden, idealleri ve ideal bazını kullanarak ispatladık. Ayrıca, *n*-polygonal sayılarının Pisagor üçlüsü olarak verilen $p_n^a+p_n^b=p_n^c$ eşitliğini $p_n^a+p_n^b+p_n^c+2(n-1)(n-4)=p_n^d$ eşitliğine genişleterek ispatladık. (Bircan ve Şenay 2007)

3. TAMSAYILARIN TEMSİL PROBLEMİ

Bu bölümde tamsayıların ikinci dereceden formlarla temsil problemini ele alacağız. Bunun için aşağıdaki tanımla başlamak uygun olacaktır.

Tanım 3.1. $x_0, y_0 \in \mathbb{Z}$ olmak üzere bir m tamsayısı için;

$$ax_0^2 + bx_0y_0 + cy_0^2 = m,$$

oluyorsa $f(x,y)$ formu m tamsayısını *temsil eder* ya da m tamsayısı $f(x,y)$ formu ile temsil edilir denir. $(x_0, y_0) = 1$ ise temsil *primitiftir*. Bu problemde genel olarak,

"i) Verilen bir formla hangi tamsayılar temsil edilebilir?

ii) Verilen bir tamsayıyı hangi formlar temsil eder?

iii) Bir form bir tamsayıyı temsil ediyorsa; aynı tamsayıyı temsil eden kaç tane form vardır ve bu temsiller nasıl hesaplanır?"

sorularına cevap aranır. 17. ve 18. yüzyılda birçok matematikçi bu soruların cevabını araştırmış ve formları sınıflandırmaya çalışmışlardır. Bu konuyla ilgili olarak ciddi çalışmalar ilk olarak Gauss'un 1801'de yayınladığı '*Disquisitiones Arithmeticae*' adlı kitabında görülmüştür. Daha sonra 19. yüzyılın ortalarında ideal teorisi geliştirilmiş ve iki değişkenli kuadratik form teorisinin kuadratik cisimlerin sınıf grubu ile eşleştirilebildiği görülmüştür. (Buell 1989)

Bu problemin en temel sorusu; verilen bir n pozitif tamsayısı için hangi p asalları, x ve y tamsayı olmak üzere;

$$p = x^2 + ny^2$$

biçiminde bir formla temsil edilebildiğidir.

Fermat, Euler, Lagrange, Legendre ve Gauss'un çalışmalarında bu probleme elementer yaklaşımlar görülebilir. Bu matematikçiler $n>3$ için $p=x^2+ny^2$ yi içeren bazı konjektürler vermişlerdir. Euler'in konjektürlerinden birisi;

$$p=x^2+27y^2 \Leftrightarrow \begin{cases} p\equiv 1 \pmod 3 \text{ ve } x^3\equiv 2 \pmod p \\ \text{nin tamsayı çözümleri vardır.} \end{cases} \tag{3.1}$$

şeklindedir.

İndirgenmiş formun ve sınıf sayısının yardımıyla cins teorisinin elementer yaklaşımlarını geliştirebiliriz ki, bu $n>3$ için $p=x^2+ny^2$ nin hangi p ler için gerçeklendiğini bulmamızı sağlar. (3.1) deki durum için cins teorisi aşağıdaki türden kısmi sonuçları ispatlayabilir:

$$p=\left\{\begin{array}{c} x^2+27y^2 \\ veya \\ 4x^2+2xy+7y^2 \end{array}\right\} \Leftrightarrow p\equiv 1 \pmod 3 \tag{3.2}$$

olup burada x^2+27y^2 ve $4x^2+2xy+7y^2$ aynı cinstedir. Dolayısıyla bazı kongrüanslarla birbirinden ayrılamaz. Bu ise cins teorisi ve kompozisyon arasındaki ilişkidir. Gauss, (3.1) i ispatlamak için kübik resiprositeyi kullanmıştır. Benzer olarak, aynı cinsteki formları birbirinden ayırmak için yüksek dereceden resiprosite kanunlarının önemini fark etmiştir. Kübik ve kuadratik resiprosite kanunlarını ifade edebilmek için $\mathbb{Z}[e^{2\pi i/3}]$ ve $\mathbb{Z}[i]$ halkalarındaki aritmetiği dikkate almamız gerekir.

$n>0$ ve keyfi olduğu durumlarda $p=x^2+ny^2$ yi çözmek için sınıf cismi teorisine ihtiyacımız vardır. Sınıf cisim teorisi aşağıdaki genel sonucu ispatlamamızı ve cins teorisinin temel teoremleri için yeni ispatlar geliştirmemizi sağlar.

Teorem 3.1. *$n\equiv 1,\ 2 \pmod 4$, kareçarpansız pozitif bir tamsayı olsun. O zaman n yi ve de $f_n(x)$ in diskriminantını bölmeyen bir p asalı için,*

$$p = x^2 + ny^2 \Leftrightarrow \begin{cases} (-n/p) = 1 \; ve \; f_n(x) \equiv 0 \pmod{p} \\ nin \; tamsayı \; çözümleri \; \text{var} dır. \end{cases}$$

olacak şekilde bir $f_n(x) \in \mathbb{Z}[x]$ *indirgenemez polinomu vardır.*

Bu teoremin ifadesi elementer olmasına rağmen, $f_n(x)$ polinomu karmaşıktır. Burada, $f_n(x)$, $K = \mathbb{Q}(\sqrt{-n})$ in Hilbert sınıf cismi L nin primitif elemanının minimal polinomudur.

Bu teoreme örnek olarak $n = 14$ durumunu verebiliriz. $\alpha = \sqrt{2\sqrt{2} - 1}$ olacak şekilde, $K = \mathbb{Q}(\sqrt{-14})$ Hilbert sınıf cismi $L = K(\alpha)$ olur. Teorem 3.1 den bir p asalı için

$$p = x^2 + 14y^2 \Leftrightarrow \begin{cases} (-14/p) = 1 \; ve \; (x^2+1)^2 \equiv 8 \pmod{p} \\ \text{nin bir tamsayı çözümü vardır,} \end{cases} \tag{3.3}$$

olacaktır ki bu bizim $x^2 + 14y^2$ biçimindeki form için esas temsil sorumuzun cevabıdır. Ayrıca Hilbert sınıf cismi sayesinde cins teorisinin temel teoremlerinin yeni ispatlarını verebiliriz.

Fakat bu teoride bazı boşluklar vardır; en belirgin olanı $x^2 + 27y^2$ ve $x^2 + 14y^2$ için bulunan sonuçlardır. (3.1) ifadesi Teorem 3.1 den elde edilmez, çünkü $n = 27$ kare çarpansız değildir. Dolayısıyla, bu durumda bütün pozitif n ler için geçerli olan tek bir teorem olması gerekir. Teorem 3.1 in bütün n ler için bu aşamaya kadar geçerli olmayışının sebebi $\mathbb{Z}[\sqrt{-n}]$ in genel anlamda $\mathbb{Q}(\sqrt{-n})$ deki bütün tamsayılar halkası olmayışıdır. Amacımız, Teorem 3.1 in bütün pozitif n ler için geçerli olduğunu göstermektir. Bunun için, genel n ler için $\mathbb{Z}[\sqrt{-n}]$ halkasına çalışırız ki, bu bizi sanal kuadratik cisimlerde mertebe kavramına götürür. Teorem 3.1 in her $n > 0$ için olduğunu göstermek için $f_n(x)$ polinomu, halka sınıf cisminin primitif elemanının minimal polinomu olacak şekilde Artin'in resiprosite teoremini kullanırız. Halka sınıf cismi, Hilbert sınıf cisminin bir genelleştirilmesidir. Ayrıca,

sınıf cismi yüksek dereceden resiprosite teoremleriyle bağlantılıdır. Bu problemde $n > 0$ sayısı için $f_n(x)$ polinomunu da nasıl bulacağımız da önemli bir sorudur. (3.1) ve (3.3) deki $f_{27}(x)$ i ve $f_{14}(x)$ i biliyoruz. Fakat bu örneklerde kullanılan metotları genelleştirmek oldukça zordur. Bu durumda kompleks çarpma kullanılır. Ayrıca burada kompleks çarpmanın temel fikri olan eliptik fonksiyonlara çalışmak gerekir. Halka sınıf cismini oluşturmak içinse $j-$ fonksiyonuna ihtiyacımız vardır. $j(\sqrt{-n})$ in minimal polinomu olan sınıf denklemini hesaplamak bizi $p = x^2 + ny^2$ nin çözümlerine götürür. (Cox 1989)

Temsil problemine diğer bir örnek olarak elementer sayılar teorisinden bilinen (1, 0, 1) formuyla temsilleri de içeren aşağıdaki teoremi de verelim:

Teorem 3.2.

a) a ve b tamsayılar olacak şekilde $a^2 + b^2 = m$ *formu,* $4k-1$ *formundaki herhangi bir* p *asalına bölünebiliyorsa, o zaman;* $p \mid a, p \mid b$ ve $p^2 \mid m$ *dir.*

b) $x^2 + y^2 = 2$ *formunun tek tamsayı çözümü,* x *ve* y *nin işaretleri bağımsız olacak şekilde* $(x, y) = (\pm 1, \pm 1)$ *dir.*

c) p*,* $4k+1$ *biçiminde bir asal ise o zaman* $x^2 + y^2 = p$ *formunun* $(x, y) = (a, b)$ *biçiminde bir çözümü vardır ki, bu denklemin tek çözümleri* $(x, y) = (\pm a, \pm b)$ *ve* $(\pm b, \pm a)$ *şeklinde olup işaretlerin seçiminden bağımsızdır.*

d) p_i *ler* $4k+1$ *biçimindeki asallar olmak üzere;* $m = 2^t p_1^{r_1}, ..., p_s^{r_s}$ *biçiminde asalların kuvvetlerinin çarpımı olsun.* $\{(a_j, b_j)\} \in \mathbb{Z}$ *her bir* j *için* $x^2 + y^2 = p_j$ *nin çözümü olsun. O zaman* $i = \sqrt{-1}$*, olmak üzere* $x^2 + y^2 = m$ *denkleminin bütün çözümleri;*

$$m = (1+i)^t (1-i)^t (a_1 + ib_1)^{r_1} (a_1 - ib_1)^{r_1}$$

$$\vdots$$

$$= (a_s + ib_s)^{r_s} (a_s - ib_s)^{r_s}$$

olup sağ taraf herhangi bir form için $(a+ib)(a-ib)$ *şeklinde yazılabilir.* (Buell 1989)

Örnek 3.1.

$$x^2 - y^2 = 113 \tag{3.4}$$

Diophantine denklemini dikkate alalım. Bu denklemde, 113 ün iki kare farkı olarak temsillerini bulmak istiyoruz. $(x, y) \in \mathbb{Z}^2$ böyle bir temsilse o zaman; $(\pm x, \pm y)$ de 113 ü temsil eden sayılar olacaktır. 113, $\mathbb{Z}$ de bir kare olmadığından x ve y sıfırdan farklıdır. Bu nedenle $x > y > 0$ olduğunu varsayıyoruz. Şimdi (3.4) ü;

$$(x-y)(x+y) = 113$$

şeklinde çarpanlara ayıralım. 113 asal bir sayı ve $\mathbb{Z}$ de tek çarpanlama geçerli olduğundan;

$$x + y = 113 \text{ ve } x - y = 1$$

olacaktır. Böylece (3.4) ün bütün çözümleri

$$\{\pm 57, \pm 56\}$$

olacaktır. Burada, çözümleri $x^2 - y^2$ tamsayı katsayılı ve iki lineer polinomun çarpımı olduğu ve $\mathbb{Z}$ de tek çarpanlama olduğu için bulabildik. Fakat sayılar büyüdükçe Diophantine denklemi değiştikçe çözümlerin sayısını bulmak ve bulunan çözümlerin bütün çözümler olup olmadığına cevap vermek zorlaşmaktadır. Örneğin, bir pozitif d tamsayısı için $x^2 - dy^2 = 1$ formundaki Diophantine denklemini çözmek için genel bir metot yoktur. Bazı denklemlerin tamsayı çözümlerinin olmadığını da dikkate alırsak temsil probleminin zorluğu daha iyi anlaşılacaktır. (Buchmann ve Vollmer 2007)

Şimdi, sonuçlar bölümünde gereksinim duyacağımız aşağıdaki önemli tanım ve teoremleri vermek yerinde olacaktır.

Tanım 3.2.

1. $a,b \in \mathbb{Z}^*$ ve $a \geq b$ olmak üzere a^2+ab+b^2 formuna β*-temsili* denir.

2. a^2+ab+b^2 ve c^2+cd+d^2 formundaki β-temsilleri $a \neq c$ veya $b \neq d$ ise *farklıdır* denir.

3. En az bir β-temsili olan bir tamsayıya β*-sayısı* denir.

4. Bir β-sayısı asal ise, β*-asalı* denir. (Nair 2004)

Teorem 3.3. *3 ün dışındaki bütün* β*-asalları* $6k+1$ *formundadır.*

İspat. $p = a^2+ab+b^2$ ve $a \equiv m \pmod 6$, $b \equiv n \pmod 6$ ve $a^2+ab+b^2 \equiv z \pmod 6$ olsun. Burada kongrüansın temel özelliklerinden $m^2+mn+n^2 \equiv z \pmod 6$ olacaktır. $m = 0,...,5$ ve $n = 0,...,5$ için z sadece 0, 1, 2, 3, 4 değerlerini alacaktır. Yani p $6k$, $6k+1$, $6k+3$ ve $6k+4$ değerlerini alacaktır. Burada $6k$ ve $6k+4$ her zaman bileşik sayıdır. $6k+3$, $k=0$ dışında yani $p \neq 3$ olduğunda bileşik sayıdır. Böylece, p nin alacağı asal değerler sadece 3 ve $6k+1$ formunda olacaktır. (Nair 2004)

Tanım 3.3. M kenarları x ve y hipotenüsü z olan bir dik açılı üçgen olsun ve x, y ve z, $x^2+y^2=z^2$ yi sağlasın. Eğer x, y ve z doğal sayılar ise M pisagor üçgeni, (x, y, z) de pisagor üçlüsüdür. Eğer x, y ve z doğal sayıları $(x,y)=1$ veya $(y,z)=1$ veya $(z,x)=1$ şartlarını sağlıyorsa (Bir tanesi gerçekleniyorsa hepsi gerçeklenir) M'ye primitif pisagor üçgeni ve (x, y, z), $(y \neq z)$ ye *primitif pisagor üçlüsü* denir. Bir pisagor üçgeninin alanına *pisagor sayısı* denir. Dolayısıyla, primitif pisagor üçgeninin alanı primitif pisagor sayısıdır. Ayrıca her pisagor sayısı 6 ile bölünebilir. (Mohanty 1990)

Son olarak aşağıdaki şekilde, belirli tipteki asalların temsil edildiği iki değişkenli kuadratik formların listesini verelim.(Weisstein 2006)

Asalın Formu	Temsili
$4n+1$	x^2+y^2
$8n+1, 8n+3$	x^2+2y^2
$8n\pm1$	x^2-2y^2
$6n+1$	x^2+3y^2
$12n+1$	x^2-3y^2
$20n+1, 20n+9$	x^2+5y^2
$10n+1, 10n+9$	x^2-5y^2
$14n+1, 14n+9, 14n+25$	x^2+7y^2
$28n+1, 28n+9, 28n+25$	x^2-7y^2
$30n+1, 30n+49$	x^2+15y^2
$60n+1, 60n+49$	x^2-15y^2
$30n-7, 30n+17$	$5x^2+3y^2$
$60n-7, 60n+17$	$5x^2-3y^2$
$24n+1, 24n+7$	x^2+6y^2
$24n+1, 24n+19$	x^2-6y^2
$24n+5, 24n+11$	$2x^2+3y^2$
$24n+5, 24n-1$	$2x^2-3y^2$

Tablo 1. İki değişkenli kuadratik formlarla temsil edilen bazı asallar

4. KUADRATİK SAYI CİSİMLERİ VE KUADRATİK FORMLAR

4.1. Kuadratik Sayı Cisimleri ve Cebirsel Sayılar

Cebirsel sayıların özel bir sınıfı olan rasyonel katsayılı kuadratik sayılar, rasyonel katsayılı kuadratik denklemlerin çözümleridir. a, b ve d rasyonel olmak üzere $a+b\sqrt{d}$ formundaki sayılardır. Kare olmayan d rasyonel sayısını ve $a,\ b\in\mathbb{Q}$ olmak üzere $a+b\sqrt{d}$ formundaki sayıların kümesini göz önüne alalım. Böyle bir kümeye *kuadratik sayı cismi* adı verilir ve $\mathbb{Q}(\sqrt{d})$ ile gösterilir. $d>0$ ise $\mathbb{Q}(\sqrt{d})$ nin her elemanı reeldir ve dolayısıyla *reel kuadratik cisim* adını alır. $d<0$ ise $\mathbb{Q}(\sqrt{d})$ reel olmayan sayıları da içerir ki, *sanal kuadratik cisim* adını alır. (Buell 1989) Örnek olarak $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{45})$, $\mathbb{Q}(1+\sqrt{20})$ birbirlerine eşit olan kuadratik sayı cisimleridir. (Buchmann ve Vollmer 2007)

Lemma 4.1. *d kare olmayan bir tamsayı ve $K=\mathbb{Q}(\sqrt{d})$ olsun. O zaman $\alpha,\ \beta\in K$ ise $\alpha\pm\beta,\ \alpha\beta\in K$ ve $\beta\neq 0$ olmak şartıyla $\alpha/\beta\in K$ dır.*

İspat. Toplama, çıkarma ve çarpma oldukça kolaydır. Burada $\alpha=1$ olan özel durumu ele alabiliriz. Şayet $1/\beta\in K$ ise o zaman çarpma kuralından $\alpha/\beta=\alpha(1/\beta)\in K$ dır. Burada $\beta=a+b\sqrt{d}$ olmak üzere;

$$\frac{1}{\beta}=\frac{1}{a+b\sqrt{d}}=\frac{a-b\sqrt{d}}{(a+b\sqrt{d})(a-b\sqrt{d})}=\frac{a-b\sqrt{d}}{a^2-b^2d}$$

$a^2 - b^2 d$ nin sıfır olup olmadığını kontrol etmemiz gerekir. Eğer $a^2 - b^2 d = 0$ ise ya $b \neq 0$ yada $b = 0$ dır. $b \neq 0$ olduğunda $d = (a/b)^2$ olur ki hipotezle çelişir. $b = 0$ ise o zaman $a = 0$ olur bu da $\beta = 0$ gerektirir ki, yine hipotezle çelişir. Böylece,

$$\frac{1}{\beta} = \frac{a}{a^2 - b^2 d} + \frac{-b}{a^2 - b^2 d}\sqrt{d} \in K$$

olup istenendir.

Burada paydayı eşleniği ile çarparak rasyonalize ettik. Dolayısıyla $\beta = a + b\sqrt{d}$ ise eşleniği $\beta^* = a - b\sqrt{d}$ dir. Aşağıdaki lemmayı ispatsız olarak verelim.

Lemma 4.2. *$\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ olsun. O halde $(\alpha^*)^* = \alpha$, $(\alpha + \beta)^* = \alpha^* + \beta^*$, $(\alpha - \beta)^* = \alpha^* - \beta^*$, $(\alpha\beta)^* = \alpha^*\beta^*$ ve $\beta \neq 0$ olmak üzere $(\alpha/\beta)^* = \alpha^*/\beta^*$ olur.*

$1/\beta$ nın $\mathbb{Q}(\sqrt{d})$ nin elemanı olduğunu göstermek ve sıfır olmayan rasyoneli elde etmek için β yı β^* ile çarptık. Dolayısıyla β nın *normunu* $N(\beta) = \beta\beta^*$ olarak tanımlayabiliriz. Aynı şekilde β nın *izini* $T(\beta) = \beta + \beta^*$ olarak tanımlarız. β nın normu ve izi rasyonel tamsayılardır. O halde, β ve β^*;

$$(x - \beta)(x - \beta^*) = x^2 - T(\beta)x + N(\beta) = 0$$

rasyonel katsayılı denklemin kökleridir. Bu denkleme β nın *karakteristik denklemi* adı verilir. İz, toplama ve çıkarmayı; norm ise çarpma ve bölmeyi ifade eder.

Lemma 4.3. *Eğer $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ ise o zaman $T(\alpha \pm \beta) = T(\alpha) \pm T(\beta)$,*

$\mathrm{N}(\alpha\beta)=\mathrm{N}(\alpha)\mathrm{N}(\beta)$ ve $\beta \neq 0$ olmak üzere $N(\beta) \neq 0$ ve $N(\alpha/\beta) = N(\alpha)/N(\beta)$ dır.

İspat. Öncelikle,

$T(\alpha \pm \beta) = (\alpha \pm \beta) + (\alpha \pm \beta)^* = \alpha \pm \beta + \alpha^* \pm \beta^* = (\alpha \pm \alpha^*) + (\beta \pm \beta^*) = T(\alpha) \pm T(\beta)$

olacaktır. Benzer olarak

$$N(\alpha\beta) = (\alpha\beta)(\alpha\beta)^* = \alpha\beta\alpha^*\beta^* = (\alpha\alpha^*)(\beta\beta^*) = N(\alpha)N(\beta)$$

dır. Son olarak $\beta \neq 0$ ise $N(\beta) \neq 0$ olup Lemma 4. 2 nin ispatından

$$N(\alpha/\beta) = (\alpha/\beta)(\alpha/\beta)^* = (\alpha/\beta)(\alpha^*/\beta^*) = (\alpha\alpha^*)/(\beta\beta^*) = N(\alpha)/N(\beta)$$

olacaktır. Sanal kuadratik cisimlerde $\beta^* = \overline{\beta}$, yani kompleks eşleniğine eşit olur. Dolayısıyla $N(\beta) = \beta\overline{\beta} = |\beta|^2 \geq 0$, fakat reel kuadratik cisimlerde genel olarak $\overline{\beta} = \beta \neq \beta^*$ olur ve $N(1) = 1$ ve $N(\sqrt{d}) = -d$ dir. Yani bu durumda norm, hem pozitif ve hem de negatif değerleri içerir.

Burada, kuadratik cisimlerin sayısının ne kadar olduğu sorusu ortaya çıkar. Şayet $\mathbb{Q}(\sqrt{d_1})$ ve $\mathbb{Q}(\sqrt{d_2})$ aynı ise bunu nasıl açıklayabiliriz? Aşağıdaki sonuç bize bu soruların cevabını verir.

Teorem 4.1. *Eğer* $K_1 = \mathbb{Q}(\sqrt{d_1})$ *ve* $K_2 = \mathbb{Q}(\sqrt{d_2})$ *ise o zaman* $K_1 = K_2$ *olması ancak ve ancak* d_1/d_2 *nin bir rasyonelin karesi olmasıyla mümkündür.*

İspat. İspatı için bakınız. (Chapman 2002)

Aşağıdaki önerme kuadratik cisimleri birbirinden nasıl ayırt edebileceğimizi söyler. d nin kare çarpansız olması $d = \pm 1$ veya $d = \pm p_1 p_2 ... p_k$, (p_k lar farklı asallar) olduğu anlamına gelir.

Teorem 4.2. *K kuadratik cisim olmak üzere* $d \neq 1$ *ve kare çarpansız bir tamsayı ile tek olarak belirlenebilir.*

İspat. a ve b tamsayı olmak üzere $K = \mathbb{Q}\sqrt{a/b}$ ise o zaman $K = \mathbb{Q}(\sqrt{b^2(a/b)}) = \mathbb{Q}(\sqrt{ab})$ dir. Böylece r bir tamsayı olmak üzere $K = \mathbb{Q}(\sqrt{r})$ diyebiliriz. Burada r kare çarpansız değilse c birden büyük bir tamsayı olduğunda $c^2 \mid r$ dir. O halde $K = \mathbb{Q}(\sqrt{r/c^2})$ dir. d kare çarpansız oluncaya kadar kare çarpanları atalım. Sonuç olarak $K = \mathbb{Q}(\sqrt{d})$ yi elde ederiz. Burada $d \neq 1$ olduğuna ilgi çekelim ki, $\mathbb{Q}(\sqrt{1})$ kuadratik bir cisim değildir. Şimdi tekliği ispatlamak istersek

d_1 ve d_2 kare çarpansız olmak üzere $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$ olsun. s bir rasyonel sayı olmak üzere $d_1/d_2 = s^2$ olsun. Buradan d_1 ve d_2 nin aynı işarete sahip olacağı açıktır. u ve v tamsayılar olmak üzere $s = u/v$ dersek $d_1 v^2 = d_2 u^2$ elde ederiz. Eğer p; d_1 i bölen bir asal sayı ise o zaman p, $d_1 v^2$ ve aynı şekilde $d_2 u^2$ nin tek kuvvetten asal çarpanı olur. Bu aynı zamanda $p \mid d_2$ demektir. Benzer olarak d_2 nin her asal çarpanı aynı zamanda d_1 inde asal çarpanıdır. d_1 ve d_2 kare çarpansız olduğundan aynı çarpanlara sahiptir ve aynı işaretleri taşırlar. Dolayısıyla eşittirler. (Chapman 2002)

Cebirsel tamsayıları tanımlarken gerekli olacağından $\mathbb{Z}$ tamsayılarına rasyonel tamsayılar diyeceğiz. $f(x)$, rasyonel katsayılı bir polinom olmak üzere $f(x) = 0$ ı gerçekleyen α kompleks sayısına *cebirsel sayı* denir. $f(x)$, katsayıları rasyonel tamsayı olan bir monik polinom olmak üzere $f(x) = 0$ denklemini sağlayan herhangi bir cebirsel sayıya *cebirsel tamsayı* denir. Rasyonel sayı katsayılı $f(x) = 0$ denklemini $f(x)$ in katsayılarını paydalarının en küçük ortak katlarıyla çarparak $f(x)$ polinomunu rasyonel tamsayı katsayılı hale getirebiliriz. (Buell 1989) Bazı cebirsel tamsayılara *i,* $\sqrt{2}$, $\sqrt[3]{10}$, $(1+\sqrt{5})/2$ ve $2\cos 2\pi/9$ u ve cebirsel sayılara ise $(1+i)/2$, $\sqrt{1/5}$ ve $\sin 2\pi/7$ yi örnek verebiliriz. (Mazur 2008)

Teorem 4.3. *Cebirsel tamsayı olan tek rasyonel sayılar, rasyonel tamsayılardır.*

İspat. $\gcd(a,b)=1$ olmak üzere $a/b \in \mathbb{Q}$ olsun. Açık olarak $a/b,\ x - a/b = 0$ denkleminin bir çözümüdür. a/b nin bir cebirsel sayı olduğunu biliyoruz. a bir rasyonel tamsayı yani $b = 1$ ise, o zaman $a/b = a$ bir cebirsel tamsayıdır. a/b nin cebirsel bir tamsayı olduğunu varsayalım ve $b > 1$ olsun. O halde c_i rasyonel tamsayı katsayı olmak üzere

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \ldots + c_1(a/b) + c_0 = 0$$

denklemini yazabiliriz. Katsayıları b^n ile çarparak,

$$a^n + c_{n-1}a^{n-1}b + \ldots + c_1 ab^{n-1} + c_0 b^n = 0$$

denklemini elde ederiz. b birinci terim haricinde bütün terimleri böldüğünden, birinci terimi de bölmek zorundadır. Bu ise $\gcd(a,b) > 1$ olduğu anlamına gelir ki çelişkidir.

Sonuç olarak cebirsel tamsayı olmayan bazı cebirsel sayılar vardır. Ayrıca Cebirsel sayıların toplamlarının ve çarpımlarının yine bir cebirsel sayı olduğunu belirtmemiz gerekir. Bu aynı zamanda cebirsel tamsayılar için de geçerlidir.

Kuadratik cebirsel sayı cisimleri için verilen teoremlerin ve tanımların bir çoğu bütün sayı cisimleri için geçerlidir. Burada teoremleri sadece kuadratik sayı cisimleri için ispatlayacağız.

Tanım 4.1. a, b, c rasyonel tamsayılar olmak üzere bir α kompleks sayısı

$$ax^2 + bx + c = 0 \tag{4.1}$$

denklemini sağlıyorsa *kuadratik cebirsel sayı* denir. Eğer (4.1) denkleminde $a = 1$ ise kuadratik cebirsel tamsayı

$$x^2 + bx + c = 0 \tag{4.2}$$

denklemini sağlıyorsa kuadratik cebirsel sayı olarak adlandırılır. Kuadratik cebirsel sayılar tam olarak

$$\frac{-b + e\sqrt{d}}{2a} \tag{4.3}$$

formundaki kompleks sayılardır. Burada, a, b, d ve e rasyonel tamsayılar ve d nin 1 dışında kare çarpanı yoktur. d nin 1 olduğunu kabul etmemiz bütün rasyonel sayıların kuadratik cebirsel sayılar ve rasyonel tamsayıların kuadratik cebirsel tamsayılar olduğu anlamına gelir. Yani, d nin 1 olması (4.1) polinomunun iki lineer polinomun çarpımı şeklinde yazılabilmesi demektir. Ayrıca $\mathbb{Q}(\alpha)$ nın; $\mathbb{Q}$ yu ve α yı

kapsayan en küçük sayı cismi olduğunu belirtelim. Burada d ye kuadratik bir α cebirsel sayısının *radikantı* denir.

Teorem 4.4. *α radikantı d olan herhangi bir kuadratik cebirsel sayı olsun. O zaman,*

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d}) = \{t + u\sqrt{d} : t, u \in \mathbb{Q}\}$$

olur. Eğer d tamkare değilse, o zaman $\mathbb{Q}(\sqrt{d})$; $\mathbb{Q}$ nun skaler cismi üzerinde 2 boyutlu vektör uzayıdır ve $\mathbb{Q}$ üzerinde bazı $(1, \sqrt{d})$ dir.

İspat. $\mathbb{Q}(\alpha)$ nın herhangi bir ζ elemanı α nın rasyonel sayılar ile çarpılan sonlu kuvvetlerinin toplamıdır. Bununla birlikte α rasyonel sayısı, tamsayı katsayılı kuadratik (4.2) denklemini sağladığından α^2 için $-(b/a)\alpha - c/a$ değişimini yapabiliriz ve birinciden daha büyük kuvvetleri 1 e indirgeyebiliriz. Böylece $\mathbb{Q}(\alpha) = \{t + u\sqrt{d} : t, u \in \mathbb{Q}\}$ olur. Buradan aynı işlemler $\mathbb{Q}(\sqrt{d})$ nin aynı küme olduğunu gösterir. Bu küme de bir vektör uzayıdır.

$d \neq 1$ olan kare çarpansız (1 dışında) bir rasyonel sayı olmak üzere Δ yı

a) Eğer $d \equiv 2$ veya $d \equiv 3 \pmod 4$ ise $\Delta = 4d$;
b) Eğer $d \equiv 1 \pmod 4$ ise $\Delta = d$.

şeklinde tanımlarız.

Burada d ve Δ tanımlandığı için $\mathbb{Q}(\sqrt{d})$ yi radikantı d ve diskriminantı Δ olan kuadratik sayı cismi olarak adlandırabiliriz. Burada $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta})$ olduğuna ilgi çekilir. Dolayısıyla, daha sonraki bölümlerde cisim diskriminantı olarak d kabul edilmiştir.

Teorem 4.5. *d, $d \neq 1$ olan kare çarpansız bir rasyonel sayı olsun. d radikantının kuadratik cebirsel sayılar kümesi;*

$\{a+b\sqrt{d} : a,b \in \mathbb{Z}\}$ *eğer* $d \equiv 2,3 \pmod 4$*;*

$\{a+b\sqrt{d}/2 : a,b \in \mathbb{Z}, a \equiv b \pmod 2\}$ *eğer* $d \equiv 1 \pmod 4$ *ise,*

Bu küme alışılagelmiş toplama ve çarpmaya göre bir halkadır.

İspat. Yukarıdaki tanımları ve (4.1) ve (4.3) denklemlerini göz önüne alarak kuadratik cebirsel α sayısının kuadratik cebirsel bir tamsayı olması ancak ve ancak $b^2-4c=e^2d$ olmak üzere $(-b+e\sqrt{d})/2$ formunda olmasıdır. $b^2-4c=e^2d$ denklemini mod 4 e göre dikkate alırsak; $d \equiv 2$ veya $d \equiv 3 \pmod 4$ olacaktır ki, *b* ve *e* her ikisi birden ya çift ya da tek olmak zorundadır.

Teorem 4.5 te tanımlanan halkayı $\mathbb{Q}(\sqrt{d})$ nin tamsayılar halkası olarak adlandırırız.

Daha sonraki bölümlerde karışıklığa yol açmamak için cebirsel tamsayı yerine kuadratik cebirsel tamsayı ifadesi kullanılacaktır.

4.1.1. Kuadratik cismin diskriminantı

$\mathbb{Q}(\sqrt{D})$ için $\mathfrak{O}_1$ deki bir $\mathfrak{M}$ modülü, ξ_1 ve ξ_2, $\mathfrak{O}_1$ e ait olmak üzere iki elemanlı bazla;

$$\mathfrak{M} = [\xi_1, \xi_2], \tag{4.4}$$

şeklinde ifade edilir.

$$\Delta = \Delta(\mathfrak{M}) = \begin{vmatrix} \xi_1 & \xi_2 \\ \xi_1' & \xi_2' \end{vmatrix} = \xi_1\xi_2' - \xi_1'\xi_2 \tag{4.5}$$

modulün diferenti olarak tanımlanır. $\Delta \neq 0$ olması için gerek ve yeter şart ξ_1 ve ξ_2 nin lineer bağımsız olmasıdır. (ya da buna denk olarak $\mathfrak{M}$ nün boyutu 2 olmalıdır.) Buradan, $\Delta = \xi_2 \xi_2' [(\xi_1 / \xi_2) - (\xi_1 / \xi_2)']$ olup; böylece $\Delta = 0$ olması için gerek ve yeter şart (ξ_1 / ξ_2) nin eşleniğine eşit olmasıdır ki, sonuç olarak bu r/s gibi bir rasyonel kesire eşit olmalıdır. Bu, ξ_1 ve ξ_2 için lineer bağımsızlığı (tamsayı katsayılı) ortadan kaldırır. (Örneğin $r\xi_2 - s\xi_1 = 0$).

D_0, $D = n^2 D_0$ $(n \in \mathbb{Z})$ olacak şekilde D nin kare çarpansız bir çekirdeği olsun. O zaman,

$$w_0 = \begin{cases} \dfrac{1+\sqrt{D_0}}{2}, & D_0 \equiv 1 \pmod 4 \text{ ise} \\ \sqrt{D_0}, & D_0 \not\equiv 1 \pmod 4 \text{ ise} \end{cases}$$

şeklinde tanımlayalım. O zaman, $\mathbb{Q}(\sqrt{D})$ deki kuadratik tamsayıların bazı $[1, w_0]$ dır. Bu modül $\mathfrak{O} = [1, w_0]$ olarak gösterilir. $\mathfrak{O}_n$ deki tamsayıların $x + ynw_0$ formunda olduğunu söylersek bu durumda $\mathfrak{O}_n$ in bazı için birçok durum söz konusudur.

$$w = \frac{1+\sqrt{D}}{2} = \frac{1+n\sqrt{D_0}}{2},\ D_0 \equiv D \equiv 1 \pmod 4 \ (n \text{ tek}) \text{ ise,} \tag{4.6}$$

$(w = nw_0 - (n-1)/2)$ olduğuna ve,

$$w = \frac{\sqrt{D}}{2} = \frac{n\sqrt{D_0}}{2},\ D \equiv 0, D_0 \equiv 1 \pmod 4 \ (n \text{ çift}) \text{ ise,} \tag{4.7}$$

$(w = nw_0 - n/2)$ olduğuna ilgi çekilir.

$$w = \sqrt{D} = n\sqrt{D_0},\ D_0 \not\equiv 1 \pmod 4 \ (\text{herhangi bir } n) \text{ ise,} \tag{4.8}$$

O zaman, herhangi bir durumda $\mathfrak{O}_n$ tamlık bölgesindeki bütün tamsayıların modülü,

$$\mathfrak{O}_n = [1,\ nw_0], \tag{4.9}$$

olup bunun diferenti,

$$\Delta = \Delta(\mathfrak{O}_n) = n(w_0 - w_0') = \begin{cases} n\sqrt{D_0},\ D_0 \equiv 1 \pmod 4 \\ 2n\sqrt{D_0},\ D_0 \not\equiv 1 \pmod 4, \end{cases} \tag{4.10}$$

olacaktır. Daha önemli bir büyüklük ise,

$$d(\mathfrak{M}) = d = \Delta^2, \tag{4.11}$$

olup $\mathfrak{M}$ modülünün diskriminantıdır. Bu her zaman bir tamsayı olup;

$$d(\mathfrak{O}_n) = \begin{cases} n^2 D_0,\ D_0 \equiv 1 \pmod 4 \text{ ise} \\ 4n^2 D_0,\ D_0 \not\equiv 1 \pmod 4 \end{cases} \tag{4.12}$$

olacaktır.

Genel olarak, $\mathfrak{M}$; $\mathfrak{O}_n$ deki tamsayıların modülü ise; $j = [\mathfrak{O}_n / \mathfrak{M}]$, $\mathfrak{M}$ nin $\mathfrak{O}_n$ deki indeksi olmak üzere;

$$\Delta(\mathfrak{M}) = j\Delta(\mathfrak{O}_{n^n}),\ \text{ ve }\ d(\mathfrak{M}) = j^2 d(\mathfrak{O}_n). \tag{4.13}$$

olur. Bu sonuç determinantların çarpma özelliğinden hemen elde edilir. Genellikle $\mathfrak{O}_1$ in d diskriminantına '$\mathbb{Q}(\sqrt{D_0})$ cisminin diskriminantı' veya bu cismin *temel diskriminantı* denir.

Şimdi, $d(\mathfrak{O}_1) = d$ yi göz önüne alalım. O zaman ya

$$D_0 = d \equiv 1 \pmod 4 \text{ ya da } D_0 = d/4 \not\equiv 1 \pmod 4,$$

olup $D_0(\neq 1)$ kare çarpansız olduğunu belirtmeliyiz. Artık daha önce vermiş olduğumuz notasyonları; birleştirecek olursak;

$$w_n = n\left(\frac{d-\sqrt{d}}{2}\right), \tag{4.14}$$

ve

$$\Delta(\mathfrak{O}_n) = n\sqrt{d} \text{ olup öteyandan } d(\mathfrak{O}_n) = n^2 d$$

olmak üzere; $n \geq 1$

$$\mathfrak{O}_n = [1, w_n],$$

şeklinde yazabiliriz. (Cohn 1980)

4.2. Gauss Tamsayıları

Tamsayıların temsil problemi bölümünde temsil probleminin Diophantine denklemlerinin çözümüyle yakından ilgisi olduğunu söylemiştik. Bunun için bazı Diophantine denklemlerinin çözümlerinin bulunmasında Gauss tamsayıları kullanılır.

Tanım 4.2. Herhangi a ve b tamsayıları için $i = \sqrt{-1}$ olmak üzere $a+bi$ şeklindeki sayıya *Gauss tamsayısı* denir. Bu tür sayıların cümlesi $\mathbb{Z}[i]$ ile gösterilir. Eğer $\alpha \in \mathbb{Z}[i]$ ise $(a+bi)(a-bi) = a^2 + b^2$ sayısına α nın *normu* denir ve $N(\alpha)$ gösterilir.

Basit bir hesaplama ile bu çok önemli büyüklüğün çarpımsal özeliğinin bulunduğu yani $\alpha, \beta \in \mathbb{Z}[i]$ için $N(\alpha\beta) = N(\alpha)N(\beta)$ olduğu kolaylıkla gösterilebilir.

Gauss tamsayıları için bölünebilmeyi, tamsayılarda verilen bölme işlemine benzer biçimde tanımlayabiliriz. Gerçekten eğer $\beta = \alpha.\gamma$ olacak biçimde bir $\gamma \in \mathbb{Z}[i]$ varsa α tamsayısı β yı böler denir ve $\alpha \mid \beta$ şeklinde gösterilir.

Her $\alpha \in \mathbb{Z}[i]$ tamsayısı için $\varepsilon \mid \alpha$ olacak şekilde bir ε tamsayısı varsa buna $\mathbb{Z}[i]$ nin bir tersinir elemanı denir. Ayrıca $\mathbb{Z}[i]$ nin tersinir bir elemanı 1i bölen herhangi bir tamsayı olarak tanımlanır. Buna göre

$$\frac{1}{\alpha} = \frac{1}{a+bi} = \frac{a-bi}{N(\alpha)}$$

olduğundan, α ancak ve ancak $(a^2+b^2) \mid a$ ve $(a^2+b^2) \mid b$ ise $\mathbb{Z}[i]$ nin bir tersinir elemandır. Eğer $a \neq 0$ ve $b \neq 0$ ise $a^2+b^2 > \max(|a|,|b|)$ olduğu göz önüne alınırsa ya a veya b nin sıfır olması gerektiği anlaşılır. Buna göre $a=0$ ise $b^2 \mid b$ olur ki bu $b = \pm 1$ olmasını $b=0$ ise bu da $a = \pm 1$ olmasını gerektirir.

$\mathbb{Z}[i]$ nin bütün tersinir elemanları $\pm 1, \pm i$ dir ve $\mathbb{Z}[i]$ nin herhangi bir ε tersinir elemanı için $\varepsilon\alpha$ tamsayısına α tamsayısı ile *ilgilidir* denir. Buna göre 1 ile ilgili olan tamsayılar birim olacaktır. Birimlerden ve ilgililerden başka bir tamsayıya bölünemeyen sıfırdan ve birimden farklı bir tamsayıya *asal sayı* denir. Buna göre bir asalla ilgili olan sayılarda keza asaldırlar. Şu halde π gibi bir asalın

$$1,\ \pi,\ -1,\ -\pi,\ i,\ i\pi,\ -i,\ -i\pi$$

trivial olan bölenleri dışında hiçbir böleni yoktur.

Şimdi, $\mathbb{Z}[i]$ nin asallarına ait tam bir karakterizasyonu aşağıdaki teoremle verelim.

Teorem 4.6. *Bir π tamsayısının bir Gauss asalı olmasının gerek ve yeter koşulu,*

(1) π ya $1-i$ dir veya bununla ilgilidir,

(2) π ya $4k+3$ biçiminde rasyonel asaldır veya bu biçimde bir asalla ilgilidir,

(3) $4k+1$ biçimindeki herhangi bir p rasyonel asalı için $N(\pi) = p$ dir.

ifadelerinin geçerli olmasıdır.

İspat. Bakınız (Şenay 2007)

$\mathbb{Z}[i]$ nin özellikleri yardımıyla, $4k+1$ biçimindeki her asalın iki kare toplamı olarak temsil edilebileceğini göstermek için; öncelikle p nin bir Gauss asalı olmayacağını göstermeliyiz. -1, $4k+1$ biçimindeki asallar için ikinci dereceden bir kalan olduğundan, bir $x \in \mathbb{Z}$ için $x^2 \equiv -1 \pmod{p}$ olacaktır. O halde, $p \mid x^2+1$ ve sonuçta $p \mid (x+i)(x-i)$ dir. $\mathbb{Z}[i]$ bir Öklid bölgesi olduğundan ve her Öklid bölgesi bir tek çarpanlama bölgesi olduğundan $\mathbb{Z}[i]$ tek çarpanlama bölgesidir. Ayrıca, $\mathbb{Z}[i]$ nin her indirgenemez elemanı aynı zamanda bir asal elemanıdır. Buradan, π, $\mathbb{Z}[i]$ nin bir asal elemanı olmak üzere her $\alpha, \beta \in \mathbb{Z}[i]$ için, $\pi \mid \alpha\beta$ olması ya $\pi \mid \alpha$ veya $\pi \mid \beta$ olmasını gerektireceğinden, p bir Gauss asalı olsaydı buna göre $p \mid x+i$ veya $p \mid x-i$ olacaktı. Ancak açık olarak her iki durumda mümkün olamayacağından p bir Gauss asalı olamaz. O zaman $\mathbb{Z}[i]$ nin tersinir olmayan α, β elemanları için $p = \alpha\beta$ olur. Buradan $p^2 = N(p) = N(\alpha)N(\beta)$ ve $N(\alpha)$ ile $N(\beta)$ nın her ikisi de 1 olamayacağından, $N(\alpha) = N(\beta) = p$ bulunur. Böylece herhangi $u, v \in \mathbb{Z}$ için $\alpha = u + iv$ ise $p = u^2 + v^2$ elde edilir.

Son olarak; $\mathbb{Z}[i]$ de tek çarpanlama özeliğinden yararlanarak bir n tamsayısının iki kare toplamı olarak bütün temsillerinin $S(n)$ sayısının hesaplanması ile ilgili teoremi ispatlayalım.

Teorem 4.7. *İki kare toplamı olarak ifade edilen $n \geq 1$ tamsayısının standart biçimi, p_j ve q_j ler sırasıyla $4k+1$ ve $4k+3$ biçiminde asallar olmak üzere $n = 2^a \prod_j p_j^{a_j} \prod_j q_j^{b_j}$ ('Herhangi bir n pozitif tamsayısının iki kare toplamı olarak gösterilebilmesi için gerek ve yeter koşul n nin standart biçimindeki $4k+3$ şeklindeki her asal böleninin kuvvetinin çift olmasıdır.' teoreminden b_j kuvvetleri çifttir) ise;*

$$S(n) = 4\prod_j (a_j + 1)$$

olur. Özel olarak $4k+1$ biçimindeki bir p asalı için $S(p^m) = 4(m+1)$ dir.

Not. Hiçbir terimi bulunmayan böyle bir çarpımın 1 olduğu kabul edilecektir.

İspat. İddiayı kanıtlamak için, $s^2+t^2=n$ yani $(s+ti)(s-ti)=n$ olacak şekilde $(s,t)\in\mathbb{Z}^2$ ikililerinin sayısını bulmalıyız. Şimdi her bir p_j asalı için; $p_j=u_j^2+v_j^2$ olacak şekilde u_j ve v_j tamsayıları bulunacaktır. Bunu, $4k+1$ biçimindeki bir p asalı için $mp=x^2+y^2$ olacak şekilde en küçük pozitif tamsayı m ise $m=1$ olup, $p=x^2+y^2$ yazabiliriz. Böylece n in $\mathbb{Z}[i]$ de $1-i$, $u_j\pm v_j i$ ve q_j Gauss asalları için

$$n=i^a(1-i)^{2a}\prod(u_j+v_ji)^{a_j}(u_j-v_ji)^{a_j}\prod q_j^{b_j}$$

şeklinde bir çarpanlarına ayrılışı vardır.

Şimdi ε, $\mathbb{Z}[i]$ de tersinir, $0\le h\le 2a, 0\le k_j,l_j\le a_j$ ve $0\le m_j\le b_j$ olmak üzere $s+ti$ nin herhangi bir çarpanı

$$\varepsilon(1-i)^h\prod(u_j+v_ji)^{k_j}(u_j-v_ji)^{l_j}\prod q_j^{m_j} \tag{4.15}$$

olacaktır. Üstelik standart biçimin tekliği teoremi gereği (4.15) şeklindeki bütün farklı ifadeler bizi n tamsayısının farklı çarpanlarına götürecektir. Buna göre eşlenik almak suretiyle $s-ti$ nin

$$\overline{\varepsilon}(1+i)^h\prod(u_j-v_ji)^{k_j}(u_j+v_ji)^{l_j}\prod q_j^{m_j} \tag{4.16}$$

elde edilir. Böylece yukarıdaki $(s+ti)(s-ti)=n$ eşitliğinden

$$n=2^h\prod p_j^{k_j+l_j}\prod q_j^{2m_j}$$

elde edilir ki, sonuçta n için bu iki eşitlikten $h=a$, $k_j+l_j=a_j$ ve $2m_j=b_j$ bulunur. Bu durumda t ve m_j nin n ile tamamıyla belirlendiğini, her bir j indisine karşılık u_j için tam a_j+1 seçimin ve bir u_j seçildikten sonra v_j nin belirtilebileceği sonucuna varırız. Açık olarak ε tersinir elemanı için dört ayrı seçim yapılabileceğinden $s+ti$ için de $4\prod(a_j+1)$ seçim söz konusudur. (Şenay 2007)

4.3. İki Değişkenli Kuadratik Formlar

R birimli değişmeli bir halka ve f, R üzerinde derecesi 2 olan iki değişkenli homojen bir polinom olsun. Böylece, $a, b, c \in \mathbb{R}$ ve $\mathbb{R}$ üzerinde herhangi x ve y değişkenleri için $f = ax^2 + bxy + cy^2$ olacaktır. Bu polinomu,

$$4af(x,y) = 4a^2x^2 + 4abxy + 4acy^2$$

$$= 4a^2x^2 + 4abxy + 4acy^2 + by^2 - by^2$$
$$= (2ax + by)^2 - (b^2 - 4ac)y^2$$

şeklinde yazabiliriz. Burada $b^2 - 4ac$ bir kare olduğunda; örneğin $e \in R$ ve $b^2 - 4ac = e^2$ ise o zaman

$$4af(x,y) = (2ax + by)^2 - (b^2 - 4ac)y^2 = (2ax + (b+e)y)(2ax + (b-e)y)$$

olup birinci dereceden iki homojen polinomun çarpımı olur. Bu durumda f polinomu ile çalışmak birinci dereceden polinomla çalışmak anlamına gelir. Dolayısıyla kuadratik polinomlarla çalışmak için $b^2 - 4ac$ nin kare olduğu durumları hariç tutmamız gerekir. Kısaca, $\mathbb{Z}$ üzerinde *iki değişkenli kuadratik polinoma*, $b^2 - 4ac$ ifadesi herhangi bir tamsayının karesi olmaması şartıyla $\mathbb{Z}$ üzerinde iki değişkenli kuadratik polinom denir. (Feyzioğlu 2004) Kısaca, a, b, c formun sırasıyla birinci, ikinci ve üçüncü katsayıları olmak üzere $f = (a, b, c)$ şeklinde gösterilir. $b^2 - 4ac$ ye f in diskriminantı denir. Burada diskriminant D ile gösterilmiştir. a, b, c katsayıları tamsayı ise tamsayı form olarak adlandırılır. Eğer bir f formu tamsayı form ise D bu formun diskriminatı olmak üzere $D \equiv 0 \pmod 4$ tür. Şayet, herhangi bir tamsayı mod 4 e göre 0'a veya 1'e kongrüent ise bu tamsayı iki değişkenli kuadratik bir formun diskriminantıdır. Ek olarak; $f = (a, b, c)$ formu tamsayı ise $b \equiv D \pmod 2$ dir.

İki değişkenli kuadratik formlar diskriminantlarına bağlı olarak aşağıdaki gibi sınıflandırabilir; burada aksi belirtilemediği sürece iki değişkenli kuadratik form yerine kısaca form denilecektir.

Tanım 4.3.

1. Bir f formunun pozitif belirli olması için $D<0$ ve $a>0$ olması gerekir.
2. Bir f formunun negatif belirli olması için $D<0$ ve $a<0$ olması gerekir.
3. Bir f formunun pozitif yarı-belirli olması için $D\le 0$ ve ($a>0$ veya $c>0$) veya ($a<0$ *veya* $c<0$) olması gerekir.
4. Bir f formunun negatif yarı-belirli olması için $D\le 0$ ve ($a<0$ veya $c>0$) olması gerekir.
5. Bir f formunun belirsiz olması için gerek ve yeter şart $D>0$ olmasıdır.

Tanım 4.4. $D\equiv 0 \pmod 4$ ve $D\equiv 1 \pmod 4$ olduğu durumda sırasıyla $(1,\ 0,\ \frac{-D}{4})$, $(1,\ 1,\ \frac{1-D}{4})$ formları D diskriminantına sahiptir. Bu formlara D diskriminantının *esas formu* denir.

4.3.1. Lineer dönüşümler

Bir $ax^2+bxy+cy^2$ formundan $a'x'^2+b'x'y'+c'y'^2$ formuna dönüşüm matris notasyonu ile gösterilebilir. Değişkenlerin değişimi aşağıdaki şekilde yazılabilir ve dönüşüm matrisinin determinantının ± 1 olduğuna ilgi çekilmelidir;

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

$f=(a,\ b,\ c)$ formu ile elemanları tamsayılardan oluşan 2×2 M_f matrisi ile ifade edersek;

$$M_f := \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}$$

olacaktır. Bu matris f in a, b, c katsayıları ile tek olarak belirlendiği gibi, karşıt olarak f de M_f ile tek olarak belirlenir.

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}^t M_f \begin{pmatrix} x \\ y \end{pmatrix}$$

olacaktır. $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in Mat_2(\mathbb{Z})$ olacak şekilde değişkenlerin değişimini;

$$\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x' \\ y' \end{pmatrix}$$

şeklinde yazabiliriz. Buradan,

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}^t M_f \begin{pmatrix} x \\ y \end{pmatrix} = \left(A\begin{pmatrix} x' \\ y' \end{pmatrix} \right)^t M_f \left(A\begin{pmatrix} x' \\ y' \end{pmatrix} \right)$$

$$= \begin{pmatrix} x' \\ y' \end{pmatrix}^t \left(A^t M_f A \right) \begin{pmatrix} x' \\ y' \end{pmatrix}$$

bulunur. Böylece $f\begin{pmatrix} x \\ y \end{pmatrix} = f'\begin{pmatrix} x' \\ y' \end{pmatrix}$ olup, burada f', $M_{f'}$ matrisi $A^t M_f A$ ya eşit olan tek formdur. Böylece

$$A^t M_f A = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

$$= \begin{pmatrix} f(\alpha,\gamma)^t & a\alpha\beta + \frac{1}{2}b(\alpha\delta+\beta\gamma) + c\gamma\delta \\ a\alpha\beta + \frac{1}{2}b(\alpha\delta+\beta\gamma) + c\gamma\delta & f(\beta,\gamma)^t \end{pmatrix}$$

olup,

$$f' = (f(\alpha,\gamma)^t, 2a\alpha\beta + b(\alpha\delta+\beta\gamma) + 2c\gamma\delta, f(\beta,\delta)^t)$$

$$= (a',b',c')$$

elde edilir. $f(a,b,c)$ formunun diskriminantı $-4\det M_f$ e eşit olacaktır. Böylece f' nün diskriminantı

$$-4\det M_{f'} = -4\det(A^t M_f A) = \det A^t (-4\det M_f)\det A = (\det A)^2(-4\det M_f)$$

olur. Bu sayı ancak ve ancak $\det A \neq 0$ olduğunda bir tamsayının karesi olmayacaktır. Böylece homojen f' polinomu ancak ve ancak $\det A \neq 0$ olduğunda iki değişkenli bir kuadratik form olacaktır.

f formu $\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x' \\ y' \end{pmatrix}$ ($\det A \neq 0$)değişkenlerinin değişimi sonucunda f' formuna dönüşür. Matrisi $M_{f'} = A^t M_f A$ olan f' formuna f in A altında dönüşümü denir ve f^A veya $(a,b,c)^A$ olarak yazılır. Bazen bu notasyon $f \xrightarrow{A} f'$ veya $(a,b,c) \xrightarrow{A} (a',b',c')$ şeklinde kullanılır ki $f' = f^A$ veya $(a',b',c') = (a,b,c)$ anlamına gelir. Benzer şekilde, A nın f i f' ne dönüştürdüğü de söylenebilir.

Bu dönüşümün özelliklerini aşağıdaki lemma ile ispatsız olarak vereceğiz.

Lemma 4.4. *f bir form olsun. Bu durumda aşağıdakiler geçerlidir;*

(1) $A, B \in Mat_2(\mathbb{Z})$ ve $\det A \neq 0$, $\det B \neq 0$ olmak üzere $(f^A)^B = f^{AB}$ dir.

(2) I, $Mat_2(\mathbb{Z})$ de birim matris olmak üzere $f^I = f$ dir.

Aşağıdaki lemma f ve f^A nın diskriminantları arasındaki ilişkiyi verir.

Lemma 4.5. *f iki değişkenli kuadratik form ve $A \in Mat_2(\mathbb{Z})$, $\det A \neq 0$ olmak üzere $D(f^A) = D(f)(\det A)^2$ olur.* (Feyzioğlu 2004)

4.3.2. İki değişkenli kuadratik formların denkliği

$f = (a,b,c)$ bir form $A \in Mat_2(\mathbb{Z})$ ve $\det A \neq 0$ olmak üzere; $A = \begin{pmatrix} \alpha & \beta \\ \delta & \delta \end{pmatrix}$ olsun. Herhangi bir m tamsayısı $f' := (a',b',c') := f^A$ ve f ile temsil edilebilir. Gerçekten $\begin{pmatrix} x_0' \\ y_0' \end{pmatrix}$, m nin f' ile temsili ise,

$$x_0 = \alpha x_0' + \beta y_0'$$
$$y_0 = \gamma x_0' + \delta y_0'$$

diyebiliriz. Yani, $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = A \begin{pmatrix} x_0' \\ y_0' \end{pmatrix}$ ve buradan $f\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = f^A \begin{pmatrix} x_0' \\ y_0' \end{pmatrix} = m$ olacaktır. Böylece $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, m nin f ile bir temsilidir. Böylece eğer X_0', m nin f^A ile bir temsili oluyorsa o zaman AX_0' da m nin f ile bir temsilidir. Dolayısıyla,

$$f^A\begin{pmatrix} x_0' \\ y_0' \end{pmatrix} = f\left(A\begin{pmatrix} x_0' \\ y_0' \end{pmatrix}\right)$$

yazabiliriz. Böylece $\{m \in \mathbb{Z} : m, f^A$ ile temsil edilebilir.$\} \subseteq$ $\{m \in \mathbb{Z} : m, f$ ile temsil edilebilir.$\}$. Burada $A \in Mat_2(\mathbb{Z})$ ve $\det A \neq 0$ dır.

Bunlara ek olarak, A nın $Mat_2(\mathbb{Z})$ deki tersinin A^{-1} olduğunu varsayalım. O zaman Lemma 4.4 ten $(f^A)^{A^{-1}} = f^{AA^{-1}} = f^I = f$ olacaktır. f ile f^A nın rollerini değiştirmekle $\{m \in \mathbb{Z} : m, f^A$ ile temsil edilebilir.$\} \supseteq$ $\{m \in \mathbb{Z} : m, f$ ile temsil edilebilir.$\}$ olacaktır.

Sonuç olarak,

$$\{f\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \in \mathbb{Z} : x_0, y_0 \in \mathbb{Z}\} = \{f'\begin{pmatrix} x_0' \\ y_0' \end{pmatrix} \in \mathbb{Z} : x_0, y_0 \in \mathbb{Z}\}$$

olur. Bu, $Mat_2(\mathbb{Z})$ de tersi olan herhangi bir $A \in Mat_2(\mathbb{Z})$ için geçerlidir.Yani, bunu $Mat_2(\mathbb{R})$ halkasındaki tersinirlerin grubuna ait olan herhangi bir A matrisi için geçerlidir. $Mat_2(R)$ deki tersinirler grubu $\{A \in Mat_2(\mathbb{Z});\ \det A \in \{+1, -1\}\}$ olup $GL(2,\mathbb{Z})$ ile gösterilir.

Teorem 4.8. *f, iki değişkenli kuadratik bir form ve $A \in GL(2,\mathbb{Z})$ olsun. O zaman f ile temsil edilebilen tamsayıların kümesi f^A ile temsil edilen tamsayıların kümesi ile çakışır. Yani,*

$$\{f\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \in \mathbb{Z} : x_0, y_0 \in \mathbb{Z}\} = \{f^A\begin{pmatrix} x_0' \\ y_0' \end{pmatrix} \in \mathbb{Z} : x_0', y_0' \in \mathbb{Z}\}.$$

Burada $f^A = f'$ olacak şekilde bir $A \in GL(2,\mathbb{Z})$ matrisi var ise f ve f' formları; denktir. Gauss A matrisinin determinantının +1 e eşit olması gerektiğini söylemiştir. Bunu $GL(2,\mathbb{Z})$ in bir alt grubu olan $SL(2,\mathbb{Z}) = \{A \in Mat_2(\mathbb{Z});\ \det A = 1\}$ olarak tanımlamıştır.

Tanım 4.5. f ve f' iki form olsun. $f^A = f'$ olacak şekilde bir $A \in SL(2,\mathbb{Z})$ matrisi varsa f formu, f' formuna '*denktir*' denir ve $f \sim f'$ şeklinde yazılır.

Tanım 4.6. f ve f' iki form olsun. $f^A = f'$ olacak şekilde bir $A \in GL(2,\mathbb{Z})$ matrisi varsa f formu, f' formuna '*has olmayan denktir*' denir.

$SL(2,\mathbb{Z})$ grubu bütün formların kümesi üzerinde hareket eder. $f \sim f'$ bağıntısı f ve f' nün aynı $SL(2,\mathbb{Z})$ yörüngesi üzerinde yer aldığını söyler. Böylece $\sim$ bağıntısı bir denklik bağıntısıdır. Bu denklik bağıntısı bütün formların kümesini ayrık sınıflara böler. 'f ve f' aynı sınıftadır' veya '$f \sim f'$ olmak şartıyla f, f' nün sınıfındadır' şeklinde ifade edilir. Formların sınıfı daha sonra ayrıntılı bir şekilde işlenecektir.

Benzer olarak, $GL(2,\mathbb{Z})$ bütün formların kümesi üzerinde hareket eder. İki formun has olmayan denkliği ise bu formların ancak ve ancak aynı $GL(2,\mathbb{Z})$ yörüngesinde olmasıyla mümkündür. Dolayısıyla has denklik yerine '$SL(2,\mathbb{Z})$' denkliği, has olmayan denklik yerine $GL(2,\mathbb{Z})$ denkliği kullanılabilir.

Denk formlar aynı tamsayıları temsil eder. Fakat aynı tamsayıları temsil eden formların denk olması gerekmez. Ayrıca denk formlar aynı diskriminanta sahiptirler.

4.3.3. İki değişkenli kuadratik formların indirgenebilirliği

Örnek 3.1 de f i lineer çarpanlarına ayırarak 113 ün temsillerini bulmuştuk. Bu kesimde bunun ne zaman mümkün olabileceğini göreceğiz.

İki değişkenli bir lineer formu (bilineer) $l(X,Y)=dX+cY$ formunda bir polinom olup, $c,\ d$ katsayıları rasyonel sayı ise formun rasyonel olarak adlandırıldığını hatırlatıp aşağıdaki teoremi verelim;

Teorem 4.9. *$f=(a,\ b,\ c)$ tamsayı katsayılı iki değişkenli bir kuadratik form olsun. O halde, aşağıdaki ifadeler denktir:*

1. f in diskriminantı bir tamsayının karesidir.

2. f formu, iki değişkenli rasyonel iki lineer formun çarpımıdır.

3. f formu, iki değişkenli tamsayılı iki lineer formun çarpımıdır.

4. $(x,y)=(0,0)$ ve $f(x,y)=0$ olan $(x,y)\in\mathbb{Z}^2$ vardır.

İspat. Bakınız (Buchmann ve Vollmer 2007).

Tanım 4.7. Bir f formu Teorem 4.9 un özelliklerini sağlıyorsa f formuna *indirgenebilir* denir.

Bir pozitif belirli $(a,\ b,\ c)$ kuadratik formu $|b|\le a\le c$ şartını sağlıyorsa 'indirgenmiştir' denir. Ayrıca $|b|\le\sqrt{\frac{|D|}{3}}$ ve $a\le\sqrt{\frac{|D|}{3}}$ olacaktır.

D diskriminantlı pozitif belirli formların denklik sınıflarının sayısı *sınıf sayısı* olarak adlandırılır. Fakat aynı sınıfta iki ya da daha fazla indirgenmiş form olabilir. Bu yüzden iki farklı formun denk olup olmadığını kontrol etmemiz gerekir.

Aşağıdaki tabloda diskriminantı D olan indirgenmiş formlar ve sınıf sayıları verilmiştir.

D	$h(D)$	D diskriminantının indirgenmiş formları
-4	1	x^2+y^2
-8	1	x^2+2y^2
-12	1	x^2+3y^2
-20	2	$x^2+5y^2,\ 2x^2+2xy+3y^2$
-28	1	x^2+7y^2
-56	4	$x^2+14y^2,\ 2x^2+7y^2,\ 3x^2\pm 2xy+5y^2$
-108	3	$x^2+27y^2,\ 4x^2\pm 2xy+7y^2$
-256	4	$x^2+64y^2,\ 4x^2+4xy+17y^2,\ 5x^2\pm 2xy+13y^2$

Tablo 2. D diskriminantının indirgenmiş formları ve sınıf sayısı

5. KUADRATİK FORMLAR VE İDEALLER

5.1. İdealler

$\mathbb{Q}(\sqrt{-5})$ cismindeki gibi bazı sayı cisimlerinde çarpanlarına ayrılamayan cebirsel tamsayılar için tek çarpanlamanın geçerli olmayışı matematikçileri (Kummer ve Dedekind) ideal çarpanlara çalışmaya yöneltmiştir. Bu çarpanlar 'idealleştirilmiş' sayılardan çok modüllerin özel tiplerini içerir.

Modül notasyonunda kümeleri göstermek için önceki gibi $\mathfrak{M}, \mathfrak{N}...$ sembollerini kullanacağız. α, β cebirsel tamsayılar olmak üzere; $\mathfrak{D}_n$ kuadratik tamlık bölgesindeki bir $\mathfrak{a}$ idealini; $\mathfrak{D}_n$ deki modül olarak $\xi \in \mathfrak{D}_n$ ise $\xi\alpha \in \mathfrak{a}$ özelliğiyle tanımlarız. Sembolik olarak;

$$\alpha, \beta \in \mathfrak{a}, \quad \xi \in \mathfrak{D}_n, \tag{5.1}$$

ise o zaman,

$$\alpha \pm \beta \in \mathfrak{a}, \text{ (modül özeliği)} \tag{5.2}$$

$$\alpha\xi \in \mathfrak{a} \text{ (idealleri absorblama özeliği)} \tag{5.3}$$

İdeallere iki açıdan bakılabilir. Birincisi ideali, tanımlı bir modül bazı ile modül olarak ve her elemanını koordinatlar cinsinden ele almaktır. İkincisi ise, notasyonların detaylarına kısıtlanmaksızın (5.1)-(5.3) deki gibi teorik olarak tanımlamaktır. Modül bazını

$$\alpha = ax + (b + cw_n)y;$$

$$\xi = r + sw_n, \quad \alpha\xi = X + w_n Y,$$

olacak şekilde, $\mathfrak{a} = [a,\ b + cw_n]$ olacaktır. Burada, bütün $r,\ s,\ x,\ y$ tamsayıları için,

$$(r + sw_n)[ax + (b + cw_n)y] = aX + (b + cw_n)Y \tag{5.4}$$

olacak şekilde $X,\ Y$ tamsayıları bulunur. Fakat henüz modül kavramı tamamıyla hesaplanabilir özellikte değildir. Örneğin, modül olarak kabul edilen bir ideal modülün indeksi olan j gibi rasyonel tamsayıları içerir. Modül bazı yaklaşımı gerçekte kuadratik formlarla ilgili hesaplamalarda kullanılır. (5.4) e benzer olarak ideal tanımını aşağıdaki şekilde yapabiliriz.

$$\alpha, \beta \in \mathfrak{a},\ \ \xi, \eta \in \mathfrak{O}_n \text{ ise o zaman } \alpha\xi + \beta\eta \in \mathfrak{a} \text{ dır.} \tag{5.5}$$

$\mathfrak{O}_n$ deki $\mathfrak{a}$ idealinin elemanların eşlenikleri ile oluşturulan kümeyi dikkate alalım. Bunlar $\mathfrak{O}_n$ de idealler oluştururlar ve bunlara *eşlenik idealler* denir ve $\mathfrak{a}'$ ile gösterilir.

İdealler; kongrüanslarda modüllerden daha kullanışlıdır. Örneğin, $\mathfrak{M}$ bir modül olmak üzere; modül işlemleriyle kongrüansı aşağıdaki şekilde yazabiliriz.

$$\begin{aligned} &\alpha \equiv \beta \ (\text{mod } \mathfrak{M}), \quad \alpha, \beta \in \mathfrak{O}_n \\ &\gamma \equiv \delta \ \ (\text{mod } \mathfrak{M}) \quad\ \ \gamma, \delta \in \mathfrak{O}_n, \end{aligned}$$

ise o zaman;

$$\alpha \pm \gamma \equiv \beta \pm \delta \ (\text{mod } \mathfrak{M})$$

olacaktır. Bununla birlikte, bir $\mathfrak{a}$ ideali ile çarpma yapabiliriz.

$$\begin{aligned} &\alpha \equiv \beta \ (\text{mod } \mathfrak{a}), \quad \alpha, \beta \in \mathfrak{O}_n \\ &w\alpha \equiv w\beta (\text{mod } \ \mathfrak{a}), \text{ herhangi bir } w \in \mathfrak{O}_n, \text{ için} \end{aligned}$$

Böylece ($\beta = 0$ olduğunda) 'idealin elemanlarını'; gerçekte rasyonel sayılardan cebirsel sayılara 'bir tamsayının katlarının' genelleştirilmesi olarak düşünebiliriz.

$\mathfrak{O}_n$ in sabit bir elemanı α için $\mathfrak{O}_n$ deki esas ideali; $\xi \in \mathfrak{O}_n$ olmak üzere $\alpha\xi$ ların kümesi olarak tanımlar ve $\mathfrak{a} = (\alpha)$ şeklinde belirtiriz. Bir tamlık bölgesindeki bütün idealler asal ise, esas ideal tamlık bölgesi olarak adlandırılır.

5.1.1. İdeallerin toplamı ve baz

İdeallerin toplamını;

$$\mathfrak{a} + \mathfrak{b} = \{\alpha + \beta\}, \quad \alpha \in \mathfrak{a},\ \beta \in \mathfrak{b}, \tag{5.6}$$

şeklinde tanımlarız. Burada, iki idealin toplamının yine bir ideal olduğunu belirtmeliyiz. Bunu (5.5) tanımını doğrudan kullanarak görebiliriz.

Aşağıdaki özelikler kolaylıkla gerçeklenebilir.

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}, \quad \text{(değişme özeliği)} \tag{5.7}$$

$$\mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c}, \quad \text{(birleşme özeliği)} \tag{5.8}$$

$$\mathfrak{a} + \mathfrak{b} \supseteq \mathfrak{a} \tag{5.9}$$

Şimdi,

$$\mathfrak{a} + \mathfrak{b} = (\mathfrak{a}, \mathfrak{b}),$$

notasyonunu verelim. Burada, özellikle $\mathfrak{a} = (\alpha)$, $\mathfrak{b} = (\beta)$ ise;

$$\begin{cases} \mathfrak{a} + \mathfrak{b} = (\alpha) + \mathfrak{b} = (\alpha, \beta), \\ \mathfrak{a} + \mathfrak{b} = (\alpha) + (\beta) = (\mathfrak{a}, \beta). \end{cases} \tag{5.10}$$

yazarız. Burada (5.7) nin $(\mathfrak{a},\mathfrak{b})=(\mathfrak{b},\mathfrak{a})$, (5.8) in $\mathfrak{a}+(\mathfrak{b},\mathfrak{c})=(\mathfrak{a},\mathfrak{b})+\mathfrak{c}$ olup buradan $(\mathfrak{a},(\mathfrak{b},\mathfrak{c}))=((\mathfrak{a},\mathfrak{b}),\mathfrak{c})$ olduğunu söyleyebiliriz.

Kısaca, $A=(\alpha_1,\ \alpha_2,...,\ \alpha_n)$ ve $B=(\beta_1,\ \beta_2,...,\ \beta_n)$, K cisminin idealleri olmak üzere;

$$\begin{cases} A+B=(\alpha_1,...,\alpha_n,\beta_1,...,\beta_m) \\ AB=(\alpha_1\beta_1,...,\alpha_1\beta_n,...,\alpha_n\beta_1,...,\alpha_n\beta_m) \end{cases}$$

şeklinde tanımlayabiliriz. (Duverney 1998)

Örnek 5.1. $K=\mathbb{Q}(i\sqrt{5})$ kuadratik sayı cismini göz önüne alalım. $A=(3,1+i\sqrt{5})$ve $B=(3,1-i\sqrt{5})$ olsun. O zaman $A+B=(3,\ 1+i\sqrt{5},\ 1-i\sqrt{5})$ elde ederiz. O halde, $1=3-2\in(A+B)$ olur. Böylece, $(1)\subset(A+B)$ dir. Karşıt olarak, $(A+B)\subset(1)$ elemanları K cisminden olan bir halkaya eşit olur. O halde $A+B=(1)$ olur. Benzer biçimde $AB=(3\cdot 3,\ 3(1-i\sqrt{5}),3(1+i\sqrt{5}),6)$ olur. O halde, $3=9-6\in(A+B)$ ve (3) olur. Fakat $x=3(3x_1+(1-i\sqrt{5})x_2+(1+i\sqrt{5})x_3+2x_4)\in(3)$ olmak üzere $\forall x\in(AB)$, $x=x_1.3.3+x_2.3(1-i\sqrt{5})+x_3.3(1+i\sqrt{5})+x_4.6$ (x_i ler halkanın elemanları) Böylece, $(AB)\subset(3)$ olup sonuç olarak $AB=(3)$ olur. Burada A ve B, K cisminin tamsayılarının idealleridir. (Duverney 1998)

Genel ideal bazı notasyonun iki veya daha fazla varyasyonları kolaylıkla düşünülebilir ve de tutarlı olur. Böylece,

$$\mathfrak{a}=(\alpha_1,\alpha_2,...,\alpha_s)=\alpha_1\mathfrak{O}_n+\alpha_2\mathfrak{O}_n+...+\alpha_s\mathfrak{O}_n$$

ideali

$$\left\{\xi_1\alpha_1+\xi_2\alpha_2+...+\xi_s\alpha_s\right\},\quad \xi_i\in\mathfrak{O}_n.$$

toplamlarından oluşur. Burada $\alpha_1,\alpha_2,...,\alpha_s$ cebirsel tamsayıları $\mathfrak{a}$ için bir *ideal bazı* oluştururlar. Fakat ξ_i ler cebirsel tamsayılar (rasyonel olmak zorunda değil)

olduğunda ve $\alpha_i$ler 'minimal' (ideal elemanlarının ξ_i lerle tek türlü gösteriminden dolayı) olmak zorunda olmadıklarından, ideal bazı modül bazı ile karıştırılmamalıdır.

Bu notasyonu, elementer sayılar teorisi ile karşılaştırabiliriz. $a,b \in \mathbb{Z}$ için $\gcd(a,b) = g$ olsun. O zaman, $(g) = ax + by$ olacaktır. $\mathfrak{O}_n$ deki $\mathfrak{a}$ idealini temsil eden $(a,b,\alpha,...,\lambda)$ ideal bazı notasyonunu $(g,\alpha,...,\lambda)$ notasyonu ile değiştirebiliriz. Özellikle, $g = 1$ ise $a = (1)$ dir. Ayrıca, kuadratik tamlık bölgesindeki her idealin sonlu bir bazının olduğunu söyleyebiliriz.

İdeal bazı ile daha genel olan modül bazının ilişkisini aşağıdaki şekilde verelim.

Teorem 5.1. $[\alpha,\beta]$ *modülü bir ideal oluşturuyorsa, o zaman* $[\alpha,\beta] = (\alpha,\beta)$ *olur ki, bu modül bazının aynı zamanda ideal bazı olduğunu belirtir.*

İspat. $[\alpha,\beta]$ ideal olmasa dahi, açık olarak $(\alpha,\beta) \supseteq [\alpha,\beta]$ olduğuna ilgi çekilir. Fakat $[\alpha,\beta]$ bir ideal ise $[\alpha,\beta] \ni \alpha$ ve $[\alpha,\beta] \ni \beta$ olduğu gerçeğinden hareketle buradan $[\alpha,\beta] \supseteq (\alpha) + (\beta) = (\alpha,\beta)$ olur. (Cohn 1980)

5.1.2. İdeal bazının dönüştürülmesi

İdeal bazındaki elemanların sayısının kuadratik modülün bazının iki elemana sahip olduğu gerçeğiyle hesaplanamayacağı açıktır. İdeal bazının esnekliği aşağıdaki basit dönüşüm kurallarıyla netleştirilebilir;

a) İdeal bazının elemanları tekrar düzenlenebilir.

b) Tekrar eden elemanlar çıkarılabilir.

c) Herhangi bir baz elemanı, diğer baz elemanları tarafından belirlenebilen idealin bir elemanı ise bu eleman çıkarılabilir.

e) Özellikle sıfır baz elemanı çıkarılabilir.

f) Bir baz elemanı, tersiyle kendisinin çarpımı ile yer değiştirebilir.

Gerçekte her zaman kuadratik bir ideali, (bir modülün baz işlemlerini kapsadığından) bir idealin baz işlemlerini kullanarak iki elemanlı forma indirgeyebiliriz. Fakat her bir idealin bir modül olarak yazılmadığı durumda iki ideal bazı eşit idealleri belirlediği zaman bu durum her zaman açık olmayacaktır. Örneğin, $\mathfrak{O}_n = [1, w_n]$ olduğunda herhangi bir ideal için;

$$(\alpha, \beta, ...) = \alpha\mathfrak{O}_n + \beta\mathfrak{O}_n + ... = [\alpha, \alpha w_n, \beta, \beta w_n, ...]$$

olacaktır. Aşağıdaki örnek ideal bazının genel olarak modül bazından daha esnek olduğunu ve çarpanlara ayırma problemlerinde tercih edildiğini gösterir.

Örnek 5.2. $\mathfrak{O}_n = \mathfrak{O}_1 = [1, \sqrt{3}]$ olsun. Yukarıdaki kurallara göre $(33, 7 - 3\sqrt{3}) = (4 + 3\sqrt{3})$ olduğunu adım adım gösterelim.

Çözüm.

$(33, 7 - 3\sqrt{3}) = (33,\ 7 - 3\sqrt{3},\ (7 - 3\sqrt{3})(7 + 3\sqrt{3})) = (33,\ 7 - 3\sqrt{3},\ 22) = (33,\ 22,\ 7 - 3\sqrt{3},\ 11)$
$= (7 - 3\sqrt{3},\ 11) = (4 + 3\sqrt{3},\ 11) = ((4 + 3\sqrt{3}),\ (4 + 3\sqrt{3})(4 - 3\sqrt{3})) = (4 + 3\sqrt{3}).$

$\mathfrak{O}_n$ de tersinir olmayan iki $\mathfrak{a}$ ve $\mathfrak{b}$ ideali, $\mathfrak{p} \mid \mathfrak{ab}$ ise o zaman $\mathfrak{p} \mid \mathfrak{a}$ veya $\mathfrak{p} \mid \mathfrak{b}$ oluyorsa $\mathfrak{p}$ ye *asal ideal* denir.

5.2. İki Değişkenli Kuadratik Formlar ve İdealler

Bu bölümde $\mathfrak{O}_1$ deki ideallerle formlar arasındaki ilişkiden bahsedilmiştir. İlk bakışta bir ideal ve onun eşleniğinin aynı forma karşılık geldiğini düşünebiliriz. Örneğin, $\mathfrak{j}=[\alpha,\beta]$ ve $\mathfrak{j}'=[\alpha',\beta']$ idealleri için modül bazını kullanırsak her zaman aynı formu elde ederiz;

$$N(\alpha x+\beta y)=N(\alpha' x+\beta' y)=(\alpha x+\beta y)(\alpha' x+\beta' y)$$

$$=Ax^2+Bxy+Cy^2$$

$\mathfrak{j}\mathfrak{j}'\sim(1)$ olduğundan, $\mathfrak{j}$ ve $\mathfrak{j}'$ yü birbirinden ayırmazsak buradan; $\mathfrak{j}$ nin bir sınıfı J için $J^2=I$ olacaktır ki, bu da sınıf yapısıyla çelişir.

5.2.1. Bir idealin sıralı bazı

α ve β, $\mathfrak{O}_1$ de sabit elemanlar ve x ve y değişken rasyonel tamsayılar olmak üzere, $\mathbb{Q}(\sqrt{d})$ için $\mathfrak{O}_1$ deki $\mathfrak{j}$ idealini modül bazıyla

$$\mathfrak{j}=[\alpha,\beta]=\{x\alpha+y\beta\} \tag{5.11}$$

dikkate alalım. Yani, bu bütün $\alpha x+\beta y$ lerin kümesidir. Şimdiye kadar $[\alpha,\beta]$ ve $[\beta,\alpha]$ arasında bir ayırım yapmadık. Fakat şimdi her iki elemanlı bazı $\Delta/\sqrt{d}$ oranı pozitif veya

$$\frac{\Delta}{\sqrt{d}}=\frac{1}{\sqrt{d}}\begin{vmatrix}\alpha & \beta\\ \alpha' & \beta'\end{vmatrix}=\frac{\alpha\beta'-\beta\alpha'}{\sqrt{d}}>0 \tag{5.12}$$

şartıyla '*sıralı*' olarak dikkate alalım. $\pm\Delta/\sqrt{d} = N[\mathrm{j}] > 0$ olduğu kuadratik cismin diskriminantı bölününde gösterilmiştir. Şayet $(\alpha\beta' - \beta\alpha')/\sqrt{d} < 0$ ise o zaman bunun yerine $[\beta, \alpha]$ yı sıralayarak (β yerine α dersek, tersi de doğru) (5.12) de pozitif bir oran elde ederiz. Böylece, $N(\mathrm{j})$ için

$$\left|\alpha\beta' - \beta\alpha'\right| = N[\mathrm{j}]\,|\sqrt{d}\,|$$

yerine daha güçlü olan

$$\alpha\beta' - \beta\alpha' = N[\mathrm{j}]\sqrt{d} \tag{5.13}$$

kullanırız. Böylece, bazın değişimini dikkate almış oluruz. Bazlar sıralı ise o zaman

$$[\alpha, \beta] = [\gamma, \delta] \tag{5.14}$$

olması için gerek ve yeter şart

$$\begin{aligned} \alpha &= P\gamma + Q\delta, \\ \beta &= R\gamma + S\delta, \end{aligned} \tag{5.15}$$

olmasıyla mümkündür. Burada P, Q, S, R dar anlamda unimodüler dönüşüm belirleyecek şekilde,

$$PS - QR = +1 \tag{5.16}$$

olacaktır. Yani, burada (5.16) nın sadece $+1$ olduğuna ± 1 olmadığına ilgi çekilir. Bunun ispatı için aşağıdaki eşitliği yazmak yeterli olacaktır.

$$\begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix} = \begin{vmatrix} P & Q \\ R & S \end{vmatrix} \begin{vmatrix} \gamma & \delta \\ \gamma' & \delta' \end{vmatrix} \tag{5.17}$$

Teorem 5.2. *Bir idealin iki sıralı bazı; dar anlamda unimodular dönüşüm altında denktir ve terside doğrudur.*

Artık bütün bazları sıralı olarak kabul edebiliriz. Böylece (5.11) den

$$\mathfrak{j}' = [\beta', \alpha'] = \{y\alpha' + x\beta'\} \tag{5.18}$$

olur ve eşleniğini alma işlemi elemanların sırasını değiştirme işleminin (rasyonel) bir karşılığıdır.

5.2.2. Dar anlamda denk idealler

Burada sıralı bazları dikkate alarak denkliği tekrar ele alacağız. Mesela p, $\mathfrak{O}_1$ de sıfır olmayan bir tamsayı olmak üzere

$$\begin{aligned} p\mathfrak{j} = p[\alpha, \beta] &= [p\alpha, p\beta] \text{ eğer } N(p) > 0, \\ &= [p\beta, p\alpha] \text{ eğer } N(p) < 0, \end{aligned}$$

Bunu (5.12) deki gibi determinantlarda doğrudan yer değiştirme ile,

$$(p\alpha)(p\beta') - (p\beta)(p\alpha)' = N(p)(\alpha\beta - \beta\alpha')$$

olacaktır. Bu durumda aşağıdaki tanımı verelim.

Tanım 5.1. İki $\mathfrak{j}$ ve $\mathfrak{k}$ idealleri eğer $N(p\sigma) > 0$ olacak şekilde

$$p\mathfrak{j} = \sigma\mathfrak{k}$$

oluyorsa bu ideallere *dar anlamda denktir* denir. Bu $\mathfrak{j} \approx \mathfrak{k}$ şeklinde yazılır.

Burada aynı zamanda $N(p^*\sigma^*) < 0$ olduğu durumlarda başka denklik bağıntıları olabilir. Burada (5.12) açısından bu denklik bağıntıları hariç tutulmuştur.

Teorem 5.3. *Alışılagelmiş anlamda denk olan iki ideal aşağıdaki koşulları sağlayan bir cisimde dar anlamda da denktir.*

a) $D<0$ *veya*

b) $D>0$ *temel tersinir negatif normlu ise,*

Diğer durumlarda,

c) $D>0$ *olduğunda, eğer* $\mathfrak{j}\sim\mathfrak{k}$ *(alışılagelmiş denklikte) ise, temel tersinir pozitif normludur. Dar anlamda denklikte ise ya* $\mathfrak{j}\approx\mathfrak{k}$ *ya da* $\sqrt{d}\,\mathfrak{j}\approx\mathfrak{k}$ *dir.*

İspat. a) açıktır; çünkü normlar her zaman pozitiftir. b) $D>0$ olması durumunda η_1 temel tersinir olsun. Eğer $N(\eta_1)=-1$ ise (2) deki $\mathfrak{j}\approx\mathfrak{k}$ yi garantilemek; $N(p\sigma)<0$ olduğunda ($N(p\eta_1\sigma)>0$ olduğundan), (2) yerine $p\eta\mathfrak{j}_1=\sigma\mathfrak{k}$ eşitliğini kullanarak kolaydır. c) için $\mathfrak{j}\sim\mathfrak{k}$ ise öteyandan $\mathfrak{j}\not\approx\mathfrak{k}$ olduğuna ilgi çekilir. Buradan $p\mathfrak{j}=\sigma\mathfrak{k}$ ve $N(p\sigma)<0$ olacaktır. Daha sonra $\sqrt{D}\mathfrak{k}=\mathfrak{k}^*$ oluşturursak, buradan $\sqrt{D}\,p\mathfrak{j}=\sigma\mathfrak{k}^*$ olup, öte yandan $N(p\sigma\sqrt{d})=N(p\sigma)N(\sqrt{d})=-DN(p\sigma)>0$ iken $\sqrt{D}\mathfrak{k}=\mathfrak{k}^*$ olup buradan $\sqrt{D}\,p\mathfrak{j}=\sigma\mathfrak{k}^*$ olacaktır. Böylece eğer $\mathfrak{j}\sim\mathfrak{k}$ ve $\mathfrak{j}\not\approx\mathfrak{k}$ ise o zaman $\mathfrak{j}\approx\sqrt{D}\mathfrak{k}$ dir.

Şimdi sadece $N(\eta_1)>0$ olduğunda, $\mathfrak{k}^*\not\approx\mathfrak{k}$ olduğunu görmek için $(1)\not\approx(\sqrt{D})$ olduğunu gerçeklememiz gereklidir. $(1)\approx(\sqrt{D})$ ise o zaman $p(1)=\sigma(\sqrt{D})$ olup bu da bazı η^* için $p\eta^*=\sigma\sqrt{D}$ olup öte yandan $N(p\sigma)>0$ dır. Fakat $N(\eta^*)N(p)=-DN(\sigma)$ olduğunda $N(p\eta^*)=N(\sigma\sqrt{D})$ olur. Böylece $(1)\approx(\sqrt{D})$ ise $N(\eta^*)<0$ olacaktır.

d diskriminantlı $\mathbb{Q}(\sqrt{d})$ nin dar anlamda denklik sınıflarının sayısını $h_+(d)$ ile gösterelim. $h(d)$ ise alışılagelmiş denklik sınıflarının sayısı olsun. Bir başka deyişle, bir formun alışılagelmiş denklik sınıflarının sayısı sonlu olup d diskriminantının indirgenmiş formlarının sayısıdır. Aşağıdaki teoremle bu ikisi arasındaki kıyaslamayı yapmış oluruz.

Teorem 5.4. $D<0$ *ise veya* $D>0$ *ve* $N(\eta_1)<0$ *ise* $h(d)=h_+(d)$ *dir.* $D>0$ ve $N(\eta_1)>0$ *ise* $2h(d)=h_+(d)$ *dir.*

5.2.3. Kuadratik formların denklik sınıfları

Burada kuadratik formlarda bazın nasıl değiştiğini inceleyeceğiz.

$$f(x,y) = ax^2 + bxy + cy^2, \tag{5.19}$$

olsun ve burada $D = b^2 - 4ac$ diskriminantının bir tam kare olmadığını varsayıyoruz. Fakat D kare çarpansız olmak zorunda değildir. p, q, r, s tamsayı katsayıları ile değişkenlerin değişimini dikkate alalım. Determinant $ps - qr \neq 0$ olmak üzere,

$$\begin{aligned} x &= px^* + qy^* \\ y &= rx^* + sy^* \end{aligned} \tag{5.20}$$

dir. Dolayısıyla,

$$\begin{aligned} a^* &= ap^2 + bpr + cr^2 \\ b^* &= 2apq + b(ps + qr) + crs \\ c^* &= aq^2 + bqs + cs^2 \end{aligned} \tag{5.21}$$

olacak şekilde

$$\begin{aligned} f(x,y) &= a(px^* + qy^*)^2 + b(px^* + qy^*)(rx^* + sy^*) + c(rx^* + sy^*)^2 \\ &= a^* x^{*2} + b^* x^* y^* + c^* y^{*2} = f^*(x^*, y^*) \end{aligned} \tag{5.22}$$

buluruz. Burada

$$\begin{aligned} D^* &= b^{*2} - 4a^* c^* = (ps - qr)^2 (b^2 - 4ac) \\ D^* &= (ps - qr)^2 D \end{aligned} \tag{5.23}$$

olur ki, burada $ps - qr = \pm 1$ olduğunda diskriminant değişmez olarak kalır.

$f(x,y)$ ve $f^*(x^*,y^*)$ formları determinantı $ps-qr=+1$ olan bazı dönüşümlerle (5.20) ve (5.22) de olduğu gibi birbirleriyle ilişkilendirilir. $ps-qr=+1$ olması durumunda denklik *has denkliktir* ve $f \approx f^*, ps-qr=-1$ olması durumunda denklik has olmayan denkliktir ve $f \sim f^*$ ile gösterilir.

Genel olarak aksi belirtilmediği sürece formların has olmayan denkliği ile ilgilenilmiştir. Formların denkliği f, f_1 sembolleriyle ve benzer olarak ideal sınıfları ile gösterilir.

$ps-qr=+1$ olan (5.20) tipindeki dönüşümler determinantın temel özelliklerinden, transitif, simetrik ve refleksif olduğundan genel anlamda bir denklik sınıflarından söz edebiliriz.

Bu nedenle,

$$f(x,y) \sim f(y,x) \sim f(-x,y) \sim f(y,-x) \sim f(-x,-y) \sim f(x,-y) \sim f(-y,x) \sim f(-y,-x),$$
$$f(x,y) \approx f(y,-x) \approx f(-y,x) \approx f(-x,-y)$$

trivial olup öte yandan,

$$f(x,y) \approx f(y,x) \text{ veya } f(x,y) \approx f(x,-y) \ldots \text{vs},$$

$$f(x,y) \approx -f(x,y) \text{ ve hatta } f(x,y) \sim -f(x,y) \ldots \text{vs}$$

kolaylıkla trivial olmayabilir. $f(x,y)$ nin eşleniği $f(x,-y)=f'(x,y)$ ve negatifi $-f(x,y)$ dir. Aynı zamanda (5.21) de

$$a^* = f(p,r) \tag{5.24}$$

olduğuna ilgi çekilir. Burada $(p,r)=1$ olan (5.24) deki ifadeye a^* ın $f(x,y)$ formu ile *has temsili* denir.

Teorem 5.5. *a^* tamsayısının bir form ile her has temsil, en yüksek dereceli terimin katsayısı a^* tamsayısına eşit olan has denk forma eşittir.*

İspat. İspatı için (5.24) de $ps - qr = +1$ olacak biçimde sadece q ve s sayılarını bulmamız yeterlidir.

Böylelikle has temsillere çalışmak bizi denk formlara çalışmaya götürür.

Teorem 5.6. *$f_1(x,y)$ ve $f_2(x,y)$ formları aynı D diskriminantına sahipse ve aynı p asalını temsil ediyorlarsa ya $f_1(x,y) \approx f_2(x,y)$ ya da $[f_1'(x,y) =] f_1(x,-y) \approx f_2(x,y)$ dir.*

İspat. Teorem 5.5 ten , f_1^* ve f_2^* formlarını buluruz öyle ki

$$f_i \approx f_i^*(x,y) = px^2 + b_i xy + c_i y^2 \quad (i = 1,2) \tag{5.25}$$

olur. O zaman

$$D = b_1^2 - 4pc_1 = b_2^2 - 4pc_2 \tag{5.26}$$

dir. p yi tek alarak; $b_1^2 \equiv b_2^2 \pmod p$ böylece $b_1 \equiv \pm b_2 \pmod p$ ve b_1 ve b_2 nin her ikisi birden ya tek ya da çifttir. Bu nedenle, $b_2 = \pm b_1 + 2hp$ dir. $f_1^*(x + hy, \pm y) = f_3^*(x,y)$ yazarsak, o zaman benzer olarak $f_3^*(x,y) = f_2^*(x,y)$ olacaktır. (ilk ve ikinci katsayılar çakışırken üçüncü katsayı diskriminant ile belirlenir.) (Cohn 1980)

5.2.4. Karşılık gelme prosedürü

İdeallerin formlara nasıl karşılık geldiğini açıklamak için aşağıdaki iki kısa tanımı hatırlatmak yerinde olacaktır.

Bir f formu bütün katsayıları ± 1 dışında herhangi bir rasyonel sayıya bölünemiyorsa *primitiftir* denir.

Bir $\mathfrak{j}$ ideali (1) dışında herhangi bir rasyonel ideale bölünemiyorsa böyle ideale *primitif* denir.

Lemma 5.1. *Eğer* $\mathfrak{j}=[\alpha,\beta]$, d *diskriminantlı* $\mathbb{Q}(\sqrt{d})$ *cisminde sıralı bir ideal ise*

$$f(x,y)=N(\alpha x+\beta y)/N[\mathfrak{j}]=ax^2+bxy+cy^2$$

formu tamsayı katsayılıdır ve diskriminantı d *olan primitif formdur. (Burada* $N[\mathfrak{j}]$ *idealin normudur ve her zaman pozitiftir.* $N[\alpha x+\beta y]$ *eşleniklerin bir çarpımı olup negatif olabilir.)*

İspat.

$$N(\alpha x+\beta y)=(\alpha x+\beta y)(\alpha' x+\beta' y)=Ax^2+Bxy+Cy^2 \tag{5.28}$$

olacak şekilde genişletirsek burada katsayılar $\mathfrak{j}\mathfrak{j}'$ ye aittir. Burada $N[\mathfrak{j}]=\mathfrak{j}\mathfrak{j}'$, $f(x,y)$ nin A, B, C katsayılarını içerdiğinden (dolayısıyla böldüğünden)

$$\begin{aligned} A&=\alpha\alpha' &&=aN[\mathfrak{j}]\\ B&=\alpha\beta'+\alpha'\beta &&=bN[\mathfrak{j}]\\ C&=\beta\beta' &&=cN[\mathfrak{j}] \end{aligned} \tag{5.29}$$

olur. Bununla birlikte,

$$b^2-4ac=(B^2-4AC)/N^2[\mathfrak{j}]$$

$$=(\alpha\beta'-\beta\alpha')^2/N^2[\mathfrak{j}]=d,$$

olup burada d cismin diskriminantıdır.

Burada cisim diskriminantının 4 dışında bir kare böleni yoktur. Bu yüzden $d=4D$ ve $D\not\equiv 1 \pmod 4$ olduğunda a, b, c nin mümkün olan tek ortak bölenleri 2 dir.

Eğer $(2) = t^2$ yazarsak o zaman ($4 \mid d$ ve Kronecker sembolü $(d/2) = 0$ olduğunda) o zaman,

$$\begin{aligned}
(\alpha) &= t^u a, \qquad \text{A=N}(\alpha)=2^{\text{u}}\ \textit{.tek sayı},\\
(\beta) &= t^v b, \qquad \text{C=N}(\beta)=2^{\text{v}}\ \textit{.tek sayı},\\
(\text{j}) &= t^w \text{j}_1 \qquad \text{N(j)=}2^{\text{w}}\ \textit{.tek sayı},
\end{aligned}$$

olur ki burada $w = \min(u, v)$ ve $\mathfrak{a}$, $\mathfrak{b}$, j_1 idealleri t ile aralarında asaldır.

Böylece (5.29) dan a veya c tektir. (5.27) de tanımlanan form $[\alpha, \beta]$ bazlı j idealine ait olup

$$\begin{cases} f = f[\alpha, \beta] = f(\text{j}), \\ \text{j} = [\alpha, \beta] \to f, \ \text{'j, } f \text{ ye gider'} \end{cases} \tag{5.30}$$

olur.

Lemma 5.2. *$\pm t$, A, B, C nin en büyük ortak böleni olmak üzere,*

$$\begin{aligned} f(x, y) &= Ax^2 + Bxy + Cy^2 \\ &= t(ax^2 + bxy + cy^2) \end{aligned} \tag{5.31}$$

primitif olmak zorunda olmayan bir kuadratik form olsun. $B^2 - 4AC > 0$ ise $t > 0$ olsun ve *$B^2 - 4AC < 0$ ise $a > 0$ olacak biçimde t yi seçelim. $d = b^2 - 4ac$ ve d yi $\mathbb{Q}(\sqrt{d})$ nin cisim diskriminantı olduğunu varsayalım. Yani, kare çarpansız d için $d \equiv 1 \pmod 4$ veya $d/4$ için $d \equiv 0 \pmod 4$, kare çarpansız tamsayı $\not\equiv 1 \pmod 4$ olsun.*

O zaman,

$$j = [\alpha, \beta] = \begin{cases} [a, (b - \sqrt{d})/2], \ a > 0, \text{ herhangi bir } d \text{ için} \\ [a, (b - \sqrt{d})/2]\sqrt{d}, \ a < 0, \ d > 0 \end{cases} \tag{5.32}$$

bir tamsayı olup sıralı bir bazı vardır.

İspat. İlk önce $d \equiv 1 \pmod 4$ ise j nin baz elemanları b tek olduğundan tamsayılardır ve eğer $d \equiv 0 \pmod 4$ olduğunda b çift olduğu için aynı durum geçerlidir. (5.28)i kullanarak $\Delta / \sqrt{d} > 0$ olduğunu görürüz. Gerçekte $d > 0$ olduğunu varsayarak (ki bu zor olan durumdur) $a > 0$ olduğunda $\Delta = a\sqrt{d},\ a < 0$ ise $\Delta = a(-d)\sqrt{d}$ buluruz. Böylece baz sıralıdır.

j (veya $\mathrm{j}/\sqrt{d}$) nin primitif olduğunu görmek için, a ve $\beta = (b - \sqrt{d})/2$ yi bölen $u > 1$ rasyonel sayısının bulunacağına ilgi çekilir. Böylece u, β' yü böler ki u, $\beta - \beta' = -\sqrt{d}$ yi veya u^2, d yi böler ki $d \equiv 0 \pmod 4$ olduğunda varsayımımızdan dolayı u nun değeri 2 ye kısıtlanır. Fakat $d \equiv 0 \pmod 4$ ise b ve a çift olmalıdır. Böylece, 2 nin β yı bölmesi için $\sqrt{d}/2$, 2 ile bölünebilmelidir. Fakat cisim diskriminantının yapısından dolayı 4, $\sqrt{d}$ yi bölmez. ($d/4$ kare çarpansızdır)

Yukardaki lemmanın diskriminant özelliklerini sağlayan A, B, C katsayılı bir f kuadratik formu olsun,

$$\begin{cases} [\alpha, \beta] = j = j(A,\ B,\ C) = j(f), \\ f \to \mathrm{j}\ '\!f,\ \mathrm{j\ ye\ gider'} \end{cases} \tag{5.33}$$

burada j, (5.32) de gösterilen baz ile f formu tarafından belirlenmiş bir idealdir.

Özetlemek gerekirse, cisim diskriminantı $d = b^2 - 4ac$ $(a > 0)$ olan bir $f = ax^2 + bxy + cy^2$ primitif formunu ele aldık. Lemma 5.2 ye göre j(a, b, c) sıralı bazını oluşturuyoruz. Bu j ideali ve bunu sıralı bazı ile başlayarak Lemma 5.1 e göre $f^*(\alpha, \beta)$ kuadratik formunu yeniden oluşturalım. O zaman adımları tersine çevirdiğimizde $f^* = f$ olduğunu görürüz. Bu kolay kısmıdır.

Daha sonra, sıralı bazı $\mathrm{j} = [\alpha, \beta]$ olan primitif bir idealle başlayalım. Bundan, Lemma 5.1 e göre $f[\alpha, \beta]$ kuadratik formunu oluştururuz.

$$f[\alpha,\beta]=\frac{N(\alpha)x^2+(\alpha\beta'+\beta\alpha')xy+N(\beta)y^2}{N[\mathrm{j}]}$$

$f[\alpha,\beta]$ formuyla başlayarak Lemma 5.2 den sıralı bazlı ve genel olarak farklı olan j^* idealini elde ederiz:

$$\mathrm{j}^*=[\alpha^*,\beta^*]=\begin{cases}\left[\dfrac{N(\alpha)}{N(\mathrm{j})},\dfrac{\alpha\beta'+\beta\alpha'}{2N[\mathrm{j}]}-\dfrac{\sqrt{d}}{2}\right], & \text{eğer } d<0 \text{ veya } d>0, N(\alpha)>0 \text{ ise}\\ \left[\dfrac{N(\alpha)}{N(\mathrm{j})},\dfrac{\alpha\beta'+\beta\alpha'}{2N[\mathrm{j}]}-\dfrac{\sqrt{d}}{2}\right]\sqrt{d}, & \text{eğer } d>0,\ N(\alpha)<0 \text{ ise.}\end{cases} \tag{5.34}$$

$N[\mathrm{j}]>0$ olduğunu hatırlatarak öteyandan $N(\alpha)<0$ ($d>0$ olduğunda) olabilir. O zaman,

$$\gamma=\begin{cases}\alpha', & N(\alpha)>0 \text{ ve } d>0 \text{ veya } d<0 \text{ ise}\\ \alpha'\sqrt{d}, & N(\alpha)<0 \text{ ve } d>0\end{cases}$$

olacak şekilde

$$N[\mathrm{j}][\alpha^*,\beta^*]=[\alpha,\beta]\gamma, \tag{5.35}$$

olduğu kolaylıkla gerçeklenebilir. Gerçekten (5.35) doğrudur, baz elemanından baz elemanı elde edilebilir. Böylece her zaman $N(\gamma)>0$ olur. Ayrıca $N[\mathrm{j}]\alpha^*=\alpha\gamma$ olduğunu kolaylıkla görebiliriz. Öteyandan j nin bazının sıralamasından ikinci baz elemanının ifadesi,

$$\alpha\beta'-\beta\alpha'=\sqrt{d}\,N[\mathrm{j}]$$

olacaktır. Dönüşümden ,

$$\frac{\alpha\beta'+\beta\alpha'}{2}-\frac{\sqrt{d}\,N[\mathrm{j}]}{2}=\beta\alpha';$$

olup $N[\mathrm{j}]\beta^*=\beta\gamma$ olacaktır. Eğer

$$f \to \mathrm{j} \to f^* \tag{5.36}$$

ise o zaman $f = f^*$ (aynı form) ($d < 0,\ a < 0$ durumu dışında) olacaktır. Eğer

$$\mathrm{j} \to f \to \mathrm{j}^* \tag{5.37}$$

oluşturursak o zaman eşitlikten ziyade ;

$$\mathrm{j}^* \approx \mathrm{j} \tag{5.38}$$

denkliğini elde ederiz. (Cohn 1980)

5.2.5. Karşılık gelme teoremi

(5.37) deki ilişki bizi daha genel bir durum oluşturmaya zorlar.

Teorem 5.7. *Diskriminantı, cisim diskriminantına eşit olan iki* f_1 *ve* f_2 *formu*

$$f_1 \approx f_2 \tag{5.39}$$

gerçekliyorsa ve $f_1 \to \mathrm{j}_1, f_2 \to \mathrm{j}_2$ *oluyorsa o zaman*

$$\mathrm{j}_1 \approx \mathrm{j}_2 \tag{5.40}$$

olur. Karşıt olarak iki ideal (5.40)ı gerçeklerse o zaman Lemma 5.1 den f_1 *ve* f_2 *formları bulunur ve diskriminantları cisim diskriminantına eşit olan ve (5.39) u sağlayan bu formlar* $\mathrm{j}_1 \to f_1$ ve $\mathrm{j}_2 \to f_2$ *ile gösterilir.*

İspat. Öncelikle $d < 0$ olduğunda, teoremin herhangi bir uygulamasına zarar vermeden kendimizi $f_i(x, y) = a_i x^2 + b_i xy + c_i y^2,\ a_i > 0$ durumuna kısıtlayabiliriz.

İlk bölümü ispatlamak için $f_1(x,y)$ ve $f_2(X,Y)$ has denk formlarını $\mathrm{j}(f_1)$ ve $\mathrm{j}(f_2)$ ye göre (5.36) zincirine göre tekrar oluşturalım. $\mathrm{j}(f_1) \approx \mathrm{j}(f_2)$ olduğunu göstermek istiyoruz. $\mathrm{j}(f_1) = \mathrm{j}_1 = [\alpha_1, \beta_1]$, $\mathrm{j}(f_2) = \mathrm{j}_2 = [\alpha_2, \beta_2]$ olsun.

$$\begin{aligned} f_1(x,y) &= (\alpha_1 x + \beta_1 y)(\alpha_1' x + \beta_1' y) / N[\mathrm{j}_1], \\ f_2(X,Y) &= (\alpha_2 X + \beta_2 Y)(\alpha_2' X + \beta_2' Y) / N[\mathrm{j}_2], \end{aligned} \tag{5.41}$$

olsun ki, burada

$$\begin{aligned} X &= px + qy, \qquad ps - qr = 1 \\ Y &= rx + sy, \end{aligned} \tag{5.42}$$

tamsayı dönüşümü vardır. Fakat, sayısal olarak ve (5.42) dönüşümü altında $f_1(x,y) = f_2(X,Y)$ olur. $f_1(x,y) = 0$ daki noktalar $f_2(X,Y) = 0$ daki noktalara dönüşmelidir. Böylece ya

$$\frac{x}{y} = -\frac{\beta_1}{\alpha_1} \text{ ve } \frac{X}{Y} = -\frac{\beta_2}{\alpha_2} \tag{5.43}$$

ya da

$$\frac{x}{y} = -\frac{\beta_1'}{\alpha_1'} \text{ ve } \frac{X}{Y} = -\frac{\beta_2}{\alpha_2} \tag{5.44}$$

(5.42) dönüşümü ile çakışmalıdırlar.

Öncelikle (5.43) ü deneyelim. O zaman;

$$-\frac{\beta_2}{\alpha_2} = \frac{X}{Y} = \frac{px+qy}{rx+sy} = \frac{p(x/y)+q}{r(x/y)+s} = \frac{p(-\beta_1/\alpha_1)+q}{(-\beta_1/\alpha_1)+s} = \frac{-p\beta_1 + q\alpha_1}{-r\beta_1 + s\alpha_1} \tag{5.45}$$

olur. Böylece, kabulumuzle birlikte,

$$\frac{\alpha_2}{s\alpha_1 - r\beta_1} = \frac{\beta_2}{-q\alpha_1 + p\beta_1} = \frac{\lambda}{\mu} \text{ (kabul)}$$

$$\begin{cases} \mu\alpha_1 = (-r\beta_1 + s\alpha_1)\lambda, \\ \mu\beta_2 = (p\beta_1 - q\alpha_1)\lambda \end{cases} \tag{5.46}$$

olur. Burada $N(\mu) > 0$ varsayabiliriz. $N(\mu) < 0$ (zorunlu olarak) olduğunda $d > 0$ olup μ, $-dN(\mu)$ normlu $\mu\sqrt{d}$ ile yerdeğiştirebilir. Daha sonra,

$$\mu j_2 = [\mu\alpha_2, \mu\beta_2] = [s(\lambda\alpha_1) - r(\lambda\beta_1), -q(\lambda\alpha_1) + p(\lambda\beta_1)] \tag{5.47}$$

olacaktır. Fakat $ps - qr = +1$ olduğundan

$$\mu j_2 = [\lambda\alpha_1, \lambda\beta_1], \tag{5.48}$$

olup ve böylece $j_1 = [\alpha_1, \beta_1]$ ve $j_2 = [\alpha_2, \beta_2]$, μj_2 gibi sıralıdır. O zaman $N(\lambda) > 0$ olup;

$$\mu j_2 = \lambda j_1 \text{ veya } j_1 \approx j_2 \tag{5.49}$$

dir. Şimdi (5.44) seçeneğinin imkansız olduğunu gösterelim. (5.44) deki adımları tekrar takip ederek (5.46) yerine aşağıdakini elde ederiz.

$$\begin{cases} \mu\alpha_2 = (-r\beta_1' + s\alpha_1')\lambda, \\ \mu\beta_2 = (p\beta_1' - q\alpha_1')\lambda \end{cases} \tag{5.50}$$

Aynı şekilde , $N(\mu) > 0$ a kısıtlanarak ve (5.48) e benzer şekilde

$$\mu j_2 = [\mu\alpha_2, \mu\beta_2] = [\lambda\alpha_1', \lambda\beta_1'] \tag{5.51}$$

olup burada $[\alpha_1', \beta_1']$ doğru olarak sıralı değildir. Fakat $[\lambda\alpha_1', \lambda\beta_1']$, (5.42) deki unimodüler dönüşümle sıralıdır. Böylece, $N(\lambda) < 0$ dır. (5.42) den

$$f_2(1,0) = f_1(s, -r)$$

veya

$$\frac{N(\alpha_2)}{N[\mathrm{j}_2]} = \frac{N(\alpha_1, s-\beta_1, r)}{N[\mathrm{j}_1]} \tag{5.52}$$

olur. $N[\mathrm{j}] > 0$ olduğundan $N(\alpha_2)$ ve $N(-r\beta_1' + s\alpha_1')$ aynı işaretlidirler ve (5.50) den $N(\mu)$ ve $N(\alpha)$ da aynı şekildedir. Bu sonuçta (5.44) ile çelişkilidir.

Teorem 5.7 nin karşıtını ispatlamak daha kolaydır. $\mathrm{j} = [\alpha_1, \beta_1] = [\alpha_2, \beta_2]$ iki sıralı bazı için $f[\alpha_1, \beta_1] \approx f[\alpha_2, \beta_2]$ dir. (Lemma 5.1 den oluşturulur) O zaman,

$$\begin{aligned} &\alpha_2 = p\alpha_1 + q\beta_1, \quad ps - qr = 1, \text{ olup} \\ &\beta_2 = r\alpha_1 + s\beta_1 \end{aligned} \tag{5.53}$$

dir. Böylece $\alpha_2 x + \beta_2 y = \alpha_1(px + ry) + \beta_1(qx + sy)$ ve o zaman (5.27) den

$$f_2(x, y) = f_1(px + ry, qx + sy) \text{ veya } f_1[\alpha_1, \beta_1] \approx f_2[\alpha_2, \beta_2]$$

olur. Sonuç olarak, $N(p\sigma) > 0$ olduğunda $\mathrm{j}_1 \approx \mathrm{j}_2$ veya $p\mathrm{j}_1 = \sigma \mathrm{j}_2$ dir. Doğal olarak, $N(p) > 0,\ N(\sigma) > 0$ (gerekirse $\sqrt{d}$ çarpanı ile birlikte) olacaktır. O zaman j nin bazı, f yi sadece bir denklik sınıfı içerisinde etkilediğinden;

$$p[\alpha_1, \beta_1] = \sigma[\alpha_2, \beta_2], \tag{5.54}$$

$$f[\alpha_1, \beta_1] = f[\alpha_2, \beta_2], \tag{5.55}$$

(5.54) ün her iki tarafı Lemma 5.1 e göre işleme tabi tututularak gerçeklenebilir ki, ispat tamamdır.

Burada ispat (5.44) ün gerçeklenmediği gösterilirken sıralı bazların $f(x, y)$ nin çarpanlarını nasıl birbirinden ayrıldığını iyi bir şekilde ifade eder. Bu nedenle sıralı baz bir ideali ve eşleniğini birbirinden ayırır. Sıralı bazı korumak için sadece dar anlamda veya has olan denklik sınıflarını kullanacağız.

Teorem 5.7 nin denk bir formu aşağıdaki teoremdir.

Teorem 5.8. *Karşılık gelme prosedüründeki Lemma 5.1 ya da Lemma 5.2 ile* f_1 *ve* $\mathfrak{j}_1$ *arasındaki bağlantı ve* f_2 *ve* j_2 *arasındaki bağlantı (herzaman aynı olmak zorunda değil) bu denkliklerin birinin diğerini kastettiği anlamına gelir. Yani*

$$\begin{aligned} \mathfrak{j}_1 &\approx \mathfrak{j}_2 \\ f_1 &\approx f_2 \end{aligned} \tag{5.57}$$

olacaktır.

($\mathfrak{j}(f)$ *sadece,* $d<0$ *olduğu durumda en büyük dereceli terimin katsayısı pozitif ve diskriminantı cisim diskriminantına eşit ve* d *olan ve* f *formları için oluşturulduğu sürece geçerlidir.)*

Teorem 5.9. f, *diskriminantı* d *olan ve pozitif cisim diskriminantına eşit olan bir form ise o zaman* $\mathbb{Q}(\sqrt{d})$ *deki bazı* η_1 *temel tersinirler için* $f(x,y)\approx -f'(x,y)$ *olması için gerek ve yeter şart* $N(\eta_1)=-1$ *dir.*

İspat. $N(\eta_1)=-1$ olsun. Let $\mathfrak{j}=[\alpha,\beta]$, f e gidecek şekilde;

$$\mathfrak{j}\to f(x,y)=N(\alpha x+\beta y)/N[\mathfrak{j}]$$

olup, şimdi $\mathfrak{j}=\eta_1\mathfrak{j}=[\eta_1\alpha,-\eta_1\beta]$, sıralamayı hatırlarsak ve $N(\mathfrak{j})=N(\eta_1\mathfrak{j})$ olduğundan

$$N(\eta_1\alpha x-\eta_1\beta y)/N[\eta_1\mathfrak{j}]=-f(x,-y)$$

dir. Karşıt olarak $f\approx -f'$ olsun. O zaman $\mathfrak{j}\to f$ ise, daha önce olduğu gibi,

$$\mathfrak{j}\sqrt{d}=[\sqrt{d}\alpha,-\sqrt{d}\beta],N(\sqrt{d}\alpha x-\sqrt{d}\beta y)/N[\sqrt{d}\mathfrak{j}]=-f(x,-y)$$

olur. O zaman $N(\eta_1)=-1$ olduğunda $\sqrt{d}\mathfrak{j}\approx\mathfrak{j}$ veya $(\sqrt{d})\approx(1)$ olur.

5.3. Kompozisyon ve Sınıf Grubu

Temel anlamda kompozisyonu açıklamak için x^2+5y^2 formunu göz önüne alalım. Bir p asalının x^2+5y^2 formuyla temsil edilebilmesi için gerek ve yeter şart $p \equiv 1,9 \pmod{20}$ olmasıdır. Aynı şekilde bu p asalının $2x^2+2xy+3y^2$ formuyla temsil edilebilmesi için gerek ve yeter şart $p \equiv 3,7 \pmod{20}$ olmasıdır. Buradan p ve q asalları için;

$$\left.\begin{aligned} p,q \equiv 3,7 \ (\mathrm{mod}\, 20) &\Rightarrow pq = x^2+5y^2 \\ p \equiv 3,7 \ (\mathrm{mod}\, 20) &\Rightarrow 2p = x^2+5y^2 \end{aligned}\right\} \tag{5.58}$$

olacaktır. Lagrange, $2x^2+2xy+3y^2$ formuyla temsil edilen iki sayının çarpımının x^2+5y^2 formunda olduğunu iddia etmiş ve aşağıdaki özdeşliği yazarak;

$$(2x^2+2xy+3y^2)(2z^2+2zw+3w^2) = (2xz+xw+yz+3yw)^2+5(xw-yz)^2 \tag{5.59}$$

iddiasını ispatlamıştır. Euler'in

$$p = \left\{\begin{matrix} x^2+14y^2 \\ 2x^2+7y^2 \end{matrix}\right\} \Leftrightarrow p \equiv 1,9,15,23,25,29 \pmod{56}$$

konjektürünü ispatlamak için;

$$\left.\begin{aligned} p = x^2+14y^2 \text{ veya } 2x^2+7y^2 &\Leftrightarrow p \equiv 1,9,15,23,25,29 \pmod{56} \\ p = 3x^2 \pm 2xy+5y &\Leftrightarrow p \equiv 3,5,13,19,27,45 \pmod{56} \end{aligned}\right\} \tag{5.60}$$

ve;

$$p \equiv 3,5,13,19,27,45 \pmod{56} \Leftrightarrow 3p = x^2+14y^2$$

olduğunu göstermemiz gerekir. (5.60) ı kullanarak $3x^2 \pm 2xy+5y$ ile temsil edilen bir sayının 3 katının veya daha genel anlamda, böyle iki sayının çarpımının

x^2+14y^2 formunda olduğunu göstermemiz gerekir. Böylece (5.59) için başka bir özdeşliğe ihtiyacımız vardır ki, bu da

$$(ax^2+2bxy+cy^2)(az^2+2bzw+cw^2)=(axz+bxw+byz+cyw)^2+n(xw-yz)^2 \quad (5.61)$$

olup dikriminantı $-4n$ olan herhangi bir form için geçerlidir. Bunu $n=14$ durumunda $3x^2+2xy+5y^2$ ye uygularsak ispatı tamamlamış oluruz.

Bu özel örnekten anlaşılabileceği gibi, gerçekte yaptığımız kuadratik formların kompozisyonudur.

Legendre, Lagrange'ın (5.59) özdeşliğini genelleştirmek için daha önce yapılan (5.61) özdeşliğinin daha genel bir durumunun olabileceğini düşündü ve kompozisyon tanımını verdi. Buna göre, $f(x,y)$ ve $g(x,y)$, D diskriminantlı primitif pozitif formlar olmak üzere, $F(x,y)$ formu;

$$B_i(x,y;z,w)=a_ixz+b_ixw+c_iyz+d_iyw, \quad (i=1,2)$$

x,y ve z,w değişkenlerine göre bilineer form olduğunda,

$$f(x,y)g(z,w)=F(B_1(x,y;z,w)B_2(x,y;z,w)),$$

şartını sağlıyorsa aynı diskriminantlı $F(x,y)$ formuna bunların *kompozisyonu* denir.

İki form farklı yollarla kompoze edilebilir ve sonuçta elde edilen formlar has olarak denk olmak zorunda değildir.

Böylece x^2+5y^2, $2x^2+2xy+3y^2$ nin kendisiyle bir kompozisyonudur. Kompozisyonun önemli sonuçlarından biri; $F(x,y)$, $f(x,y)$ ve $g(x,y)$ den oluşuyorsa $f(x,y)$ ve $g(x,y)$ ile temsil edilen sayıların çarpımı $F(x,y)$ ile temsil edilir. Buna ek olarak, diskriminantları aynı olan iki formun kompozisyonunun oluşturulabileceğini Legendre ispatlamıştır.

$$f(x,y)=ax^2+2bxy+cy^2 \text{ ve } g(x,y)=a'x^2+2b'xy+c'y^2$$

nin diskriminantları $-4n$, a ve a' aralarında asal olsun. Çin kalan teoremine göre;

$$\left.\begin{aligned} B &= \pm b \pmod{a} \\ B &= \pm b' \pmod{a'} \end{aligned}\right\} \tag{5.62}$$

olacak şekilde bir B sayısı vardır. Buradan $B^2 + n \equiv b^2 + (ac - b^2) \equiv 0 \pmod{a}$ ve $a \mid B^2 + n$ olur. Aynı durum a' için de geçerli olduğundan böylece, $aa' \mid B^2 + n$ olacaktır. Legendre;

$$F(x, y) = aa'x^2 + 2Bxy + \frac{B^2 + n}{aa'} y^2$$

formunun $f(x, y)$ ve $g(x, y)$ nin bir kompozisyonu olduğunu göstermiştir.

(5.62) deki $\pm$ işaretlerinden dolayı iki form dört farklı yolla kompoze edilebilir. Örneğin $14x^2 + 10xy + 21y^2$ ve $9x^2 + 2xy + 30y^2$ formları

$$126x^2 \pm 38xy + 5y^2,\ 126x^2 \pm 74xy + 13y^2$$

formlarına kompoze edilebilir ve bu formlar farklı sınıflarda yer alırlar.

Legendre'ın en önemli fikirlerinden biri her form bir indirgenmiş forma denk olduğundan, indirgenmiş formların kompozisyonuyla çalışmak yeterli olacaktır. Aşağıdaki sonuç tablosu; bir diskriminantın mümkün olan bütün formlarının komposizyonunu verir. Legendre $n = 41$ durumuna bakmış ve indirgenmiş formları aşağıdaki şekilde adlandırmıştır;

$$\left.\begin{aligned} A &= x^2 + 41y^2 \\ B &= 2x^2 + 2xy + 21y^2 \\ C &= 5x^2 + 6xy + 10y^2 \\ D &= 3x^2 + 2xy + 14y^2 \\ E &= 6x^2 + 2xy + 7y^2 \end{aligned}\right\} \tag{5.63}$$

Daha sonra aşağıdaki şekilde bunların kompozisyonu ifade etmiştir.

$AA = A$	$BB = A$	$CC = A$ veya B	$DD = A$ veya C	$EE = A$ veya C
$AB = B$	$BC = C$	$CD = D$ veya E	$DE = B$ veya C	
$AC = C$	$BD = E$	$CE = D$ veya E		
$AD = D$	$BE = D$			
$AE = E$				

Tablo 3. Verilen indirgenmiş formların kompozisyonu

Bu şeklin bir grubun çarpım tablosuna benzediğine ancak ikili işlemin tek değerli olmadığına ilgi çekilmelidir. Burada sanki Legendre'in bir şeyleri yanlış yaptığı izlenimi elde ediyoruz. Buradaki problem; (5.63) te 5 form listelenmiş fakat sınıf sayısı 8 dir. (C, D, E her biri iki indirgenmiş form verirken A ve B sadece bir tane verir.) Bu Legendre'in çalışmasındaki belirsizliktir. Has denklikten ziyade denkliğe çalıştığımız sürece, (5.62) deki $\pm$ işaretlerinden dolayı indirgenmiş formun ortadaki $2b$ katsayısının işaretini sabitleyemeyiz.

Buradan kompozisyon, diskriminantı D olan formların sınıfları üzerinde bir grup işlemi verir. Kompozisyon yukarda tanımlandığı üzere çok-değerli bir işlemdir. Böylece (5.62) deki işaretler öyle düzgün seçilmeli ki, $f(x, y)$ ve $g(x, y)$ yi has denklik sınıfları içinde değiştirdikçe sonuçtaki kompozisyonların hepsi has olarak denk olsunlar.

İki formun birçok farklı yolla kompoze edilebileceğini ve sonuçtaki formların has olarak denk olmak zorunda olmayacağını belirtelim. Yukarıda iki formun kompozisyonunun 4 farklı sınıfta yer aldığını göstermiştik. Böylece formların

sınıfları üzerinde iyi tanımlı bir işlem tanımlamak istiyorsak; kompozisyon notasyonunu kısıtlamamız gerekiyor. Gauss bunu vermiş olduğumuz kompozisyon tanımından;

$$a_1b_2 - a_2b_1 = \pm f(1,0),\ a_1c_2 - a_2c_1 = \pm g(1,0) \tag{5.64}$$

olduğunu ispatlamış ve (5.64) deki işaretlerin her ikisi de + olduğunda kompozisyonu *doğrudan kompozisyon* olarak tanımlamıştır.

Gauss'un kompozisyon teorisinin en önemli sonucu; sabit bir diskriminant için doğrudan kompozisyon, formların sınıflarının kümesini sonlu bir abelyen gruba dönüştürür. Fakat ne yazık ki doğrudan kompozisyon kullanılması zor bir kavram olup; Gauss'un bunu kullanarak yaptığı grup yapısının ispatı çok uzun ve karmaşıktır. Bu konuda Dirichlet'in tanımını vermeden önce aşağıdaki lemmayı vermek uygun olacaktır.

Lemma 5.3. *$f(x,y) = ax^2 + 2bxy + cy^2$ ve $g(x,y) = a'x^2 + b'xy + c'y^2$ formlarının diskriminantları D ve $\gcd(a, a', (b+b')/2 = 1$ olsun. (b ve b' aynı işaretli olduğundan $(b+b')/2$ bir tamsayıdır.) O zaman mod $2aa'$ ne göre tek bir B tamsayısı vardır ki;*

$$\begin{aligned} B &\equiv b \pmod{2a} \\ B &\equiv b' \pmod{2a'} \\ B^2 &\equiv D \pmod{4aa'} \end{aligned}$$

olur. (Cox 1989)

İspat. İlk adım bu kongrüansları standart formda yazmaktır. Bir B sayısı ilk iki kongrüansı sağlıyorsa o zaman;

$$B^2 - (b+b')B + bb' \equiv (B-b)(B-b') \equiv 0 \pmod{4aa'},$$

olup buradan üçüncü kongrüans;

$$(b+b')B \equiv bb' + D \pmod{4aa'},$$

bulunur ki, bunu 2 ye bölmekle;

$$(b+b')/2.B \equiv (bb'+D)/2 \ (\text{mod } 2aa') \tag{5.65}$$

elde edilir. İlk iki kongrüansı sırasıyla a ve a' ile çarpar ve (5.65) ile birleştirirsek lemmanın ifadesindeki bu üç kongrüans

$$\left.\begin{aligned} &a'B \equiv a'b \ (\text{mod } 2aa') \\ &a.B \equiv ab' \ (\text{mod } 2aa') \\ &(b+b')/2.B \equiv (bb'+D)/2 \ (\text{mod } 2aa') \end{aligned}\right\} \tag{5.66}$$

kongrüanslarına denk olur. Aşağıdaki Lemma bize bu kongrüansların çözülebilirliğinin cevabını verir.

Lemma 5.4. $p_1, q_1, ..., p_r, q_r, m,$ $\gcd(p_1, q_1, ..., p_r, m) = 1$ *olan sayılar olsun. O zaman*

$$p_i B \equiv q_i \ \text{mod } m, \ \ i = 1, ..., r$$

kongrüanslarının $\text{mod}\, m$ *e göre tek bir çözümünün olması için gerek ve yeter şart;*

$$p_i q_j \equiv p_j q_i \ \text{mod}\, m \tag{5.67}$$

olmasıdır.

İspat. Bakınız (Cox 1989)

Şimdi Dirichlet'in kompozisyon tanımını verebiliriz.

$f(x,y) = ax^2 + 2bxy + cy^2$ ve $g(x,y) = a'x^2 + 2b'xy + c'y^2$, $D < 0$ olan primitif pozitif belirli formlar ve $\gcd(a, a', (b+b')/2) = 1$ olsun. $f(x,y)$ ve $g(x,y)$ nin *Dirichlet kompozisyonu*

$$F(x,y) = aa'x^2 + 2Bxy + \frac{B^2 + n}{aa'} y^2 \tag{5.68}$$

olup B, Lemma 3.2 ile belirlenen bir tamsayıdır. $F(x,y)$ nin temel özelliklerini aşağıdaki önerme ile verelim.

Teorem 5.10. *Yukarıda verilen $f(x,y)$ ve $g(x,y)$ ile tanımlanan (3.7) deki $F(x,y)$ Dirichlet kompozisyonu, diskriminantı D olan primitif pozitif belirli form olup, $F(x,y)$; $f(x,y)$ ve $g(x,y)$ nin (5.68) e göre doğrudan kompozisyonudur.*

İspat. Bakınız (Cox 1989)

Genel olarak Dirichlet kompozisyonu doğrudan kompozisyon değildir. Çünkü bütün doğrudan kompozisyonlar $\gcd(a,a',(b+b')/2)=1$ şartını sağlamaz. Fakat (5.68) deki gibi bir formül kompozisyon için kullanımda kolaylık sağlar. Lemma 5.3 teki kongrüans şartlarının Legendre tarafından kullanılan (5.62) ile benzer olduğu görülmüştür. $D=-4n$ ve $\gcd(a,a')=1$ olduğunda Dirichlet'in formülü Legendre tarafından verilen formüle indirgenir.

Aşağıdaki teorem kompozisyonun bir diğer önemli sonucudur.

Teorem 5.11. $D\equiv 0,1 \pmod 4$ *ve negatif, $C(D)$, diskriminantı D olan primitif pozitif belirli formlarının sınıflarının kümesi olsun. O zaman Dirichlet kompozisyonu $C(D)$ üzerinde iyi tanımlı ikili bir işlem oluşturur ki, bu $C(D)$yi mertebesi sınıf sayısı $h(D)$ olan sonlu bir abelyen gruba dönüştürür. Ayrıca, $C(D)$ nin etkisiz elemanı*

$$x^2-\frac{D}{4}y^2 \qquad D\equiv 0 \pmod 4 \text{ ise}$$

$$x^2+xy+\frac{1-D}{4}y^2 \qquad D\equiv 1 \pmod 4 \text{ ise}$$

esas formunu kapsayan bir sınıf ve bu $ax^2+bxy+cy^2$ formunu kapsayan sınıfın tersi, $ax^2-bxy+cy^2$ yi kapsayan sınıftır.

Burada $C(D)$ ye *sınıf grubu* veya *formların sınıf grubu* denir. D diskriminantının esas formunun bulunduğu sınıfa *esas sınıf* denir. $D=-4n$

olduğunda esas form x^2+ny^2 dir. $ax^2-bxy+cy^2$ formuna $ax^2+bxy+cy^2$ formunun *karşıtı* denir. Karşıt form Dirichlet kompozisyonu altında tersi verir.

İspat. $f(x,y)=ax^2+bxy+cy^2$ ve $g(x,y)$ verilen tipte formlar olsun. Lemma 5.6 ve bir $f(x,y)$ formu ve M tamsayısı verildiğinde, $f(x,y)$, M ile aralarında asal olan sayıları has olarak temsil edildiğinden $g(x,y)$ yi, $\gcd(a,a')=1$ olmak üzere $g(x,y)=a'x^2+b'xy+c'y^2$ has denk formuyla yer değiştirebiliriz. O zaman bu formlar için bir Dirichlet kompozisyonu tanımlanmış olur ki, bu Dirichlet kompozisyonunun $C(D)$ deki herhangi bir sınıf çifti için tanımlanmış olduğunu ispatlar. Daha sonra bunun grup yapısını ispatlamak için aşağıdakilerin ispatlanması gerekir;

i) Bu işlem bütün sınıflar üzerinde iyi tanımlıdır.

ii) Bu ikili işlem $C(D)$ yi abelyen bir gruba dönüştürür.

(i) ve (ii) nin ispatları Dirichlet kompozisyonunun tanımından yapılır. Fakat ideal sınıflarını kullanarak daha kolay yapılabilir. Şimdi bunların doğru olduğunu kabul ederek esas sınıfın $C(D)$ nin etkisiz elemanı olduğunu gösterelim. Esas formu $f(x,y)=ax^2+bxy+cy^2$ ile kompoze etmek için en büyük ortak bölen şartının sağlandığına ve böylece Dirichlet kompozisyonunun tanımlandığına ilgi çekilir. Ayrıca $B=b$ nin Lemma 5.3 ün şartlarını sağladığını görebiliriz ki, (5.68) formülüyle Dirichlet kompozisyonu $F(x,y)$, verilen $f(x,y)$ formuna indirgenir. Bu esas sınıfın etkisiz olduğunu ispatlar.

Sonuç olarak; verilen $f(x,y)=ax^2+bxy+cy^2$ formunun karşıtı $f'(x,y)=ax^2-bxy+cy^2$ dir. $\gcd(a,a,(b+(-b))/2)=a$ ve $a>1$ olabileceğinden Dirichlet kompozisyonunu doğrudan uygulayamayız. Şayet $(x,y)\to(-y,x)$ has denkliğini kullanırsak; $f'(x,y)$ yi $g(x,y)=cx^2+bxy+ay^2$ ile değiştirebiliriz. $\gcd(a,c,(b+b)/2)=\gcd(a,c,b)=1$ olduğundan Dirichlet formüllerini $f(x,y)$ ve $g(x,y)$ ye uygulayabiliriz. Böylece, $B=b$ nin Lemma 5.3 ün şartlarını sağladığını

görebiliriz ki, buradan Dirichlet kompozisyonu $acx^2+bxy+y^2$ dir. Bu formun esas forma has olarak denk olduğunu söyleyebiliriz. Bu da teoremin ispatını tamamlar.

Son olarak Legendre'ın kompozisyon teorisinden bahsedeceğiz. Karışıklığa yol açmamak için sınıf ile (bütün formlar verilen forma has olarak denktir) Lagrangian sınıfını (bütün formlar verilen forma denktir) ayırt edeceğiz. Legendre, Lagrangian sınıflarının kompozisyonuna çalışırken Teorem 5.11 de sınıfların kompozisyonu verilmiştir. Bir formun Lagrangian sınıfı, kendi sınıfının ve bu formun karşıtının sınıfının birleşimidir. Teorem 5.11 e göre bu Lagrangian sınıfı, bir sınıf ile bunun $C(D)$ sınıf grubundaki terslerinin birleşimidir. Böylece Legendre'ın tanımladığı işlem çok-değerli bir işlem olup bu çarpma '$\sim$', $x \in C(D)$ için x^{-1} ile tanımlanan bir denklik bağıntısı olmak üzere $C(D)/\sim$ cümlesini üretir. (5.63) teki diskriminantı -164 olan formlara ait Legendre örneği $C(-164) \simeq \mathbb{Z}/8\mathbb{Z}$ olduğunu gösterir. Ayrıca $C(-164)/\sim$nın Tablo 3 te verilen yapıya izomorf olduğu kolaylıkla gösterilir.

$C(D)$ sınıf grubundaki mertebesi ≤ 2 olan elemanlar kompozisyon ve cins teorisinde önemli bir rol oynarlar. Böyle sınıflarda yer alan indirgenmiş formları bulmak aşağıdaki lemma ile mümkün olur.

Lemma 5.5. *Diskriminantı D olan bir $f(x,y)=ax^2+bxy+cy^2$ indirgenmiş formunun $C(D)$ sınıf grubundaki mertebesinin ≤ 2 olması için gerek ve yeter şart $b=0,\ a=b$* veya *$a=c$ olmasıdır.*

İspat. $f'(x,y)$, $f(x,y)$ nin karşıtı olsun. Teorem 5.11 den $f(x,y)$ nin sınıfının mertebesinin ≤ 2 olması ancak ve ancak $f(x,y)$ ve $f'(x,y)$ nin has olarak denk olmasıyla mümkündür. Burada indirgenme tanımına göre dikkate alınması gereken iki durum vardır.;

i) $|b|<a<c$: Burada $f'(x,y)$ indirgenmiş form olup; her primitif pozitif belirli form tek bir indirgenmiş forma has olarak denk olduğundan bu iki formun has denk olması için gerek ve yeter şart $b=0$ olmasıdır.

ii) $a = b$ veya $a = c$: Bu durumda her primitif pozitif belirli form tek bir indirgenmiş forma has denk olduğundan bu iki form her zaman has olarak denktir ki, ispatı tamamlar.

Bu teoremin nasıl işlediğine, Legendre'ın diskriminantı -164 olan formlarla ilgili örneğini verebiliriz. (5.63) te indirgenmiş formlar listelenmiştir ve Lemma 5.5 sadece $2x^2 + 2xy + 21y^2$ nin mertebesinin 2 olduğunu gösterir. Sınıf sayısı 8 olduğundan sonlu abelyen grupların yapısından $C(-164)$ sınıf grubu $\mathbb{Z}/8\mathbb{Z}$ olmalıdır.

Sınıf grubundaki mertebesi 2 olan elemanların sayısını hesaplamak için indirgenmiş formları listelemeye gerek olmadığını belirtmemiz gerekir;

Teorem 5.12. $D \equiv 0,1 \pmod 4$ *negatif ve r, D yi bölen tek asalların sayısı olsun. Bu durumda bir s sayısını şu şekilde tanımlayalım;*

$D \equiv 1 \pmod 4$ *ise o zaman* $s = r$ *dir.*

$D \equiv 0 \pmod 4$ *ise o zaman* $n > 0$ *olmak üzere* $D = -4n$ *olur ve s aşağıdaki şekil ile belirlenir ki O zaman* $C(D)$ *sınıf grubunun, tam olarak mertebesi* ≤ 2 *olan* 2^{s-1} *tane elemanı vardır.*

n	s
$n \equiv 3 \mod 4$	r
$n \equiv 1,2 \mod 4$	$r+1$
$n \equiv 4 \mod 8$	$r+1$
$n \equiv 0 \mod 8$	$r+2$

Tablo 4. $D \equiv 0 \pmod 4$ olduğunda $D = -4n$, $(n > 0)$ durumunda $C(D)$ sınıf grubundaki mertebesi 2 olan elemanların sayısı

İspat. İspatın daha kolay olması için $n \equiv 1 \pmod 4$ olacak şekilde $D = -4n$ durumunu dikkate alacağız. $-4n$ diskriminantlı formun $ax^2 + 2bxy + cy^2$ şeklinde yazılabileceğini hatırlatarak ispatın temel fikrinin $2b = 0, a = 2b$ veya $a = c$ şartlarını sağlayan indirgenmiş formların sayısını saymak olduğunu belirtelim. (Lemma 5.5 ile) Bu, bize $C(-4n)$ deki mertebesi ≤ 2 olan sınıfların sayısını verir. n tek olduğundan, r nin n nin asal bölenlerinin sayısı olduğuna ilgi çekilir.

Öncelikle, $2b = 0$ olan formları, yani $ac = n$ olan $ax^2 + cy^2$ formlarını dikkate alalım. a ve c aralarında asal ve pozitif olmak zorunda olduğundan a için 2^r tane seçim yapılabilir. İndirgemek için, $a < c$ olmalıdır ki, bu tipte 2^{r-1} indirgenmiş form elde ederiz.

Daha sonra $a = 2b$ veya $a = c$ formlarını dikkate alalım. b ve k aralarında asal ve $0 < b < k$ olmak üzere $n = bk$ olsun. Yukarıdakine benzer şekilde böyle b'lerden 2^{r-1} tane vardır. $c = (b + k)/2$ olsun ve $2bx^2 + 2bxy + cy^2$ formunu dikkate alalım. Buradan, diskriminant $-4n$ ve $n \equiv 1 \pmod 4$ olduğundan, katsayıları aralarında asal olur. Dolayısıyla, 2^{r-1} tane indirgenmiş form elde ederiz.

$2b < c$: Burada, $2bx^2 + 2bxy + cy^2$ indirgenmiş formdur.

$2b > c$: Burada, $2bx^2 + 2bxy + cy^2$, $(x, y) \to (-y, x + y)$ ile $cx^2 + 2(c - b)xy + cy^2$ ye has olarak denktir.

$2b > c \Rightarrow 2(c - b) < c$ olduğundan form indirgenir.

Daha sonraki adım; bu işlemlerin $a = 2b$ veya $a = c$ olan bütün indirgenmiş formları verip vermediğini kontrol etmektir. Böylece, mertebesi ≤ 2 olan

$2^{r-1}+2^{r-1}=2^{r}$ eleman olacaktır ki, bu durumda $s=r+1$ olduğu da görülür. Kalan diğer durumlar da benzer şekilde gösterilebilir. (Cox 1989)

Burada, $\mathfrak{j}_1$ ve $\mathfrak{j}_2$ ideallerine karşılık gelen $f_1(x,y)$ ve $f_2(x,y)$ formlarının kompozisyonunu aşağıdaki teoremle verelim.

Teorem 5.13. $\mathfrak{O}_1$ deki iki $\mathfrak{j}_1$ ve $\mathfrak{j}_2$ idealleri, diskriminantları cisim diskriminantına eşit olan $f_1(x,y)$ ve $f_2(x,y)$ kuadratik formlarına karşılık gelsin. O zaman

$$\mathfrak{j}_3=\mathfrak{j}_1.\mathfrak{j}_2 \text{ (ideal çarpma)}$$

olmak üzere diskriminantı aynı olan $f_3(x_3,y_3)$ formu, $f_3=f(\mathfrak{j}_3)$ ise,

$$f_3(x_3,y_3)=f_1(x_1,y_1)f_2(x_2,y_2) \text{ (alışılagelmiş çarpma)}$$

dir. Burada, yeni x_3 ve y_3 değişkenleri A_i ve B_i tamsayı katsayılarının bilineer formları olarak

$$x_3=A_1x_1x_2+A_2x_1y_2+A_3x_2y_1+A_4x_2y_2$$
$$y_3=B_1x_1x_2+B_2x_1y_2+B_3x_2y_1+B_4x_2y_2$$

şeklinde tanımlanır. (Cohn 1980)

5.4. Karakterler

Bu bölümde *m* modülüne göre kalan sınıflarını analitik olarak ayırt etmemize imkan sağlayan önemli bir kavram verilmiştir. Bu açıdan, kalan sınıflarını temsil etmeyi yani;

$$y\equiv a \pmod{\mathfrak{m}}$$

kongrüsansı ile verilen a tamsayılarını reel veya kompleks olabilen $\chi(a)$ sayıları ile temsil etmeyi deneyeceğiz ki, $\chi(a)$ ya *karakter* denir. (Cohn 1980)

Genel anlamda G, elemanları $\mathsf{a}_1, \mathsf{a}_2, ..., \mathsf{a}_h$ olan ve (burada $\mathsf{a}_1 = e$, birim elemandır) mertebesi h olan sonlu abelyen grubu olmak üzere,

$$\chi(\mathsf{a}_i) \neq 0, \tag{5.70}$$

$$\chi(\mathsf{a}_i)\chi(\mathsf{a}_j) = \chi(\mathsf{a}_i\mathsf{a}_j) \tag{5.71}$$

özelikleriyle, $\chi : G \to \mathbb{C}$ ye bir fonksiyondur. (Chandrasekharan 1968)

Ve

$$\chi(\mathsf{a}_1), \chi(\mathsf{a}_2), ..., \chi(\mathsf{a}_h) \tag{5.72}$$

olarak yazabiliriz. Burada (5.71) de $\mathsf{a}_1 e = \mathsf{a}_1$ i kullanarak $\chi(e) = 1$ olduğunu görebiliriz. Bununla birlikte, h grubun mertebesi ise, grubun herhangi bir a elemanı için $\mathsf{a}^h = e$ olacaktır. Böylece $[\chi(\mathsf{a})]^h = \chi(\mathsf{a}^h) = 1$ ve $\chi(\mathsf{a})$ birimin h-ıncı köküdür. Bu denklemde uygun bir *t* için;

$$\chi(\mathsf{a}) = \exp(2\pi i t / h) = \cos 2\pi t / h + i \sin 2\pi t / h \tag{5.73}$$

olacaktır. Yani, $t = 0, 1, 2, ..., h-1$ değerleri için birimin böyle h tane kökü vardır. Böylece, χ karakterlerinin (5.72) deki değerlerle belirlenen mümkün olan bütün değerleri en fazla h^h olabilir. Gerçekte tam olarak h tane karakter vardır. İki karakterin farklı olması için gerek ve yeter şart bir veya daha fazla grup elemanları için farklı değerler almasıdır.

$\{\chi_1\chi_2\}$ ile gösterilen iki farklı karakterin çarpımı keyfi bir a grup elemanı için aşağıdaki şekilde alışılagelmiş çarpma kullanılarak,

$$\{\chi_1\chi_2\}(\mathsf{a}) = \chi_1(\mathsf{a})\chi_2(\mathsf{a}) \tag{5.74}$$

şeklinde tanımlanan, $\{\chi_1\chi_2\}(\mathsf{a})$ bir karakterdir. Dolayısıyla, $\{\chi_1\chi_2\}(\mathsf{a})$ hiçbir zaman sıfır olmaz. Bununla birlikte, a_i ve a_j grup elemanları için; $(1 \le i, j \le h)$ olmak üzere,

$$\{\chi_1\chi_2\}(\mathsf{a_i a_j}) = \chi_1(\mathsf{a_i a_j})\chi_2(\mathsf{a_i a_j}) = \chi_1(\mathsf{a_i})\chi_1(\mathsf{a_j})\chi_2(\mathsf{a_i})\chi_2(\mathsf{a_j})$$
$$= \{\chi_1\chi_2\}(\mathsf{a_i})\{\chi_1\chi_2\}(\mathsf{a_j})$$

dir. Böylece $\chi_1\chi_2$ (5.70) ve (5.71) deki karakter özeliklerini sağlar. χ_i^n i de bu şekilde tanımlayabiliriz. Böylelikle, X karakter grubunu elde ederiz. $\{\chi_1/\chi_2\}$ yi bölüm karakteri olarak adlandırıp alışılagelmiş bölmeyi kullanarak,

$$\{\chi_1/\chi_2\}(\mathsf{a}_i) = \chi_1(\mathsf{a}_i)/\chi_2(\mathsf{a}_i)$$

yazabiliriz. Ayrıca birim karakterini de bütün a_i ler için;

$$\chi_0(\mathsf{a}_i) = 1 \qquad (5.75)$$

şeklinde tanımlarız. Çarpma altında, kalan sınıfları açısından, grup elemanı a yı $y \equiv a$ 'kalan sınıfı' ile özdeşleştireceğiz. $\chi(\mathsf{a})$ ve $\chi(a)$, 'mod m' ve $(a,m)=1$ anlamında değiştirerek kullanılacaktır. Ayrıca, $(a,m) \neq 1$ olduğunda (5.73) teki çarpma kuralı ile çelişmeksizin $\chi(a) = 0$ yazabiliriz.

Örnek olarak; mod 5 e göre ilk indirgenmiş kalanları göz önüne alalım. $y^4 \equiv 1 \pmod 5$ öyleki (5.73 ten) $\chi(\mathsf{a})$, sadece $i, -1, -i, +1$ değerlerinden birini alır.

$\mathsf{a} = e$ $y \equiv 1$	a_2 2	a_3 3	a_4 4
$\chi_0(\mathsf{a}) = 1$	1	1	1
$\chi_1(\mathsf{a}) = 1$	i	-i	-1

$\chi_3(\mathsf{a}) = 1$	$-i$	i	-1
$\chi_2(\mathsf{a}) = 1$	-1	-1	1

Tablo 5. Mod 5 e göre indirgenmiş kalanlar

Kalan sınıfları üzerinde grup özeliğini göstermek için aşağıdaki ifadeleri göz önüne alacağız.

$$2.3 \equiv 1 \pmod 5 \tag{5.76}$$

$$\chi_j(2)\chi_j(3) = \chi_j(1), \tag{5.77}$$

$$(-i)(i) = 1, \qquad (j = 3 \text{ alalım}). \tag{5.78}$$

Karakterlerin grup özeliğini göstermek için aşağıdaki ilişkiye ilgi çekelim;

$$\chi_2(\mathsf{a}) = \chi_1(\mathsf{a})^2, \ \ \chi_3(\mathsf{a}) = \chi_1(\mathsf{a})^3, \ \ \chi_0(\mathsf{a}) = \chi_1(\mathsf{a})^4, \tag{5.79}$$

$$\chi_3(\mathsf{a}_j) = \chi_1(\mathsf{a}_j)^3, \tag{5.80}$$

$$i = (-i)^3, \ \ \text{(örneğin } j = 3 \text{ alalım.)} \tag{5.81}$$

Buradan mod 5 in devirli yapısının karakterlere nasıl uyarlandığını ve taşınabildiğini anlayabiliriz.

Mod 8 e göre oluşturulan Tablo 6 gözönüne alındığında;

$\mathsf{a} = e$	a_2	a_3	a_4

$y \equiv 1$	3	5	7
$\chi_0(\mathsf{a}) = 1$	1	1	1
$\chi_1(\mathsf{a}) = 1$	-1	-1	1
$\chi_3(\mathsf{a}) = 1$	1	-1	-1
$\chi_2(\mathsf{a}) = 1$	-1	1	-1

Tablo 6. Mod 8 e göre indirgenmiş kalanlar

$$\begin{cases} \chi_1^2 = \chi_2^2 = \chi_3^2 = \chi_0, \\ \chi_1\chi_2 = \chi_3, \ \ \chi_2\chi_3 = \chi_1, \ \ \chi_3\chi_1 = \chi_2. \end{cases}$$

özelliklerini gerçeklediğini söyleyebiliriz. Bu özellikler daha sonraki bölümde sözünü edeceğimiz bir genelleştirmeye yol açar.

5.4.1. Karakterlerin toplam sayısı

Mertebesi h olan bir abelyen grubun h farklı karakteri vardır. Bu sonucu görebilmek için

$$G = Z(h)$$

şeklindeki h mertebesinin tek bir devrini göz önüne alalım. G nin elemanları a üreteci ile

$$\mathsf{a},\ \mathsf{a}^2, ..., \mathsf{a}^h (= e)$$

olarak yazılır. O zaman $\chi(\mathsf{a})$ nın değerleri $\exp 2\pi iu/h$ formundadır ve

$$\chi(\mathsf{a}^{\mathsf{t}}) = \exp 2\pi itu/h \qquad (0 \le t < h) \tag{5.82}$$

olur. O halde u değiştiği sürece

$$\chi_u(\mathsf{a}^{\mathsf{t}}) = \exp 2\pi itu/h, \qquad (0 \le u < h) \tag{5.83}$$

şeklinde h farklı karakterleri elde ederiz. Böylece her bir karakter için (veya her bir sabit u için) t, 0 dan $h-1$ e kadar değiştikçe h tane grup elemanı üretilmiş olur. (5.82) ve (5.83) deki karakterler χ fonksiyonunun grup üzerinde sağladığı bütün özellikleri sağlar.

Şayet $a \equiv 2$ ve a^t nin $2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 3,\ 2^0 \equiv 1$ ardışık değerlerini aldığına ilgi çekersek Tablo 5 deki mod 5 e göre indirgenmiş kalanlarla karşılaştırma daha da açık bir hale gelir.

$G = Z(h_1) \times Z(h_2)$ mertebesi $h_1 h_2$ olan bir abelyen grup ve bu da mertebeleri sırasıyla h_1 ve h_2 olan iki devirli gruba parçalanabilsin. Yani,

$$Z(h_1) = \{a_1, a_1^2, ..., a_1^{h_1} (= e)\},$$

$$Z(h_2) = \{a_1, a_2^2, ..., a_2^{h_2} (= e)\},$$

olsun. Böylece G nin genel bir elemanı,

$$g = \mathsf{a}_1^{t_1} \mathsf{a}_2^{t_2}, \quad 0 \le t_1 < h_1, \quad 0 \le t_2 < h_2. \tag{5.84}$$

olacaktır. O zaman

$$\chi_{u_1 u_2}(g) = \exp 2\pi i (t_1 u_1 / h_1 + t_2 u_2 / h_2) \tag{5.85}$$

olup u_1 ve u_2 değiştikçe sırasıyla h_1 ve h_2 modüllerine göre,

$$0 \le u_1 < h_1, \qquad (0 \le u_2 < h_2) \tag{5.86}$$

biçiminde indirgenir. Böylelikle, bütün $h_1 h_2$ (farklı) karakterlerini üretmiş oluruz. Tablo 6 daki mod 8 e göre kalan sınıflarını göz önüne alırsak burada $h_1 = h_2 = 2$, $\chi_0, \chi_1, \chi_2, \chi_3$ kolaylıkla $u_1 = 0,1$ ve $u_2 = 0,1$ olduğunda (5.85) teki dört $\chi_{u_1 u_2}$, karakteriyle özdeşleştirilmiş olur.

Böylece, G mertebesi h olan bir abelyen grup olduğunda (G nin devirli yapısını kullanarak), h tane karakter olduğunu gösterebiliriz. Ayrıca bu karakterler grubu G ile aynı devirli yapıya sahiptir. Özel olarak

$$G = Z(h_0) \times Z(h_1) \times ... \times Z(h_s) \tag{5.87}$$

olup G nin keyfi bir elemanı

$$\mathsf{a}_0^{t_0}, \mathsf{a}_1^{t_1}, ..., \mathsf{a}_s^{t_s}, (t_i \bmod h_i) \tag{5.88}$$

olacaktır. (Cohn 1980)

Karakterlerle ilgili yukarıdaki bilgilere ek olarak; ikinci dereceden denklemlerin çözümünde kullanılan Legendre sembolü ile karakterler arasındaki ilişkiyi ve gerekli olan ön teoremleri verelim.

Lemma 5.6. *Bir $f(x, y)$ formunun bir m tamsayısını has olarak temsil etmesi için gerek ve yeter koşul bazı $b, c \in \mathbb{Z}$ için $f(x, y)$ nin $mx^2 + bxy + cy^2$ formuna has olarak denk olmasıdır.*

İspat. Bakınız (Cox 1980)

Lemma 5.7. *$D \equiv 0,\ 1 \pmod 4$ bir tamsayı ve m, D ile aralarında asal olan bir tek tamsayı olsun. O zaman m nin diskriminantı D olan bir primitif formla has olarak temsil edilebilmesi için gerek ve yeter şart D nin m modülüne göre ikinci dereceden bir kalan olmasıdır.*

İspat. $f(x,y)$, m yi has olarak temsil ediyorsa Lemma 5.6 ya göre $f(x,y)=mx^2+2bxy+cy^2$ olduğunu varsayabiliriz. Böylece $D=b^2-4mc$ ve $D\equiv b^2 \bmod m$ olacaktır.

Karşıt olarak, $D\equiv b^2 \pmod m$ olduğunu varsayalım. m tek olduğundan, D ve b nin aynı işaretli olduklarını varsayabiliriz. (gerektiğinde b, $b+m$ ile yer değiştirilebilir.) $D\equiv 0,\ 1 \pmod 4$, $D\equiv b^2 \pmod{4m}$ anlamına gelir ki, bu da bazı c ler için $D=b^2-4mc$ olacaktır. O zaman $mx^2+bxy+cy^2$ m yi has olarak temsil eder ve diskriminantı D dir. m, D ile aralarında asal olduğundan katsayılar da aralarında asaldır.

Lemma 5.8. $D\equiv 0,\ 1 \pmod 4$ *sıfır olmayan bir tamsayı ise* D *yi bölmeyen* p *tek asalları için* $\chi[p]=(D/p)$ *olacak şekilde* $\chi:(\mathbb{Z}/D\mathbb{Z})^*\to\{\pm 1\}$ *bir tek homomorfizm vardır. Ayrıca,*

$$\chi([-1])=\begin{cases}1, & D>0\\ -1, & D<0\end{cases}$$

dır.

Aşağıdaki teoremin temel fikri; bir p tek asalının D diskriminantlı indirgenmiş formla temsil edilebilmesi için gerek ve yeter koşulları veren her zaman bir $p\equiv \alpha,\ \beta,\ \gamma... \bmod D$ kongrüansının bulunduğunu söyler. İndirgenmiş formları bulmayı bildiğimizden karşılıklı ikinci dereceden kalanlar teoremi $(D/p)=1$ olacak şekilde bu $\alpha,\ \beta,\ \gamma... \bmod D$ kongrüans sınıflarını bulmamızı kolaylaştırır.

Teorem 5.14. $D\equiv 0,\ 1 \pmod 4$ *ve negatif ve* $\chi:(\mathbb{Z}/D\mathbb{Z})^*\to\{\pm 1\}$ *Lemma 5.8 de belirtilen homomorfizm olsun. O zaman,* D *yi bölmeyen bir* p *tek asalı için* $[p]\in \mathrm{Ker}(\chi)$ *olması için gerek ve yeter şart* p *nin* D *diskriminantlı* $h(D)$ *sayıda indirgenmiş formlarından biriyle temsil edilebilmesidir.* (Cox 1989)

İspat. Öncelikle, burada $\mathrm{Ker}(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^*$ in indeksi 2 olan bir alt grup olduğunu sonuçta $(\mathbb{Z}/D\mathbb{Z})^*$ ın normal alt grubu olduğunu belirtelim. Ayrıca, χ nın tanımı gereği $[p] \in \mathrm{Ker}(\chi)$ olması için gerek ve yeter şart $(D/p) = 1$ dir. Lemma 5.7 den bu son şart diskriminantı D olan primitif pozitif belirli bir formla temsil edilmeye denktir. Ayrıca, her primitif pozitif form tek bir indirgenmiş forma has olarak denk olduğundan ispat tamamlanır.

5.5. Cins Teorisi

Elementer anlamda cins teorisini tanımlamak amacıyla; $h(-4n) > 1$ olmak üzere $p = x^2 + ny^2$ formunu karakterize edebilmek için $n = 5$ olduğu durumu ele alalım. Burada ikinci dereceden kalanlar teoreminden ve Tablo 2 den

$$p \equiv 1,\ 3,\ 7,\ 9 \bmod 20 \Leftrightarrow \left(\frac{-5}{p}\right) = 1 \tag{5.89}$$

$$\Leftrightarrow p = x^2 + 5y^2 \text{ veya } 2x^2 + 2xy + 3y^2$$

olduğunu söyleyebiliriz.

Diskriminantları aynı olan indirgenmiş formları birbirinden ayırmak için bir metoda ihtiyacımız vardır ki burada cins teorisi devreye girer. Lagrange, Fermat'ın ve Euler'in konjektürlerini ispatlamak için kuadratik formları kullanmıştır. Bunu, indirgenmiş formlarla çalışmak yerine $(\mathbb{Z}/D\mathbb{Z})^*$ de tek bir formla temsil edilen kongrüans sınıflarını kullanarak yapmıştır. Böylelikle, aynı sınıfı temsil eden formları tekrar gruplamıştır ki bu da cins teorisinin temel fikridir.

Şimdi bu gruplamanın nasıl olduğuna bakalım. $D = -20$ olduğunda;

$$x^2+5y^2,\ (\mathbb{Z}/20\mathbb{Z})^*\ \text{de}\ 1,\ 9\ \text{u ve,} \tag{5.90}$$

$$2x^2+2xy+3y^2,\ (\mathbb{Z}/20\mathbb{Z})^*\ \text{de}\ 3,\ 7\ \text{yi temsil eder.}$$

Benzer şekilde $D=-56$ için;

$x^2+14y^2,\ 2x^2+7y^2,\ (\mathbb{Z}/56\mathbb{Z})^*$ de 1, 9, 15, 23, 25, 29 u temsil eder.

$3x^2\pm 2xy+5y^2,\ (\mathbb{Z}/56\mathbb{Z})^*$ de 3, 5, 13, 19, 27, 45 i temsil eder. (5.91)

Lagrange, $(\mathbb{Z}/D\mathbb{Z})^*$ deki diskriminantı D olan bir form ile temsil edilen denklik sınıflarını belirlemek için sistematik bir prosedür vermiştir. Çeşitli indirgenmiş formları ve bunlara karşılık gelen kongrüans sınıflarını listelemiştir. Bu Lagrange göre diskriminantları aynı olan formları gruplamanın doğal bir yoludur.

Genel anlamda, D diskriminantlı iki primitif pozitif belirli form, $(\mathbb{Z}/D\mathbb{Z})^*$ da aynı değerleri temsil ediyorsa aynı cinstedir. Denk formların aynı sayıları temsil ettiğini ve böylece aynı cinste olduklarına ilgi çekilir. (Lemma 5.7) Ayrıca her bir cins sonlu sayıda form sınıflarını içerir. Yukarıdaki örnekler; $D=-20$ olduğunda her biri tek bir sınıftan oluşan 2 cins olduğunu gösterir. $D=-56$ olduğunda yine 2 cins vardır fakat burada her cins 2 sınıftan oluşur.

Cins teorisini Teorem 5.14 ile birleştirirsek teori daha da netleşir. Burada temel fikir, cins teorisi, kongrüans sınıfları ve indirgenmiş formlarla temsiller arasındaki bağlantıyı daha da netleştirir. Örneğin, $D=-20$ olduğunda (5.89) $p\equiv 1,\ 3,\ 7,\ 9\ (\text{mod } 20)\Leftrightarrow x^2+5y^2$ veya $2x^2+2xy+3y^2$ olduğunu söyler. Bunu (5.90) ile birleştirecek olursak;

$$\begin{aligned} &p=x^2+5y^2 \Leftrightarrow p\equiv 1,\ 9\ (\text{mod } 20)\\ &p=2x^2+2xy+3y^2 \Leftrightarrow p\equiv 3,\ 7\ (\text{mod } 20)\end{aligned} \tag{5.92}$$

elde ederiz. Burada 2 cins $(\mathbb{Z}/20\mathbb{Z})^*$ de ayrık sınıfları temsil eder. (5.91) de $D=-56$ olduğunda aynı durumu görebiliriz;

$$p = x^2 + 14y^2 \text{ veya } 2x^2 + 7y^2 \Leftrightarrow 1,\ 9,\ 15,\ 23,\ 25,\ 29 \pmod{56}, \qquad (5.93)$$

$$p = 3x^2 \pm 2xy + 5y^2 \Leftrightarrow 3,\ 5,\ 13,\ 19,\ 27,\ 45 \pmod{56}$$

olacaktır.

Şimdi yukarıdaki durumları Teorem 5.14 ile birleştirip genelleştirecek olursak, yukarıdaki örneklerin genel bir durumu yansıttığını göstermeliyiz. Esas formu; $D \equiv 0,\ 1 \pmod 4$ ve negatif olmak üzere;

$$p = x^2 - \frac{D}{4}y^2 \quad D \equiv 0 \pmod 4$$

$$p = x^2 + xy + \frac{1-D}{4}y^2 \quad D \equiv 1 \pmod 4$$

olarak tanımlamıştık. Bu esas form indirgenmiş olup $D = -4n$ olduğunda $x^2 + ny^2$ yi elde ederiz. Esas formu kullanarak D diskriminantlı bir formla temsil edilen $(\mathbb{Z}/D\mathbb{Z})^*$ deki kongrüans sınıflarını karakterize edebiliriz.

Lemma 5.9. *$D \equiv 0,\ 1 \pmod 4$ ve negatif tamsayısı için, $\mathrm{Ker}(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^*$ ve $f(x,y)$, de diskriminantı D olan bir form olsun.*

i) Diskriminantı D olan bir esas formla temsil edilen $(\mathbb{Z}/D\mathbb{Z})^*$ deki kalan sınıfları *$H \subset \mathrm{Ker}(\chi)$ alt grubunu oluştururlar.*

ii) $f(x,y)$ ile temsil edilen $(\mathbb{Z}/D\mathbb{Z})$ teki kalan sınıfları $\mathrm{Ker}(\chi)$ da bir H kalan sınıfını oluştururlar.

İspat. Bakınız (Cox 1989)

H nın farklı kalan sınıfları ayrık olduklarından, Lemma 5.9 daki farklı cinsler $(\mathbb{Z}/D\mathbb{Z})^*$ de farklı kalan sınıflarını temsil eder. Bu bize cinsleri, $\mathrm{Ker}(\chi)$ da H nın H' kalan sınıflarını tanımlamamıza müsade eder. H' nün *cinsini*, H' nün $\bmod D$ ye

göre değerlerini temsil eden diskriminantı D bütün formları temsil ettiğini söyleyebiliriz.

Aşağıdaki teorem elementer cins teorisinin temel sonucudur;

Teorem 5.15. *$D \equiv 0,\ 1 \pmod 4$ negatif ve Lemma 5.9 daki gibi $H \subset \mathrm{Ker}(\chi)$ olsun. H', $\mathrm{Ker}(\chi)$ da H nın bir kalan sınıfı ve p, D yi bölmeyen bir tek asal ise $[p] \in H'$ olması için gerek ve yeter şart p nin H' nün cinsinde diskriminantı D olan indirgenmiş bir formla temsil edilmesidir.* (Cox 1989)

Bu teorem (5.92) ve (5.93) örneklerini genelleştirir. Ayrıca, bu teorem verilen bir cinste bazı formlarla temsil edilen bir asalı karakterize eden kongrüans şartlarının her zaman bulunduğunu gösterir.

6. SONUÇLAR

Bu bölümde daha önce tamsayıların temsil probleminde tanımlarını vermiş olduğumuz β-temsilleri ile ilgili sonuçlarımızı verelim.

Teorem 6.1. *β-asalı olan Pisagor sayısı yoktur.*

İspat. 3'ün dışındaki bütün β-asalları $6k+1$ formunda olduğundan ve bütün pisagor sayıları 6 ile bölünebildiğinden β-asalı olan pisagor sayısının olmadığı sonucu açıktır.

Teorem 6.2. *İki β-sayısının çarpımı β-sayısıdır.*

İspat. Lemma 5.2. nin ispatındaki metodu uygulayarak ispatı yapalım. İki β-sayısının çarpımının β-sayısı olduğunu idealler açısından ispatlamak mümkündür.

Verilen bir cisimde $\mathfrak{O}_1$ deki ideallerden elde edilen primitif kuadratik formların her iki sınıfının aşağıdaki tipte olduğunu söyleyebiliriz.

$$\begin{cases} f_1(a,b) = x_1a^2 + xab + x_2z_0b^2 & x_1 > 0 \\ f_2(a,b) = x_2a^2 + xab + x_1z_0b^2 & x_2 > 0 \end{cases} \tag{6.1}$$

Burada diskriminantlar eşit olduğundan genel olarak $\mathbb{Q}$ cismindeki ideallerin ürettiği primitif kuadratik formların her iki sınıfının orta katsayısı aynı olan formlar olduğu gözönüne alınırsa genel olarak

$$\begin{cases} f_1(a,b) = x_1a^2 + xab + z_1b^2 & x_1 > 0 \\ f_2(a,b) = x_2a^2 + xab + z_2b^2 & x_2 > 0 \end{cases} \quad (x_1, x_2) = 1$$

notasyonlarına göre

$$x^2 - 4x_1z_1 = x^2 - 4x_2z_2 = d$$

olup $x_1 z_1 = x_2 z_2$ dir. $(x_1, x_2) = 1$ olduğundan x_1, z_2 yi x_2, z_1 i böler. Bu (6.1) de yeni bir notasyon olarak verilmiştir ve $d = x^2 - 4x_1 x_2 z_0$ dır.

Burada (6.1) deki formların, $\lambda = (x - \sqrt{d})/2$ olmak üzere

$$\mathrm{j}_1 = [x_1, \lambda]$$

$$\mathrm{j}_2 = [x_2, \lambda]$$

olduğu göz önüne alınırsa

$$\mathrm{j}_1 = \left[1, (x - \sqrt{d})/2\right]$$

$$\mathrm{j}_2 = \left[1, (x - \sqrt{d})/2\right]\sqrt{d}$$

idealleri tarafından üretildiği göürülür. $x_1 > 0$ ve $x_2 > 0$ durumuna kısıtlanacak olursak

$$\lambda^2 = x\lambda - x_1 x_2 z_0$$

denklemi gerçeklenir. Burada a_i ve b_i keyfi rasyonel tamsayılar olmak üzere j_1 ve j_2 ideallerinin sırasıyla,

$$\begin{cases} \alpha_1 = x_1 a_1 + \lambda b_1, & \alpha_1 \in \mathrm{j}_1 \\ \alpha_2 = x_2 a_2 + \lambda b_2, & \alpha_2 \in \mathrm{j}_2 \end{cases}$$

nin cümleleri olduğuna ilgi çekelim. Böylece

$$\begin{cases} \alpha_1 \alpha_2 = x_1 x_2 a_1 a_2 + x_1 \lambda a_1 b_2 + x_2 \lambda a_2 b_1 + b_1 b_2 \lambda^2 \\ \alpha_1 \alpha_2 = x_1 x_2 (a_1 a_2 - z_0 b_1 b_2) + \lambda (x_1 a_1 b_2 + x_2 a_2 b_1 + x b_1 b_2) \end{cases}$$

olacaktır. Diğer bir ifadeyle, a_3 ve b_3 Teorem 5.13 ile belirtilen bilineer ifadelerle verilen,

$$\begin{cases} a_3 = a_1 a_2 - z_0 b_1 b_2 \\ b_3 = x_1 a_1 b_2 + x_2 a_2 b_1 + x b_1 b_2 \end{cases} \tag{6.2}$$

yeni değişkenler olmak üzere,

$$\alpha_1 \alpha_2 = x_1 x_2 a_3 + \lambda b_3 \tag{6.3}$$

şeklinde yazılır.

Sonuç olarak (6.3) ten

$$\mathrm{j}_1 \mathrm{j}_2 = [x_1 x_2, \lambda]$$

olur. İlk olarak buradan $\mathrm{j}_1 \mathrm{j}_2$ çarpımı, çarpım özelliği gereği $x_1 x_2$ ve $x_1 \lambda$, $x_2 \lambda$ ve böylece λ yı da ($(x_1, x_2) = 1$ olduğundan) içerir. Sonuçta, $\mathrm{j}_1 \mathrm{j}_2 \supseteq [x_1 x_2, \lambda]$ dır. Fakat, $[x_1 x_2, \lambda]$ modülünün $\mathfrak{O}_1 = [1, \lambda]$ daki indeksi açık olarak, indeks tanımı gereği $x_1 x_2 (= N[\mathrm{j}_2] N[\mathrm{j}_2],$ ki $\mathrm{j}_1 \mathrm{j}_2$ nin $\mathfrak{O}_1$ deki indeksidir). Böylece $\mathrm{j}_1 \mathrm{j}_2$ ve bunun $[x_1 x_2, \lambda]$ alt kümesinin, $\mathfrak{O}_1$ deki indeksleri aynı olduğundan bunlar aynıdırlar.

Buradan $f(\mathrm{j}_1 \mathrm{j}_2) = f_3$ ise,

$$f_3(a, b) = x_1 x_2 a^2 + xab + z_0 b^2$$

dir. Bu ifade, (6.1) ve (6.2) ye göre düzenlenecek olursa,

$$f_1(a_1, b_1) f_2(a_2, b_2) = f_3(a_3, b_3)$$

bulunur ki bu da ispatı tamamlar. (Bircan ve Şenay 2007)

Teorem 6.3. *β-sayısı olan iki Fibonacci sayısının çarpımı β-sayısıdır fakat Fibonacci sayısı değildir.*

İspat. İki $\beta-$sayısının çarpımının $\beta-$sayısı olacağı Teorem 6.2 nin doğal sonucudur. Ancak iki Fibonacci sayısının çarpımının yine bir Fibonacci sayısı olmadığı göz önüne alınırsa ispat biter.

Bilindiği gibi Fermat'tan bu yana sayılar teorisinin en önemli problemlerinden biri bir tamsayının ve özel olarak bir asalın kareler toplamı olarak ifade edilmesidir. Genel olarak n değişkenli bir kuadratik form bilinen metodlarla bu n değişkenlerinin kareleri toplamı olarak da gösterilebilir.

Bir f kuadratik formu $x_1,\ x_2,...,\ x_n$ lerle bir fonksiyon olarak; $a_{s,r}=a_{r,s}$ eşitliğini gerçekleyen katsayılarla

$$f(x_1,\ x_2,...,\ x_n)=\sum_{r=1}^{n}\sum_{s=1}^{n}a_{r,s}x_r x_s$$

şeklinde ifade edilir. Burada, f in Δ determinantı, yukarıdaki eşitlikte verilen $a_{r,s}$ katsayılarından oluşan determinanttır. Sıfır olmayan bütün $x_1,\ x_2,...,\ x_n$ ler için f pozitif belirlidir. $\xi_1,\ \xi_1,...,\xi_n$ reel katsayılı lineer formlar olmak üzere ve $\sqrt{\Delta}$ determinantıyla

$$f=\xi_1^2+\xi_2^2+...+\xi_n^2$$

olarak ifade edilebilir. (Wright ve Hardy 1960)

Tanım 6.1. $n\in\mathbb{N}$ ve $n\geq 3$ olmak üzere mertebesi a olan $n-$polygonal sayısı p_n^a;

$$P_n^a:=\sum_{k=0}^{a-1}((n-2)k+1)=(n-2)\frac{a^2}{2}-(n-4)\frac{a}{2}$$

şeklinde tanımlanır.

$a,\ b,\ c$ doğal sayıları, $P_n^a+P_n^b=P_n^c$ eşitliğini gerçekliyorlarsa n-polygonal sayıların Pisagor üçlüsünü oluştururlar.

Aşağıdaki teorem böyle üçlüleri tanımlar.

Teorem 6.4. $a,\ b,\ c \in \mathbb{N}$ ve $n \geq 3$ olsun. $r,\ s$ ve t doğal sayıları

$$r((n-2)^2 r - (n-4)) = 2st$$

eşitliğini gerçeklemek üzere $(a,\ b,\ c)$ üçlüsünün n-polygonal sayıların bir Pisagor üçlüsü olmasının gerek ve yeter koşulu,

$$\begin{aligned} a &= (n-2)r + t \\ b &= (n-2)r + s \\ c &= (n-2)r + s + t \end{aligned}$$

eşitliklerinin gerçeklenmesidir. (Scheffold 2001)

E. Scheffold'un verdiği bu sonucu aşağıdaki şekilde genişlettik. Bulduğumuz eşitliği *magma* bilgisayar programı ile ispatladık.

Teorem 6.3. *a,b,c,d ve $n \geq 3$ doğal sayıları için, $r,\ s$ ve t doğal sayıları $r = t+2,\ n = s = t+3$ eşitliklerini gerçeklemek üzere*

$$P_n^a + P_n^b + P_n^c + 2(n-1)(n-4) = P_n^d$$

olmasının gerek ve yeter koşulu

$$\begin{aligned} a &= (n-2)^2 - r^2 - t^2 + s^2 \\ b &= 2(n-2)r - 2ts \\ c &= 2(n-2)t + 2rs \\ d &= (n-2)^2 + r^2 + t^2 + s^2 \end{aligned}$$

olmasıdır.

İspat.

$$
\begin{aligned}
&Qt<t> \;:=\; PolynomialRing(Rationals());\\
&r \;:=\; t+2;\\
&s \;:=\; r+1;\\
&n \;:=\; s;\\
&a \;:=\; (n-2)\,\hat{}\,2-r\,\hat{}\,2-t\,\hat{}\,2+s\,\hat{}\,2;\\
&b \;:=\; 2*(n-2)*r-2*t*s;\\
&c \;:=\; 2*(n-2)*t+2*r*s;\\
&d \;:=\; (n-2)\,\hat{}\,2+r\,\hat{}\,2+t\,\hat{}\,2+s\,\hat{}\,2;\\
&P \;:=\; function(n,a)\\
&pna \;:=\; (n-2)*a\,\hat{}\,2/2-(n-4)*a/2;\\
&return\;\; pna;\\
&end\;\; function;\\
&LHS \;:=\; P(n,a)+P(n,b)+P(n,c)+2*(n-1)*(n-4);\\
&RHS \;:=\; P(n,d)\\
&LHS\;\; eq\;\; RHS;\\
&true
\end{aligned}
$$

(Bircan ve Şenay 2007)

7. KAYNAKLAR

Bircan, N., Şenay, H., 2007 Elemantary results on special number sequences and representation of binary quadratic forms, Int. Journal of Contemp. Math. sciences, vol.2, no 9-12, 565-569.

Bircan, N., Şenay, H., 2007 The parametric representation for diophantine equation $x^2 + y^2 + z^2 = t^2$ of polygonal numbers, Int. Math. Forum, vol.2, no 57-60, 2889-2891.

Buchmann, J., Vollmer, U., 2007 Binary Quadratic Forms An Algorithmic Approach, Springer-Verlag.

Buell, D. A., 1989. Binary Quadratic Forms, Springer-Verlag, New York, Berlin

Brown, E., 1972 Binary quadratic forms of determinant $-pq$, Journal of Number Theory, 4, 5, 408-410.

Brown E., 1973 The power of 2 dividing the class number of a binary quadratic discriminant, Journal of Number Theory, 5, 413-419,

Borovoi, M., 2000 On representation of integers by indefinite ternary quadratic forms, http://uk.arxiv.org/PS_cache/math/pdf/0006/0006141v1.pdf .

Chandrasekharan, K., 1968. Introduction to Analytic Number Theory, Springer-Verlag Berlin, Heidelberg, New York

Chapman R., 2002. Notes on Algebraic Numbers, http://www. secamlocal. ex.ac.uk / people/staff/rjchapma/notes/algn.pdf

Cohn, H., 1980. Advanced Number Theory, Dover Publications Inc., New York.

Cox, D., A., 1989 Primes of the Form $x^2 + ny^2$, John Wiley&Sons Inc. , New York

Davenport, H., 1992. The Higher Arithmetic, Cambridge University Press, NewYork

Dickson, L.E., 1971. History of the Theory of Numbers, Chelsea Publishing Company, Vol.3

Dirichlet, L., E., 1999. Lectures on Number Theory, The American Mathematical Society

Duverney, D., 1998. Théorie des Nombres, Dunod, Paris

Feyzioğlu**,** K., A., 2004 Math 487 Ders Notları http:// feyzioglu. boun. edu. tr/ akfindex.html

Hardy, G.H., Wright, 1960. E.M. An Introduction to the Theory of Numbers, Oxford University Press, Ely House, London W. 1

Kim M. H., Oh B. , K., 1997 Representations of positive definite senary integral quadratic forms by a sum of squares, Journal of Number Theory*,* 63, 89-100.

Kitaoka Y., 1973 Quarternary even positive definite quadratic forms of prime discriminant, Nagoya Mathematical Journal*,* 52, 147-161.

Koch, F., H., 1993 'Representation of primes by binary quadratic forms of discriminant - 256q and -128q', Glasgow Math., 35, 261-268.

Mazur B., 2008. Algebraic Numbers, Princeton Companion to Mathematics Proof, http://www.dms.umontreal.ca/~andrew/Courses/PDFcourses/Mazur.AlgNumbers .pdf

Mohanty S.**,** 1990 Pythagorean numbers, Fibonacci Quarterly 28, 31-42.

Murty, R., Osburn, R., 2004 Representations of integers by certain positive definite binary quadratic forms, http://arxiv.org/PS_cache/math/pdf/0412/0412237.pdf,

Nair U., 2004 Elementary results on the binary quadratic form a^2+ab+b^2, http://front.math.ucdavis.edu/math.NT

Nesin A., 2004. Halkalar, Asallar ve İndirgenemezler (1), Matematik Dünyası, Kadıköy Matbaa, Bahar.

Scheffold, E., 2001 Pythagorean triples of polygonal numbers, The American Mathematical Monthly, 108, 3 Academic Research Library pg.257.

Sun Z.H., 2003 Congruences for fibonacci numbers, http://202.195.112.2/xsjl/szh/ ConFn.pdf

Şenay, H., 2007. Sayılar Teorisi Dersleri, Dizgi Ofset Matbaacılık, Konya.

Weisstein, E. W**.,** 2006 Prime Representation, From Mathworld- A Wolfram Web Resource, http://mathworld.wolfram.com/PrimeRepresentation.html

Voight J., 2004 Binary quadratic forms that represent almost the same primes, http://front.math.ucdavis.edu/author/Voight-J*.

ÖZGEÇMİŞ

1978 yılı Silifke/İçel doğumlu olup, ilkokul, ortaokul ve liseyi sırasıyla Mersin'deki Barbaros İlkokulu ve İçel Anadolu Lisesi'nde tamamladım. 1997 yılında Selçuk Üniversitesi Eğitim Fakültesi Matematik Anabilim Dalı'nda okumaya hak kazandım. 2001 yılında mezun oldum ve 2 ay süreyle Konya, İçeriçumra Kenan Evren İlköğretim Okulu'nda Matematik Öğretmenliği yaptım. Aynı yılda Selçuk Üniversitesi Fen Bilimleri Enstitüsü Matematik Eğitimi Programında yüksek lisansa başlayarak 2003 te tamamladım. 2004 yılında S.Ü. Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda doktora eğitimime başladım. Doktora tez aşamasında TÜBİTAK TR-Access Mobility bursuyla Boğaziçi Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü'nde ve daha sonra Berlin Teknik Üniversitesi Matematik Enstitüsü'nde araştırmalarda bulundum. 2001 yılında Selçuk Üniversitesi Eğitim Fakültesi Matematik Eğitimi Anabilim Dalı'na Araştırma görevlisi olarak atandım ve halen bu görevime devam etmekteyim.

Nihal BİRCAN

Konya, 2008