T.C
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Burç BAYRAK

TRAKYA ÜNİVERSİTESİ
FEN FAKÜLTESİ
MATEMATİK BÖLÜMÜ

YÜKSEK LİSANS TEZİ
CEBİR VE SAYILAR TEORİSİ
ANABİLİM DALI

T.C
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

İKİLİ KUADRATİK FORMLAR VE YAPILARI

Burç BAYRAK

YÜKSEK LİSANS TEZİ

CEBİR VE SAYILAR TEORİSİ ANABİLİM DALI

Tez Yöneticisi : Yrd. Doç. Dr. Fitnat KARAALİ TELCİ

2011
EDİRNE

T.C
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

İKİLİ KUADRATİK FORMLAR VE YAPILARI

Burç BAYRAK

YÜKSEK LİSANS TEZİ

CEBİR VE SAYILAR TEORİSİ ANABİLİM DALI

Bu Tez **24/08/2011** Tarihinde Aşağıdaki Jüri Tarafından Kabul Edilmiştir.

Prof. Dr. Hülya İŞCAN

Üye

Doç. Dr. Şaban AKTAŞ

Üye

Yrd. Doç. Dr. Fitnat KARAALİ TELCİ

Danışman

ÖZET

İkili kuadratik formların yapılarını incelemeyi amaçlayan bu çalışmada izlenen plan aşağıdaki biçimdedir;

I. Bölümde konuyla ilgili önbilgiler verilmiştir.

II. Bölümde ikili kuadratik formların tipleri ve kare çarpansız bir tamsayı olan " d " nin sınıf sayısı incelenmiştir.

III. Bölümde kuadratik formların otomorfları üzerine çalışılmıştır.

IV. Bölümde pozitif belirli bir form ile temsil edilen bir tamsayının bölenleri ve ikili kuadratik formlar için Mass formülü verilmiştir.

V. Bölümde $\mathbb{Q}\left(\sqrt{d}\right)$ cisminin sınıf sayısı ile ikili kuadratik formlar arasındaki ilişki incelenmiştir.

ABSTRACT

The plan followed in this study, which aims to determine the structures of binary quadratic forms, may be outlined as below.

In Chapter I, pertinent backgrounds which are related to issue are given.

In Chapter II, the types of binary quadratic forms and the class number of "d" which is an integer of square free are determined.

In Chapter III, the automorphs of binary quadratic forms are given.

In Chapter IV, the divisions of an integer which are represented with a positive definite form and Mass formula for binary quadratic forms are given.

In Chapter V, the relation between class number of the field $\mathbb{Q}\left(\sqrt{d}\right)$ and binary quadratic forms are studied.

ÖNSÖZ

Tez çalışmam süresince yardımlarını esirgemeyen değerli hocalarım Yrd. Doç. Dr. Fitnat KARAALİ TELCİ ile Prof. Dr. Hülya İŞCAN' a ve maddi, manevi desteğiyle yanımda olan aileme teşekkürlerimi sunarım.

Burç BAYRAK

İÇİNDEKİLER

GİRİŞ

Bu tez çalışmasında a,b,c ler $\mathbb{Z},\mathbb{Q}$ ya da $\mathbb{R}$ den seçilmek üzere ikinci dereceden, iki değişkenli $f(x,y)=ax^2+bxy+cy^2$ ikili kuadratik formlarının genel yapılarının incelenmesi amaçlanmıştır. İkili kuadratik formların özellikleri katsayılarının tamsayı, rasyonel sayı ve reel sayı olmasına bağlıdır.

İkili kuadratik formlar ilk olarak Fermat tarafından iki kare toplamı olarak yazılabilen tamsayılar için çalışılmıştır. İkili kuadratik formlar ile Pell denklemleri arsındaki bağlantı kurulduktan sonra bu formlar Pell denklemi olarak ele alınmıştır. Lagrange' ın 1773 yılındaki çalışmalarıyla gelişmeye başlayan kuadratik formlar teorisi ilk olarak Legendre sayesinde belirli bir düzen içerisinde incelenmiştir. Lagrange' ın geliştirip Legendre' ın sistematik bir biçimde incelediği kuadratik formlar teorisi Gauss tarafından daha da geliştirilmiştir. Gauss' un "Disquisitiones Arithmeticae" adlı kitabında formlarda denklik, indirgeme ve bileşke problemleri üzerine çalışılmıştır. Gauss' un bu çalışmaları ikiden çok değişkeni olan kuadratik formların aritmetik teorisi ile cebirsel sayılar teorisini güçlü bir şekilde etkilemiş, cebirsel sayılar teorisinde önemli bir rol oynayan kuadratik cisimler yerine daha genel olan sayı cisimleri ile çalışılmıştır.

Sayı cisimlerinin yapılarının belirlenmesinde, ideal sınıfları grubunun mertebesi olarak tanımlanan sınıf sayısının hesaplanması önemlidir. Ancak ideal sınıfları grubu yardımı ile sınıf sayısı hesabı kolay olmadığından bir çok yöntem geliştirilmiştir. Bu yöntemlerden biri de kuadratik Diophant denklemleri çözümlerinin elde edilmesidir.

d kare çarpansız bir tamsayı olmak üzere her kuadratik form, indirgenmiş bir forma denk olup d diskriminantlı indirgenmiş formların sayısı sonlu olduğundan indirgenmiş formların denklik sınıflarının sayısı da sonludur. Bununla birlikte $\mathbb{Q}\left(\sqrt{d}\right)$ nin kesirsel idealleri ile d diskriminantlı kuadratik formlar arasında bire bir eşleme var olduğundan indirgenmiş formların denklik sınıfları sayısı da $\mathbb{Q}\left(\sqrt{d}\right)$ cisminin sınıf sayısıdır.

İkili kuadratik formları ve genel yapılarını incelemeyi amaçlayan bu tez çalışmasının I. Bölümünde; temel kavramlar, ikili kuadratik formlar ile ilgili genel bilgiler ve sınıf sayısı tanımı verilmiştir.

Çalışmanın II. Bölümünde; pozitif belirli ve belirsiz tipteki formların özellikleri incelenerek bu tipteki formlar yardımı ile cismin sınıf saısının hesaplama yöntemi verilmiştir.

III. Bölümünde; ikili kuadratik formların otomorflarının genel özellikleri ve pozitif belirli formlar ile belirsiz tipteki formların otomorflarına yer verilmiştir.

IV. Bölümünde; aşağıdaki makalelerden yararlanarak pozitif belirli form ile temsil edilen bir tamsayının bölenleri ve ikili kuadratik formlar için Mass formülü incelenmiştir.

William C. JAGY' nin 2008 yılında yayınlanan makalesinde $d \le -11$ ve p asalı özdeşlik formu ile temsil ediliyor iken np nin pirimitif formla öz temsili var ise n ninde aynı pirimitif formla öz temsilinin var olduğunu göstermiştir.

John Paul COOK' un 2010 yılında yayınlanan makalesinde d diskriminantlı pozitif belirli f formuyla öz temsili olan $n \in \mathbb{Z}_+$ nın aynı diskriminantlı tüm öz temsillerinin sayısını tespit etmiştir. Ayrıca temsil ile öz temsil arasındaki ilişkiden yaralanarak $n \in \mathbb{Z}_+$ nın tüm temsillerinin sayısını bir formülle ifade etmiştir.

V. Bölümde; konuyla ilgili tanımlar verildikten sonra d kare çarpansız bir tamsayı olmak üzere $\mathbb{Q}\left(\sqrt{d}\right)$ kuadratik sayı cisminin kesirsel idealleriyle d diskriminantlı formlar arasındaki ilişkiye yer verilmiştir.

1. BÖLÜM
TEMEL KAVRAMLAR VE GENEL BİLGİLER

1.1 Temel Kavramlar

Tanım 1.1.1 : F bir cisim ve $S \subseteq F$ olsun. S, F deki işlemlerle bir cisim ise S cismine F cisminin bir **"alt cismi"** denir.

Tanım 1.1.2 : F cismi bir K cisminin alt cismi ise K ya F cisminin bir **"genişlemesi"** denir ve K/F veya $K \mid F$ ile gösterilir. Ayrıca K/F bir cisim genişlemesi ise K, F üzerinde bir vektör uzayı olarak düşünülebilir.

Tanım 1.1.3 : K/F bir cisim genişlemesi ise $Boy_F K$ ya K cisminin F üzerindeki **"genişleme derecesi"** denir ve $[K:F]$ ile gösterilir. Eğer $[K:F] < \infty$ ise K/F genişlemesine **"sonlu genişleme"** denir.

Tanım 1.1.4 : K/F bir cisim genişlemesi olsun. $a \in K$ için $f(a) = 0$ olacak şekilde sıfırdan farklı bir $f(x) \in F[x]$ polinomu varsa a ya F cismi üzerinde bir **"cebirsel elemandır"** denir ve $a\ ceb/F$ ile gösterilir.

Tanım 1.1.5 : Bir kompleks sayı $\mathbb{Q}$ üzerinde cebirsel ise **"cebirsel sayı"** olarak adlandırılır.

Tanım 1.1.6 : α bir cebirsel sayı olsun. Eğer α, $\mathbb{Z}$ üzerinde cebirsel ise α ya **"cebirsel tamsayı"** denir.

Tanım 1.1.7 : F üzerinde cebirsel olan bir $\alpha \in K$ yı kök kabul eden $F[x]$ deki asal ve monik polinoma a nın sağladığı **"minimal polinom"** denir. a nın sağladığı minimal

polinom $f(x) \in F[x]$ ise minimal polinomun derecesi $Irr(a,F) = \deg(f)$ ile gösterilir.

Teorem 1.1.8 : d kare çarpansız bir tamsayı ve $k = \mathbb{Q}(\sqrt{d})$ nin cebirsel tamsayılar kümesi $\mathcal{O}_d$ olsun.

$$w_d = \begin{cases} \sqrt{d}; & \text{eğer } d \equiv 2,3 \pmod 4 \text{ ise,} \\ \dfrac{1+\sqrt{d}}{2}; & \text{eğer } d \equiv 1 \pmod 4 \text{ ise,} \end{cases}$$

olmak üzere $\mathcal{O}_d$ nin her elemanı $x, y \in \mathbb{Z}$ için $x + yw_d$ şeklinde yazılabilir.

Sonuç 1.1.9 : $\mathcal{O}_d = \{x + yw_d \mid x, y \in \mathbb{Z}\}$ cebirsel tamsayılar kümesi

$$\oplus : \mathcal{O}_d \times \mathcal{O}_d \to \mathcal{O}_d$$
$$(a_1 + b_1 w_d, a_2 + b_2 w_d) \mapsto (a_1 + a_2) + (b_1 + b_2) w_d$$

ve

$$\odot : \mathcal{O}_d \times \mathcal{O}_d \to \mathcal{O}_d$$
$$(a_1 + b_1 w_d, a_2 + b_2 w_d) \mapsto a_1 a_2 + b_1, b_2 w_d$$

işlemleriyle $\mathbb{Q}(\sqrt{d})$ nin bir alt halkası olup bir tamlık bölgesi oluşturur.

Tanım 1.1.10 : $\mathbb{Q}(\sqrt{d})$ cisminin cebirsel tamsayılar kümesi $\mathcal{O}_d$ ye $\mathbb{Q}(\sqrt{d})$ nin **"tamlık halkası"** ve $\{1, w_d\}$ ye de $\mathcal{O}_d$ tamlık halkasının **"tamlık tabanı"** denir.

Tanım 1.1.11 : K bir cisim ve $K \subseteq \mathbb{C}$ olsun. $[K : \mathbb{Q}] < \infty$ ise K ya bir **"sayı cismi"** denir. Özel olarak $[K : \mathbb{Q}] = 2$ ise K cismi **"kuadratik sayı cismi"** olarak adlandırılır.

Teorem 1.1.12 : K bir sayı cismi olsun. $K = \mathbb{Q}(\alpha)$ olacak şekilde uygun bir $\alpha \in K$ vardır.

Teorem 1.1.13 : K bir sayı cismi olsun. $\sigma : K \to \mathbb{C}$ ye bire bir homomorfizması vardır.

Teorem 1.1.14 : $K = \mathbb{Q}(\alpha)$ bir sayı cismi ve $[K:\mathbb{Q}] = n$ olsun. Bu durumda $i = 1, 2, ..., n$ için n tane farklı $\sigma_i : K \to \mathbb{C}$ gömme homomorfizması vardır ve α_i ler α nın eşlenikleri olmak üzere $\sigma_i(\alpha) = \alpha_i$ elemanı K nın $\mathbb{Q}$ üzerindeki minimal polinomunun köküdür.

Tanım 1.1.15 : $K = \mathbb{Q}(\alpha)$ bir sayı cismi ve $[K:\mathbb{Q}] = n$ olsun. $i = 1, 2, ..., n$ için σ_i ler K nın gömme homomorfizmaları olmak üzere $x \in K$ için x in **"normu"** ve **"izi(trace)"** sırasıyla

$$N : K \to \mathbb{C}, \qquad N(x) = \prod_{i=1}^{n} \sigma_i(x)$$

$$Tr : K \to \mathbb{C}, \qquad Tr(x) = \sum_{i=1}^{n} \sigma_i(x)$$

biçiminde tanımlanır.

1.2 Genel Bilgiler

Genel olarak n değişkenli bir **"kuadratik form"**, $1 \le i, j \le n$ için a_{ij} ler $\mathbb{Z}, \mathbb{Q}$ ya da $\mathbb{R}$ den seçilmek üzere

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j$$

biçiminde ifade edilir. İki değişkenli bir kuadratik forma **"binary (ikili) kuadratik form"** denir ve

$$f(x,y) = ax^2 + bxy + cy^2$$

biçiminde ifade edilir. $f(x,y)$ kuadratik formunun diskriminantı $d(f) = b^2 - 4ac$ biçiminde tanımlanır. Ayrıca diskriminantı $d(f) = b^2 - 4ac$ olan $f(x,y)$ formunun daha kolay bir gösterimi de $f(x,y) = f = (a,b,c)$ biçimindedir. Eğer $ebob(a,b,c) = 1$ ise f formuna **"pirimitif form"** denir.

Bu tez çalışmasında ikili kuadratik formlar yerine form kavramı kullanılacaktır.

Teorem 1.2.1 : $f(x,y) = ax^2 + bxy + cy^2$ **,** d diskriminantlı**,** tam katsayılı ikili kuadratik form olsun. Eğer $d \neq 0$ ve d tam kare değilse $a \neq 0$, $c \neq 0$ dır ve $f(x,y) = 0$ denkleminin tamsayılardaki tek çözümü $x = y = 0$ dır.

Kanıt:

Eğer $a = 0$ veya $c = 0$ ise $a.c = 0$ ve olacağından d nin tam kare olmamasıyla çelişir. $\therefore$ $a \neq 0$ ve $c \neq 0$ dır.

$(x_0, y_0) \in \mathbb{Z}^2$, $f(x,y) = 0$ ın herhangi bir tamsayı çözümü olsun. Eğer $y_0 = 0$ ise $f(x_0, 0) = ax_0^2$ olur. $a \neq 0$ olduğundan $x_0 = 0$ elde edilir. Eğer $x_0 = 0$ ise benzer biçimde $f(0, y_0) = cy_0^2$ ve $c \neq 0$ olduğundan $y_0 = 0$ bulunur. Bu durumda $x_0 = y_0 = 0$ olduğunda $f(x_0, y_0) = 0$ bulunur.

$x_0 \neq 0$ ve $y_0 \neq 0$ olsun. $f(x,y) = ax^2 + bxy + cy^2$ binary kuadratik formundan

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

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

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

$$4af(x,y) = (2ax+by)^2 - dy^2 \qquad (1.1)$$

ifadesi elde edilir. $f(x_0, y_0) = 0$ olduğundan (1.1) ifadesinden $(2ax_0 + by_0)^2 = dy_0^2$ bulunur. $y_0 \neq 0$ ve $d \neq 0$ olduğundan $dy_0^2 \neq 0$ ve çarpanlara ayrılmanın tekliğinden d nin tam kare olması gerekir. Buda d nin tamkare olmayışıyla çelişir.

$\therefore$ $d \neq 0$ ve tam kare değilse $a \neq 0$, $c \neq 0$ dır ve $f(x_0, y_0) = 0$ denkleminin tam sayılardaki tek çözümü $x = y = 0$ dır.

Tanım 1.2.2 : Bir $f(x,y)$ kuadratik formu hem pozitif hem de negatif değerler alabiliyorsa f ye **"belirsiz(indefinite) form"** denir. Eğer her $x, y \in \mathbb{Z}$ için $f(x,y) \geq 0$ ise f ye **"pozitif yarı belirli (semidefinite) form"** , her $x, y \in \mathbb{Z}$ için $f(x,y) \leq 0$ ise f ye **" negatif yarı belirli (semidefinite) form"** denir. Pozitif yarı belirli bir form için $f(x,y) = 0$ denkleminin çözümü sadece $x = y = 0$ ise **"pozitif belirli form"** olarak adlandırılır. Benzer şekilde negatif yarı belirli bir form için $f(x,y) = 0$ denkleminin çözümü sadece $x = y = 0$ ise **"negatif belirli form"** olarak adlandırılır.

$f(x,y) = x^2 - 2y^2$ formu $f(1,0) = 1$ ve $f(0,1) = -2$ değerlerini aldığından belirsiz formdur.

$f(x,y) = x^2 - 2xy + y^2 = (x-y)^2$ formu her $x, y \in \mathbb{Z}$ için $f(x,y) \geq 0$ olup $f(1,1) = 0$ olduğundan pozitif yarı belirli formdur.

$f(x,y) = x^2 + y^2$ formu pozitif belirli forma örnektir.

Bir kuadratik formun pozitif belirli, negatif belirli, yarı belirli veya belirsiz form olup olmadığı diskrininanta bağlı olarak belirlenebilir.

Teorem 1.2.3 : $f(x,y) = ax^2 + bxy + cy^2$, d diskriminantlı , tam katsayılı ikili kuadratik form olsun. Eğer

i) $d > 0$ ise $f(x,y)$ belirsiz formdur.

ii) $d = 0$ ise $f(x,y)$ yarı belirli formdur fakat belirli form değildir.

iii) $d < 0$ ise a ve c aynı işaretli olup bunların işaretleri pozitif olması halinde pozitif belirli, negatif olması halinde negatif belirlidir.

Eğer f pozitif belirli form ise $-f$ negatif belirli form olup bunun terside doğrudur. Bu yüzden belirli formların özelliklerini incelerken sadece pozitif belirli formlarla çalışmak yeterlidir.

Kanıt :

$f(x,y) = ax^2 + bxy + cy^2$ kuadratik formunun diskriminantına d diyelim.

i) $d > 0$ olsun. Bu durumda

$f(1,0) = a$ ve $f(b,-2a) = -ad$ dir.

$a \neq 0$ ise $f(1,0) = a$ ile $f(b,-2a) = -ad$ ters işaretlidir.

Benzer şekilde

$c \neq 0$ ise $f(0,1) = c$ ile $f(-2c,b) = -cd$ olduğundan yine ters işaretlidir.

Şu halde $a = c = 0$ halini incelemek yeterlidir.

$a = c = 0$ için $d = b^2 > 0,\ b \neq 0$ dır.

Bu hal için $f(1,1) = b$ ve $f(1,-1) = -b$ olacağından f nin hem pozitif hem de negatif değerlerinin olacağı anlaşılır.

ii) $d = 0$ olsun.

$a \neq 0$ ise

$$4af(x,y) = (2ax + by)^2 - dy^2$$

Eşitliğinden f nin sıfırdan farklı değerlerinin a ile aynı işaretli olduğu anlaşılır. Ayrıca $f(b,-2a) = -ad = 0$ dır. $a \neq 0$ kabul ettiğimizden f belirli değildir. Eğer $c = 0$ ise $d = b^2 = 0$ olacağından $b = 0$ ve $f(x,y) = ax^2$ olur ki f nin işareti a nın işareti ile aynı olur. $f(0,1) = 0$ olduğundan f yarı belirli ama belirli değildir.

iii) $d < 0$ olsun.

$$4af(x,y) = (2ax + by)^2 - dy^2$$

eşitliğindeki $4af(x,y)$ nin önceki teoremden $x = y = 0$ hariç her $x, y \in \mathbb{Z}$ için pozitif değerler aldığı anlaşılır.Şu halde pozitif belirlidir. Ayrıca

$$d = b^2 - 4ac \Rightarrow 4ac = b^2 - d \geq -d > 0$$

olduğundan a ile c aynı işaretlidir. Budurumda bu işaret pozitif ise pozitif belirli, negatif ise negatif belirlidir.

Örnekler:

1) $f(x,y)=x^2-3y^2$ formu için $f(1,0)=1$ ve $f(0,1)=-3$ olduğundan ya da $d(f)=d=-12<0$ olup teoremin (i) koşulundan f belirsiz bir formdur.

2) $f(x,y)=x^2-2xy+y^2$ formunda her $x,y\in\mathbb{Z}$ için $f(x,y)\geq 0$ olup $f(1,1)=0$ olduğundan ya da $d(f)=d=0$ ve $a>0$ olduğundan teoremin (ii) koşulundan f pozitif belirlidir.

3) $f(x,y)=x^2+y^2$ formunda her $x,y\in\mathbb{Z}$ için olup $x=y=0$ için $f(x,y)=0$ olduğundan ya da $d(f)=d=-4<0$ ve x^2 nin katsayısı 1>0 olduğundan teoremin (iii) koşulundan f pozitif belirlidir.

Teorem 1.2.4 : d bir tam sayı olsun. Diskriminantı d olan bir kuadratik formun mevcut olması için gerekli ve yeterli koşul $d\equiv 0,1(\bmod 4)$ olmasıdır.

Kanıt:

$\Rightarrow$: Her $b\in\mathbb{Z}$ için $b^2\equiv 0,1(\bmod 4)$ olduğundan

$d=b^2-4ac\equiv 0,1(\bmod 4)$ tür.

$\Leftarrow$: $d\in\mathbb{Z}$, $d\equiv 0(\bmod 4)$ için

$f(x,y)=x^2-\frac{d}{4}y^2$ formunun diskriminantı $d(f)=-4.1.\frac{-d}{4}=d$ dir.

$d\in\mathbb{Z}$ ve $d\equiv 1(\bmod 4)$ için $f(x,y)=x^2+xy-\left(\frac{d-1}{4}\right)y^2$ formunun diskriminantı

$d(f)=1-4.1.-\left(\frac{d-1}{4}\right)=d$ olur.

Tanım 1.2.5 : a bir tam sayı, $m>1$ ve $ebob(a,m)=1$ olsun. Eğer $x^2\equiv a(\bmod m)$ kongrüansının çözümü varsa a ya **“** m **modülüne göre kuadratik rezidü”**, çözümü yoksa **“** m **modülüne göre non- kuadratik rezidü”** denir.

Tanım 1.2.6 : $p>2$, asal sayı olsun. $\left(\frac{a}{p}\right)$ **"Legendre sembolü"**

$$\left(\frac{a}{p}\right)=\begin{cases}1 & , \ x^2\equiv a(\text{mod } p) \quad \text{çözümü var ise}\\ -1 & , \ x^2\equiv a(\text{mod } p) \quad \text{çözümü yok ise}\\ 0 & , \ p\mid a \qquad\qquad\quad \text{ise}\end{cases}$$

şeklinde tanımlanır.

Teorem 1.2.7 : $p>2$, asal sayı olsun. O zaman

i) $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(\text{mod } p)$

ii) $\left(\frac{a}{p}\right).\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$

iii) $ebob(a,p)=1$ ise $\left(\frac{a^2}{p}\right)=1$ ve $\left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right)$

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

Teorem 1.2.8 : (QUADRATIC RECIPROCITY)

p ve q farklı tek asal sayılar olsun

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

Teorem 1.2.9 : (Çin Kalan Teoremi)

$r\in\mathbb{Z}_+$, $m_1,m_2,...,m_r$ ikişer ikişer aralarında asal pozitif tam sayılar ve $b_1,b_2,...,b_r$ keyfi tam sayılar olsun.

$$x\equiv b_1(\text{mod } m_1)$$

$$x\equiv b_2(\text{mod } m_2)$$

$$\cdots\cdots\cdots\cdots$$

$$x\equiv b_r(\text{mod } m_r)$$

kongrüans sisteminin bir ortak çözümü var ve bu çözüm modülo $m_1.m_2.....m_r$ de tektir.

Yani a ve b iki çözüm ise

$$a \equiv b \left(\mathrm{mod}\, m_1.m_2.....m_r\right) \text{dir.}$$

Teorem 1.2.10 : $r \in \mathbb{Z}_+$, $m_1, m_2, ..., m_r$ ikişer ikişer aralarında asal pozitif tam sayılar ve $m = m_1.m_2.....m_r$ olsun.

$$f(x) \equiv 0 (\mathrm{mod}\, m)$$

kongrüansının çözümünün olması için gerek ve yeter koşul her $i = 1,2,,,r$ için

$$f(x) \equiv 0 (\mathrm{mod}\, m_i)$$

kongrüansının bir çözümünün olmasıdır. Bu taktirde $f\left(x\right) \equiv 0 \left(\mathrm{mod}\, m_i\right)$ nin çözüm sayısı $N\left(m_i\right)$ ise $f\left(x\right) \equiv 0 \left(\mathrm{mod}\, m\right)$ kongrüansının çözüm sayısı

$$N(m) = \prod_{i=1}^{r} N(m_i) \text{ dir.}$$

Tanım 1.2.11 : $f\left(x, y\right)$ bir kuadratik form ve $n \in \mathbb{Z}$ için $f\left(x_0, y_0\right) = n$ olacak biçimde bir $\left(x_0, y_0\right) \in \mathbb{Z}^2$ varsa n ye $f\left(x, y\right)$ **"kuadratik formu ile temsil edilebilir"** denir. Burada $ebob\left(x_0, y_0\right) = 1$ ise bu temsile **"öz temsil(proper)"** aksi taktirde **"öz olmayan temsil"** adı verilir. Bununla birlikte $ebob\left(x_0, y_0\right) = g$ ve $f\left(x_0, y_0\right) = n$ olmak üzere $g^2 \left| n \right.$ olup n nin $f\left(x, y\right)$ temsilleri $\frac{n}{g^2}$ nin bir öz temsili olarak bulunabilir.

Tanım 1.2.12 : $f\left(x, y\right)$ kuadratik formunun diskriminantı olan d, bir tam kare ve n nin f ile temsili varsa

$$\begin{aligned} 4af\left(x, y\right) = 4an &= \left(2ax + by\right)^2 - dy^2 \\ &= \left(2ax + by - \sqrt{d}\, y\right).\left(2ax + by + \sqrt{d}\, y\right) \end{aligned}$$

elde edilir. Bu biçimdeki yazılışa **"dejenere hal"** denir.

Teorem 1.2.13 : $n \neq 0$ ve d tam sayıları verildiğinde n yi temsil eden bir d diskriminantlı kuadratik formun mevcut olması için gerekli ve yeterli koşul $x^2 \equiv d \left(\mathrm{mod}\, 4|n|\right)$ kongrüansının bir çözümünün olmasıdır.

Kanıt:

$:\Leftarrow$ $x^2 \equiv d \,\mathrm{mod}(\mathrm{mod}\, 4|n|)$ bir çözümü b olsun. Bu durumda

$$b^2 \equiv d(\mathrm{mod}\, 4|n|) \Rightarrow 4|n| \| b^2 - d$$

$$\Rightarrow \exists c \in \mathbb{Z} \ni b^2 - d = 4nc$$

$$\Rightarrow d = b^2 - 4nc \quad \text{dir.}$$

Bu da $f(x,y) = nx^2 + bxy + cy^2$ formunun diskriminantıdır. Bununla birlikte $f(1,0) = n$ olduğundan $f(x,y)$, n nin bir öz temsilidir.

$\Rightarrow$: Diskriminantı $d = b^2 - 4ac$ olan $f(x,y) = ax^2 + bxy + cy^2 = n$ formu n nin bir öz temsili olsun.

Bu durumda $\exists (x_0, y_0) \in \mathbb{Z}^2 \ni f(x_0, y_0) = n$ ve $ebob(x_0, y_0) = 1$ dir.

$ebob(x_0, y_0) = 1$ olduğundan $m_1.m_2 = 4|n|$, $ebob(m_1, y_0) = ebob(m_2, y_0) = 1$

olacak biçimde m_1 ve m_2 tam sayıları bulunabilir. $4n$ in p^α asal kuvvetli çarpanlarının çarpımı m_1 ve $m_2 = \dfrac{4|n|}{m_1}$ olsun. $4af(x,y) = (2ax + by)^2 - dy^2$ ifadesinden

$4af(x_0, y_0) = (2ax_0 + by_0)^2 - dy_0{}^2$ olup $4an \equiv 0(\mathrm{mod}\, m_1)$ olduğundan

$$(2ax_0 + by_0)^2 \equiv dy_0^2 (\mathrm{mod}\, m_1) \quad \text{elde edilir.} \quad ebob(m_1, y_0) = 1$$

olduğundan $\exists \overline{z_0}, \overline{y_0} \in \mathbb{Z} \ni m_1 \overline{z_o} + y_0 \overline{y_0} = 1$ dir. Buradan $y_0 \overline{y_0} \equiv 1(\mathrm{mod}\, m_1)$ ve $(2ax_0 + by_0)^2 \overline{y_0}^2 \equiv dy_0^2 \overline{y_0}^2 \equiv d\left(y_0 \overline{y_0}\right)^2 \equiv d(\mathrm{mod}\, m_1)$ dir. Bu durumda $u^2 \equiv d(\mathrm{mod}\, m_1)$ kongrüansının $u_1 = (2ax_0 + by_0)\overline{y_0}$ biçiminde bir çözümü vardır. Benzer şekilde a ve c yi ve ayrıca x ve y yi aralarında değiştirirsek $u^2 \equiv d(\mathrm{mod}\, m_2)$ kongrüansınında $u_2 = (2cy_0 + bx_0)\overline{x_0}$ biçiminde bir çözümünün olduğunu görürüz. Çin Kalan Teoreminden $w \equiv u_1(\mathrm{mod}\, m_1)$ ve $w \equiv u_2(\mathrm{mod}\, m_2)$ olacak şekilde bir w tam sayısı

bulunabilir. Böylece $w^2 \equiv u_1^2 \equiv d(\mathrm{mod}\, m_1)$ ve benzer biçimde $w^2 \equiv u_2^2 \equiv d(\mathrm{mod}\, m_2)$ elde edilir. $m_1 m_2 = 4|n|$ olduğundan kanıt tamamlanır.

Sonuç 1.2.14 : $d \equiv 0$ veya $1(\mathrm{mod}\, 4)$ olsun. Eğer p tek asal sayı ise p yi temsil eden d diskriminantlı ikili kuadratik formun var olması için gerekli ve yeterli koşul $\left(\frac{d}{p}\right) = 1$ olmasıdır.

Kanıt:

$\Leftarrow$: $\left(\frac{d}{p}\right) = 1$ ise d, p modülüne göre karedir.($x^2 \equiv d(\mathrm{mod}\, 4)$ kongrüansının çözümü vardır.) Hipotezden d, modül 4 e göre karedir. p tek olduğundan Çin Kalan Teoreminden d, modül $4p$ ye göre karedir. Teorem 1.2.13 den p, diskriminantı d olan bir form ile temsil edilir.

$\Rightarrow$: p yi temsil eden d diskriminantlı ikili kuadratik form varsa Teorem1.2.13 den d, $4p$ modülüne göre karedir. Buradan $\left(\frac{d}{4p}\right) = 1$ dir.

$$\left(\frac{d}{4p}\right) = \left(\frac{d}{2}\right)^2 \left(\frac{d}{p}\right) = 1 \Rightarrow \left(\frac{d}{p}\right) = 1 \text{ bulunur.}$$

Kuadratik Formların Denkliği

Formların denkliği 2×2 lik tam katsayılı $GL_2(\mathbb{Z})$ veya $SL_2(\mathbb{Z})$ deki matrisler yardımıyla verilir . Şimdi bu kümelere değinelim.

$GL_2(\mathbb{Z}) = \left\{ M \in \mathbb{Z}_2^2 \middle| \det M = \pm 1 \right\}$ olup matrislerdeki çarpma işlemine göre bir gruptur ve $SL_2(\mathbb{Z}) = \left\{ M \in \mathbb{Z}_2^2 \middle| \det M = 1 \right\}$ kümesi de aynı çarpma işlemine göre $GL_2(\mathbb{Z})$ nin bir alt grubudur. Bu alt gruba **"modüler grup"** denir .

$$S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ve } T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$SL_2(\mathbb{Z})$ nin üreteçleri olup

$$S^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \text{ve } T^2 = -I_{2x2} \text{ dır.}$$

Teorem 1.2.15: Tam katsayılı , +1 determinantlı 2 x 2 lik matrisler grubu $SL_2(\mathbb{Z})$

$$S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ve } T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

ile üretilmiş olup her $M \in SL_2(\mathbb{Z})$ matrisi $k \in \mathbb{N}$ ve $i_k, j_k \in \mathbb{Z}$ olmak üzere

$$M = S^{i_1} T^{j_1} S^{i_2} T^{j_2} \ldots S^{i_k} T^{j_k}$$

olarak yazılabilir.

Kanıt:

$M \in SL_2(\mathbb{Z})$ olsun. M , S ve T nin kuvvetleri ile birim oluncaya kadar soldan çarpılırsa istenilen elde edilmiş olur. Şimdi S ve T nin kuvvetlerinin nasıl belirlendiğini gösterelim.

$M \in SL_2(\mathbb{Z})$ ise M, TM, T^2M, T^3M matrislerinden biri $\beta > 0$ ve $\beta \geq |\delta|$ koşulunu sağlayan $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ dır.

$\delta \neq 0$ ise

$\begin{bmatrix} \alpha + \gamma n & \beta + \delta n \\ \gamma & \delta \end{bmatrix}$ istenileni elde etmek için n yi $|\delta| > \beta + \delta n \geq 0$ sağlıyacak biçimde seçerek

$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ matrisi S^n ile çarpılır. Bu şekilde devam edilecek olursa sonunda sağ üst veya sağ alt bileşenlerden biri sıfır olur.

$\begin{bmatrix} \alpha & 0 \\ \gamma & \delta \end{bmatrix}$ yı ifade etmemiz gerekirse T matrisi uygulanır. Determinant tanımından $\alpha = \delta = \pm 1$ olduğu görülür.

$\begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix}$ yı ifade etmemiz gerekirse T^2 uygulanır.

Bundan sonra birim elde edilinceye kadar $T^3S^\gamma T$ ile çarparsak istenen birim elde edilmiş olur.

$$M=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \text{ için}$$

$$TM=\begin{bmatrix} -c & -d \\ a & b \end{bmatrix}$$

$$T^2M=\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$$

$$T^3M=\begin{bmatrix} c & d \\ -a & -b \end{bmatrix}$$

olup bu matrisler arsında $\beta>0$ ve $\beta \geq |\delta|$ koşulunu sağlayan $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ matrisi

$b>0$ ve $b \geq d$ ise M ye

$b \geq 0$ ve $b<d$ ise T^3M ye

$b \leq 0$ ve $b \geq d$ ise TM ye

$b<0$ ve $b<d$ ise T^2M ye eşittir.

Örnek:

$M=\begin{bmatrix} 3 & 2 \\ -2 & -1 \end{bmatrix} \in SL_2(\mathbb{Z})$ matrisini S ve T matrislerine bağlı olarak yazalım.

$$M=\begin{bmatrix} 3 & 2 \\ -2 & -1 \end{bmatrix}=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$b=2>0$ ve $d=-1$ olup $b \geq d$ olduğundan M , $\beta \geq |\delta|$ koşulunu sağlar.

$S^nM=\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.\begin{bmatrix} 3 & 2 \\ -2 & -1 \end{bmatrix}=\begin{bmatrix} 3-2n & 2-n \\ -2 & -1 \end{bmatrix}$ elde edilir. Burada $\beta+\delta n=2-n$ ve $\delta=-1$ dir. n yi $|\delta|>\beta+\delta n$ sağlıyacak şekilde seçersek $|-1|>2-n\geq 0$ den $n=2$ bulunur. Buradan $S^2M=\begin{bmatrix} -1 & 0 \\ -2 & -1 \end{bmatrix}=M'$ matrisi elde edilir. M' matrisi için $b=0$ ve $b>d=-1$ olduğundan TM' matrisi $\beta \geq |\delta|$ koşulunu sağlar. M' matrisini soldan T ile çarparsak

$TM' = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.\begin{bmatrix} -1 & 0 \\ -2 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}$ matrisi bulunur. TM' matrisinde $\delta = 0$ olduğundan n nin seçimi δ dan bağımsızdır.

$S^n TM' = \begin{bmatrix} 2-n & 1 \\ -1 & 0 \end{bmatrix}$ olup $n = 2$ için $S^2 TM' = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = M''$ dir. M'' matrisi soldan T matrisi ile çarpılırsa

$TM'' = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_{2x2}$ bulunur.

$T.M'' = T.S^2.T.M' = T.S^2.T.S^2 M = I_{2x2}$ olup $S, T \in SL_2(\mathbb{Z})$ olduğundan tersleri vardır ve M matrisi

$$M = S^{-2}T^{-1}S^{-2}T^{-1}$$

biçiminde ifade edilir. Formların denkliğini vermeden önce denklik kavramını ifade ederken kullanılan fonksiyonları verelim.

$$\varphi : GL_2(\mathbb{Z}) \longrightarrow \mathbb{Z}[x,y] \times \mathbb{Z}[x,y]$$

$$U = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \mapsto \varphi(U) = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}.\begin{bmatrix} x \\ y \end{bmatrix} = (\alpha x + \beta y, \gamma x + \delta y)$$

fonksiyonu tanımlansın. φ fonksiyonu bire birdir.

Gerçektende

$\forall U_1 = \begin{bmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{bmatrix}, U_2 = \begin{bmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{bmatrix} \in GL_2(\mathbb{Z})$ için

$$U_1 = U_2 \Leftrightarrow \alpha_1 = \alpha_2,\ \beta_1 = \beta_2,\ \gamma_1 = \gamma_2,\ \delta_1 = \delta_2$$

$$\Leftrightarrow \alpha_1 x + \beta_1 y = \alpha_2 x + \beta_2 y, \qquad \gamma_1 x + \delta_1 y = \gamma_2 x + \delta_2 y$$

$$\Leftrightarrow (\alpha_1 x + \beta_1 y, \gamma_1 x + \delta_1 y) = (\alpha_2 x + \beta_2 y, \gamma_2 x + \delta_2 y)$$

$$\Leftrightarrow \varphi(U_1) = \varphi(U_2)$$

Benzer şekilde $U = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in GL_2(\mathbb{Z})$ için de

$$\varphi_U : \mathbb{Z}^2 \quad \rightarrow \quad \mathbb{Z}^2$$

$$(x,y) \mapsto \varphi_U(x,y) = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}$$

fonksiyonunun tanımlanabileceği açıktır. Yukarıda tanımlanan φ fonksiyonu yardımıyla $A=\left\{ f=(a,b,c)\ kuadratik\ form \middle| d(f)=b^2-4ac \right\}$ olmak üzere

$$\begin{aligned} \phi : A\times GL_2(\mathbb{Z}) &\longrightarrow A \\ (f,U) &\mapsto \phi((f,U))=(\det U).f(\varphi(U)) \end{aligned}$$

biçiminde bir fonksiyon tanımlanabilir. ϕ nin iyi tanımlılığını göstermek için $(f_1,U_1),(f_2,U_2)\in A\times GL_2(\mathbb{Z})$ alalım.

$$\begin{aligned} (f_1,U_1)=(f_2,U_2) &\Leftrightarrow f_1=f_2 \text{ ve } U_1=U_2 \\ &\Leftrightarrow \phi((f_1,U_1))=(\det U_1).f_1(\varphi(U_1)) \\ &\quad =(\det U_2).f_2(\varphi(U_2))=\phi((f_2,U_2)) \end{aligned}$$

dir.

$$U=\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\in \mathbb{Z}_2^2 \qquad \text{için} \tag{1.2}$$

$$f(\varphi(U))=f(\alpha,\gamma)X^2+\left(2(a\alpha\beta+c\gamma\delta)+b(\alpha\delta+\beta\gamma)\right)XY+f(\beta,\delta)Y^2$$

formu elde edilir. Buradaki

$$X=\alpha x+\beta y \text{ ve } Y=\gamma x+\delta y \tag{1.3}$$

biçiminde tanımlıdır. $f(\varphi(U))=(A,B,C)$ ile gösterilirse

$$\begin{aligned} A&=a\alpha^2+b\alpha\gamma+c\gamma^2=f(\alpha,\gamma) \\ B&=2(a\alpha\beta+c\gamma\delta)+b(\alpha\delta+\beta\gamma) \\ C&=a\beta^2+b\beta\delta+c\delta^2=f(\beta,\delta) \end{aligned} \tag{1.4}$$

ve

$$d'=B^2-4AC=(\alpha\delta-\beta\gamma)^2.d \tag{1.5}$$

olup $d=d'$ olması için gerekli ve yeterli koşul $\alpha\delta-\beta\gamma=\pm 1$ olmasıdır.

$\det U\neq 0$ ise

$$\phi((f,U))(X,Y)=(\det U).f(\varphi(U)) \tag{1.6}$$

biçimindedir.

Tanım 1.2.16 : $f(x,y)=ax^2+bxy+cy^2$ ve $g(x,y)=AX^2+BXY+CY^2$ iki kuadratik form olsun.

1. $f\mathscr{R}g \Leftrightarrow \exists U\in GL_2(\mathbb{Z}) \ni \phi(f,U)=g$ biçiminde tanımlanan $\mathscr{R}$ bir denklik bağıntısı olup f formu g formuna **"denktir"** denir. Bir f formuna denk olan formların kümesi de f nin **"denklik sınıfı"** olarak adlandırılır.

2. $f\sim g \Leftrightarrow \exists U\in SL_2(\mathbb{Z}) \ni \phi(f,U)=g$ biçiminde tanımlanan $\sim$ bir denklik bağıntısı olup f formu g formuna **"has denktir"** denir. Bir f formuna has denk olan formların kümesi de f nin **"has denklik sınıfı"** olarak adlandırılır.

3. $f \not\mathscr{R}\ g \Leftrightarrow \exists U\in GL_2(\mathbb{Z}) \ni \det U=-1$ ve $\phi(f,U)=g$ biçiminde tanımlanan $\not\mathscr{R}$ bir denklik bağıntısı olup f formu g formuna **"has olmayan denktir"** denir. Bir f formuna has olmayan denk olan formların kümesi de f nin **"has olmayan denklik sınıfı"** olarak adlandırılır.

Verilen bir d diskriminantlı $f(x,y)=ax^2+bxy+cy^2$ kuadratik formu

$$M(f)=\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \text{ ve } X=\begin{bmatrix} x \\ y \end{bmatrix} \tag{1.7}$$

olmak üzere

$$\left[f(x,y)\right]=X^T M(f) X$$

biçiminde ifade edilir. Buradaki $M(f)$ matrisine **" f kuadratik formunun matrisi"** denir.

Özellik:

$d(f)=d=b^2-4ac$ olmak üzere $\det(M(f))=-\dfrac{d(f)}{4}$ dir.

Eğer f , f' ne ve f' de f'' denk ise

f den f' ne

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

f' den f'' ne

$$\begin{bmatrix} x'' \\ y'' \end{bmatrix} = \begin{bmatrix} \varepsilon & \eta \\ \zeta & \vartheta \end{bmatrix} \cdot \begin{bmatrix} x' \\ y' \end{bmatrix}$$

ve f den f'' ne

$$\begin{bmatrix} x'' \\ y'' \end{bmatrix} = \begin{bmatrix} \varepsilon & \eta \\ \zeta & \vartheta \end{bmatrix} \cdot \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \varepsilon\alpha + \eta\gamma & \varepsilon\beta + \eta\delta \\ \zeta\alpha + \vartheta\gamma & \zeta\beta + \vartheta\delta \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix}$$

geçişleri vardır.

Teorem 1.2.17 : Denk kuadratik formların diskriminantları aynıdır.

Kanıt:

$f \mathrel{\mathscr{R}} g \Leftrightarrow \exists M \in GL_2(\mathbb{Z}) \ni \phi(f, M) = g$ dir. Bu durumda $G = M^T . M(f) .$ sağlanır.

$$-\frac{d(g)}{4} = \det(M(g)) = \det(M^T . M(f) . M) = \det(f) = -\frac{d(f)}{4}$$

Ancak teoremin tersi her zaman doğru değildir. Örneğin; $f(x, y) = 2x^2 - y^2$ ve $g(x, y) = -x^2 + 2y^2$ kuadratik formlarının diskrriminantları eşit olmasına rağmen denk değildirler.

Teorem 1.2.18 : f ve g denk iki form olsun. Her $n \in \mathbb{Z}$ için n nin f ile öz temselleriyle n nin g ile öz temsilleri arasında 1-1 eşleme vardır.

II. BÖLÜM
KUADRATİK FORMLARIN TİPLERİ

2.1 Pozitif Belirli Formlar

Bu bölümdeki öncelikli amacımız $d<0$ diskriminantlı pozitif belirli formların her bir denklik sınıfı için indirgenmiş formları belirlemektir.

Tanım 2.1.1 : $f=(a,b,c)$, d diskriminantlı pozitif belirli bir form olsun. Eğer

$$|b|\le a\le c \tag{2.1}$$

ise $f=(a,b,c)$ formuna **"indirgenmiş form"** denir.

Önerme 2.1.2 : $f=(a,b,c)$, $d<0$ diskriminantlı indirgenmiş bir form ise $|b|\le\sqrt{-d/3}$ tür.

Kanıt :

$$\begin{aligned} 4b^2\le 4ac=b^2-d &\Rightarrow 3b^2\le -d \\ &\Rightarrow b^2\le -d/3 \\ &\Rightarrow |b|\le\sqrt{-d/3} \quad \text{tür.} \end{aligned}$$

Teorem 2.1.3 : $d<0$ diskriminantlı indirgenmiş formların sayısı sonludur.

Kanıt :

Aynı diskriminantlı formlar için Önerme 2.1.2 den dolayı mümkün olan b lerin kümesi $-\sqrt{-d/3}\le b\le\sqrt{-d/3}$ aralığındaki tamsayılar olup diskriminant korunduğundan d diskriminantlı indirgenmiş formlara ait b ler $4ac=b^2-d$ eşitliğini sağlar. Bunedenle $d<0$ diskriminantlı indirgenmiş formların sayısı sonludur.

Teorem 2.1.4 : d diskriminantlı her f pozitif belirli formu aynı diskriminantlı bir indirgenmiş forma denktir.

Kanıt :

$f=(a,b,c)$ **,** d diskriminantlı indirgenmemiş bir form olsun.

a) $c<a$ ise ;

$$\begin{bmatrix} 0 & -1 \\ 1 & \delta \end{bmatrix}$$

matrisine karşılık gelen dönüşümler $u=-y$, $v=x+\delta y$ olup

$$f(u,v)=f(-y,x+\delta y)=\left(c,-b+2c\delta,a-b\delta+c\delta^2\right)$$

$$=(a',b',c') \quad \text{dir.}$$

$|b'|\le|a'|\Rightarrow|-b+2c\delta|\le|c|$ sağlayacak biçimde $\delta\in\mathbb{Z}$ seçildiğinde

$$(a,b,c)\sim\left(c,-b+2c\delta,a-b\delta+c\delta^2\right)=(a',b',c')$$

formu elde edilir. Eğer $a'\le c'$ ise f indirgenmiş olur. Aksi taktirde $a'\le c'$ oluncaya kadar işleme devam edilir.

b) $a<c$ ancak $b\notin[-a,a]$ ise b yi küçültmeden önce f formuna $\delta=0$ için $\begin{bmatrix} 0 & -1 \\ 1 & \delta \end{bmatrix}$ matris dönüşümü uygulanarak $f=(a,b,c)\sim(c,-b,a)=\left(a',b'c'\right)=f'$ formu elde edilir. f' formuna

$$\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}$$

matrisene karşılık gelen $u=x+\beta y$, $v=y$ matris dönüşümleri uygulandığında

$$f'(u,v)=\left(a',2a'\beta+b',a'\beta^2+b'\beta+c'\right)=\left(a'',b'',c''\right)$$

formu bulunur. $a'\le a'\beta^2\le a'\beta+c'$ olduğundan b'' , $b'+2a'b'<a'$ olacak şekilde seçildiğinde $a'<a'\beta^2+b'\beta+c'\Rightarrow a''<c''$ elde edilir. bundan sonra ilk durumda olduğu gibi ard arda $\begin{bmatrix} 0 & -1 \\ 1 & \delta \end{bmatrix}$ matrisi uygulanarak indirgenmiş form elde edilir.

Örnek : $f(x,y)=(3,5,4)$ formu aşağıdaki biçimde indirgenir.

$5\notin[-3,3]$ olduğundan f indirgenmiş bir form değildir. f ye $\begin{bmatrix}0 & -1\\ 1 & \delta_1\end{bmatrix}$ matrisine karşılık gelen $u=-y$ ve $v=x+\delta_1 y$ dönüşümlerini uygulandığında

$$f(u,v)=\left(4,8\delta_1-5,4\delta_1^2-5\delta_1+3\right)$$

formu elde edilir. $|8\delta_1-5|\le 3$ olacak şekilde δ_1=1 alındığında $f=(3,5,4)\sim(4,3,2)=f'$ formu elde edilir. 2<4 olduğundan işleme devam edilir. Bu durumda f'ne $\begin{bmatrix}0 & -1\\ 1 & \delta_2\end{bmatrix}$ matrisi uygulandığında

$$f'=(4,3,2)\sim\left(2,4\delta_2-3,2\delta_2^2-3\delta_2+4\right)$$

formu bulunur. $\delta_2=1$ için $f=(3,5,4)\sim(4,3,2)\sim(2,1,3)$ indirgenmiş elde edilir.

Teorem 2.1.5 : **1)** $(a,b,a)\sim(a,-b,a)$

2) $(a,a,c)\sim(a,-a,c)$

formları dışında has denk olan birbirinden farklı indirgenmiş form yoktur.

Kanıt :

(a,b,c) ve $\left(a',b',c'\right)$ birbirine has denk iki indirgenmiş form ise (1.4) den $a'=a\alpha^2+b\alpha\gamma+c\gamma^2$ olacak şekilde $\alpha,\gamma\in\mathbb{Z}$ vardır. $a'\le c'=a$ olduğundan

$$a\ge a'=a\alpha^2+b\alpha\gamma+c\gamma^2\underset{a<c}{\ge}a\left(\alpha^2+\gamma^2\right)+b\alpha\gamma\underset{|b|<a}{\ge}a\left(\alpha^2+\gamma^2\right)-a|\alpha\gamma|\ge a|\alpha\gamma|$$

elde edilir. Buradan $(\alpha,\beta)=(0,\pm1),(\pm1,0)$ olmalıdır.

I. Durum : $\alpha=\pm1,\ \gamma=0$ ise

$\begin{bmatrix}1 & \beta\\ 0 & \delta\end{bmatrix}\in SL_2(\mathbb{Z})$ matrisi ile $(a,b,c)\sim(a,b+2a\beta,*)$ ve $\begin{bmatrix}-1 & \beta\\ 0 & \delta\end{bmatrix}\in SL_2(\mathbb{Z})$ matrisi ile $(a,b,c)\sim(a,b-2a\beta,*)$ denk formları elde edilir.

$\beta=0$ için $|b\pm2a\beta|=|b|\le a$ dır.

$\beta=1$ için $|b-2a\beta|=|b-2a|\underset{|b|\le a}{\geq}|a-2a|=|-a|=a$ dir. Budurumda $\beta=1$ için $|b-2a\beta|\geq a$ olup $|b-2a\beta|\leq a$ sağlayan $b-2a\beta$ değeri $\pm a$ olarak bulunur. $\beta=-1$ içinde benzer işlemler yapıldığında $b-2a\beta=\pm a$ olduğu görülür. Buradan $a=b$ ve $a=-b$ için $(a,a,c)\sim(a,-a,c)$ elde edilir.

II. Durum : $\alpha=0$ ve $\gamma=\pm1$ ise $\begin{bmatrix}0 & \beta\\ \pm1 & \delta\end{bmatrix}$ olup determinanttan $\beta=\pm1$ olması gerekir. Budurumda $\beta=-1$ için $(a,b,c)\sim\left(c,-b+2c\delta,a-b\delta+c\delta^2\right)$ ve $\beta=1$ için

$$(a,b,c)\sim\left(c,-b-2c\delta,a+b\delta+c\delta^2\right)$$

formuna denktir. $\delta=0$ ise (a,b,c) ve $(c,-b,a)$ formlarının her ikiside indirgenmiştir. Budurumda $(a,b,a)\sim(a,-b,a)$ olması için $a=c$ olmalıdır. $\delta=\pm1$ ise $(a,c,c)\sim(c,-c,a)$ olup $a\leq c$ ve $c\leq a$ olduğundan $(a,a,a)\sim(a,-a,a)$ dır.

III. Durum : $\alpha=\pm1$ ve $\gamma=\pm1$ ise $a\geq a'\geq a|\alpha\gamma|=a$ olduğundan $a=a'=a\pm b+c$ dir. Budurumda $\left(a',b',c'\right)=(a,b,\pm b)$ olup $a=\pm b$ olduğundan indirgenmiş formdur.

$(a,0,a)$ formu $\pm T$ dönüşümü altında ve (a,a,a) formu $\pm P$ ve $\pm P^2$ dönüşümleri altında kendine denktir. $(P=T.S)$

Teorem 2.1.6 : d diskriminantlı her pozitif belirli form(Teorem 2.1.5 deki istisnai durum hariç) bir tek indirgenmiş forma denktir.

Teorem 2.1.7 : Belirli bir diskriminant değeri için denklik sınıflarının sayısı sonludur.

Tanım 2.1.8 : d diskriminantlı $f=(a,b,c)$ formuna karşılık gelen ikinci dereceden denklem $ax^2+bx+c=0$ olup bu denklemin

$$\omega=\frac{-b+\sqrt{d}}{2a}$$

köküne f formunun **"esas kökü"** denir.

Pozitif belirli formları indirgemek için kullanılan diğer yöntem de aşağıdaki biçimdedir.

a) $\mathrm{Re}(\omega) \le 1/2 \Leftrightarrow |b| \le a$ elde etmek için S^n veya S^{-n} matrisine karşılık gelen dönüşümler uygulanır.

b) $|\omega| > 1 \Leftrightarrow a \le c$ elde etmek için T matrisine karşılık gelen dönüşümler uygulanır.

Gerekli ise işlemler tekrarlanır.

Örnek : $f = (2,3,2)$ formu yukarıda verilen yöntemle aşağıdaki biçimde indirgenir. 2<3 olduğundan $S^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ matrisine karşılık gelen $u = x + ny$, $v = y$ dönüşümü uygulanmalıdır.

$$f(u,v) = f(x+ny, y) = (2, 4n+3, 2n^2+3n+2)$$

formu elde edilir. $n = -1$ için

$f(x-y, y) = g(x,y) = (2,-1,1)$ dir. 2>1 olduğundan $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ matrisne karşılık gelen $u = -y$ ve $v = x$ dönüşümleri g ye uygulanırsa

$$g(-y, x) = h(x, y) = (1,1,2)$$

indirgenmiş formu elde edilir.

Tanım 2.1.9 : d negatif bir tamsayı olsun. d diskriminantlı, tam katsayılı, pirimitif formların has denklik sınıflarının sayısına **"d nin sınıf sayısı"** denir ve $h(d)$ ile gösterilir.

Örnek : $d = -71$ diskriminantlı formların kümesi üzerinde tanımlı has denklik bağıntısına göre sınıf sayısı $h(-71)$ i bulmaya çalışalım.

$d = -71$ diskriminantlı formların kümesi

$$A = \left\{ f = (a,b,c) \text{ kuadratik form} \middle| d = b^2 - 4ac = -71 \right\}$$

olmak üzere $f, g \in A$ için

$$f \sim g \Leftrightarrow \exists M \in SL_2(\mathbb{Z}) \ni \phi(f, M) = g(x, y)$$

biçiminde tanımlı $\sim$, A üzerinde bir denklik bağıntısı olduğundan $A/\sim$ bölüm kümesidir . $A/\sim = \{[f] \mid f \in A\}$ kümesinin elemanları denklik sınıfları olup her bir denklik sınıfı $[f] = \{g \in A \mid f \sim g\}$ biçiminde ifade edilir. Her kuadratik form aynı diskriminantlı bir tek indirgenmiş forma denk olduğundan (Teorem 2.1.5 deki istisna hariç) her bir denklik sınıfının temsilcisi indirgenmiş form olarak alındığında birbirinden farklı indirgenmiş formların sayısı sınıf sayısını verecektir.

$d = -D = -71 \Leftrightarrow D = 71$ olup Önerme 2.1.2 den $h = (a, b, c)$ indirgenmiş formlarının b leri için $|b| \le \sqrt{71}/3$ bir üst sınırdır. Budurumda aday b ler b = -4,-3,-2,-1,0,1,2,3,4 olarak bulunur. Ancak denk formların diskriminantları aynı olduğundan b ler diskriminant formülünü de sağlamalıdır.

$d = b^2 - 4ac \Leftrightarrow 4ac = b^2 - d = b^2 + D = b^2 + 71$ olup aday b ler arasından ancak $b = \pm 1, \pm 3$ dört ile bölünebilir.

$b = \pm 1$ için ;

$4ac = 1^2 + 71 = 72 \Leftrightarrow ac = 18$ $a, c > 0$ olduğundan çarpımı 18 i veren pozitif tam sayıları için aday formlarımız belirlenmiş olur.

$f_1 = (1,1,18)$ (indirgenmiş)

$f_2 = (2, \pm 1, 9)$ (indirgenmiş)

$f_3 = (3, \pm 1, 6)$ (indirgenmiş)

$f_4 = (6, \pm 1, 3)$ (indirgenmemiş)

$f_5 = (9, \pm 1, 2)$ (indirgenmemiş)

$f_6 = (18, \pm 1, 1)$ (indirgenmemiş)

$\therefore b = \pm 1$ için farklı denklik sınıfları $(1,1,18), (2, \pm 1, 9), (3, \pm 1, 6)$ olup 5 tanedir.

Benzer şekilde $b = \pm 3$ için

$4ac = 3^2 + 71 = 80 \Leftrightarrow ac = 20$ olup çarpımı 20 olan a ve c sayıları için aday formlarımız

$g_1 = (1, \pm 3, 20)$ (indirgenmemiş)

$g_2 = (2, \pm 3, 10)$ (indirgenmemiş)

$g_3 = (4, \pm 3, 5)$ (indirgenmiş)

$g_4 = (5, \pm 3, 4)$ (indirgenmemiş)

$g_5 = (10, \pm 3, 2)$ (indirgenmemiş)

$g_6 = (20, \pm 3, 1)$ (indirgenmemiş)

$b = \pm 3$ için indirgenmiş formlar $(4, \pm 3, 5)$ olup 2 tanedir. Bu durumda $d = -71$ diskriminantlı indirgenmiş formların sayısı 7 olduğundan $h(-71) = 7$ dir.

2.2 Belirsiz Formlar

Pozitif belirli formlarda verilen bir denklik sınıfı içinde aslında tek bir indirgenmiş form olmasına rağmen $d>0$ diskriminantlı belirsiz formların denklik sınıfları içinde birden fazla indirgenmiş form olabilir. Bu bölümde belirsiz formlardaki indirgenmiş formların nasıl bulunacağını ve bu indirgenmiş formların devirlerini açıklayacağız.

Tanım 2.2.1 : (a,b,c), $d>0$ diskriminantlı belirsiz bir form olsun.

Eğer ;

$$0<b<\sqrt{d} \quad \text{ve}$$
$$\sqrt{d}-b<2|a|<\sqrt{d}+b \tag{2.2}$$

ise (a,b,c) formuna **"indirgenmiştir"** denir.

Önerme 2.2.2 : (a,b,c), $d>0$ diskriminantlı indirgenmiş belirsiz bir form ise $\sqrt{d}-b<2|c|<\sqrt{d}+b$ dir.

Kanıt: (a,b,c), $d>0$ diskriminantlı inidrgenmiş belirsiz bir form olsun.

(a,b,c) indirgenmiş bir form ise $\sqrt{d}-b<2|a|<\sqrt{d}+b$ dir.

$$\sqrt{d}-b<2|a| \Rightarrow \frac{\left(\sqrt{d}+b\right)}{\sqrt{d}+b}.\left(\sqrt{d}-b\right)=\frac{-4ac}{\sqrt{d}+b}=\frac{|2a||2c|}{\sqrt{d}+b}<|2a| \Rightarrow |2c|<\sqrt{d}+b \;\ldots..(*)$$

$$|2a|<\sqrt{d}+b \Rightarrow |2a|<\left(\sqrt{d}+b\right).\frac{\left(\sqrt{d}-b\right)}{\sqrt{d}-b}=\frac{|2a||2c|}{\sqrt{d}-b}$$

$$\Rightarrow |2a|<\frac{|2a||2c|}{\sqrt{D}-b} \Rightarrow \sqrt{D}-b<|2c| \;\ldots..(**)$$

(*) ve (**) dan $\sqrt{d}-b<|2c|<\sqrt{d}+b$ elde edilir.

Önerme 2.2.3 : $d>0$ diskriminantlı indirgenmiş formların sayısı sonludur.

Kanıt : indirgenmiş formlar için b katsayıları $0<b<\sqrt{d}$ aralığından seçileceğinden bu aralıktaki b lerin sayısı sonludur. Bununla birlikte diskriminant değeri bilindiğinden

$d = D = b^2 - 4ac \Rightarrow 4ac = b^2 - D$ nin a ve c çarpanlarının sayısı da sonlu sayıdadır. Bunedenle indirgenmiş formların sayısı sonludur.

Önerme 2.2.4 : Her belirsiz form aynı diskriminantlı bir indirgenmiş forma denktir.

Kanıt : $f = (a,b,c)$, $d > 0$ diskriminantlı indirgenmemiş belirsiz bir form olsun.

$$\sqrt{d} - 2|c| < -b + 2c\delta < \sqrt{d}$$

olacak şekilde seçilen $\delta \in \mathbb{Z}$ için $(a,b,c) \sim \left(c, -b + 2c\delta, a - b\delta + c\delta^2\right)$ dır.

$\left|a - b\delta + c\delta^2\right| < |c|$ ise bu işlem tekrarlanarak $|A| \le |C|$ ve $\sqrt{d} - 2|A| < B < \sqrt{d}$ sağlayan (A,B,C) indirgenmiş formu elde edilir. Bununla birlikte bir diğer yöntemde

$$\left|\sqrt{d} - B\right|.\left|\sqrt{d} + B\right| = 4|A||C|$$

olduğundan ele alınan formun indirgenmiş olması için $|A| \le |C|$ ve $\left|\sqrt{d} + B\right| > 2|C|$ oluncaya kadar belirtilen işlem tekrarlanır. Budurumda $|A| \le |C|$ iken $\left|\sqrt{d} + B\right| > 2|C|$ olduğunda

$$\left|\sqrt{d} + B\right| > 2|C| \underset{|A| \le |C|}{\geq} 2|A| > \sqrt{d} - B$$

olup buda $0 < B < \sqrt{d}$ olmasını gerektirir. Bu sebeple (A,B,C) formu indirgenmiş bir formdur.

Örnek : $d = 25$ diskriminantlı $f = (2,1,-3)$ formunun indirgenmiş formu aşağıdaki biçimde indirgenir.

$2|a| = 4 \notin (4,6)$ olduğundan f formu indirgenmemiştir. f formuna $\begin{bmatrix} 0 & -1 \\ 1 & \delta \end{bmatrix} \in SL_2(\mathbb{Z})$ matrisine karşılık gelen dönüşümler uygulanırsa

$$(2,1,-3) \sim \left(-3, -1 - 6\delta, 2 - \delta - 3\delta^2\right)$$

denk formu elde edilir. Ancak $5 - 2|-3| < -1 - 6\delta < 5$ koşulunu sağlayan $\delta \in \mathbb{Z}$ olmadığından işlemin devam edebilmesi için $\left|2 - \delta - 3\delta^2\right| < |-3| = 3$ sağlayan $\delta \in \mathbb{Z}$ ler

bulunup bu δ lar için işleme devam edilmelidir. Bu koşulu sağlayan $\delta \in \mathbb{Z}$ ler -1,0 ve 1 dir.

$\delta_1 = 1$ için $(2,1,-3) \sim (-3,-7,-2)$ olup $\begin{bmatrix} 0 & -1 \\ 1 & \delta_1' \end{bmatrix} \in SL_2(\mathbb{Z})$ matris dnüşümü uygulandığında $(-3,-7,-2) \sim \left(-2, 7-4\delta_1', -3+7\delta_1' - 2\delta_1'^2\right)$ formu elde edilir. Buradan

$$5-2|-2| < 7-4\delta_1' < 5 \Rightarrow 1 < 7-4\delta_1' < 5$$

$$\Rightarrow -6 < -4\delta_1' < -2 \Rightarrow 1/2 < \delta_1' < 3/2$$

olarak bulunur. Bu aralıktaki δ_1' nın tamsayı değeri $\delta_1' = 1$ olup

$$(2,1,-3) \sim (-3,-7,-2) \sim (-2,3,2)$$

indirgenmiş formu elde edilir.

$\delta_2 = 0$ için $(2,1,-3) \sim (-3,-1,2)$ dir ve $\begin{bmatrix} 0 & -1 \\ 1 & \delta_2' \end{bmatrix} \in SL_2(\mathbb{Z})$ matris dönüşümü uygulandığında $(-3,-1,2) \sim \left(2, 1+4\delta_2', -3+\delta_2'+2\delta_2'^2\right)$ denk formu elde edilir. Ancak $5-2|2| < 1+4\delta_2' < 5$ eşitsizliğini sağlayan $\delta_2' \in \mathbb{Z}$ yoktur. Bunedenle $\left|-3+\delta_2'+2\delta_2'^2\right| < 2$ sağlayan $\delta_2' \in \mathbb{Z}$ ler bulunmalıdır. Bu δ_2' ler -1,0 ve 1 olup

$\delta_{2,1}' = -1$ için $(2,1,-3) \sim (-3,1,2) \sim (2,-3,2) \sim (-2,3,2)$ indirgenmiş formu elde edilir.

$\delta_{2,2}' = 0$ için $(2,1,-3) \sim (-3,-1,2) \sim (2,1,-3)$ formuna geri dönülür.

$\delta_{2,3}' = 1$ için $(2,1,-3) \sim (-3,-1,2) \sim (2,5,0)$ denk formu bulunur ve bu form indirgeme koşullarını sağlamadığından diğer köke geçilir.

$\delta_3 = -1$ için $(2,1,-3) \sim (-3,5,0)$ olup işlem sonlanır. Bu durumda $(2,1,-3)$ formuna denk $(-2,3,2)$ indirgenmiş formu elde edilir.

Tanım 2.2.5 : (a_1,b_1,c_1) ve (a_2,b_2,c_2) iki belirsiz form olsun. Eğer $c_1 = a_2$ ve $b_1 + b_2 \equiv 0 \left(\mathrm{mod}\, 2|a_2|\right)$ ise (a_1,b_1,c_1) ve (a_2,b_2,c_2) formları **"komşudur"** denir. Bu durumda (a_2,b_2,c_2) formu (a_1,b_1,c_1) formunun **"sağ komşuluğu"** , (a_1,b_1,c_1) formu da (a_2,b_2,c_2) formunun **"sol komşuluğu"** olarak adlandırılır.

Tanım 2.2.6 : Bir f formunun f ye denk olan $f_0 = f \sim f_1 \sim f_2 \sim ... \sim f_n \sim ...$ biçimindeki sağ yada sol komşuluklarından biri yine f nin kendisi ise $(f_0 = f, f_1, f_2, ..., f_n, ...)$ ye **" f formunun bir devridir"** denir ve bir devirdeki formların sayısıda o devrin **"periyodu"** olarak adlandırılır.

Teorem 2.2.7 : Verilen bir $d > 0$ diskriminant değeri için indirgenmiş formların kümesi komşu formların devirlerinin bileşimi biçiminde yazılabir.

Kanıt : $f = (a,b,c)$ formu $d > 0$ diskriminantlı indirgenmiş bir form olsun. f nin ard arda sağ komşulukları alındığında bu komşuluklar arasında indirgenmiş formlarda bulunur. İndirgenmiş formların sayısı sonlu olduğundan belli bir adımdan sonra ilk indirgenmiş forma dönülür. Eğer daha fazla indirgenmiş form yoksa işlem tamamlanır aksi taktirde seçtiğimiz forma geri dönülmediyse işlem tekrarlanır. Komşu formlar

$$\begin{bmatrix} 0 & -1 \\ 1 & \dfrac{b_1 + b_2}{2a_2} \end{bmatrix}$$

matris dönüşümü altında denk olup denkliğin geçiş özelliğinden bir devir içindeki tüm formlar birbirine denktir.

Örnek : $d = 25$ diskriminantlı $(-2,3,2)$ formunun indirgenmiş sağ komşuluklarını bulunuz.

$(-2,3,2) \sim (2,b_2,c_2)$ olacak şekilde $-5 < b_2 < 5$ aralığından $\dfrac{3+b_2}{2.2} \in \mathbb{Z}$ seçilirse $b_2 = 1$ için $(-2,3,2) \sim (2,1,-3)$ sağ komşuluğu elde edilir. Benzer işlemler yapılarak devam edilirse

$$(-2,3,2) \sim (2,1,-3) \sim (-3,-1,2) \sim (2,-3,-2) \sim (-2,-1,3) \sim (3,1,-2)$$

devri elde edilir.

Teorem 2.2.8 : İki indirgenmiş formun denk olması için gerekli ve yeterli koşul aynı devirde olmalarıdır.

Tanım 2.2.9 : (k, kn, c) biçimindeki forma **"ambiguous form"** denir. Bununla birlikte (a,b,a) formunun denklik sınıfında ambiguous form olduğundan (a,b,a) formu ambiguous form olarak görülebilir.

$$(a,b,a) \sim (a,b+2a,b+2a) \sim (b+2a,-b-2a,a) \sim (b+2a,b+2a,a)$$

Tanım 2.2.10 : $(a,-b,c)$ formuna (a,b,c) formunun **"tersi"** denir ve bir ambiguous form kendi tersine has denktir. $b = ka$ için $\delta = k$ seçildiğinde
$(a,b,c) \sim (c,-b,a) \sim (a,b-2a\delta, c-b\delta+c\delta^2) = (a,-b,c)$ olduğu görülür.

Tanım 2.2.11 : (a,b,c) ve (c,b,a) formlarına **"ilgili formlar"** denir.

Önerme 2.2.12 : Bir devrin periyodu her zaman çifttir.

Kanıt : (a,b,c) , f indirgenmiş formunun devrindeki herhangi bir eleman olsun. (a,b,c) formuna $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ matrisine karşılık gelen matris dönüşümleri uygulandığında $(a,b,c) \sim (c,-b,a)$ denk formu elde eldir. $(c,-b,a)$ formu (a,b,c) formunun sağ komşuluğu olduğundan (a,b,c) formu f indirgenmiş formunun devrinde ise $(c,-b,a)$ formu da aynı devirde olmak zorundadır. Bu nedenle f nin devrinin periyodu çifttir.

Önerme 2.2.13 : f' ve f aynı devirde olmayan iki ilgili form ise bu devirlerden herhangi birinde bulunan bir formun ilgili formu diğer devirdedir. Böyle devirlere **"ilgili devir"** denir.

Kanıt : $f = (a,b,c)$ ve $f' = (c,b,a)$ farklı devirlerde bulunan iki ilgili form olsun. $b + b' \equiv 0 \pmod{2|c|}$ olacak şekilde $f = (a,b,c)$ formunun (c,b',c') biçiminde bir sağ komşuluğu vardır. Benzer şekilde $f' = (c,b,a)$ formunun da $b + b' \equiv 0 \pmod{2|c|}$ sağlayan bir (a',b',c) sol komşuluğu vardır. Diskriminanttan $a' = c'$ olduğu görülür. Bu durumda $(a',b',c) = (c',b',c)$ ve (c,b',c') formları ilgili formlardır. Bu şekilde devam

edildiğinde devirlerden herhangi birindeki bir formun ilgili formunun diğer devirde olduğu görülür.

Önerme 2.2.14 : Tam olarak iki ambiguous form içeren bir devir kendisiyle ilgili bir devirdir. Tersine kendisiyle igili bir devir tam olarak iki ambiguous form içerir.

Kanıt : $f=(a,b,c)$ ve $f'=(c,b,a)$ kendi kendiyle ilgili olan bir devrin iki ilgili formu ise Önerme 2.2.13 nin kanıtına benzer şekilde f nin sağ ve f' nün sol komşuluklarının ilgili formlar olduğu kolaylıkla görülebilir. f nin sağ komşuluklarından ve f' nün sol komşuluklarından ilerlenecek olursa devir uzunlukları sonlu olduğu için sonlu bir adımdan sonra

$f=(a,b,c)\sim(c,b_1,c_1)\sim(c_1,b_2,c_2)\sim\ldots\sim(c_{k-1},b_k,c_k)\sim(c_k,b_{k+1},c_{k+1})\sim\ldots\sim$
$(c_{n-1},b_n,c)\sim(c,b,a)=f'$

elde edilir. $b+b_1=b+b_n\equiv 0\left(\bmod 2|c|\right)$ olduğundan (c,b_1,c_1) ve (c_{n-1},b_{n-1},c) formları ilgili formlardır. Bu şekilde devam edilerek (c_{k-1},b_k,c_k) formu ile (c_k,b_{k+1},c_{k+1}) formlarının ilgili formlar olduğu görülür. $b_k+b_{k+1}=b_k+b_k=2b_k\equiv 0\left(\bmod 2|c_k|\right)$ olduğundan $c_k|b_k$ dır.

$\therefore(c_k,b_k,c_{k+1})$ formu ambiguous formdur. Benzer şekilde f nin sol ve f' nün sağ komşuluklarından ilerlenecek olursa farklı bir ambiguous form elde edilir. Bu durumda devir tamamlanmış olduğundan kendi kendiyle ilgili bir devirde iki ambiguous form vardır.

Tersine (a',b',c') iki ambiguous form içeren bir devrin herhangi bir elemanı olsun. (a',b',c') nin sağ komşulukları alınarak devam edildiğinde (a',b',c') nün sağ komşuluklarından biri (a,ak,c) biçimindeki bir ambiguous formdur. Bu formun sağ komşuluklarından biri (a,ak,c) ile ilgili (c,ak,a) formu olup (a,ak,c) formunun sol , (c,ak,a) formunun da sağ komşuluğu alındığında

$$f=(a',b',c')\sim\ldots\sim(a''',b''',a)\sim(a,ak,c)\sim\ldots\sim(c,ak,a)\sim(a,b'',c'')$$

denkliği elde edilir. f nin diskriminantı d olmak üzere $\left(-\sqrt{d},\sqrt{d}\right)$ aralığındaki $b'',b'''\in\mathbb{Z}$ için $ak+b''=ak+b'''\equiv 0\left(\mathrm{mod}\,2|a|\right)$ olduğundan $b''=b'''$ olup diskriminant formülünden $a'''=c''$ olduğu görülür. Bu durumda $\left(a''',b''',a\right)=\left(c'',b'',a\right)\sim\left(a,b'',c''\right)$ denk ilgili formları elde edilir. Bu şekilde devam edilecek olursa sonlu bir adımdan sonra $\left(a',b',c'\right)\sim\left(c',b',a'\right)$ ilgili formu elde edilir. O halde f nin devri kendisiyle ilgili bir devirdir.

Verilen bir belirsiz formun has denklik sınıfındaki indirgenmiş formları bulmak için daha kullanışlı bir yöntem aşağıdaki biçimde verilir.

Tanım 2.2.15 : $f=(a,b,c)$ formu için $\rho(f)=(c,-b,a)$ formuna f nin **"normali"** ve ρ ya f nin **"normalleştiricisi"** denir. Daha açık olarak

$$s=s(f)=\begin{cases} sign(c).\left[\dfrac{b}{2|c|}\right]=sign(c).\left[\dfrac{|c|+b}{2|c|}\right]\ ;\ |c|\geq\sqrt{D} \\ sign(c).\left[\dfrac{\sqrt{D}+b}{2|c|}\right]\ ;\ |c|<\sqrt{D} \end{cases} \tag{2.3}$$

olmak üzere

$$\rho(f)=\left(c,-b+2sc,cs^2-bs+a\right)\text{ dir.}$$

Tam katsayılı formlar için $\sqrt{D}$ ile $\left[\sqrt{D}\right]$' nın yeri değiştirilebilir. Bununla birlikte

$$U_f=\begin{bmatrix}0 & -1\\ 1 & s(f)\end{bmatrix}$$

matrisi için $\rho(f)=\phi\left(f,U_f\right)$ olarak elde edilir.

Örnek : $d=29$ diskriminantlı $f=(5,-3,-1)$ formu indirgenmiş bir formdur.

$|-1|<\sqrt{29}$ olduğundan $s=s(f)=sign(-1).\left[\dfrac{\sqrt{29}-3}{2|-1|}\right]=-1$ dir. Bu durumda

$\rho(f)=(-1,5,1)$ indirgenmiş formu elde edilir. $\rho(f)$ e bir kez daha ρ uygulandığında $\rho^2(f)=(1,5,-1)$ indirgenmiş formu elde edilir. Buda belirsiz formların has denklik sınıflarında birden fazla indirgenmiş formun olduğunu gösterir.

Bir denklik sınıfındaki indirgenmiş formların sayısı

Verilen bir $f=(a,b,c)$ indirgenmiş belirsiz formunun denklik sınıfındaki tüm indirgenmiş formların sayısını bulmak için

$$\sigma(f)=\phi\left(f,\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\right)=(-a,b-c)$$

biçiminde bir σ operatörü tanımlanır. Bu durumda

$$\sigma\rho(f)=\rho\sigma(f)=\left(-c,-b+2sc,-\left(a-bs+cs^2\right)\right)$$

elde edilir. Bununla birlikte f ile $\sigma(f)$ denktir ancak has denk olmaları gerekmez.

Önerme 2.2.16 :

a) f ve $\sigma(f)$ has denk ise f nin denklik sınıfı f nin has denklik snıfına eşittir.

b) f ve $\sigma(f)$ has olmayan denk ise f nin denklik sınıfı , birbirinden farklı f ve $\sigma(f)$ in has denklik sınıflarının bileşimidir.

Kanıt :

a) $f=(a,b,c)$ ve $\sigma(f)$ has denk iken g, f nin denklik sınıfındaki herhangi bir form olsun.

g nin f ye has denk olduğu gösterilmelidir. Eğer g, f ye has olmayan denk ise $\det U=-1$ olmak üzere

$$g=\phi(f,U)=(\det U).f\left(\varphi(U)\right)=Ax^2+Bxy+Cy^2$$

olup g, $\sigma(f)$ ye has denktir. Gerçektende g, f ye has olmayan denk ise

$\phi(f,U)=g\Rightarrow\exists U^{-1}\in GL_2(\mathbb{Z})\ni\det U^{-1}=-1$ için $f=\phi\left(g,U^{-1}\right)$ dir.

$$\sigma(f)=\sigma\left(\phi\left(g,U^{-1}\right)\right)$$

olup g, $\sigma(f)$ ye has denktir .Ancak f, $\sigma(f)$ ye has denk olduğundan g, f ye has denk olur ki buda g nin f ye has olmayan denk oluşuyla çelişir. O halde f, $\sigma(f)$ ye has denk ise f nin denklik sınıfı f nin has denklik sınıfına eşittir.

b) f ve $\sigma(f)$ has olmayan denk olsun. Bu durumda f ve $\sigma(f)$nin has denklik sınıfları farklıdır. Bununla birlikte $\sigma(f)$ nin has denklik sınıfı f nin has olmayan denklik sınıfına eşit olduğundan f nin denklik sınıfı $f$nin ve $\sigma(f)$ nin has denklik sınıflarının bileşimidir.

f tam katsayılı bir form olsun. f nin has ya da has olmayan denklik sınıfındaki indirgenmiş formları bulmak için $\rho^i(f)_{i\in\mathbb{Z}}$ dizisi ya da $\rho^i(f)_{i\in\mathbb{Z}}$ dizisine göre daha kullanışlı olan $(\sigma\rho)^i(f)_{i\in\mathbb{Z}}$ dizisi kullanılır.

Örneğin ; $f=(1,3,-2)$ formunun

$$\rho^i(f)_{i\in\mathbb{Z}}=\left(c_i,-b_i+2s(f_i)c_i,c_is(f_i)^2-b_is(f_i)+a_i\right)$$

dönüşümü altındaki devri

$$\{(1,3,-2),(-2,1,2),(2,3,-1),(-1,3,2),(2,1,-2),(-2,3,1)\}$$

iken

$$(\rho\sigma)^i(f)_{i\in\mathbb{Z}}=\left(-c_i,-b_i+2s(f_i)c_i,-\left(a_i-b_is(f_i)+c_is(f_i)^2\right)\right)$$

dönüşümü altındaki devri

$$\{(1,3,-2),(2,1,-2),(2,3,-1)\} \text{ dir.}$$

$\rho^i(f)_{i\in\mathbb{Z}}$ ve $(\sigma\rho)^i(f)_{i\in\mathbb{Z}}$ periyodik olup $\rho^i(f)_{i\in\mathbb{Z}}$ in periyot uzunluğu $(\sigma\rho)^i(f)_{i\in\mathbb{Z}}$ nin periyot uzunluğunun iki katıdır. Bununla birlikte $\sigma(f)\in\{\rho^i(f)_{i\in\mathbb{Z}}\}$ olduğundan Önerme 2.2.16 den f nin has ve has olmayan denklik sınıfları eşittir.

Tanım 2.2.17 : d pozitif bir tamsayı olsun. d diskriminantlı, tam katsayılı, pirimitif formların denklik sınıfları sayısına **"d nin sınıf sayısı"** ve $h(d)$ ile gösterilir.

Örnek : $d=1173$ diskriminantlı formların kümesi üzerinde tanımlanan denklik bağıntısına göre sınıf sayısı $h(1173)$ aşağıdaki gibi bulunur.

$d=1173$ diskriminantlı her $f=(a,b,c)$ indirgenmiş formu $0<b<\sqrt{1173}\simeq 34.249$ ve diskriminant formülünü sağlayacağından aday formlar için b ler

$b=1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33$ olabilir.

$b=1$ için $-4ac=d-b^2\Rightarrow ac=-293$ (293 asal)

$(1,1,-293),(-1,1,293),(293,1,-1),(-293,1,1)$ (indirgenmemiş)

$b=3$ için $-4ac=d-b^2\Rightarrow ac=-291=-3.97$

$(1,3,-291),(-1,3,291),(291,3,-1),(-291,3,1)$ (indirgenmemiş)

$(3,3,-97),(-3,3,97),(97,3,-3),(-97,3,3)$ (indirgenmemiş)

$b=5$ için $-4ac=d-b^2\Rightarrow ac=-287=-7.41$

$(1,5,-287),(-1,5,287),(287,5,-1),(-287,5,1)$ (indirgenmemiş)

$(7,5,-41),(-7,5,41),(41,5,-7),(-41,5,7)$ (indirgenmemiş)

$b=7$ için $-4ac=d-b^2\Rightarrow ac=-281$ (281 asal)

$(1,7,-281),(-1,7,281),(281,7,-1),(-281,7,1)$ (indirgenmemiş)

$b=9$ için $-4ac=d-b^2\Rightarrow ac=-273=-3.7.13$

$(1,9,-273),(-1,9,273),(273,9,-1),(-273,9,1)$ (indirgenmemiş)

$(3,9,-91),(-3,9,91),(91,9,-3),(-91,9,3)$ (indirgenmemiş)

$(21,9-13),(-21,9,13),(13,9,-21),(-13,9,21)$ (indirgenmiş)

Benzer şekilde devam edilecek olursa $b=17,23,33$ içinde indirgenmiş formlar elde edilir. $d=1173$ diskriminantlı tüm indirgenmiş formlar

$(21,9,-13),(-21,9,13),(13,9,-21),(-13,9,21),(13,17,-17),(-13,17,17),(17,17,-13)$

$(-17,17,13),(7,23,-23),(-7,23,23),(23,23,-7),(-23,23,7),(1,33,-21),(-1,33,21)$

$(21,33,-1),(-21,33,1),(3,33,-7),(-3,33,7),(7,33,-3),(-7,33,3)$

olup bu indirgenmiş formlara ρ uygulanırsa

A) $(1,33,-21) \sim (-21,9,13) \sim (13,17,-17) \sim (-17,17,13) \sim (13,9,-21) \sim (-21,33,1)$

B) $(-1,33,21) \sim (21,9,-13) \sim (-13,17,17) \sim (17,17,-13) \sim (-13,9,21) \sim (21,33,-1)$

C) $(3,33,-7) \sim (-7,23,23) \sim (23,23,-7) \sim (-7,33,3)$

D) $(-3,33,7) \sim (7,23,-23) \sim (-23,23,7) \sim (7,33,-3)$

biçiminde devirler elde edilir. f ve $\sigma(f)$ has denk olmadığından f nin denklik sınıfı f ve $\sigma(f)$ nin denklik sınıflarının bileşimidir. Bu durumda f nin denklik sınıfı, $f=(1,33,-21)$ ile $g=(-1,33,21)$ kuadratik formlarının devirlerinin bileşimi olup benzer şekilde diğer devirlerin bileşiminin de ayrı bir denklik sınıfı olduğu görülebilir. $d=1173$ diskriminantlı tam katsayılı formlar kümesi üzerinde tanımlanan denklik bağıntısına göre iki farklı denklik sınıfı olduğundan $h(1173)=2$ olarak bulunur.

Tanım 2.2.18 : f tam katsayılı belirsiz bir form olsun.

i) g, f ye has denk bir form olmak üzere f nin has devri $\left(\rho^i(g)\right)_{i\in\mathbb{Z}}$ dizisidir.

ii) $g=(A,B,C)$ ve $A>0$ olmak üzere g, f ye has olmayan denk olsun. f nin devri $\left((\sigma\rho)^i(g)\right)_{i\in\mathbb{Z}}$ dizisidir.

Önerme 2.2.19 : f tam katsayılı bir form ve $(f=f_0, f_1, f_2, \ldots f_{l-1})$ de f nin devri olsun.

a) f nin periyodu l tek ise f ve $\sigma(f)$ nin has devri

$$\left(f_0, \sigma(f_1), f_2, \sigma(f_3), \ldots, f_{l-1}, \sigma(f_0), f_1, \ldots, \sigma(f_{l-1})\right)$$

dir. Bu durumda f nin denklik sınıfı f nin has denklik sınıfına eşittir.

b) f nin periyodu l çift ise f nin has devri $\left(f_0, \sigma(f_1), \sigma(f_2), \ldots, \sigma(f_{l-1})\right)$ ve $\sigma(f)$ nin has devri $\left(\sigma(f_0), f_1, f_2, \ldots, f_{l-1}\right)$ dir. Ayrıca f nin denklik sınıfı; birbirinden farklı f ve $\sigma(f)$ nin has denklik sınıflarının bileşimidir.

Kanıt :

a) l tek olsun. $M=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ olmak üzere $M^2=I_{2x2}$ olduğundan $\sigma(f)=\sigma(\rho\sigma)^l(f)=\sigma(\sigma\rho)^l(f)=\sigma\left(\sigma^l\left(\rho^l(f)\right)\right)=\rho^l(f)$ dir. Bu nedenle f ve $\sigma(f)=\rho^l$ has denktir. Önerme 2.2.16 den f nin denklik sınıfı f nin has denklik sınıfına eşittir. f nin denklik sınıfında $\sigma(f)$ de olduğundan $i=1,2,3,...,l-1$ için f_i , f nin has denklik sınıfında iken $\sigma(f_i)$ de f nin has denklik sınıfındadır. Buradan f nin denklik sınıfı

$$\left(f_0,\sigma(f_1),f_2,\sigma(f_3),...,f_{l-1},\sigma(f_0),f_1,...,\sigma(f_{l-1})\right) \text{ dır.}$$

b) l çift olsun. Bu durumda $f=(\sigma\rho)^l(f)=\rho^l(f)$ olup $0\le i\le l$ için

$$\sigma(f)=\sigma\left(\rho^l(f)\right)=\sigma\left(\phi\left(f_i,U_{f_i}\right)\right)$$

olduğundan f, $\sigma(f)$ ye has olmayan denktir. f ve $\sigma(f)$ has olmayan denk olduğundan Önerme 2.2.16 den f nin denklik sınıfı f ve $\sigma(f)$ nin has denklik sınıflarının bileşimidir. f nin devri $i=0,1,2,...,l-1$ için $\left\{(\sigma\rho)^i(f)\right\}$ olup her $i=0,1,2,...,l-1$ için $(\sigma\rho)(f_i)=\sigma\left(\varphi\left(f_i,U_{f_i}\right)\right)=f_{i+1}$ olduğundan f_i, f_{i+1} e has olmayan denktir. Bunedenle f nin has devri $\left\{f_0,\sigma(f_1),\sigma(f_2),...,\sigma(f_{l-1})\right\}$ dir. Benzer şekilde $\sigma(f)$ nin has devride $\left\{\sigma(f_0),f_1,f_2,...,f_l\right\}$ olarak bulunur.

$a>0$ olmak üzere $f=(a,b,c)$ olsun. f nin $(f_0,f_1,f_2,...,f_{l-1})$ devri aşağıdaki şekilde hesaplanır.

$f=(a_0,b_0,c_0)=f_0$ ve her $i=0,1,2,...,l-1$ için $s_i=\left|s(f_i)\right|=\left[\dfrac{b_i+\sqrt{D}}{2|c_i|}\right]$ olsun. Bu durumda

$$f_{i+1}=(a_{i+1},b_{i+1},c_{i+1})=\left(|c_i|,-b_i+2s_i|c_i|,-\left(a_i+b_is_i+c_is_i^2\right)\right)$$

olup f_{i+1} in diğer bir yazılışı

$$f_{i+1} = \phi\left(f_i, \begin{bmatrix} 0 & 1 \\ -1 & |s(f_i)| \end{bmatrix} \right), i \in \mathbb{Z}$$

dir. $f_i = \phi(f, T_i)$ sağlayan

$$T_i = \begin{bmatrix} p_i & p_{i+1} \\ q_i & q_{i+1} \end{bmatrix} \in GL_2(\mathbb{Z})$$

matrisini hesaplamak için $T_0 = I_{2x2}$ ve $i \geq 0$ için $p_{i+2} = s_i p_{i+1} + p_i$, $q_{i+2} = s_i q_{i+1} + q_i$ rekürans bağıntıları tanımlanır.

Örnek : $d = 73$ diskriminantlı $f = (1, 7, -6)$ indirgenmiş formunun devri aşağıdaki biçimde bulunur.

i	0	1	2	3	4	5	6	7	8	9
a_i	1	6	2	3	4	4	3	2	6	1
b_i	7	5	7	5	3	5	7	5	7	7
$-c_i$	6	2	3	4	4	3	2	6	1	6
p_i	1	0	1	3	7	10	17	44	149	193
q_i	0	1	1	4	9	13	22	57	193	250
s_i	1	3	2	1	1	2	3	1	7	

Tablo 2.1

f nin periyodu 9 olduğundan Önerme 2.2.19 den f nin has devir uzunluğu 18 dir.

Önerme 2.2.20 : f , $d > 0$ diskriminantlı indirgenmiş bir form olsun.

a) $i \geq 2$ için $p_{i+1} > p_i > 0$ ve $p_{i+2} \geq 2p_i$

b) $i \geq 2$ için $q_{i+1} > q_i > 0$ ve $q_{i+2} \geq 2q_i$

c) $i \geq 2$ için $p_i \geq 2^{\left[(i-2)/2\right]}$

d) $i \geq 2$ için $q_i \geq 2^{\left[(i-1)/2\right]}$

e) $i \geq 0$ için $p_{i+2} \leq \left(\sqrt{D}+1\right)^i$

f) $i \geq 0$ için $q_{i+1} \leq \left(\sqrt{D}+1\right)^i$ dir.

Kanıt :

a) f , $d > 0$ diskriminantlı indirgenmiş bir form ise $1 \leq \left|s(f)\right| < \sqrt{D}$ dir. $p_0 = 1, p_1 = 0$ olup $p_{i+2} = s_i p_{i+1} + p_i$ rekürans bağıntısından $i = 0$ için $p_2 = s_0 p_1 + p_0 = 1$ ve $i = 1$ için $p_3 = s_1 p_2 + p_1 = s_1.1 + 0 = s_1$ elde edilir.

$i \geq 2$ için $p_{i+2} = s_i p_{i+1} + p_i \underset{s_i \geq 1}{\geq} p_{i+1} + p_i > p_{i+1} > 0$ dır. Buradan $i \geq 3$ için $p_{i+2} > 2p_i$ ve $i = 2$ için $p_4 = s_2 p_3 + p_2 \underset{s_2 \geq 1}{\geq} p_3 + p_2 = s_1 + 1 \underset{s_1 \geq 1}{\geq} 2 = 2p_2$ olduğundan $i \geq 2$ için $p_{i+2} \geq 2p_i$ dir. Önermenin b) şıkkı da benzer şekilde kanıtlanır.

c) $i \geq 2$ için $p_i \geq 2^{\left\lfloor (i-2)/2 \right\rfloor}$ doğru olduğu tüme varımla kanıtlanır.

$n \geq 2$ için $T(n)$ önermesi $T(n): p_n \geq 2^{\left\lfloor (n-2)/2 \right\rfloor}$ biçiminde tanımlamsın.

$k = 2$ için $p_2 = 1 = 2^{\left\lfloor (2-2)/2 \right\rfloor}$ olduğundan $T(2)$ doğrudur.

$k \in \mathbb{N}$ olmak üzere $2 < k \leq n$ için $T(k)$ önermesi doğru olsun. Bu durumda $2 < k \leq n$ için $p_k \geq 2^{\left\lfloor (k-2)/2 \right\rfloor}$ sağlanır.

$k = n$ için $T(n)$ önermesinin doğru olduğu göstermelidir.

$p_n \underset{1'den}{\geq} 2p_{n-2} \underset{\substack{T(n-2) \\ doğru}}{\geq} 2.2^{\left\lfloor (n-4)/2 \right\rfloor}$ dir.

$n-4$ çift ise $n-4/2 \in \mathbb{Z} \Rightarrow \left\lfloor \frac{n-4}{2} \right\rfloor = \frac{n-4}{2}$ olduğundan $p_n \geq p_{n-2} \geq 2.2^{\frac{n-4}{2}} = 2^{\frac{n-2}{2}}$ elde edilir.

$n-4$ tek ise bu durumda $n-4/2 \notin \mathbb{Z} \Rightarrow \left\lfloor \frac{n-4}{2} \right\rfloor = \left\lfloor \frac{n-5}{2} \right\rfloor = \frac{n-5}{2}$ olup

$p_n \underset{1'den}{\geq} 2p_{n-2} \underset{\substack{T(n-2) \\ doğru}}{\geq} 2.2^{\frac{n-5}{2}} = 2^{\frac{n-3}{2}} = 2^{\left\lfloor \frac{n-2}{2} \right\rfloor}$ dir.

$\therefore i \geq 2$ için $p_i \geq 2^{\left\lfloor (i-2)/2 \right\rfloor}$ dir. Önermenin d) şıkkı da benzer şekilde kanıtlanır.

e) $i \geq 0$ için $p_{i+2} \leq \left(\sqrt{D}+1\right)^i$ olduğunu da önermenin üçüncü ifadesinin kanıtına benzer şekilde tüme varımla yapalır.

$n \geq 0$ için $T(n)$ önermesi $T(n): p_{n+2} \leq \left(\sqrt{D}+1\right)^n$ olsun.

$n = 0$ için $p_2 = 1 = \left(\sqrt{D}+1\right)^0$ olduğundan $T(0)$ doğrudur.

$n = 1$ için $p_3 = s_1 \leq \sqrt{D} < \sqrt{D}+1$ olduğundan $T(1)$ doğrudur.

$k \in \mathbb{N}$ olmak üzere $2 \leq k \leq n-1$ için $T(k)$ doğru olsun. Bu durumda $2 \leq k \leq n-1$ için $p_{k+2} \leq \left(\sqrt{D}+1\right)^k$ sağlanır.

$k = n$ için $T(n): p_{n+2} \leq \left(\sqrt{D}+1\right)^n$ nın doğru olduğunu göstermelidir.

$$p_{n+2} = s_n p_{n+1} + p_n \underset{s_n \leq \sqrt{D}}{\leq} \sqrt{D}.p_{n+1} + p_n \leq \sqrt{D}.\left(\sqrt{D}+1\right)^{n-1} + \left(\sqrt{D}+1\right)^{n-2}$$

$$= \left(D+\sqrt{D}+1\right).\left(\sqrt{D}+1\right)^{n-2}$$

$\therefore i \geq 2$ için $p_i \geq 2^{\left\lfloor (i-2)/2 \right\rfloor}$ dir. Önermenin f) şıkkı da benzer biçimde kanıtlanır.

III. BÖLÜM
FORMLARIN OTOMORFLARI

3.1 Genel Bilgiler

Bu bölümde bir f formuna uygulandığında onu değiştirmeyen $GL_2(\mathbb{Z})$ deki matrislere karşılık gelen dönüşümleri inceleyeceğiz.

Tanım 3.1.1 : f bir kuadratik form olmak üzere $\phi(f,U)=f$ sağlayan $U \in GL_2(\mathbb{Z})$ matrisine **"** f **nin otomorfu"**, $\phi(f,U)=f$ sağlayan $U \in SL_2(\mathbb{Z})$ matrisine de **"** f **nin has otomorfu"** denir.

Örnek : Herhangi bir f formu için $\phi(f,I_{2x2})=\phi(f,-I_{2x2})=f$ olduğundan I_{2x2} ve $-I_{2x2}$ her formun otomorflarıdır. Bu otomorflara **"** f **nin aşikar otomorfları"** denir.

Tanım 3.1.2 : f nin otomorflarının kümesi $GL_2(\mathbb{Z})$ nin bir alt grubudur. Bu gruba **"** f **nin otomorflar grubu"** denir ve $Aut(f)$ ile gösterilir.

Gerçekten de $Aut(f)=\{U \in GL_2(\mathbb{Z}) \mid \phi(f,U)=f\}$ olup $U \in Aut(f) \Rightarrow U^{-1} \in Aut(f)$ dir. Bu durumda $U_1,U_2 \in Aut(f) \Rightarrow \phi(f,U_1.U_2^{-1})=\phi(\phi(f,U_1),U_2^{-1})=\phi(f,U_2^{-1})=f$ olduğundan $Aut(f) < GL_2(\mathbb{Z})$ dir.

Tanım 3.1.3 : f nin has otomorflarının kümesi de $SL_2(\mathbb{Z})$ nin bir alt grubudur. Bu alt gruba **"** f **nin has otomorfları grubu"** denir ve $Aut^+(f)$ ile gösterilir. $I_{2x2},-I_{2x2} \in Aut^+(f)$ olduğundan f nin has otomorflarının kümesi her zaman $I_{2x2},-I_{2x2}$ matrislerini içerir.

Tanım 3.1.4 : Eğer f nin otomorflar grubu sadece aşikar otomorflardan oluşuyorsa bu otomorflar grubuna **"** f **nin aşikar otomorflar grubu"** denir.

Tanım 3.1.5 : n reel sayısının f ile temsilleri (x,y) ve (x',y') olsun.

$$(x,y)\sim(x',y')\Leftrightarrow\exists U\in Aut^{+}(f)\ni\varphi_U(x,y)=(x',y')$$

biçiminde tanımlanan " $\sim$ " bir denklik bağıntısıdır.

Teorem 3.1.6 : $f=(a,b,c)$ katsayıları tam sayı olmayan bir form olsun. $Aut(f)$ aşikar değilse $r.f$ tam katsayılı olacak şekilde pozitif bir r tam sayısı vardır.

Kanıt : $U\in Aut(f)$ olsun. (1.7) den $M(fU)=M(f)=(\det U).U^{T}.M(f).U$ dir.

$\det(U)=1$ olarak alınırsa

$$\left(U^{T}\right)^{-1}M(f)=M(f)U \tag{3.1}$$

elde edilir. U , (1.2) de tanımlanan matris olarak düşünüldüğünde

$$M(f).U=\frac{1}{2}\begin{bmatrix}2a\alpha+b\gamma & 2a\beta+b\delta\\ 2c\gamma+b\alpha & 2c\delta+b\beta\end{bmatrix} \tag{3.2}$$

ve

$$\left(U^{T}\right)^{-1}.M(f)=\frac{1}{2}\begin{bmatrix}2a\delta-b\gamma & -2c\gamma+b\delta\\ -2a\beta+b\alpha & 2c\alpha-b\beta\end{bmatrix} \tag{3.3}$$

olduğu görülür. (3.1) , (3.2) ve (3.3) den

$$a\beta=-c\gamma,\ \ b\gamma=a(\delta-\alpha),\ \ b\beta=c(\alpha-\delta) \tag{3.4}$$

elde edilir.

$U\neq\pm I_{2x2}$ ise $\gamma\neq0$ veya $\beta\neq0$ veya $\alpha-\delta\neq0$ dir. $\gamma\neq0$ ise (3.4) den $(a,b,c)=\left(a/\gamma\right)(\gamma,(\delta-\alpha),-\beta)$ dir. Benzer şekilde (3.4) ten $\beta\neq0$ ise $(a,b,c)=\left(c/\beta\right)(-\gamma,(\alpha-\delta),\beta)$ ve $\alpha-\delta\neq0$ ise $(a,b,c)=\left(b/\delta-\alpha\right)(\gamma,\delta-\alpha,-\beta)$ elde edilir. $\det U=-1$ için kanıt benzer şekilde yapılır.

Sonuç 3.1.7 : f ve g iki kuadratik form olsun. Eğer bir $r\in\mathbb{Z}^{+}$ için $g=rf$ ise $Aut(f)=Aut(g)$ dir.

Kanıt : $U\in Aut(f)$ olsun. $gU=(rf)U=r(fU)=rf=g$ olduğundan $U\in Aut(g)$ olup $Aut(f)\subseteq Aut(g)$ dir. Tersine $V\in Aut(g)$ olsun.

$$\phi(g,V)=\phi(rf,V)=g \Leftrightarrow \phi(rf,V)=rf$$
$$\Leftrightarrow r\phi(f,V)=rf$$
$$\Leftrightarrow \phi(f,V)=f \text{ dir.}$$

Bu durumda $V \in Aut(f)$ olup $Aut(g)\subseteq Aut(f)$ elde edilir. $Aut(f)\subseteq Aut(g)$ ve $Aut(g)\subseteq Aut(f)$ olduğundan $Aut(f)=Aut(g)$ dir.

Sonuç 3.1.7 den dolayı pirimitif olmayan bir formun otomorf grubu ile o formun pirimitif şeklinin otomorf grubu aynıdır.

Tanım 3.1.8 : $N,d \in \mathbb{Z}$ için $x^2-dy^2=N$ Diophant denklemine **"Fermat-Pell denklemi"** ya da kısaca **"Pell denklemi"** denir.

Teorem 3.1.9 : $f=(a,b,c)$, d diskriminantlı pirimitif bir form olsun. $M \in SL_2(\mathbb{Z})$ ve $(x_0,y_0)\in\mathbb{Z}^2$ de $x^2-dy^2=4$ Pell denkleminin bir çözümü olmak üzere

$$M \in Aut^+(f) \Leftrightarrow M=\begin{bmatrix} \frac{x_0-by_0}{2} & -cy_0 \\ ay_0 & \frac{x_0+by_0}{2} \end{bmatrix} \text{ olmasıdır.}$$

Kanıt : $\frac{x_0-by_0}{2}, \frac{x_0+by_0}{2} \in \mathbb{Z}$ ve $\det M=1$ olduğunu göstermemiz gerekir.

$$x_0^2-dy_0^2=4 \Rightarrow x_0^2-(b^2-4ac)y_0^2=4$$
$$\Rightarrow x_0^2-b^2y_0^2+4ac=4$$
$$\Rightarrow x_0^2-b^2y_0^2=4(1-ac)$$
$$\Rightarrow 4 \mid x_0^2-b^2y_0^2$$
$$\Rightarrow \exists k\in\mathbb{Z} \ni x^2-b^2y^2=4k \text{ elde edilir.}$$

$x_0^2-b^2y_0^2=4k \Rightarrow \left(\frac{x_0-by_0}{2}\right)\left(\frac{x_0+by_0}{2}\right)=k$ olup $2 \nmid x_0-by_0$ olduğu var sayılarak $4 \nmid x_0^2-by_0^2$ çelişkisi elde edilir. $\therefore \frac{x_0-by_0}{2}\in\mathbb{Z}$ dir. Benzer işlemler $\frac{x_0+by_0}{2}$ için

de yapılırsa $\frac{x_0 + by_0}{2} \in \mathbb{Z}$ olduğu görülebilir. Bununla birlikte $\det M = \frac{x_0 - b^2 y_0^2}{4} + acy_0^2 = \frac{x_0^2 - dy_0^2}{4} = 1$ dir. Bu nedenle

$$M = \begin{bmatrix} \frac{x_0 - by_0}{2} & -cy_0 \\ ay_0 & \frac{x_0 + by_0}{2} \end{bmatrix} \in SL_2(\mathbb{Z})$$

dir.

$\Rightarrow$: $M = \begin{bmatrix} r & s \\ m & n \end{bmatrix}$, f nin has otomorfu olsun. $f(\varphi(M)) = f(x,y)$ olduğundan

$$(a,b,c) = \left(ar^2 + brm + cm^2\right)x^2 + \left(2ars + (rn + sm)b + 2cmn\right)xy$$
$$+\left(as^2 + bsn + cn^2\right)y^2 \text{ dir.}$$

$\det M = rn - sm = 1 \Rightarrow rn = 1 + sm$ olup bu eşitlik b de yerine yazıldığında

$b = 2ars + (1 + 2sm)b + 2cmn \Rightarrow 0 = ars + bsm + cmn$ elde edilir. Bu durumda

$$a = ar^2 + brm + cm^2$$
$$0 = ars + bsm + cmn$$

eşitlikleri bulunur. Birinci eşitlik s, ikinci eşitlik $-r$ ile çarpılıp taraf taraf toplanırsa $as = -cm$ (*) eşitliği ve birinci eşitlik n ikinci eşitlik m ile çarpılırsa $bm = a(n - r)$ (**) eşitliği elde edilir. (*) ve (**) eşitliklerinden $a \mid cm$ ve $a \mid bm$ olup $ebob(a,b,c) = 1$ olduğundan $a \mid m$ dir.

$a \mid m \Rightarrow \exists y_0 \in \mathbb{Z} \ni m = ay_0$ dir . (*) dan $as = -cm = -cay_0 \Rightarrow s = -cy_0$ ve (**) dan

$a(n - r) = bm = bay_0 \Rightarrow n - r = by_0$ elde edilir. Böylece

$$(n + r)^2 = (n - r)^2 + 4nr$$
$$= b^2 {y_0}^2 + 4nr$$
$$= b^2 {y_0}^2 + 4(1 + sm)$$
$$= b^2 {y_0}^2 + 4\left(1 + (-cy_0)(ay_0)\right)$$
$$= b^2 {y_0}^2 + 4\left(1 - ac{y_0}^2\right)$$

$$= \underbrace{\left(b^2 - 4ac\right)}_{d} y_0{}^2 + 4$$

$$= dy_0{}^2 + 4 \quad \text{bulunur.}$$

$n = \dfrac{x_0 - by_0}{2}$ ve $r = \dfrac{x_0 + by_0}{2}$ olmak üzere $x_0 = n + r$ olup $(n+r)^2 = dy_0{}^2 + 4 \Rightarrow x_0{}^2 - dy_0{}^2 = 4$ olduğundan Pell denkleminin bir çözümüdür.

$\Leftarrow$: $(x_0, y_0) \in \mathbb{Z}^2$, $x^2 - dy^2 = 4$ Pell denkleminin bir çözümü olmak üzere

$$M = \begin{bmatrix} \dfrac{x_0 - by_0}{2} & -cy_0 \\ ay_0 & \dfrac{x_0 + by_0}{2} \end{bmatrix} \in SL_2(\mathbb{Z})$$ olsun. $M \in Aut^+(f)$ olduğu gösterilmelidir.

$\phi(f, M) = g = (a_1, b_1, c_1)$ olsun. Bu durumda

$$a_1 = a\left(\frac{x_0 - by_0}{2}\right) + b\left(\frac{x_0 - by_0}{2}\right)(ay_0) + ca^2 y_0{}^2 = \frac{a}{4}\left(x_0{}^2 - \left(b^2 - 4ac\right) y_0{}^2\right)$$

$$= \frac{a}{4}\left(x_0{}^2 - dy_0{}^2\right) = \frac{a}{4}.4 = a \text{ ve}$$

$$b_1 = 2a\left(\frac{x_0 - by_0}{2}\right)(-cy_0) + b\left(1 + 2(-cy_0)(ay_0)\right) + 2c(ay_0)\left(\frac{x_0 + by_0}{2}\right) = b$$

$f \sim g$ olduğundan $d(f) = d(g)$ olup $a_1 = a$ ve $b_1 = b$ iken $c_1 = c$ elde edilir.

$$\therefore M = \begin{bmatrix} \dfrac{x_0 - by_0}{2} & -cy_0 \\ ay_0 & \dfrac{x_0 + by_0}{2} \end{bmatrix} \in Aut^+(f) \text{ dir.}$$

$\det M = -1$ olan $A \in GL_2(\mathbb{Z})$ matrisinin $Aut(f)$ de olması için gerekli ve yeterli koşul $(x_0, y_0) \in \mathbb{Z}^2$, $x^2 - dy^2 = -4$ Pell denkleminin bir çözümü olmak üzere

$$M = \begin{bmatrix} \dfrac{x_0 - by_0}{2} & -cy_0 \\ ay_0 & \dfrac{x_0 + by_0}{2} \end{bmatrix}$$ olmasıdır. Kanıtı Teorem 3.1.9 a benzer şekilde yapılır.

Yukarıda tanımlanan M matrisini bundan sonra

$$U(f,x,y)=\begin{bmatrix} \dfrac{x-by}{2} & -cy \\ ay & \dfrac{x+by}{2} \end{bmatrix}$$

ile göstereceğiz.

Teorem 3.1.10 : f pirimitif bir form olsun.

1. $x^2-dy^2=\pm 4$ Pell denkleminin çözümlerini $U(f,x,y)\in Aut(f)$ ye dönüştüren dönüşüm 1-1 ve örtendir.

2. $x^2-dy^2=4$ Pell denkleminin çözümlerini $U(f,x,y)\in Aut^{+}(f)$ ye dönüştüren dönüşüm 1-1 ve örtendir.

Kanıt :

$B=\left\{(x_0,y_0)\in\mathbb{Z}^2 \,\middle|\, x_0^2-dy_0^2=\pm 4\right\}$ olmak üzere

$$h: B\to Aut(f)$$

$$(x,y)\mapsto h(x,y)=U(f,x,y)$$

biçiminde bir h dönüşümü tanımlıyalım.

$(x_1,y_1),(x_2,y_2)\in B$ için $(x_1,y_1)=(x_2,y_2)\Leftrightarrow x_1=x_2, y_1=y_2$ olup

$$h(x_1,y_1)=U(f,x_1,y_1)=\begin{bmatrix} \dfrac{x_1-by_1}{2} & -cy_1 \\ ay_1 & \dfrac{x_1+by_1}{2} \end{bmatrix}$$

$$=\begin{bmatrix} \dfrac{x_2-by_2}{2} & -cy_2 \\ ay_2 & \dfrac{x_2+by_2}{2} \end{bmatrix}=U(f,x_2,y_2)=h(x_2,y_2)$$

$\therefore h$ iyi tanımlıdır.

$(x_1,y_1),(x_2,y_2)\in B$ için $h(x_1,y_1)=h(x_2,y_2)\Leftrightarrow U(f,x_1,y_1)=U(f,x_2,y_2)$ dir.

$$U(f,x_1,y_1)=U(f,x_2,y_2)\Leftrightarrow\begin{bmatrix}\frac{x_1-by_1}{2} & -cy_1\\ ay_1 & \frac{x_1+by_1}{2}\end{bmatrix}=\begin{bmatrix}\frac{x_2-by_2}{2} & -cy_2\\ ay_2 & \frac{x_2+by_2}{2}\end{bmatrix}$$ olup $a=0$

ve $c=0$ iken $ebob(a,b,c)=1$ olduğundan $b=1$ olmalıdır. Bu durumda son eşitlikte $a=0$, $c=0$ ve $b=1$ yerine yazıldığında

$$\begin{bmatrix}\frac{x_1-y_1}{2} & 0\\ 0 & \frac{x_1+y_1}{2}\end{bmatrix}=\begin{bmatrix}\frac{x_2-y_2}{2} & 0\\ 0 & \frac{x_2+y_2}{2}\end{bmatrix}$$

elde edilir. Matris eşitliğinden $(x_1,y_1)=(x_2,y_2)$ olduğu görülür.

$a\neq 0$ olsun. Bu durumda $ay_1=ay_2$ olduğundan $y_1=y_2$ dir. $y_1=y_2$ olması durumunda

$\frac{x_1-by_1}{2}=\frac{x_2-by_2}{2}\Rightarrow x_1-x_2=b(y_1-y_2)\Rightarrow x_1=x_2$ elde edilir.

$\therefore h$ 1-1, dir.

$U\in Aut(f)$ olsun. Teorem 3.1.9 den $\exists(x_0,y_0)\in\mathbb{Z}^2$ ə $x_0^2-dy_0^2=\pm 4$ için

$h(x_0,y_0)=\begin{bmatrix}\frac{x_0-by_0}{2} & -cy_0\\ ay_0 & \frac{x_0+by_0}{2}\end{bmatrix}$ dir.

$\therefore h$ örtendir.

Örnek : $d\equiv 0(\mathrm{mod}\,4)$ olsun. Bu durumda $f=\left(1,0,-d/4\right)$ formu d diskriminantlı bir formdur. $(x_0,y_0)\in\mathbb{Z}^2$, $x^2-dy^2=\pm 4$ Pell denkleminin bir çözümü ise Teorem 3.1.9 den

$$U(f,x_0,y_0)=\begin{bmatrix}x_0/2 & dy_0/2\\ y_0 & x_0/2\end{bmatrix}$$

dir. Tersine

$$\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\in Aut(f)$$

ise $(x_0, y_0) = (2\alpha, \gamma)$ $x^2 - dy^2 = \pm 4$ Pell denkleminin bir çözümüdür.

Teorem 3.1.11 : Aynı diskriminantlı tüm pirimitif formların otomorflar grubu birbirine izomorftur.

Kanıt : f ve g, d diskriminantlı tam katsayılı iki pirimitif form olsun. Bu durumda $Aut(f)$ ve $Aut(g)$ aynı $x^2 - dy^2 = \pm 4$ Pell denkleminin çözümleri ile üretilir. (x, y) ve (a, b) $x^2 - dy^2 = \pm 4$ Pell denkleminin iki çözümü ise $\left((xa + ybd)/2 , (xb + ay)/2 \right)$ ikilisi de $\left(\frac{xa + byd}{2} \right)^2 - d\left(\frac{xb + ay}{2} \right)^2 = \frac{\left(x^2 - dy^2\right)\left(a^2 - db^2\right)}{4} = \pm 4$ olduğundan $x^2 - dy^2 = \pm 4$ Pell denkleminin diğer bir çözümüdür. Bu durumda $\left((xa + ybd)/2 , (xb + ay)/2 \right)$ bir önceki teoremde tanımladığımız B kümesinin bir elemanıdır. B üzerinde $\otimes$ işlemi

$$(x, y) \otimes (a, b) = \left((xa + ybd)/2 , (xb + ay)/2 \right)$$

biçiminde tanımlansın.

$\forall (x_1, y_1), (x_2, y_2), (a_1, b_1), (a_2, b_2) \in B$ için

$$((x_1, y_1), (a_1, b_1)) = ((x_2, y_2), (a_2, b_2)) \Leftrightarrow (x_1, y_1) = (x_2, y_2) \text{ ve } (a_1, b_1) = (a_2, b_2)$$

$$\Leftrightarrow (x_1 = x_2 \text{ ve } y_1 = y_2) \text{ ve } (a_1 = a_2 \text{ ve } b_1 = b_2)$$

dir.

$$(x_1, y_1) \otimes (a_1, b_1) = \left((x_1 a_1 + y_1 b_1 d)/2 , (x_1 b_1 + a_1 y_1)/2 \right)$$

$$= \left((x_2 a_2 + y_2 b_2 d)/2 , (x_2 b_2 + a_2 y_2)/2 \right)$$

$$= (x_2, y_2) \otimes (a_2, b_2)$$

olduğundan $\otimes$ iyi tanımlıdır.

$\forall (a_1, b_1), (a_2, b_2), (a_3, b_3) \in B$ için

$$((a_1, b_1) \otimes (a_2, b_2)) \otimes (a_3, b_3) = (a_1, b_1) \otimes ((a_2, b_2) \otimes (a_3, b_3))$$

olduğundan $\otimes$ işleminin birleşme özelliği vardır.

$(x,y)\in B$ için $(x,y)\otimes(a,b)=\left(\left.(xa+ybd)\right/2\,,\left.xb+ay\right/2\right)=(x,y)$

$$\Rightarrow \frac{xa+ybd}{2}=x \text{ ve } \frac{xb+ay}{2}=y$$

$$\Rightarrow xa+ybd=2x \text{ ve } xb+ay=2y \text{ dir.}$$

$$\left.\begin{matrix} xa+ybd=2x \\ xb+ay=2y \end{matrix}\right\}\Rightarrow\begin{bmatrix} x & yd \\ y & x \end{bmatrix}\cdot\begin{bmatrix} a \\ b \end{bmatrix}=\begin{bmatrix} 2x \\ 2y \end{bmatrix}$$

olup buradan

$$a=\frac{\begin{vmatrix} 2x & yd \\ 2y & x \end{vmatrix}}{\begin{vmatrix} x & yd \\ y & x \end{vmatrix}}=\frac{2\left(x^2-dy^2\right)}{x^2-dy^2}=2,\ b=\frac{\begin{vmatrix} x & 2x \\ y & 2y \end{vmatrix}}{\begin{vmatrix} x & yd \\ y & x \end{vmatrix}}=0 \text{ elde edilir.}$$

$\forall(x,y),(a,b)\in B$ için

$$(x,y)\otimes(a,b)=\left(\left.(xa+ybd)\right/2\,,\left.(xb+ay)\right/2\right)$$

$$=\left(\left.(ax+byd)\right/2\,,\left.(ay+xb)\right/2\right)$$

$$=(a,b)\otimes(x,y)$$

olduğundan $\otimes$ işlemi değişmeli olup $\forall(x,y)\in B$ için $\exists(a,b)=(2,0)\in B$

$\ni (x,y)\otimes(a,b)=(a,b)\otimes(x,y)=(x,y)$ dir.

$\therefore \otimes$ işleminin etkisiz elemanı vardır.

$(x,y)\in B$ için $(x,y)\otimes(a,b)=\left(\left.(xa+ybd)\right/2\,,\left.(xb+ay)\right/2\right)=(2,0)$

$\Rightarrow(a,b)=(\pm x,\pm y)\in B$ olup $\otimes$ işleminin ters elemanı vardır.

$\therefore(B,\otimes)$ değişmeli gruptur.

Teorem 3.1.10 da tanımlanan $h:B\to Aut(f)$, B ve $Aut(f)$ grupları arasında 1-1 ve örten bir fonksiyon olup $(x,y),(s,t)\in B$ için

$$h\big((x,y)\otimes(s,t)\big)=h\left(\left.(xs+ytd)\right/2\,,\left.(xt+sy)\right/2\right)$$

$$= U\left(f, {(xs+ytd)}/{2}, {(xt+sy)}/{2} \right)$$

$$= \begin{bmatrix} \dfrac{\dfrac{(xs+ytd)}{2} - \dfrac{(xt+sy)}{2}b}{2} & -c\dfrac{(xt+sy)}{2} \\ a\dfrac{(xt+sy)}{2} & \dfrac{\dfrac{(xs+ytd)}{2} + \dfrac{(xt+sy)}{2}b}{2} \end{bmatrix}$$

$$= \begin{bmatrix} \dfrac{x-yb}{2} & -cy \\ ay & \dfrac{x+yb}{2} \end{bmatrix} . \begin{bmatrix} \dfrac{s-tb}{2} & -ct \\ at & \dfrac{s+tb}{2} \end{bmatrix}$$

$$= U(f,x,y).U(f,s,t)$$

$$= h(x,y).h(s,t)$$

olduğundan grup izomorfizmasıdır. Bu nedenle $A \cong Aut(f)$ dir. Benzer şekilde $A \cong Aut(g)$ olduğu da görülebilir.

$\therefore A \cong Aut(f)$ ve $A \cong Aut(g)$ olduğundan $Aut(f) \cong Aut(g)$ dir.

Bu teoremin bir sonucu olarak aynı diskriminantlı iki formun otomorflarının sayısının aynı olduğu söylenebilir.

3.2 Pozitif Belirli Formların Otomorfları

Bu bölümde tam katsayılı pozitif belirli formların otomorflarını tanımlıyacağız. $f=(a,b,c)$ pozitif belirli bir form ve $U\in Aut(f)$ ise $f=\phi(f,U)$ olup her $(x,y)\in\mathbb{Z}^2$ için $f(x,y)\geq 0$ olduğundan $f=\phi(f,U)$ olması için $\det U=1$ olmalıdır. Bu nedenle pozitif belirli formların otomorfları has otomorflardır. Önceki bölümde verilen d diskriminantlı $f=(a,b,c)$ formunun otomorfları ile $x^2-dy^2=\pm 4$ Pell denklemi arsındaki ilişkiden yararlanılarak pozitif belirli formların otomorfları tespit edilebilir.

Örnek : Tam katsayılı -4 diskriminantlı pirimitif formların otomorflarını belirleyiniz.
Önceki teoremden tüm -4 diskriminantlı tam katsayılı pirimitif formların otomorflar grubu birbirine izomorf olduğundan -4 diskriminantlı pozitif belirli form olarak $f=(1,0,1)$ formu alınabilir. Bu formun otomorfları $x^2+4y^2=4$ Pell denkleminin çözümleriyle elde edilip $x^2+4y^2=4$ denkleminin çözümleri sadece $(\pm 2,0)$ ve $(0,\pm 1)$ olduğundan f nin otomorflar grubu

$$Aut(f)=\left\{\pm\begin{bmatrix}1&0\\0&1\end{bmatrix},\pm\begin{bmatrix}0&1\\-1&0\end{bmatrix}\right\}$$

dir. Bu otomorflar grubu devirli olup dördüncü mertebeden $T=\begin{bmatrix}0&-1\\1&0\end{bmatrix}$ matrisi ile üretilir.

Örnek : Tam katsayılı -3 diskriminantlı pirimtif formların otomorflarını belirleyiniz.
-3 diskriminantlı tüm pirimitif formların otomorflar grubu birbirine izomorf olduğundan -3 diskriminantlı pozitif belirli form olarak $f=(1,1,1)$ formu alınabilir. Bu formun otomorfları $x^2+3y^2=4$ Pell denkleminin çözümleriyle elde edilip $x^2+3y^2=4$ denkleminin çözümleri $(\pm 1,\pm 1)$ ve $(\pm 2,0)$ olduğundan f nin otomorflar grubu

$$Aut(f)=\left\{\pm\begin{bmatrix}1&0\\0&1\end{bmatrix},\pm\begin{bmatrix}0&-1\\1&1\end{bmatrix},\pm\begin{bmatrix}1&1\\-1&0\end{bmatrix}\right\}$$

dir. Bu otomorflar grubu devirli grup olup altıncı mertebeden $TS = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ ile üretilmiştir.

Teorem 3.2.1 : f , $d \neq -3,-4$ olmak üzere d diskriminantlı pozitif belirli form ise f nin otomorflar grubu aşikardır.

Kanıt : f pozitif belirli bir form ise $d < 0$ olduğundan $x^2 - dy^2 = 4 \Rightarrow x^2 - |d| y^2 = 4$ olup $|d| \geq 5$ için $x^2 - |d| y^2 = 4$ denkleminin tek çözümü $(\pm 2, 0)$ dir. Bu nedenle f nin otomorflarının grubu $Aut(f) = \{\pm I_{2x2}\}$ olduğundan aşikardır.

d diskriminantlı pozitif belirli f formunun otomorflarının sayısı "$w(f)$" ile gösterilir ve diskriminant değerine göre

$$w(f) = \begin{cases} 6, & d = -3 \quad \text{ise} \\ 4, & d = -4 \quad \text{ise} \\ 2, & d \neq -3,-4 \quad \text{ise} \end{cases}$$

değerlerini alır.

3.3 Belirsiz Formların Otomorfları

$d>0$ diskriminantlı f belirsiz formunun otomorflar grubunu Pell denklemi ile bulmak oldukça zor olduğundan bu bölümde f nin otomorflar grubunu farklı bir yöntemle belirleyeceğiz.

$A>0$ ve $f_0=(A,B,C)$ indirgenmiş form olmak üzere $f_0=\varphi(f,U)$ sağlayan $U\in GL_2(\mathbb{Z})$ olsun. f nin devrinin $(f_0, f_1, f_2,..., f_{l-1})$ olduğunu varsayalım. T_l ikinci bölümde tanımlanan matris olmak üzere $\phi(f_0,T_l)=f_0$ dir. Bu durumda T_l, f_0 ın otomorfudur.

$$\phi(f_0,T_l)=f_0 \underset{f_0=\phi(f,U)}{\Rightarrow} \phi(f,UT_l)=\phi(f,U) \underset{U\in GL_2(\mathbb{Z})}{\Rightarrow} \phi(f,UT_lU^{-1})=f$$

olduğundan $T=UT_lU^{-1}$, f nin otomorfudur. Bu otomorfa **“ f nin temel otomorfu”** denir.

Önerme 3.3.1 : $\langle T\rangle=\{T^i \mid i\in\mathbb{Z}\}$ devirli grubu sonsuz elemanlıdır ve l, f nin periyodu olmak üzere $\det(T)=(-1)^l$ dir.

Kanıt : $i\in\mathbb{Z}$ için $T^i=UT_l^iU^{-1}$ ve

$$T_l=\prod_{i=0}^{l-1}\begin{bmatrix}0 & 1\\ 1 & |s(f_i)|\end{bmatrix} \tag{3.5}$$

dir. (3.5) ve Önerme 2.2.19 den T nin ilk satır ve ilk sütunu pozitiftir. Bu da T^i nin ikinci satır ve ikinci sütununun artan bir dizi olmasını gerektirir. Bu nedenle $i\geq 0$ için T^i ler birbirinden farklıdır. O halde $\langle T\rangle$ sonsuz elemanlı bir devirdir. Bununla birlikte

$\begin{bmatrix}0 & 1\\ 1 & |s(f_i)|\end{bmatrix}$ nin determinantı -1 olup $\det(T)=(-1)^l$ dir.

Örnek : $f=(1,7,-6)$ formunun temel otomorfu aşağıdaki biçimde bulunur.

$f=(1,7,-6)$ formunun periyodu $l=9$ olup $p_{i+2}=s_i p_{i+1}+p_i$ ve $q_{i+2}=s_i q_{i+1}+q_i$ rekürans bağıntılarından yararlanılarak $T=T_l=\begin{bmatrix} p_9 & p_{10} \\ q_9 & q_{10} \end{bmatrix}$ matrisi bulunmalıdır. Rekürans bağıntılarından $p_9=193$, $p_{10}=1500$, $q_9=250$, $q_{10}=1943$ olarak bulunur. Bu durumda $T=\begin{bmatrix} 193 & 1500 \\ 250 & 1943 \end{bmatrix}$ olup $\det(T)=(-1)^9=-1$ dir.

Örnek : $f=(1,8,-3)$ formunun temel otomorfu aşağıdaki biçimde bulunur.

$f=(1,8,-3)$ formunun periyodu $l=6$ olup $p_{i+2}=s_i p_{i+1}+p_i$ ve $q_{i+2}=s_i q_{i+1}+q_i$ rekürans bağıntılarından yararlanılarak $T=T_l=\begin{bmatrix} p_6 & p_7 \\ q_6 & q_7 \end{bmatrix}$ matrisi bulunmalıdır. Rekürans bağıntılarından $p_6=14$, $p_7=117$, $q_6=39$, $q_7=326$ olarak bulunur. Bu durumda $T=\begin{bmatrix} 14 & 117 \\ 39 & 326 \end{bmatrix}$ olup $\det(T)=(-1)^6=1$ dir.

Sonuç 3.3.2 : l, $f=(a,b,c)$ belirsiz formunun periyodu ve T de f nin temel otomorfu olsun. l tek ise $k\in\mathbb{Z}$ için $T^{2k}\in Aut^+(f)$ ve $T^{2k+1}\in Aut(f)$ olup l çift ise her $k\in\mathbb{Z}$ için $T^k\in Aut^+(f)$ dir.

Kanıt : l tek ise $\det T=(-1)^l=-1$ dir. $T\in Aut(f)$ olup her $k\in\mathbb{Z}$ için $T^k\in Aut(f)$ dir. Budurumda $k\in\mathbb{Z}$ için $\det T^{2k}=1$ ve $\det T^{2k+1}=-1$ olduğundan $T^{2k}\in Aut^+(f)$ ve $T^{2k+1}\in Aut(f)$ olarak bulunur. Benzer biçimde l çift ise $\det T=(-1)^l=1$ olup her $k\in\mathbb{Z}$ için $\det T^k=1$ olduğundan $T^k\in Aut(f)$ dir.

IV. BÖLÜM
POZİTİF BELİRLİ FORM İLE TEMSİL EDİLEN BİR SAYININ BÖLENLERİ VE KUADRATİK FORMLAR İÇİN MASS FORMÜLÜ

Bu bölümde $d \le -11$ diskriminantlı pozitif belirli bir formla temsil edilen bir sayının asal çarpanlarından birinin de aynı formla temsil edilebileceğini ve $n \in \mathbb{Z}_+$ olmak üzere n yi temsil eden tüm d diskriminantlı formların sayısının nasıl hesaplanacağını göstereceğiz.

4.1 Pozitif Belirli Form İle Temsil Edilen Bir Sayının Bölenleri

Tanım 4.1.1 : Aynı diskriminantlı iki pirimitif formu, diskriminantı aynı olan üçüncü bir pirimitif forma dönüştüren ikili dönüşüme **"bileşke"** denir.

Bununla birlikte $(\alpha,\beta) \in \mathbb{Z}^2$, r nin $f=(a,b,c)$ ile öz temsili ise $\alpha\omega - \beta z = 1$ sağlayan $\omega, z \in \mathbb{Z}$ var olduğundan $f \sim f' = (r,s,t)$ olacak biçimde $\exists s,t \in \mathbb{Z}$ vardır.

Örnek : $f=(3,2,1)$ formu $d=-8$ diskriminantlı olup $(1,1) \in \mathbb{Z}^2$, 6 nın bir öz temsilidir. $f \sim f' = (6,s,t)$ olması için $M = \begin{bmatrix} \alpha & \beta \\ z & w \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ z & w \end{bmatrix} \in SL_2(\mathbb{Z})$ olacak şekilde $z, \omega \in \mathbb{Z}$ bulunmalıdır. $f(1,z) = 6 \Rightarrow z = 1$ ve $z=1$ için $\det M = 1$ olduğundan $\omega = 2$ olarak bulunur. Bu durumda $\phi\left(f, \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\right) = (6,16,11)$ olur.

Teorem 4.1.2 : $f_1 = (a_1,b_1,c_1)$ ve $f_2 = (a_2,b_2,c_2)$ olmak üzere $\beta = {(b_1+b_2)}/{2}$, $m = ebob(a,\beta)$ ve $n = ebob(m,a_2)$ olsun. Bununla birlikte $a_1x + \beta y = m$ nin x, y çözümü ve z için

$$mz/n \equiv x\left(\frac{b_2-b_1}{2}\right) - c_1 y \left(\bmod a_2/n\right)$$

çözümü verilsin. f_1 ve f_2 formlarının bileşkeleri, üçüncü katsayısı diskriminant formülüyle hesaplanan

$$\left({}^{a_1 a_2}\!/_{n^2}, b_1 + 2a_1 {}^{z}\!/_{n}, * \right)$$

formudur.

Örnek : $d = -8$ diskriminantlı $f_1 = (3,2,1)$ ve $f_2 = (3,-4,2)$ formlarının bileşkesini bulunuz.

$\beta = \dfrac{2-4}{2} = -1$, $m = ebob(3,-1)$, $n = ebob(1,3)$ ve $a_1 x + \beta y = m \Rightarrow 3x - y = 1$ dir. $(x, y) = (1,2)$, $3x - y = 1$ denkleminin bir çözümü olup bu değerler için $z \equiv -5 \equiv 1 (\mathrm{mod}\, 3)$ olarak bulunur. Eğer $z = 1$ olarak alınırsa

$$f_1 \circ f_2 = \left({}^{3.3}\!/_{1}, 2 + 2.3.1, * \right) = (9,8,*)$$

elde edilir ve buradan diskriminant formülünden * değerinin 2 olduğu görülebilir.

Tanım 4.1.3 : (a_1, b_1, c_1) ve (a_2, b_2, c_2) aynı diskriminantlı iki form olsun. Eğer $ebob\left(a_1, a_2, \dfrac{b_1 + b_2}{2} \right) = 1$ ise bu iki forma **"united formlar"** denir.

Önerme 4.1.4 : (a_1, b_1, c_1) ve (a_2, b_2, c_2) united formlar ise

$$(a_1, b_1, c_1) \sim (a_1, B, a_2 C)$$

$$(a_2, b_2, c_2) \sim (a_2, B, a_1 C)$$

olacak şekilde $(a_1, B, a_2 C)$ ve $(a_2, B, a_1 C)$ formları vardır.

Kanıt : Böyle bir B tamsayısının var olduğunu göstermek için

$$B \equiv b_1 (\mathrm{mod}\, 2a_1)$$

$$B \equiv b_2 (\mathrm{mod}\, 2a_2)$$

kongrüanslarından yararlanılır. İlk kongrüanstan $\exists \delta_1 \in \mathbb{Z}$ için $B = b_1 + 2a_1 \delta_1$ dir. İlk kongrüanstan elde ettiğimiz B değerini ikinci kongrüansta yerine yazarsak

$$B = b_1 + 2a_1 \delta_1 \equiv b_2 (\mathrm{mod}\, 2a_2) \Leftrightarrow 2a_2 \mid b_1 + 2a_1 \delta_1 - b_2$$

$$\Leftrightarrow \exists \delta_2 \in \mathbb{Z} \ni b_1 - b_2 + 2a_1 \delta_1 = 2a_2 \delta_2$$

$$\Leftrightarrow \frac{b_1-b_2}{2} \equiv -a_1\delta_1 \left(\bmod 2a_2\right)$$

elde edilir. $\frac{b_1-b_2}{2} \equiv -a_1\delta_1 \left(\bmod 2a_2\right)$ kongrüansının çözülmesi için a_1 ve a_2' nin en büyük ortak böleninin $\frac{b_1-b_2}{2}$ yi bölmesi gerekir.

$$d = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2 \Rightarrow \left(\frac{b_1-b_2}{2}\right).\left(\frac{b_1+b_2}{2}\right) = a_1c_1 - a_2c_2$$

olup formlar united olduğundan $ebob\left(a_1, a_2, \frac{b_1+b_2}{2}\right) = 1$ dir. Buradan $ebob\left(a_1, a_2\right) = m \neq 1$ ise

$$m \mid a_1c_1 - a_2c_2 \underset{m \nmid \frac{b_1+b_2}{2}}{\Rightarrow} m \mid \frac{b_1-b_2}{2}$$

olduğu görülür. $k = {a_1a_2}/{m}$ olsun. Yukarıdaki B değeri $\bmod 2k$ ya göre teklikle belirlidir. $B \equiv B_0 \left(\bmod 2k\right) \Rightarrow \exists t \in \mathbb{Z} \ni B = B_0 + 2kt$ olduğundan

$$B^2 \equiv B_0^2 + 4B_0kt + 4k^2t \equiv B_0 \equiv d \left(\bmod 4k\right)$$

dır. Şimdi $C \in \mathbb{Z}$ olmasını garanti etmek için $B^2 \equiv B_0^2 \left(\bmod 4a_1a_2\right)$ olacak şekilde $t \in \mathbb{Z}$ seçilmelidir.

$$B^2 \equiv d \left(\bmod 4a_1a_2\right) \Rightarrow 4a_1a_2 \mid B^2 - d$$

$$\Rightarrow \exists s \in \mathbb{Z} \ni B^2 - d = 4a_1a_2s$$

$$\underset{ebob(a_1,a_2)=m}{\Rightarrow} \frac{B^2-d}{4k} = 4ks$$

$$\Rightarrow \frac{B^2-d}{4k} = ms$$

$$\underset{B=B_0+2kt}{\Rightarrow} \frac{B_0^2 + 4B_0kt + 4k^2t^2 - d}{4k} = ms$$

$$\Rightarrow \frac{B_0^2-d}{4k} = -B_0t - kt^2 + ds$$

$$\Rightarrow \frac{d-B_0^2}{4k} = B_0t + kt^2 - ds$$

$$\underset{m|k}{\Rightarrow}\frac{d-B_0^2}{4k}\equiv B_0 t\left(\bmod m\right)$$

elde edilir. $B_0 = B-2kt$ olduğundan $\frac{d-B_0^2}{4k}\in\mathbb{Z}$ olup B_0 ın tanımından ve formların united oluşundan B_0 modülo m ye göre tersinirdir.

Bu durumda $t\equiv\left(\frac{d-B_0^2}{4k}\right)B_0^{-1}\left(\bmod m\right)$ olup üçüncü katsayı da diskriminant formülünden bulunur.

Örnek : $(3,2,1)$ ve $(6,8,3)$ formlarının bileşkesi aşağıdaki biçimde bulunur.

$ebob\left(3,6,\frac{2+8}{2}\right)=1$ olduğundan $(3,2,1)$ ve $(6,8,3)$ formları united dir.

$m=ebob(3,6)=3,\quad k=a_1a_2\big/_m=3.6\big/_3=6$ olup

$B^2\equiv B_0^2\equiv -8\left(\bmod 24\right)\Rightarrow B_0^2\equiv 16\left(\bmod 24\right)$ elde edilir. $B_0=4$ olarak seçildiğinde $B_0=4\equiv 1\left(\bmod 3\right)$ olduğundan $t\equiv 2\left(\bmod 3\right)$ olarak bulunur. $t=2$ olarak seçilirse $B=B_0+2kt=28$ ve diskriminanttan $a_2C=6.11\Rightarrow C=11$ olarak bulunur.

$\therefore (a_1,B,a_2C)=(3,28,66)$ dır.

Öte yandan $(3,28,66)$ formuna $S^n=\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}$ ve $T=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$ matrislerine karşılık gelen matris dönüşümleri uygulandığında $(3,28,66)$ formunun $(3,2,1)$ formuna denk olduğu görülebilir.

$f_1=(a_1,B,a_2C)$ ve $f_2=(a_2,B,a_1C)$ iki united form ise

$$\begin{bmatrix}X\\ Y\end{bmatrix}=\begin{bmatrix}1 & 0 & 0 & -C\\ 0 & a_1 & a_2 & B\end{bmatrix}.\begin{bmatrix}x_1x_2\\ x_1y_2\\ y_1x_2\\ y_1y_2\end{bmatrix}$$

dönüşümü altında

$$\left(a_1x_1^2+Bx_1y_1+a_2Cy_1^2\right).\left(a_2x_2^2+Bx_2y_2+a_1Cy_2^2\right)=\left(a_1a_2X^2+BXY+CY^2\right)$$

denklemi elde edilir. Burada $X = x_1x_2 - Cy_1y_2$, $Y = a_1x_1y_2 + a_2y_1x_2 + By_1y_2$ olup f_1 ve f_2 formlarının bileşkesi $f_1 \circ f_2 = (a_1a_2, B, C)$ olarak tanımlanır.

Örnek : $f_1 = (3, 28, 6)$ ve $f_2 = (6, 28, 33)$ united formlarının bileşkesi aşağıdaki biçimde hesaplanır.

$B = 28$, $C = 11$ olduğundan $f_1 \circ f_2 = (18, 28, 11)$ olarak bulunur. Öte yandan $f_1(x_1, y_1) = f_1(1,0) = 3$ ve $f_2(x_2, y_2) = f_2(1,1) = 67$ için

$$X = x_1x_2 - Cy_1y_2 = 1.1 - 11.0.1 = 1$$

ve

$$Y = a_1x_1y_2 + a_2y_1x_2 + By_1y_2 = 3.1.1 + 6.0.1 + 11.0 = 3$$

olduğundan $f_1(1,0).f_2(1,1) = F(1,3) = 201$ dir.

Teorem 4.1.5 : $ebob(mn, d) = 1$ ve mn nin d diskriminantlı bir f formuyla öz temsili olsun. f formu, m yi öztemsil eden g ile n yi öztemsil eden h pirimitif formlarının bileşkesidir.

Kanıt : (mn, β, γ) formu göz önüne alınırsa $d = \beta^2 - 4mn\gamma$ olup $ebob(mn, d) = 1$ olduğundan $f \sim (mn, \beta, \gamma)$ dir. Bununla birlikte $ebob(mn, \beta) = 1 \Rightarrow ebob(m, \beta) = 1$ ve $ebob(n, \beta) = 1$ olduğundan $g = (m, \beta, n\gamma)$ ve $h = (n, \beta, m\gamma)$ olarak tanımlandığında g ve h formlarının pirimitif oldukları görülür. Bu durumda bileşke tanımından $g \circ h \sim f$ elde edilir.

Tanım 4.1.6 : $d \in \mathbb{Z}$ olmak üzere d nin çift yada tek oluşuna göre sırasıyla $\left(1, 0, -d/4\right)$ ve $\left(1, 1, (1-d)/4\right)$ formları d diskriminantlı formlar olup bu formlara **"özdeşlik formu"** denir.

Önerme 4.1.7 : $d \leq -11$ ve $p \mid d$ olmak üzere özdeşlik formu p asalını temsil ediyorsa çift diskriminantlar için $p = -d/4$, tek diskriminantlar için $p = -d$ dir.

Kanıt : d çift ise özdeşlik formu $\left(1,0,-d/4\right)$ olup $D=-d/4\in\mathbb{Z}$ için p asalının özdeşlik formuyla bir temsili varsa bu durumda $p=x^2+Dy^2$ dir. $y=0$ iken $p=x^2$ olup buda p nin asal olmasıyla çelişir. $d\le -11$olması $D\ge 3$ olmasını gerektirdiğinden $y\neq 0$ için $p=x^2+Dy^2\ge D\ge 3$ dür. p , 2 den farklı bir asal olup $p\mid d=-4D$ olduğundan $p\mid D$ dir. Bu sebeple $p\le D$ olur ki buradan $p=-d/4$ olarak bulunur. d tek ise özdeşlik formu $\left(1,1,(1-d)/4\right)$ olup $k=(1-d)/4\in\mathbb{Z}$ için p asalının özdeşlik formuyla bir temsili varsa $p=x^2+xy+ky^2$ dir. $d\le -11$ olması $k\ge 3$ olmasını gerektirip $y=0$ için $p=x^2$ olduğundan $y\neq 0$ olmalıdır. Bununla birlikte $x=1$ ve $y=-2$ için $x^2+xy+ky^2=4k-1$ dir. Bu nedenle $p=x^2+xy+ky^2\ge (4k-1)/4=-d/4$ tür. Ancak $p,x,y\in\mathbb{Z}$ olduğundan $p=x^2+xy+ky^2\ge k$ ve bununla birlikte $p\mid 4k-1=-d$ dir.

$k\not\equiv 1\pmod 3$ ise $4k-1\not\equiv 0\pmod 3$ dür. Bu yüzden $4k-1$ in 1 den farklı mümkün olan en küçük böleni 5 olup $4k-1$ in kendinden farklı en büyük böleni $(4k-1)/5$ tir. Ancak $p\ge k>(4k-1)/5$ olduğundan $p=4k-1=-d$ dir.

$k\equiv 7\pmod 9$ ise $4k-1\equiv 0\pmod 9$ dir. Burada 3 ve $(4k-1)/3$, $4k-1$ in bölenleridir. Ancak $(4k-1)/3$, 3 ile bölündüğünden asal değildir.

$k\equiv 1\pmod 3$ iken $k\not\equiv 7\pmod 9$ ise $(4k-1)/3$, 3 ile bölünmez. $(4k-1)/3=4t+1$ olacak şekilde $t=(k-1)/3$ olsun. Bununla birlikte $(3,3,t+1)$ formunu tanımlanırsa 3 ün $4t+1$ ve bu nedenle $t+1$ i bölmediği açıktır. Öte yandan $x=1$ ve $y=-2$ için $3x^2+3xy+(t+1)y^2=4t+1=(4k-1)/3$ tür. $k\ge 3$ için $(4k-1)/3\in\mathbb{Z}$ olduğundan $k\ge 4$ olmalıdır. $k=4$ olduğunda $(3,3,2)\sim(2,1,2)$ özdeşlik değildir. $k>4$ için $(4k-1)/3\in\mathbb{Z}$, $t=(k-1)/3$ ve $k\not\equiv 7\pmod 9$ den $k\ge 10$ olup $(3,3,t+1)$

indirgenmelidir ve bu nedenle özdeşlik formu değildir. Bu nedenle $k \equiv 1 \pmod 3$ ve $k \not\equiv 7 \pmod 9$ ise $(4k-1)/3$ ün asal olması gerekiyorsa özdeşlikle temsil edilemez. Bu durumda $p \neq (4k-1)/3$ olduğundan ya $p \leq (4k-1)/5$ ya da $p = 4k-1$ dir. $p \geq k$ olduğundan $p = 4k-1 = -d$ dir.

Teorem 4.1.8 : $d \leq -11$ olmak üzere p asalının $1 \sim (1,*,*)$ özdeşlik formuyla temsili var olsun. Eğer np çarpımının da aynı d diskriminantlı bir f pirimitif formuyla öz temsili var ise f , n nin öz temsilidir.

Kanıt :

I. Durum : $d \not\equiv 0 \pmod p$ ise

$$f \sim (np, \beta_1, \gamma_1)$$

ve

$$1 \sim (p, \beta_2, \gamma_2)$$

olacak şekilde $\beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{Z}$ vardır. Diskriminanttan dolayı $\beta_2 \not\equiv 0 \pmod p$ olup $\frac{\beta_1 + \beta_2}{2} \equiv 0 \pmod p$ ise β_2 yerine $-\beta_2$ alınarak $\frac{\beta_1 + \beta_2}{2} \not\equiv 0 \pmod p$ olacak şekilde düzenlenebilir. Bu durumda $ebob\left(p, np, (\beta_1 + \beta_2)/2\right) = 1$ olacağından (np, β_1, γ_1) ve (p, β_2, γ_2) formları uniteddir. Önerme 4.1.4 den

$$f \sim (np, \beta_1, \gamma_1) \sim (np, B, pC)$$

ve

$$1 \sim (p, \beta_2, \gamma_2) \sim (p, B, npC)$$

olacak şekilde $B, C \in \mathbb{Z}$ vardır. f pirimitif olduğundan $ebob(n, B, C) = 1$ dir. $g = (n, B, p^2 C)$ formu tanımlanırsa $B \not\equiv 0 \pmod p$ ve $\gcd(n, B, C) = 1$ olduğundan g pirimitiftir.

$$1 \sim (p, B, n(pC))$$

ile

$$g=\left(n,B,p\left(pC\right)\right)$$

kıyaslanırsa $1\circ g\sim\left(np,B,pC\right)\sim f$ elde edilir.

$\therefore 1\circ g\sim f$ tir. Bu nedenle f ve g denk olup n, f nin bir öz temsilidir.

II. Durum : $p\mid d$ ve d çift ise

$$f\sim\left(np,2F,J\right)$$

ve

$$1\sim\left(1,0,p\right)$$

dir. Önerme 4.1.7 den çift d ler için $d=-4p$ olduğundan $1\sim\left(1,0,p\right)$ dir. Bununla birlikte I. Durumda açıklandığı üzere $f\sim\left(np,\beta_1,\gamma_1\right)$ dir.

$$p\mid d=\beta_1^2-4np\gamma_1\Rightarrow\exists s\in\mathbb{Z}\ni\beta_1^2-4np\gamma_1=ps$$

$$\Rightarrow\beta_1^2=ps+4np\gamma_1$$

$\beta_1\in\mathbb{Z}$ olduğundan $k\in\mathbb{Z}$ için $s=4k$ olarak seçilirse

$$\beta_1^2=4kp+4np\gamma_1=4\left(kp+np\gamma_1\right)$$

elde edilir. Bu durunda $kp+np\gamma_1$ tam kare olmalıdır. $F\in\mathbb{Z}$ için $kp+np\gamma_1=F^2$ olarak seçildiğinde $\beta_1=2F$ olup J katsayısı diskriminanttan bulunabilir. $d=-4p=4F^2-4npJ$ olduğundan $p\mid F$ dir. Bu durumda $\exists E\in\mathbb{Z}$ için

$$f\sim\left(np,2pE,J\right)$$

dir.

$$d=-4p=4p^2E^2-4npJ\Rightarrow 4npJ=4p+4p^2E^2$$

$$\Rightarrow 4pnJ=4p\left(1+pE^2\right)$$

$$\Rightarrow nJ=1+pE^2\ \text{ elde edilir.}$$

Buradan $1\sim\left(p,0,1\right)\sim\left(p,2pE,\underbrace{1+pE^2}_{nJ}\right)\sim\left(p,2pE,nJ\right)$ olduğu görülür.

$g=\left(n,2pE,pJ\right)$ formunu tanımlarsak

$$1\circ g=\left(p,2pE,nJ\right)\circ\left(n,2pE,pJ\right)\sim\left(np,2pE,J\right)\sim f$$

elde edilir. $f\sim g$ olduğundan f, n nin bir öz temsilidir.

III. Durum : $p \mid d$ ve d tek ise Önerme 4.1.7 den $d = -p$ ve

$$1 \sim (1,1,k)$$

$$f \sim (np, F, J)$$

dir. $F \equiv 0 \pmod{p}$ olduğundan $\exists E \in \mathbb{Z}$ için $f \sim (np, pE, J)$ olup d nin tek olması E nin tek olmasını gerektirir. Bununla birlikte $d = p^2E^2 - 4npJ = -p \Rightarrow 4nJ = 1 + pE^2$ dir. $k = {(1-p)}/{4}$ olmak üzere $(1,1,k)$ özdeşlik formuna

$$\begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}$$

matris dönüşümü uygulandığında $(1,1,k) \sim (p,-p,k)$ formu elde edilir. E tek olmak üzere $\exists B = pE, C = J \in \mathbb{Z} \ni (p,-p,k) \sim (p, pE, nJ)$ dir. $g = (n, pE, pJ)$ formunu tanımlarsak

$$1 \circ g \sim (p, pE, nJ) \circ (n, pE, pJ) = (np, pE, J) \sim f$$

elde edilir. $f \sim g$ olduğundan f, n nin bir öz temsilidir.

Örnek : $d = -23$ diskriminantlı $f = (2,1,3)$ formuyla temsil edilen 312 sayısının asal bölenlerinden birinin yine $f = (2,1,3)$ formuyla temsil edilebileceğini gösterelim.

$x = 6$ ve $y = 8$ için $f(6,8) = 312$ olup Teorem 4.1.8 i kullanabilmek için f nin öz temsil olması gerekir. $ebob(6,8) = 2$ olduğundan f, $m = {312}/{4} = 78$ in öz temsilidir. m nin asal çarpanlara ayrılışı $m = 78 = 2.3.13$ olup $p = 2,3,13$ için $d \not\equiv 0 \pmod{p}$ olduğundan $\exists \beta, \gamma \in \mathbb{Z}$ için $1 \sim (p, \beta, \gamma)$ dir. Bu durumda p asalının özdeşlik formuyla bir temsili vardır. $p = 2$ için teoremi uygularsak f, 39 un öz temsilidir. Benzer şekilde 3, özdeşlik formuyla temsil edilebileceğinden teoremin ifadesinden f, 13 ün öz temsilidir. Bu durumda $13 = 2x^2 + xy + 3y^2$ dir.

4.2 İkili Kuadratik Formlar İçin Mass Formülü

Teorem 4.2.1 : $k \in \mathbb{Z}_+$, $f=(a,b,c)$, $d<0$ diskriminantlı pozitif belirli pirimitif bir form ve $(x,y)\in\mathbb{Z}^2$ de k nın öz temsili olsun. f yi $g(x,y)=kx^2+lxy+my^2$ formuna dönüştüren $\begin{bmatrix} x & r \\ y & s \end{bmatrix} \in SL_2(\mathbb{Z})$ matrisi için $r,s\in\mathbb{Z}$ tek şekilde belirlidir. Bununla birlikte $0\le l<2k$ için $l^2 \equiv d \pmod{4k}$ sağlayan l için $d=l^2-4km$ olmak üzere tek bir $m\in\mathbb{Z}$ vardır.

Kanıt : f, $d<0$ diskriminantlı pozitif belirli bir form iken $k\in\mathbb{Z}_+$ nın f ile öz temsili $(x,y)\in\mathbb{Z}^2$ olsun. $(x,y)\in\mathbb{Z}^2$, $k\in\mathbb{Z}_+$ nın f ile öz temsili ise d diskriminantlı $g(x,y)=f(x,y)x^2+lxy+my^2$ formu da $g(1,0)=k$ olduğundan k nın öz temsilidir. k, g formu ile temsil edildiğinden $x^2 \equiv d=l^2-4km \equiv l^2 \pmod{4k}$ kuadratik rezidü olup genelliği bozmadan l, $0\le l<2k$ aralığında seçilebilir. Bununla birlikte $U=\begin{bmatrix} x & r \\ y & s \end{bmatrix} \in SL_2(\mathbb{Z})$ matrisi f yi g formuna dönüştüren bir matris ise $\phi(f,U)=(\det U).\left(f(x,y)X^2+lXY+f(r,s)Y^2\right)$ olduğundan $\det U = xs-ry=1$ olmalıdır. Bu nedenle $\det U = xs-ry=1$ denklemini sağlayan $(r,s)\in\mathbb{Z}^2$ çözümleri bulunmalıdır.

(r,s) ve (r_0,s_0), $xs-ry=1$ denkleminin herhangi iki çözümü ise

$$\left.\begin{aligned} xs-ry&=1\\ xs_0-r_0y&=1\end{aligned}\right\} \Rightarrow \begin{bmatrix} s & -r \\ s_0 & -r_0 \end{bmatrix}\cdot\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

olduğundan

$$x=\frac{\begin{vmatrix} 1 & -r \\ 1 & -r_0 \end{vmatrix}}{\begin{vmatrix} s & -r \\ s_0 & -r_0 \end{vmatrix}}=\frac{r-r_0}{\underbrace{rs_0-r_0s}_{\varepsilon\neq 0}} \Rightarrow r-r_0=\varepsilon x \Rightarrow r=r_0+\varepsilon x$$

$$y=\frac{\begin{vmatrix} s & 1 \\ s_0 & 1 \end{vmatrix}}{\begin{vmatrix} s & -r \\ s_0 & -r_0 \end{vmatrix}}=\frac{s-s_0}{\underbrace{rs_0-r_0s}_{\varepsilon\neq 0}} \Rightarrow s-s_0=\varepsilon y \Rightarrow s=s_0+\varepsilon y$$

elde edilir. O halde (r_0, s_0), $xs - ry = 1$ denkleminin bir çözümü ise diğer tüm çözümleri ε keyfi bir tamsayı olmak üzere

$$r = r_0 + \varepsilon x \quad , \quad s = s_0 + \varepsilon y$$

formülü ile verilir. (r,s), $xs - ry = 1$ denkleminin keyfi bir çözümü ise $U = \begin{bmatrix} x & r \\ y & s \end{bmatrix} \in SL_2(\mathbb{Z})$ matrisi f formunu g formuna dönüştürdüğünden

$$\begin{aligned} l &= 2axr + b(xs + yr) + 2cys \\ &= 2ax(r_0 + \varepsilon x) + b\big(x(s_0 + \varepsilon y) + y(r_0 + \varepsilon x)\big) + 2cy(s_0 + \varepsilon y) \\ &= 2axr_0 + b(xs_0 + yr_0) + 2cys_0 + 2\varepsilon\left(ax^2 + bxy + cy^2\right) \\ &= 2axr_0 + b(xs_0 + yr_0) + 2cys_0 + 2\varepsilon k \qquad \left(l_0 = 2axr_0 + b(xs_0 + yr_0) + 2cys_0\right) \\ &= l_0 + 2\varepsilon k \end{aligned}$$

elde edilir. $0 \le l < 2k$ olmasını istediğimizden $0 \le l_0 + 2\varepsilon k < 2k \Rightarrow 0 \le \frac{l_0}{2k} + \varepsilon < 1$ sağlayan tekbir $\varepsilon \in \mathbb{Z}$ vardır. Buyüzden $0 \le l < 2k$ olmak üzere $xs - ry = 1$ denklemini sağlayan tekbir $(r,s) \in \mathbb{Z}^2$ olup diskriminanttan m katsayısı tek şekilde belirlidir.

$f = (a,b,c)$, $d < 0$ diskriminantlı pozitif belirli bir form ve $(x,y) \in \mathbb{Z}^2$, $n \in \mathbb{Z}_+$ nın bir öztemsili f olsun. f ye $U = \begin{bmatrix} x & r \\ y & s \end{bmatrix} \in SL_2(\mathbb{Z})$ matrisine karşılık gelen dönüşüm uygulanırsa $f \sim \phi(f,U) = (n,B,C)$ formu elde edilebilir. Bu şekildeki formların kümesi

$$N = \left\{ \phi(f,U) = (n,B,C) \,\middle|\, U = \begin{bmatrix} x & r \\ y & s \end{bmatrix} \in SL_2(\mathbb{Z}), ebob(x,y) = 1, f(x,y) = n \right\}$$

olarak tanımlanırsa $\Gamma = \left\{ S^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \middle| S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z}) \right\}$ kümesinin elemanları yardımıyla N kümesi üzerinde bir denklik bağıntısı tanımlanabilir. Bu bağıntı n nin f ile öz temsilleri (x,y) ve (x',y') olmak üzere $f_1, f_2 \in N$ için

$$f_1 \Re f_2 \Leftrightarrow \exists m \in \mathbb{Z} \text{ için } \phi\left(f_1, \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}\right) = f_2$$

biçiminde tanımlanır. $\Re$ bağıntısı N kümesi üzerinde bir denklik bağıntısı olup $N/_{\Re}$ bölüm kümesidir. Bununla birlikte yine Γ kümesi yardımıyla

$$K=\left\{U=\begin{bmatrix}x & a\\ y & b\end{bmatrix}\in\mathbb{Z}_2^2\,\middle|\,\det U=ebob(x,y)\right\}$$

kümesi üzerinde her $U_1,U_2\in K$ için $U_1\mathfrak{B}U_2\Leftrightarrow\exists m\in\mathbb{Z}$ için $U_1\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}=U_2$ biçiminde tanımlanan $\mathfrak{B}$ bir denklik bağıntısıdır.

Önerme 4.2.2 : $n\in\mathbb{Z}$ nin f ile bir öztemsili olsun. n nin öztemsillerinin denklik sınıflarını $N/_{\Re}$ deki denklik sınıflarına götüren dönüşüm 1-1 ve örtendir.

Kanıt : $n\in\mathbb{Z}$ olmak üzere n nin f ile öz temsillerinin kümesi

$A=\left\{(x,y)\in\mathbb{Z}^2\,\middle|\,f(x,y)=n,ebob(x,y)=1\right\}$ olup her $(x,y),(s,u)\in A$ için

$$(x,y)\sim(s,u)\Leftrightarrow\exists V\in Aut^{+}(f)\ni\varphi_V(x,y)=(s,u)$$

biçiminde tanımlanan $\sim$, A kümesi üzerinde bir denklik bağıntısı olup $A/_{\sim}$ bölüm kümesidir. $A/_{\sim}$ ile $N/_{\Re}$ arasında

$$\psi:A/_{\sim}\to N/_{\Re}$$
$$\left[(x,y)\right]\mapsto\psi\left(\left[(x,y)\right]\right)=\left[\phi(f,U)\right]=\phi(f,U\Gamma)$$

fonksiyonunu tanımlıyalım.

$(x,y),(x',y')\in A$ için $\left[(x,y)\right]=\left[(x',y')\right]\Rightarrow\exists V\in Aut^{+}(f)\ni\varphi_V(x',y')=(x,y)$ dir.

Teorem 4.2.1 den

$\exists U=\begin{bmatrix}x & s\\ y & t\end{bmatrix},U'=\begin{bmatrix}x' & s'\\ y' & t'\end{bmatrix}\ni\phi(f,U)=(n,B,C)$ ve $\phi(f,U')=(n,B',C')$ dir. Bununla birlikte $V=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in Aut^{+}(f)$ ise

$VU=\begin{bmatrix} a & b \\ c & d \end{bmatrix}.\begin{bmatrix} x' & r' \\ y' & s' \end{bmatrix}=\begin{bmatrix} ax'+by' & ar'+bs' \\ cx'+dy' & cr'+ds' \end{bmatrix}=\begin{bmatrix} x & ar'+bs' \\ y & cr'+ds' \end{bmatrix}$ olup U ile VU' nün ilk sütunları aynı olduğundan $U\Gamma=VU'\Gamma$ dır. Bu durumda V , f nin otomorfu olduğundan

$$\psi\left(\left[(x,y)\right]\right)=\phi(f,U\Gamma)=\phi\left(f,VU'\Gamma\right)=\phi\left(\phi(f,V),U'\Gamma\right)=\phi\left(f,U'\Gamma\right)=\psi\left(\left[\left(x',y'\right)\right]\right)$$

dır.

$\therefore \psi$ iyi tanımlıdır.

(n,B,C) formunun f ye has denk olduğunu varsayalım. Bu durumda ilk sütunu (x,y) olan $\exists U\in SL_2(\mathbb{Z})$ için $\phi(f,U)=(n,B,C)$ dir. U matrisinin ilk sütunu (x,y) olduğundan $f(x,y)=n$ ve $\det U=1$ olduğundan $ebob(x,y)=1$ dir.

$\therefore \exists\left[(x,y)\right]\in A/_{\sim}$ ∋ $\psi\left(\left[(x,y)\right]\right)=\phi(f,U\Gamma)$ olduğundan ψ örtendir.

$\left[(x,y)\right],\left[\left(x',y'\right)\right]\in A/_{\sim}$ için

$$\psi\left(\left[(x,y)\right]\right)=\psi\left(\left[\left(x',y'\right)\right]\right)\Rightarrow\phi(f,U\Gamma)=\phi\left(f,U'\Gamma\right)$$

$$\Rightarrow\phi(f,U)\Re\phi\left(f,U'\right)$$

$$\Rightarrow\exists S^m=\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}\in\Gamma \text{ için } \phi\left(\phi(f,U),S^m\right)=\phi\left(f,U'\right)$$

$$\Rightarrow\exists S^{-m}=\begin{pmatrix}1 & -m\\ 0 & 1\end{pmatrix}\in\Gamma \text{ için } \phi(f,U)=\phi\left(\phi\left(f,U'\right),S^{-m}\right)$$

$$\Rightarrow\exists U''=U'S^{-m}\in\Gamma \text{ için } \phi(f,U)=\phi\left(f,U''\right)$$

dir. Buradan

$$\phi(f,U)=\phi\left(f,U''\right)\underset{V\in Aut^{+}(f)}{\Rightarrow}\phi(f,VU)=\phi\left(f,U''\right)$$

$$\underset{U\in SL_2(\mathbb{Z})}{\Rightarrow}\phi(f,V)=f=\phi\left(f,U''U^{-1}\right)$$

$$\Rightarrow V=U''U^{-1}$$

elde edilir. $U'\mathfrak{B}U''$ olduğundan U'' matrisinin ilk sütunu $\left(x',y'\right)$ dir. Ayrıca $U'',U^{-1}\in K$ için

$V = U'U^{-1} = \begin{bmatrix} x' & r'' \\ y' & s'' \end{bmatrix} \cdot \begin{bmatrix} s & -r \\ -y & x \end{bmatrix} = \begin{bmatrix} x's - r''y & -x'r + r''x \\ y's - s''y & -y'r + s''x \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ olup

$\varphi_V(x,y) = (\alpha x + \beta y, \gamma x + \delta y) = \left(x' \underbrace{(xs - ry)}_{1}, y' \underbrace{(xs - ry)}_{1} \right) = (x,y)$ olduğundan (x,y) ile (x',y') aynı denklik sınıfındandır. Bu nedenle $[(x,y)] = [(x',y')]$ dir.

$\therefore \psi$ 1-1 dir.

Sonuç 4.2.3 : $f = (a,b,c)$, $d < 0$ diskriminantlı pozitif belirli pirimitif bir form ve $k \in \mathbb{Z}_+$ nın f ile öz temsili olsun. Teorem 4.2.1 deki her l için k nın öz temsillerinin sayısı tam olarak $w(d)$ tanedir.

Kanıt : $l \in [0, 2k)$ olmak üzere (x,y) ve (x',y') aynı $n \in \mathbb{Z}_+$ nın f ile iki öz temsili olsun. $\exists U = \begin{bmatrix} x & r \\ y & s \end{bmatrix}, U' = \begin{bmatrix} x' & r' \\ y' & s' \end{bmatrix} \in SL_2(\mathbb{Z})$ için $\phi(f,U) = \phi(f,U') = (n,l,m)$ olduğunu varsayalım. $\phi(f,U) = \phi(f,U') \Rightarrow f = \phi(f, U'U^{-1})$ olup $V = U'U^{-1} \in Aut^+(f)$ dir. $V(x,y) = (x',y')$ olduğundan $(x,y) \sim (x',y')$ dir. Bu nedenle Teorem 4.2.1 deki koşulları sağlayan her l için k nın öz temsillerinin sayısı tam olarak $w(d)$ tanedir.

Teorem 4.2.4 : $n \in \mathbb{Z}$, $l > 0$ ve p asal olmak üzere $p \nmid n$ olsun.

$$x^2 \equiv n \pmod{p^l}$$

kongrüansının çözüm sayısı

i) $p = 2$, $l = 1$ için 1

ii) $p = 2$, $l = 2$, $n \equiv 3 \pmod 4$ için 0

iii) $p = 2$, $l = 2$, $n \equiv 1 \pmod 4$ için 2

iv) $p = 2$, $l > 2$, $n \not\equiv 1 \pmod 8$ için 0

v) $p = 2$, $l > 2$, $n \equiv 1 \pmod 8$ için 4

vi) $p>2$ için $1+\left(\frac{n}{p}\right)$ dir.

Kanıt :

i) $2\nmid n$ ise $x^2\equiv n(\mathrm{mod}\,2)$ nin tek çözümü $x\equiv 1(\mathrm{mod}\,2)$ dir.

ii) $x^2\equiv n(\mathrm{mod}\,4)\underset{n\equiv 3(\mathrm{mod}\,4)}{\Rightarrow} x^2\equiv 3(\mathrm{mod}\,4)$ kongrüansının bir çözümü yoktur.

iii) $x^2\equiv n(\mathrm{mod}\,4)\underset{n\equiv 1(\mathrm{mod}\,4)}{\Rightarrow} x^2\equiv 1(\mathrm{mod}\,4)$ kongrüansının $\mathrm{mod}\,4$ te $\bar{1},\bar{3}$ olmak üzere iki farklı çözümü vardır.

iv) $p=2$, $l>2$, $2\nmid n$ ve $n\not\equiv 1(\mathrm{mod}\,8)$ olsun. $x^2\equiv n\left(\mathrm{mod}\,2^l\right)$ kongrüansının bir çözümünün olduğunu varsayalım. $2\nmid n$ ve 2 asal olduğundan $ebob(x,2)=1$ dir. Bu nedenle $x^2\equiv n\left(\mathrm{mod}\,2^l\right)$ kongrüansının çözümü varsa x ler tek sayı olmalıdır. $n\not\equiv 1(\mathrm{mod}\,8)$ ve $l>2$ olmak üzere $x^2\equiv n\left(\mathrm{mod}\,2^l\right)$ kongrüansının tek x tamsayı çözümleri var olduğundan özel olarak $l=3$ için $x^2\equiv n\left(\mathrm{mod}\,2^3\right)$ kongrüansını da çözümü vardır. Ancak her tek tamsayının karesi $\equiv 1(\mathrm{mod}\,8)$ dir. Buda $n\not\equiv 1(\mathrm{mod}\,8)$ oluşuyla çelişir. $\therefore n\not\equiv 1(\mathrm{mod}\,8)$, $l>2$ için $x^2\equiv n\left(\mathrm{mod}\,2^l\right)$ kongrüansının çözümü yoktur.

v) $p=2$, $l>2$ ve $n\equiv 1(\mathrm{mod}\,8)$ olsun. Genelliği bozmadan n ler $0<n<2^l$ aralığından seçilebilir. $x^2\equiv n\left(\mathrm{mod}\,2^l\right)$ kongrüansının çözülebilmesi için x ler tek tamsayı olması gerektiğinden x_0 bu kongrüansın bir çözümü ise $2\nmid x_0$ dir. x ve x_0 bu kongrüansın herhangi iki çözümü olsun. Bu durumda

$$2^l \mid (x-x_0)(x+x_0)$$

olup x ve x_0 tek olduğundan hem $x-x_0$ hemde $x+x_0$ çifttir. Buradan

$$2^{l-2}\nmid \left(\frac{x-x_0}{2}\right)\left(\frac{x+x_0}{2}\right)$$

elde edilir. $\frac{x-x_0}{2}+\frac{x+x_0}{2}=x$ olduğundan 2, $\frac{x-x_0}{2}$ ve $\frac{x+x_0}{2}$ yi birlikte bölmez.

Bunedenle

$$2^{l-2} \mid \frac{x-x_0}{2} \quad \text{ya da} \quad 2^{l-2} \mid \frac{x+x_0}{2}$$

olup $x \equiv \pm x_0 \left(\mathrm{mod}\, 2^{l-1}\right)$ dir. Başka bir deyişle x_0, $x^2 \equiv n\left(\mathrm{mod}\, 2^l\right)$ kongrüansının bir çözümü ise ya x_0 ya da $-x_0$ aynı zamanda $x^2 \equiv n\left(\mathrm{mod}\, 2^{l-1}\right)$ kongrüansının da bir çözümüdür. Ayrıca $x \not\equiv x_0 \left(\mathrm{mod}\, 2^l\right)$ iken $x \equiv x_0 \left(\mathrm{mod}\, 2^{l-1}\right)$ olacak şekilde $x^2 \equiv n\left(\mathrm{mod}\, 2^l\right)$ kongrüansının hiçbir çözümü yoktur ve

$$\left.\begin{aligned} x^2 &\equiv n\left(\mathrm{mod}\, 2^l\right) \\ x^2 &\equiv n\left(\mathrm{mod}\, 2^{l-1}\right) \end{aligned}\right\}$$

sisteminin çözüm sayısı $x^2 \equiv n\left(\mathrm{mod}\, 2^l\right)$ kongrüansının çözüm sayısının yarısıdır. Bu yüzden

$$\left.\begin{aligned} x^2 &\equiv n\left(\mathrm{mod}\, 2^4\right) \\ x^2 &\equiv n\left(\mathrm{mod}\, 2^3\right) \end{aligned}\right\}$$

sisteminin çözüm sayısı 2 olup $x^2 \equiv n\left(\mathrm{mod}\, 2^4\right)$ kongrüansının çözüm sayısı 4 olarak bulunur. Benzer şekilde

$$\left.\begin{aligned} x^2 &\equiv n\left(\mathrm{mod}\, 2^5\right) \\ x^2 &\equiv n\left(\mathrm{mod}\, 2^4\right) \end{aligned}\right\}$$

sisteminin de çözüm sayısı 2 olup $x^2 \equiv n\left(\mathrm{mod}\, 2^5\right)$ kongrüansının da çözüm sayısı 4 tür. Benzer şekilde devam edilecek olursa $n \equiv 1 (\mathrm{mod}\, 8)$ olmak üzere $x^2 \equiv n\left(\mathrm{mod}\, 2^l\right)$ kongrüansının çözüm sayısının 4 olduğu görülür.

vi) $p > 2$ olsun.

a) $\left(\frac{n}{p}\right) = -1$ ise $x^2 = n(\mathrm{mod}\, p)$ kongrüansının bir çözümü yoktur. Bunedenle $x^2 = n\left(\mathrm{mod}\, p^l\right)$ kongrüansının da bir çözümü olmadığından $x^2 = n\left(\mathrm{mod}\, p^l\right)$ kongrüansının çözüm sayısı

$$0 = 1 + \left(\frac{n}{p}\right) \text{ dir.}$$

b) $\left(\frac{n}{p}\right) = 1$ olsun. Genelliği bozmadan n, $0 < n < p^l$ aralığından seçilebilir. $p \nmid n$ olduğundan $ebob(n, p) = 1$ ya da $ebob(n, p) = m \neq 1$ dir. $ebob(n, p) = m \neq 1$ olması durumunda $m \mid n$ ve $m \mid p$ olup p asal ve $m \neq 1$ olduğundan $m = p$ dir. Bu ise $p \nmid n$ olması ile çelişir. Bununla birlikte

$$x^2 = n \left(\text{mod } p^l\right) \Rightarrow p^l \mid x^2 - n$$

$$\Rightarrow \exists k \in \mathbb{Z} \ni x^2 - n = p^l k$$

$$\Rightarrow \exists k \in \mathbb{Z} \ni x^2 = n + p^l k$$

dır ve $ebob(n, p) = 1$ olması $ebob(x, p) = 1$ olmasını gerektirir. Bu durumda çözümler $0 < x < p^l$ aralığındaki $ebob(x, p) = 1$ sağlayan x ler arasındadır. x_0, $x^2 \equiv n (\text{mod } p)$ kongrüansının bir çözümü ise $f(x) = x^2 - n$ olmak üzere $f'(x_0) = 2x_0 \not\equiv 0 (\text{mod } p)$ olduğundan $x^2 \equiv n (\text{mod } p)$ kongrüansının çözümleri $x^2 \equiv n \left(\text{mod } p^l\right)$ kongrüansına tek şekilde genişletilebilir. Bunedenle $x^2 \equiv n (\text{mod } p)$ nin iki çözümü olduğundan $x^2 \equiv n \left(\text{mod } p^l\right)$ kongrüansının da iki çözümü vardır. O halde $p > 2$ ve $\left(\frac{n}{p}\right) = 1$ için $x^2 \equiv n \left(\text{mod } p^l\right)$ kongrüansının çözüm sayısı

$$2 = 1 + \left(\frac{n}{p}\right) \text{ dir.}$$

Teorem 4.2.5 : $k > 0$ ve $ebob(d, k) = 1$ olsun.

$$x^2 \equiv d (\text{mod } 4k)$$

kongrüansının çözümlerinin sayısı, f ler k nın kare çarpansız bölenleri olmak üzere

$$2 \sum_{f \mid k} \left(\frac{d}{f}\right) \text{ dir.}$$

Kanıt : x_0, $x^2 \equiv d \pmod{4k}$ kongrüansının bir çözümü ise $(x_0 + 2k)^2 \equiv x_0^2 \pmod{4k}$ olduğundan $x_0 + 2k$ da diğer bir çözümdür. $x_0 \not\equiv x_0 + 2k \pmod{4k}$ olup $x_0 \equiv x_0 + 2k \pmod{2k}$ olduğundan $x^2 \equiv d \pmod{2k}$ kongrüansının çözüm sayısı $x^2 \equiv d \pmod{4k}$ kongrüansının çözüm sayısının yarısıdır. $\alpha, \beta_1, \beta_2, ..., \beta_r \in \mathbb{Z}$ olmak üzere k nın asal çarpanlara ayrılışı $k = 2^{\alpha} p_1^{\beta_1}.p_2^{\beta_2}...p_r^{\beta_r}$ ise $\alpha \geq 1$ için $x^2 \equiv d \pmod{4k}$ kongrüansının çözüm sayısı Teorem 1.2.10 dan $N(8).N\left(p_1^{\beta_1}\right).N\left(p_2^{\beta_2}\right)...N\left(p_r^{\beta_r}\right)$ olup önceki teoremden $N(8).N\left(p_1^{\beta_1}\right).N\left(p_2^{\beta_2}\right)...N\left(p_r^{\beta_r}\right) = 4.N(p_1).N(p_2)...N(p_r)$ dir. Bu durumda $x^2 \equiv d \pmod{2k}$ kongrüansının çözüm sayısı $2.N(p_1).N(p_2)...N(p_r)$ olarak bulunur. Teorem 4.2.4 ten $2.N(p_1).N(p_2)...N(p_r) = 2^{r+1}$ dir ve bu sayı k nın kare çarpansız pozitif bölenlerinin sayısına eşittir.

d tek ise $d \equiv 1 \pmod{4}$ olup $ebob(d,k) = 1$ olduğundan $ebob(d,4k) = 1$ dir. $4k$ nın her p^l böleni için $4 \mid 4k$ olduğundan $p = 2$ iken $l \neq 1$ olup $x^2 \equiv d \pmod{p^l}$ kongrüansının çözümlerinin sayısı Teorem 4.2.4 ten

$$p = 2,\ l = 2 \text{ için } 2$$

$$p = 2,\ l > 2 \text{ için } 4 = 2.\left(1 + \left(\frac{d}{p}\right)\right)$$

$$p > 2 \text{ için } 1 + \left(\frac{d}{p}\right) \text{ dir.}$$

Teorem 1.2.10 dan $x^2 \equiv d \pmod{4k}$ kongrüansının çözüm sayısı p, k nın asal çarpanı ve f, k nın kare çarpansız böleni olmak üzere

$$2\prod_{p \mid k}\left(1 + \left(\frac{d}{p}\right)\right) = 2\sum_{f \mid k}\left(\frac{d}{f}\right)$$

d çift ise $d \equiv 0 \pmod{4}$ olup $ebob(d,k) = 1$ olduğundan k tek olmalıdır. $x^2 \equiv d \equiv 0 \pmod{4}$ kongrüansının iki çözümü olup $l > 0$ ve $p^l \mid k$ olmak üzere

$x^2 \equiv d \left(\mathrm{mod}\ p^l\right)$ kongrüansının çözüm sayısı $1+\left(\frac{d}{p}\right)$ dir. Bu durumda $x^2 \equiv d \left(\mathrm{mod}\, 4k\right)$ kongrüansının çözüm sayısı

$$2\prod_{p \mid k}\left(1+\left(\frac{d}{p}\right)\right) = 2\sum_{f \mid k}\left(\frac{d}{f}\right) \text{ dir.}$$

Tanım 4.2.6 : Aynı diskriminantlı pirimitif formların diskriminantına **"temel diskriminant"** denir

Teorem 4.2.7 (Mass Formülü) :

d temel diskriminant , $k \in \mathbb{Z}_+$ ve $ebob(d,k)=1$ olsun. k nın d diskriminantlı pozitif belirli formlarla temsillerinin sayısı $R_d\left(k\right)$ sonludur ve bu sayı

$$R_d\left(k\right) = w(d)\sum_{n \mid k}\left(\frac{d}{n}\right)$$

ile verilir.

Kanıt : $l^2 \equiv d \left(\mathrm{mod}\, 4k\right)$ sağlayan l lerin sayısı Teorem 4.2.5 den t ler k nın kare çarpansız bölenleri olmak üzere

$$2\sum_{t \mid k}\left(\frac{d}{t}\right) \text{ dir.}$$

l_0, $x^2 \equiv d \left(\mathrm{mod}\, 4k\right)$ kongrüansının bir çözümü ise $l_0 + 2k$ da $x^2 \equiv d \left(\mathrm{mod}\, 4k\right)$ nın bir çözümüdür. Ancak $0 \le l < 2k$ için l lerin sayısı

$$\sum_{t \mid k}\left(\frac{d}{t}\right)$$

olarak bulunur. Bu şekildeki her l için k nın temsillerinin sayısı tam olarak $w(d)$ tane olup l lerin sayısı $\sum_{t \mid k}\left(\frac{d}{t}\right)$ tane olduğundan $k \in \mathbb{Z}_+$ nın d diskriminantlı pirimitif formlarla temsillerinin sayısı

$$w(d)\sum_{t \mid k}\left(\frac{d}{t}\right)$$

dir. Bununla birlikte $ebob(x,y)=g$ ve (x,y), k nın öz olmayan temsili ise $\left(\frac{x}{g},\frac{y}{g}\right)$, $\frac{k}{g^2}$ nin öz temsilidir. Bu nedenle k nın her öz olmayan temsiline karşılık $ebob(x,y)=g$ olmak üzere $\frac{k}{g^2}$ nin bir $\left(\frac{x}{g},\frac{y}{g}\right)$ öz temsili karşılık gelir. Bu durumda $\frac{k}{g^2}$ nin öz temsillerinin sayısı $ebob(x,y)=g$ olan k nın öz olmayan temsillerinin sayısına eşittir. Karesi k yı bölen g lerin sayısı

$$\sum_{g^2 \mid k}\left(\frac{d}{g^2}\right)=\sum_{g^2 \mid k}\left(\frac{d}{g}\right)$$

ve t, $\frac{k}{g^2}$ nin kare çarpansız böleni olmak üzere $\frac{k}{g^2}$ nin öz temsillerinin sayısı

$$w(d)\sum_{t \mid \frac{k}{g^2}}\left(\frac{d}{t}\right)$$

olup her pozitif tamsayı $n=tg^2$ biçiminde yazılabileceğinden k nın d diskriminantlı pozitif belirli formlarla temsillerinin sayısı

$$R_d(k)=w(d)\left(\sum_{\substack{g^2 \mid k \\ g>0}}\left(\frac{d}{g}\right)\right).\left(\sum_{t \mid \frac{k}{g^2}}\left(\frac{d}{t}\right)\right)$$

$$=w(d).\sum_{\substack{g^2 \mid k \\ g>0}}\sum_{tg^2 \mid k}\left(\frac{d}{tg^2}\right)$$

$$\underset{n=tg^2}{=}w(d)\sum_{n \mid k}\left(\frac{d}{n}\right) \text{ dir.}$$

V. BÖLÜM
KUADRATİK CİSİMLER VE KUADRATİK FORMLAR ARASINDAKİ İLİŞKİ

Sayı cisimlerinin yapılarının belirlenmesinde, ideal sınıfları grubunun mertebesi olarak tanımlanan sınıf sayısının hesaplanması önemlidir. Bu bölümde d kare çarpansız bir tamsayı olmak üzere $\mathbb{Q}\left(\sqrt{d}\right)$ sayı cisminin kesirsel idealleriyle d diskriminantlı kuadratik formlarlar arasındaki ilişkiyi vereceğiz.

Tanım 5.1 : $A \neq \varnothing$ kümesi $k = \mathbb{Q}\left(\sqrt{d}\right)$ kuadratik sayı cisminin bir alt kümesi olsun. Eğer,

i) $\forall a, b \in A$ için $a - b \in A$

ii) $\forall a \in A$ ve $\forall c \in \mathcal{O}_d$ için $a.c \in A$

iii) $\exists 0 \neq r \in \mathcal{O}_d$ için $rA \subseteq \mathcal{O}_d$

koşulları gerçekleniyor ise A kümesine k cisminin bir **"kesirsel ideali"** denir.

Tanım 5.2 : R bir tamlık bölgesi ise I ve J, R nin sıfırdan farklı kesirsel idealleri olmak üzere

$$I \sim J \Leftrightarrow \exists a, b \in R \text{ için } (a)I = (b)J$$

biçiminde tanımlanan $\sim$ R nin sıfırdan farklı kesirsel ideallerinin kümesi üzerinde bir denklik bağıntısıdır. (Buradaki (a) notasyonu R nin esas idealini göstermektedir)

Tanım 5.3 : $I = \langle \alpha_1, \alpha_2 \rangle$, $\mathcal{O}_d$ nin bir ideali olsun. I idealinin normu

$$N(I) = \frac{\left| \alpha_1 \overline{\alpha_2} - \overline{\alpha_1} \alpha_2 \right|}{\sqrt{d}}$$

biçiminde tanımlanır.

d diskriminantlı $i = 1, 2, 3, ..., h(d)$ temsilleri için z_i, $a_i x^2 + b_i x + c_i = 0$ denkleminin kökü olmak üzere

$$\mathbb{Q}_i(x, y) = a_i x^2 + b_i xy + c_i y^2 = a_i \left(x - z_i y\right)\left(x - \overline{z_i} y\right)$$

kuadratik formları farklı denklik sınıfındadır ve $\mathbb{Q}_i$ formuna karşılık gelen kesirsel ideal $I_i = \mathbb{Z} + z_i\mathbb{Z}$ biçiminde tanımlanır.

Önerme 5.4 : d kare çarpansız bir tamsayı olmak üzere

i) $\mathbb{Q}\left(\sqrt{d}\right)$ nin tüm kesirsel idealleri I_i idealerinden birine denktir.

ii) $i = 1,2,3,...,h(d)$ için birbirinden farklı herhangi iki denk I_i ideali yoktur.

Kanıt : i) Genel olarak I ideali $I = w_1\mathbb{Z} + w_2\mathbb{Z} + ... + w_k\mathbb{Z}$ biçiminde yazılabilir ancak

$$I \subseteq \mathcal{O}_d = \begin{cases} \mathbb{Z}\left[\sqrt{d}\right]; d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]; d \equiv 1 \pmod 4 \end{cases}$$

olduğundan $k = 2$ olarak alınabilir. $I = \langle w_1, w_2 \rangle$ kesirsel ideali w_1 ile $-w_1$ değiştirilerek $\frac{1}{\sqrt{d}}\left(w_1\overline{w_2} - \overline{w_1}w_2\right) > 0$ olduğu varsayılabilir.

Eğer $w_1 = 0$ ya da $w_2 = 0$ ise $I = \langle w_1 \rangle$ ya da $I = \langle w_2 \rangle$ olduğundan I esas idealdir.

$w_1, w_2 \neq 0$ ise $N(I) > 0$, I idealinin normu olmak üzere

$$\begin{aligned} \mathbb{Q}_I(x,y) &= \frac{1}{N(I)}\left(xw_1 - yw_2\right)\left(x\overline{w_1} - y\overline{w_2}\right) \\ &= \frac{1}{N(I)}\left(N(w_1)x^2 - Tr\left(w_1\overline{w_2}\right)xy + N(w_2)\right) \end{aligned}$$

dir. Her i için $N(I) \mid N(w_i)$ ise x^2 ve y^2 nin katsayıları tamsayı olur. Bununla birlikte

$$\begin{aligned} N(w_1 + w_2) &= (w_1 + w_2).\left(\overline{w_1} + \overline{w_2}\right) \\ &= w_1\overline{w_1} + w_2\overline{w_2} + \left(w_1\overline{w_2} + \overline{w_1}w_2\right) \end{aligned}$$

olduğundan $N(I) \mid N(w_1 + w_2)$ ise xy nin katsayısı tamsayı olarak elde edilir. $\mathbb{Q}_I$ nin diskriminantı

$$\frac{1}{N(I)^2}\left[\left(w_1\overline{w_2} + \overline{w_1}w_2\right)^2 - 4\left(w_1w_2\right)\left(\overline{w_1w_2}\right)\right] = \left[\frac{w_1\overline{w_2} - \overline{w_1}w_2}{N(I)}\right]^2$$

olup $w_1\mathbb{Z} + w_2\mathbb{Z}$ ideali için

$$\begin{vmatrix} w_1 & \overline{w_1} \\ w_2 & \overline{w_2} \end{vmatrix}^2 = (\mathcal{O}_d : I).\begin{vmatrix} 1 & 1 \\ w & \overline{w} \end{vmatrix} = N(I)^2.d$$

olduğundan Q_I formu d diskriminantlıdır. Bu durumda $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL_2(\mathbb{Z})$ için

$$\phi\left(\mathrm{Q}_I, \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\right) = \mathrm{Q}_i(x, y)$$

olup $w_1\mathbb{Z} + w_2\mathbb{Z} = (\mu)(\mathbb{Z} + z_i\mathbb{Z})$ olduğu gösterilmelidir.

$$\phi\left(\mathrm{Q}_I, \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\right) = \frac{1}{N(I)}\left[\left((\alpha x + \beta y)w_1 - (\gamma x + \delta y)w_2\right).\left((\alpha x + \beta y)\overline{w_1} - (\gamma x + \delta y)\overline{w_2}\right)\right]$$

$$= \frac{1}{N(I)}\left[(\alpha w_1 - \gamma w_2)x + (\beta w_1 - \delta w_2)y\right]\left[\left(\alpha\overline{w_1} - \gamma\overline{w_2}\right)x + \left(\beta\overline{w_1} - \delta\overline{w_2}\right)y\right]$$

$$= \frac{N(\alpha w_1 - \gamma w_2)}{N(I)}(x - zy).\left(x - \bar{z}y\right)$$

olup $z = \frac{x}{y} = -\frac{\beta w_1 - \delta w_2}{\alpha w_1 - \gamma w_2}$ dir. $\mathrm{Q}_I = \mathrm{Q}_i$ olduğundan $z = z_i$ ya da $z = \overline{z_i}$ ve $N(\alpha w_1 - \gamma w_2) = a_i N(I) > 0$ dir. Bu durumda $(\alpha w_1 - \gamma w_2)$, $\mathcal{O}_d$ nin bir ideali olmak üzere

$$I = (\alpha w_1 - \gamma w_2)\mathbb{Z} + (-\beta w_1 + \delta w_2)\mathbb{Z}$$

$$= (\alpha w_1 - \gamma w_2)(\mathbb{Z} + z\mathbb{Z})$$

$$= (\alpha w_1 - \gamma w_2)(\mathbb{Z} + z_i\mathbb{Z})$$

olup I ideali I_i idealine denktir.

ii) $i, j \in 1, 2, ..., h(d)$ için $I_i \neq I_j$ olmak üzere $I_i \sim I_j$ olsun.

$$I_i \sim I_j \Leftrightarrow \exists \mu, \lambda \in \mathcal{O}_d \ni (\mu)I_i = I_j(\lambda) \text{ dir.}$$

$(\mu)I_i = (\mu)\langle 1, z_i\rangle = \langle \mu, \mu z_i\rangle = I_j(\lambda)$ olup $(\mu)I_i$ idealine karşılık getirilen kuadratik form

$$\mathrm{Q}_{\mu I_i} = \frac{N(\mu)x^2 - xyTr\left(\mu\left(\overline{\mu z_i}\right)\right) + N(\mu z_i)y^2}{N(\mu I_i)}$$

$$= \frac{N(\mu)\left(N(1)x^2 - xyTr(z_i) + N(z_i)y^2\right)}{N(\mu)N(I_i)}$$

$$= \frac{N(1)x^2 - xyTr(z_i) + N(z_i)y^2}{N(I_i)} = \mathbb{Q}_{I_i}(x,y)$$

olarak bulunur. Benzer şekilde $I_j(\lambda) = \langle 1, z_j \rangle(\lambda) = \langle \lambda, \lambda z_j \rangle = (\mu) I_i$ idealine karşılık gelen kuadratik form da

$$\mathbb{Q}_{I_j\lambda} = \frac{N(\lambda)x^2 - xyTr\left(\lambda\left(\overline{\lambda z_i}\right)\right) + N(\lambda z_i)y^2}{N(\lambda I_i)}$$

$$= \frac{N(1)x^2 - xyTr(z_j) + N(z_j)y^2}{N(I_j)} = \mathbb{Q}_{I_j}(x,y)$$

dir. $(\mu) I_i = I_j(\lambda)$ eşitliğinden $(\mu) I_i$ ile $I_j(\lambda)$ ideallerine karşılık gelen formlar eşit olup z_i, $\mathbb{Q}_{I_i}(x,y)$ formunun esas kökü olmak üzere $z_i = z_j$ olarak bulunur. Bu durumda $I_i = \langle 1, z_i \rangle = \langle 1, z_j \rangle = I_j$ olur ki buda $I_i \neq I_j$ oluşuyla çelişir.

$\therefore$ $i = 1,2,3,...,h(d)$ için birbirinden farklı herhangi iki denk I_i, I_j ideali yoktur.

Örnek : $(-1,33,21)$ formuna karşılık gelen ideal aşağıdaki biçimde bulunur.

$(-1,33,21)$ formunun esas kökü $-x^2 + 33x + 21 = 0 \Rightarrow z_i = \frac{33+\sqrt{1173}}{2}$ dir.

Buradan $(-1,33,21)$ formuna karşılık gelen kesirsel ideal $I_i = \mathbb{Z} + z_i\mathbb{Z} = \mathbb{Z} + \left(\frac{33+\sqrt{1173}}{2}\right)\mathbb{Z} = \langle 1, \frac{33+\sqrt{1173}}{2} \rangle$ olarak bulunur.

$I = (\alpha w_1 - \gamma w_2)(\mathbb{Z} + z_i\mathbb{Z})$ olduğundan $(-1,33,21)$ formuna karşılık gelen ideal ise

$$I = 2\mathbb{Z} + \left(33 + \sqrt{1173}\right)\mathbb{Z}$$

olarak elde edilir. Tersine $N(I_i) = -1$ ve $N(I) = -4$ olduğundan I_i ve I ideallerine karşılık

$$\mathbb{Q}_{I_i}(x,y) = \frac{N(1)x^2 - xyTr\left(\frac{33+\sqrt{1173}}{2}\right) + N\left(\frac{33+\sqrt{1173}}{2}\right)y^2}{N(I_i)}$$

$$= \frac{x^2 - 33xy - 21y^2}{-1} = (-1, 33, 21)$$

ve

$$Q_I(x,y) = \frac{N(2)x^2 - xyTr\left(2.\left(\frac{33+\sqrt{1173}}{2}\right)\right) + N\left(\frac{33+\sqrt{1173}}{2}\right)y^2}{N(I)}$$

$$= \frac{4x^2 - 132xy - 84y^2}{-4} = (-1, 33, 21)$$

formu getirilir.

Örnek : $d = -23$ diskriminantlı $(2,1,3)$ formuna karşılık gelen ideal aşağıdaki biçimde hesaplanır.

$(2,1,3)$ formunun esas kökü $2x^2 + x + 3 = 0 \Rightarrow z_i = \frac{-1+\sqrt{23}i}{4}$ dir. Bu nedenle $(2,1,3)$ formuna karşılık gelen kesirsel ideal $I_i = \mathbb{Z} + z_i\mathbb{Z} = \langle 1, \frac{-1\pm\sqrt{23}i}{4} \rangle$ olup $I = (\alpha w_1 - \gamma w_2)(\mathbb{Z} + z_i\mathbb{Z})$ olduğundan $(2,1,3)$ formuna karşılık gelen ideal ise

$$I = 4\mathbb{Z} + \left(-1 \pm \sqrt{23}i\right)\mathbb{Z}$$

olarak bulunur. $I_i = \langle 1, \frac{-1-\sqrt{23}i}{4} \rangle$ için $N(I_i) = \frac{1}{2}$ dir ve I_i idealine karşılık gelen form

$$Q_{I_i}(x,y) = \frac{N(1)x^2 - xyTr\left(\frac{-1-\sqrt{23}i}{4}\right) + N\left(\frac{-1-\sqrt{23}i}{4}\right)y^2}{N(I_i)}$$

$$= \frac{x^2 - xy\left(-\frac{1}{2}\right) + \frac{3}{2}y^2}{\frac{1}{2}}$$

$$= 2x^2 + xy + 3y^2$$

dir. Benzer şekilde $I = \langle 4, -1-\sqrt{23}i \rangle$ için $N(I) = 8$ dir ve I idealine karşılık gelen form

$$Q_I(x,y) = \frac{N(4)x^2 - xyTr\left(4.\left(-1-\sqrt{23}i\right)\right) + N\left(-1-\sqrt{23}i\right)y^2}{N(I)}$$

$$= \frac{16x^2 - xy(-8) + 24y^2}{8}$$

$$= 2x^2 + xy + 3y^2$$

olarak bulunur.

KAYNAKLAR

[1] Johannes BUCHMAN, Ulrich VOLLMER, Binary Quadratic Forms : An Algorithmic Approach. Springer-Verlag Berlin, 2007

[2] D. A. BUELL, Binary Quadratic Forms : Classical Theory and Modern Computations. Springer-Verlag New York Inc, 1989

[3] John Paul COOK, The Mass Formula for Binary Quadratic Forms, 2010

[4] F. ÇALLIALP, Sayılar Teorisi, İstanbul, 1999

[5] F. ÇALLIALP, Örneklerle Soyut Cebir,Birsen Yayınevi,2001

[6] William C. JAGY, Division and Binary Quadratic Forms, December 13, 2008

[7] I. NIVEN , H. S. ZUCKERMAN , H. L. MONTGOMERY : An Introduction to the Theory of Numbers , John Willey and Sons , Inc. , 1991

[8] Robert C. RHOADES, Heegner Points and Geodesics In Their Many Guises, March 4, 2008

ÖZGEÇMİŞ

Adı Soyadı : Burç BAYRAK
Doğum Yeri : Malatya
Doğum Tarihi : 07.08.1983
E-mail : burc_bayrak@hotmail.com

Eğitim Bilgileri

İlkokul : Ressam Şefketdağ ilkokulu
Ortaokul : Yunus Emre İlköğretim Okulu
Lise : Ataköy Yabancı Dil Ağırlıklı Lisesi
Lisans : Trakya Üniversitesi
Yabancı Dil : İngilizce