T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

İKİLİ KUADRATİK FORMLAR VE İKİLİ KUADRATİK FORMLARIN İNDİRGEME ÇEŞİTLERİ

YÜKSEK LİSANS TEZİ

Ece ÖZEL

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Enstitü Bilim Dalı	**:**	**CEBİR VE SAYILAR TEORİSİ**
Tez Danışmanı	**:**	**Yrd. Doç. Dr. Bahar DEMİRTÜRK BİTİM**

Aralık 2014

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

İKİLİ KUADRATİK FORMLAR VE İKİLİ KUADRATİK FORMLARIN İNDİRGEME ÇEŞİTLERİ

YÜKSEK LİSANS TEZİ

Ece ÖZEL

Enstitü Anabilim Dalı	:	**MATEMATİK**
Enstitü Bilim Dalı	:	**CEBİR VE SAYILAR TEORİSİ**

Bu tez 30 / 12 /2014 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Prof. Dr. Refik KESKİN	**Yrd. Dr. Bahar DEMİRTÜRK BİTİM**	**Yrd. Dr. Nesrin GÜLER**
Jüri Başkanı	**Üye**	**Üye**

ÖNSÖZ

Tez çalışmam boyunca yardımlarını benden esirgemeyen değerli danışman hocam Yrd. Doç. Dr. Bahar DEMİRTÜRK BİTİM'e, Prof. Dr. Refik KESKİN' e, hayatım boyunca maddi ve manevi desteğiyle her zaman yanımda olan aileme sonsuz teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$\left(\frac{p}{q}\right)$	: Legendre sembolü
$\equiv$	: Denktir
$a \mid b$	: a, b yi böler
$ebob(x, y)$	: x ile y nin en büyük ortak böleni
$[\![\ ]\!]$	: Tam Değer
$\binom{n}{k}$	: n nin k ' lı kombinasyonu
$\exists$	: En az bir
$\sim$	: Denklik bağıntısı
$\sum$	: Toplam sembolü
$Aut^{+}(\ )$	: Otomorf grubu
A^{T}	: A matrisinin transpozu
A^{-1}	: A matrisinin tersi
$[a_0, a_1, a_2, ...]$	: Sürekli kesir

ÖZET

Anahtar kelimeler: Kuadratik Form, Diophantine Denklemleri, Pell Denklemleri

Bu tez dört bölümden oluşmuştur. Birinci bölümde sayılar teorisinde kullanılan temel tanım ve teoremler verilmiştir. Ayrıca kuadratik formların tanımı yapılarak kuadratik formların çeşitleri verilmiştir. Bunlara ek olarak ikili kuadratik formların denklik şartlarından bahsedilmiştir. Ayrıca otomorfizm ve Pell denklemi hakkında bilgi verilmiştir

İkinci bölümde kuadratik formların indirgenmesi ele alınmıştır. Burada indirgenme çeşitleri; Langrange indirgemesi, Zagier indirgemesi ve Gauss indirgemesi başlıkları altında incelenmiştir.

Üçüncü bölümde bazı tamsayıların ikili kuadratik formlarla temsili ele alınmıştır. $Q = (A, B, C)$ belirsiz kuadratik formu tarafından temsil edilen bir m tamsayısı için $Au^2 + Buv + Cv^2 = m$ şartını sağlayan tüm (u, v) tamsayı ikililerini veren formül elde edilmiştir.

BINARY QUADRATIC FORMS AND TYPES OF REDUCTION OF BINARY QUADRATIC FORMS

SUMMARY

Keywords: Quadratic Form, Diophantine Equations, Pell Equations

This thesis consists of four chapters. The first one which presents fundamental definitions and theorems concerning number theory also deals with the definition of quadratic form and its varitions. In addition to these, automorphizm of quadratic forms and Pell equations take place in this chapter.

The second chapter aims to describe the reduction of quadratic forms; which are Langrange Reduction, Zagier reduction and Gauss Reduction.

Chapter third deals with the representation of integers via binary quadratic forms. For the integer m represented by the indefinite quadratic form $Q=(A,B,C)$, the formula which gives with all pairs of (u,v) integers such that $Au^2+Buv+Cv^2=m$ condition is obtained.

BÖLÜM 1. GİRİŞ

1.1. Temel Tanım ve Teoremler

Tanım 1.1.1. $k \geq 1$ için $a_k > 0$ olmak üzere $a_0, a_1, a_2, \ldots$ tamsayı dizisi verilsin.

$$[a_0, a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

şeklindeki bir ifadeye basit sonsuz sürekli kesir denir [4, 11].

$a_1,\ a_2, \ldots$ pozitif tamsayılar, $a_0 \in \mathbb{Z}$ ve $n \in \mathbb{N}$ olmak üzere $[a_0, a_1, a_2, \ldots, a_n]$ sürekli kesrine $[a_0, a_1, a_2, \ldots]$ sonsuz sürekli kesrinin $n.$ yaklaşımı denir ve bu değer $\frac{p_n}{q_n}$ ile gösterilir. Burada,

$$p_{-2} = 0,\ p_{-1} = 1,\ q_{-2} = 1,\ q_{-1} = 0$$

olmak üzere,

$$p_n = a_n p_{n-1} + p_{n-2}$$
$$q_n = a_n q_{n-1} + q_{n-2}$$

olarak tanımlanır [21].

Teorem 1.1.2. d tamkare olmayan pozitif bir tamsayı olmak üzere $\sqrt{d}$ kuadratik irrasyonel sayısının sürekli kesre açılımı, $a_0 = \left[\!\left[\sqrt{d}\right]\!\right]$ olmak üzere, $\sqrt{d} = \left[a_0, \overline{a_1, a_2, ..., a_{n-1}, 2a_0}\right]$ formundadır ve $\sqrt{d}$ ' nin periyodu n dir.

Tanım 1.1.3. d doğal sayı olmak üzere,

$$x^2 - dy^2 = \pm 1$$

Diophantine denklemlerine Pell denklemleri denir [1,4].

Tanım 1.1.4. d doğal sayı ve N tamsayı olmak üzere,

$$x^2 - dy^2 = N$$

Diophantine denklemine genel Pell denklemi denir [1,4].

Teorem 1.1.5. d tamkare olmayan pozitif bir tamsayı ve $\sqrt{d}$ ' nin sürekli kesir açılımının periyodu n olmak üzere

$$x^2 - dy^2 = 1$$

Pell denkleminin temel çözümü

a) n çift ise $(x, y) = (p_{n-1}, q_{n-1})$ dir.
b) n tek ise $(x, y) = (p_{2n-1}, q_{2n-1})$ dir.

Teorem 1.1.6 (Çin Kalan Teoremi). $m_1, m_2, ..., m_r$ ikişer ikişer aralarında asal olacak şekilde r tane pozitif tamsayı ve $a_1, a_2, ..., a_r$ herhangi tamsayılar olmak üzere

$$\begin{aligned} x &\equiv a_1 (\mathrm{mod}\, m_1) \\ x &\equiv a_2 (\mathrm{mod}\, m_2) \\ &\vdots \\ x &\equiv a_r (\mathrm{mod}\, m_r) \end{aligned} \qquad \textbf{(1.1)}$$

kongrüanslarının ortak çözümü vardır. (1.1)' in herhangi bir çözümü x_0 ise herhangi bir x tamsayısının (1.1) kongrüans sistemini sağlaması için gerekli ve yeterli koşul x ' in herhangi bir $k \in \mathbb{Z}$ ve $m = m_1 m_2 ... m_r$ için $x = x_0 + km$ formunda olmasıdır [2,3,10].

Tanım 1.1.7. $a, m \in \mathbb{Z}$ ve $ebob(a,m) = 1$ olmak üzere, $x^2 \equiv a (\mathrm{mod}\, m)$ kongrüansının çözümü varsa a tamsayısına m modülüne göre bir kuadratik rezidü denir. Eğer çözüm yoksa, a tamsayısına m modülüne göre bir kuadratik nonrezidü denir [7].

Tanım 1.1.8 (Legendre Sembolü). p tek asal sayı olsun. a bir kuadratik rezidü ise $\left(\frac{a}{p}\right) = 1$, eğer a bir kuadratik nonrezidü ise $\left(\frac{a}{p}\right) = -1$, eğer $p \mid a$ ise $\left(\frac{a}{p}\right) = 0$ şeklinde tanımlanır [3].

Teorem 1.1.9. p tek asal sayı olsun. Bu durumda

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

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,

(3) $a \equiv b (\text{mod } p)$ ise $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(4) $(ab, p) = 1$ ise $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$,

(5) $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

dir [7].

Teorem 1.1.10 (Kuadratik Resiprosite). p ve q farklı tek asal sayılar ise,

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

dir [7,10].

Tanım 1.1.11 (Jakobi Sembolü). Q bir pozitif tek tamsayı olsun. q_i ler farklı olmak zorunda olmayan tek asal sayılar olmak üzere, $Q = q_1 q_2 ... q_s$ olsun. $(\frac{P}{Q})$ Jakobi sembolü

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right)$$

şeklinde tanımlanır. Burada $(\frac{P}{q_j})$ Legendre sembolüdür [7].

1.2. Kuadratik Form

Bir P halkası üzerinde r değişkenli n. dereceden bir $form$ $P[x_1,...,x_r]$ ile gösterilen homojen bir polinomdur ve bu form sabit dereceli $n=a_1+...+a_r$ ile $x_1^{a_1}...x_r^{a_r}$ tek terimlilerin $P-$ lineer kombinasyonudur. Böylece $a_{ij}\ (1\le i,j\le r)$ katsayıları P tanım kümesinden olmak üzere, bir $x_1,...,x_r$ r değişkenli q kuadratik formu $q=\sum_{i,j}a_{ij}x_ix_j$ formunun ifadesidir.

Bir ikili kuadratik form genellikle

$$Q(x,y)=Ax^2+Bxy+Cy^2$$

şeklinde yazılabilen iki değişkenli bir kuadratik formdur. Bu form $Q=(A,B,C)$ şeklinde gösterilir.

Tanım 1.2.1. Bir $Q(x,y)=Ax^2+Bxy+Cy^2$ formunda $A,B,C\in\mathbb{Z}$ ise bu kuadratik forma tam form denir.

Tezin bu kısmından sonra tam formlarla ilgilenilecektir.

Tanım 1.2.2. $d=B^2-4AC$ tamsayısına Q formunun diskriminantı denir. d diskriminantı yerine bazen $d(Q)$ kullanılabilir. Örneğin $(1,0,1)$, $d=-4$ diskriminantlı x^2+y^2 formunu belirtir [5].

Tanım 1.2.3. $Q(x,y)=n$ olacak şekilde x,y tamsayıları varsa n tamsayısı Q tarafından temsil edilebilirdir denir ve buradaki $x,\ y$ tamsayıları aralarında asalsa n tamsayısının Q tarafından temsiline öz temsil denir [5].

Örnek olarak 4 sayısı $Q=(1,0,3)$ tarafından öz temsil edilebilirdir çünkü $Q(1,1)=4$ tür. Ancak $Q(2,0)=4$ temsili öz temsil değildir.

Tanım 1.2.4. Bir $Q(x,y)=Ax^2+Bxy+Cy^2$ kuadratik formunda $ebob(A,B,C)=1$ ise (A,B,C) formuna primitif form denir [5].

1.3. Kuadratik Formların Çeşitleri

Tanım 1.3.1. $x,y\in\mathbb{Z}$ olmak üzere, $Q(x,y)$ formu hem pozitif hem de negatif değerler alıyorsa Q formuna belirsiz form denir. $Q(x,y)\geq 0$ $(Q(x,y)\leq 0)$ ise Q formuna pozitif yarı belirli (negatif yarı belirli) form denir. $Q(x,y)=0$ iken $x=y=0$ oluyorsa Q formuna belirli form denir [5].

Örnek 1.3.2. $Q(x,y)=x^2-2y^2$ formu belirsizdir. Çünkü $Q(1,0)=1$ ve $Q(0,1)=-2$ dir.

$Q(x,y)=x^2-2xy+y^2=(x-y)^2$ formu $Q(1,1)=0$ olduğundan pozitif yarı belirlidir ancak belirli form değildir.

$Q(x,y)=x^2+y^2$ formu pozitif belirli formdur. Çünkü $Q(x,y)=0$ için tek çözüm $x=y=0$ dır.

Teorem 1.3.3. $Q(x,y)=Ax^2+Bxy+Cy^2$ tamsayı katsayılı ve d diskriminantlı bir ikili kuadratik form olsun. $d\neq 0$ ve d bir tamkare değilse $A\neq 0$, $C\neq 0$ dır. $Q(x,y)=0$ için tek çözüm $x=y=0$ dır [7].

İspat: d tamkare olmayan sıfırdan faklı bir tamsayı olmak üzere $Q(x,y)=Ax^2+Bxy+Cy^2$ tamsayı katsayılı ve d diskriminantlı bir form olsun. O zaman $A\neq 0$ ve $C\neq 0$ dır. Çünkü $A=C=0$ alınırsa $A.C=0$ ve $d=B^2-4AC=B^2$ olur bu da d ' nin tamkare olmaması ile çelişir. $x_0=0$, $y_0=0$ için $Q(x_0,y_0)=0$ dır. $y_0=0$ olursa $A\neq 0$ olduğundan $Ax_0^{\,2}=0$ dan $x_0=0$ olur.

Benzer şekilde $x_0 = 0$ olursa $y_0 = 0$ olur. Sonuç olarak $x_0 \neq 0$ ve $y_0 \neq 0$ alalım. $Ax^2 + Bxy + Cy^2$ formunun her iki tarafını $4A$ ile çarpalım.

$$4AQ(x,y) = (2Ax + By)^2 - dy^2 \qquad \textbf{(1.2)}$$

olup $Q(x_0, y_0) = 0$ olduğundan $(2Ax_0 + By_0)^2 = dy_0{}^2$ olur. Ancak $dy_0{}^2 \neq 0$ dır ve tek türlü çarpanlara ayrılmadan d tamkare olur bu da d ' nin tamkare olmaması ile çelişir.

Teorem 1.3.4. $Q(x,y) = Ax^2 + Bxy + Cy^2$, d diskriminantlı ve tamsayı katsayılı bir ikili kuadratik form olsun. Bu durumda

1. $d > 0$ ise Q belirsiz formdur.
2. $d = 0$ ise Q yarı belirli formdur.
3. $d < 0$ ve A,C aynı işaretli ise Q belirli formdur. ($A,C > 0$ ise pozitif belirli $A,C < 0$ ise negatif belirlidir).

İspat: 1. $d > 0$ olsun. Q formunun hem pozitif hem negatif değer aldığı gösterilmelidir. $Q(1,0) = A$ ve $Q(B,-2A) = -Ad$ olur. $A \neq 0$ için Q formu her iki işareti de alır. Benzer şekilde $Q(0,1) = C$ ve $Q(-2C,B) = -Cd$ dir. $C = 0$ olmadıkça Q formu her iki işareti de alır. $A = C = 0$ olma durumu ele alınsın. Buradan $0 < d = B^2$ olduğundan $B \neq 0$ dır. Bu durumda $Q(1,1) = B$ ve $Q(1,-1) = -B$ olur. Böylece Q her iki işareti alır.

2. $d = 0$ ve $A \neq 0$ olsun. $Ax^2 + Bxy + Cy^2$ formunun her iki tarafını $4A$ ile çarpalım. $4AQ(x,y) = (2Ax + By)^2 - dy^2$ olup $4AQ(x,y) \geq 0$ bulunur. Böylece $A \geq 0$ ise $Q(x,y) \geq 0$ ya da $A \leq 0$ ise $Q(x,y) \leq 0$ olup Q yarı belirlidir. $Q(B,-2A) = -Ad = 0$ olup $Q(x,y) = 0$ iken $x = y = 0$ olmadığından Q belirli değildir.

Şimdi de $d=0$ ve $A=0$ olsun. $d=B^2$ olur ancak $d=0$ olduğundan $B=0$ olur. Bu durumda $Q(x,y)=Cy^2$ olur. Burada sıfırdan farklı C ile aynı işaretli değerler vardır ancak $Q(1,0)=0$ olup Q formu belirli değildir.

3. $d<0$ olsun. $Q(x,y)=Ax^2+Bxy+Cy^2$ formunun her iki tarafını $4A$ ile çarpalım. Buradan $4AQ(x,y)=(2Ax+By)^2-dy^2$ elde ederiz. $(2Ax+By)^2-dy^2>0$ olur çünkü $d<0$ dır. $4AQ(x,y)$ bütün $(x,y)\neq(0,0)$ çiftleri için pozitif olur. Böylece Q belirlidir. $Q(1,0)=A$ ve $Q(0,1)=C$ olduğundan A ve C aynı işaretli olup pozitifse Q pozitif belirli form, negatifse negatif belirli form olur.

Örnek 1.3.5. $Q(x,y)=-2x^2+3xy-2y^2$ ikili kuadratik formu $d(Q)=B^2-4AC=-7$, $A=-2<0$ ve $C=-2<0$ olduğundan negatif belirli form olur.

$Q(x,y)=2x^2-3xy+2y^2$ kuadratik formu da pozitif belirli olur çünkü $d(Q)=-7$, $\mathrm{A}=2>0$ ve $\mathrm{C}=2>0$ dır.

$Q(x,y)=x^2+3xy+y^2$ kuadratik formunda $d(Q)=5>0$ olduğundan belirsiz formdur.

Teorem 1.3.6. $d\in\mathbb{Z}$ olsun. $d\equiv 0(\mathrm{mod}\,4)$ veya $d\equiv 1(\mathrm{mod}\,4)$ olması için gerekli ve yeterli koşul en az bir tane d diskriminantlı bir ikili tam kuadratik formun olmasıdır [7].

İspat: $B^2\equiv 0,1(\mathrm{mod}\,4)$ olduğundan $d=B^2-4AC\equiv 0,1(\mathrm{mod}\,4)$ olur.

Tersi için ilk olarak $d \equiv 0 \pmod 4$ alalım. $x^2 - \left(\frac{d}{4}\right) y^2$ formunun diskriminantı d dir. Benzer şekilde, $d \equiv 1 \pmod 4$ alalım. $x^2 + xy - \left(\frac{d-1}{4}\right) y^2$ formunun diskriminantı d dir.

Teorem 1.3.7. $n \neq 0$ ve $n, d \in \mathbb{Z}$ olsun. n tamsayısını öztemsil eden d diskriminantlı bir ikili kuadratik formun olması için gerekli ve yeterli şart $x^2 \equiv d \pmod{4|n|}$ kongrüansının bir çözümünün olmasıdır.

İspat: $x^2 \equiv d \pmod{4|n|}$ kongrüansının bir çözümü $B^2 - d = 4nC$ eşitliğini sağlayacak şekilde B olsun. Bu durumda $Q(x, y) = nx^2 + Bxy + Cy^2$ ikili kuadratik formu d diskriminantına sahip bir tam form olur. Ayrıca $Q(1,0) = n$, n tamsayısının bir öztemsilidir.

Tersine, n tamsayısının $Q(x_0, y_0)$ biçiminde bir öztemsili, $B^2 - 4AC = d$ diskriminantlı $Q(x, y) = Ax^2 + Bxy + Cy^2 = n$ formu olsun. $ebob(x_0, y_0) = 1$ olduğundan $m_1.m_2 = 4|n|$, $ebob(m_1, y_0) = 1$ ve $ebob(m_2, x_0) = 1$ olacak biçimde m_1, m_2 tamsayıları vardır. $ebob(m_1, y_0) = 1$ olduğundan $y_0 \overline{y_0} \equiv 1 \pmod{m_1}$ olacak biçimde $\overline{y_0} \in \mathbb{Z}$ vardır. (1.2)' ye göre $4An = (2Ax_0 + By_0)^2 - dy_0^2$ olup $m_1 4|n|$ olduğundan $(2Ax_0 + By_0)^2 \equiv dy_0^2 \pmod{m_1}$ yazılabilir. Buradan

$$(2Ax_0 + By_0)^2 (\overline{y_0})^2 \equiv dy_0^2 (\overline{y_0})^2 \pmod{m_1}$$

yani

$$((2Ax_0 + By_0)(\overline{y_0}))^2 \equiv d(y_0 \overline{y_0})^2 \pmod{m_1}$$

olur. $y_0 \overline{y_0} \equiv 1 \pmod{m_1}$ olduğu kullanılırsa

$$((2Ax_0 + By_0)(\overline{y_0}))^2 \equiv d \pmod{m_1}$$

bulunur. O halde $u^2 \equiv d \pmod{m_1}$ kongrüansının bir çözümü $u = u_1 = (2Ax_0 + By_0)\overline{y_0}$ olur. A ile C nin ve x ile y nin rolleri değiştirilirse, $u^2 \equiv d \pmod{m_2}$ nin de bir çözümünün olduğu görülür. Yani $u = u_2$ bulunur. Bu durumda Çin Kalan Teoreminden $w \equiv u_1 \pmod{m_1}$ ve $w \equiv u_2 \pmod{m_2}$ olacak biçiminde bir w tamsayının olduğu söylenebilir. Böylece $w^2 \equiv {u_1}^2 \equiv d \pmod{m_1}$ ve benzer şekilde $w^2 \equiv {u_2}^2 \equiv d \pmod{m_2}$ olup buradan $w^2 \equiv d \pmod{m_1 m_2}$ elde edilir. $m_1 m_2 = 4|n|$ olduğundan $w^2 \equiv d \pmod{4|n|}$ elde edilir ki bu da istenendir.

Sonuç 1.3.8. $d \equiv 0 \pmod 4$ veya $d \equiv 1 \pmod 4$ olsun. p tek asal sayı ise p' yi temsil eden d diskriminantlı bir ikili kuadratik formun olması için gerekli ve yeterli koşul $\left(\frac{d}{p}\right) = 1$ olmasıdır.

İspat: $\Rightarrow)$ p' yi temsil eden d diskriminantlı ikili kuadratik form varsa Teorem 1.3.7' e göre $x^2 \equiv d \pmod{4p}$ olan bir x tamsayısı vardır. Buradan $\left(\frac{d}{4p}\right) = 1$ bulunur. Tanım 1.1.11' den

$$\left(\frac{d}{4p}\right) = \left(\frac{d}{2}\right)^2 \cdot \left(\frac{d}{p}\right) = 1 \text{ olup } \left(\frac{d}{p}\right) = 1$$

elde edilir.

$\Leftarrow)$ $\left(\frac{d}{p}\right) = 1$ ise d, p modülüne göre karedir. $\left(\frac{d}{4}\right) = \left(\frac{d}{2}\right)^2 = 1$ olduğundan $x^2 \equiv d \pmod 4$ olan bir x tamsayısı vardır. Yani d , mod4'e göre karedir. p tek

olduğundan Çin kalan teoreminden d , mod $4p$ ' ye göre karedir. Teorem 1.3.7' den p , diskriminantı d olan bir form ile temsil edilir.

1.4. İkili Kuadratik Formların Denkliği

$d=-4$ diskriminantlı $Q=(2,2,1)$ formunu ele alalım. $Q(x,y)=2x^2+2xy+y^2=(x+y)^2+x^2$ olur. $Q=(2,2,1)$ ve $Q=(1,0,1)$ aynı sayıyı temsil ederler. Buradan $Q(x,y)=Q(x+y,y)$ ve $Q\ (x,y)=Q(x,y-x)$ elde edilir. Bu gibi birbirine dönüşen formlara denk formlar denir. Denk formları tanımlamak için modüler gruplar kullanılır.

$rs-tu=\pm 1$ olacak şekilde $r,s,t,u\in\mathbb{Z}$ tamsayılarının oluşturduğu 2×2 lik matrisler kümesi çarpma işlemine göre bir gruptur. Bu grup

$$GL_2(\mathbb{Z})=\left\{\begin{pmatrix} r & s \\ t & u \end{pmatrix}:\ r,s,t,u\in\mathbb{Z},\ ru-st=\pm 1\right\}$$

ile gösterilir. Bu matrislerin determinantının sadece 1 olanlarının kümesi de çarpma işlemine göre bir grup oluşturur aynı zamanda bu grup $GL_2(\mathbb{Z})$ grubunun alt grubudur ve bu grup

$$SL_2(\mathbb{Z})=\left\{\begin{pmatrix} r & s \\ t & u \end{pmatrix}:\ r,s,t,u\in\mathbb{Z},\ ru-st=1\right\}$$

ile gösterilir.

Tanım 1.4.1. $GL_2(\mathbb{Z})$ grubunun alt grubu olan $SL_2(\mathbb{Z})$ grubuna modüler grup denir [6].

$S=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}$ ve $T=\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}$ matrisleri $SL_2(\mathbb{Z})$ grubunun üreteçleridir.

Herhangi bir $S=\begin{pmatrix}r & s\\ t & u\end{pmatrix}\in SL_2(\mathbb{Z})$ matrisi ve bir $Q=(A,B,C)$ kuadratik formu ile yeni bir $Q'=(A',B',C')$ kuadratik formu aşağıdaki şekilde elde edebilir. S^T, S matrisinin transpozu olmak üzere,

$$Q'(x,y)=Q\left((x,y)S^T\right)=Q\left((x,y)\begin{pmatrix}r & t\\ s & u\end{pmatrix}\right)=Q(rx+sy,tx+uy)$$

olup

$$Q'(x,y)=Q\left(\begin{pmatrix}r & s\\ t & u\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}\right)=Q(rx+sy,tx+uy)$$

$$=A(rx+sy)^2+B(rx+sy)(tx+uy)+C(tx+uy)^2$$
$$=Ar^2x^2+2Arsxy+As^2y^2+Brtx^2+Bruxy+Bstxy+Bsuy^2+Ct^2x^2+2ctuxy+Cu^2y^2$$
$$=\left(A^2+Brt+Ct^2\right)x^2+\left(2(Ars+Ctu)+B(ru+st)\right)xy+\left(As^2+Bsu+Cu^2\right)y^2$$

bulunur. Burada A',B',C'

$$\begin{aligned}A'&=Ar^2+Brt+Ct^2,\\ B'&=2(Ars+Ctu)+B(ru+st),\\ C'&=As^2+Bsu+Cu^2\end{aligned}\qquad\textbf{(1.3)}$$

şeklinde tanımlanan tamsayılardır. Bulunan bu yeni Q' ikili kuadratik formu $Q'=Q|_S$ ile gösterilebilir. Benzer şekilde $Q=Q'|_{S^{-1}}$ olduğunu gösterebiliriz.

$$Q'|_{S^{-1}} = Q'\left(\begin{pmatrix} u & -s \\ -t & r \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) = Q'(ux - sy, -tx + ry)$$
$$= A'(u^2x^2 - 2usxy + s^2y^2) + B'(-tux^2 + ruxy + tsxy - rsy^2) + C'(t^2x^2 - 2trxy + r^2y^2)$$

olup buradan

$$Q'|_{S^{-1}} = Ax^2(ru - st)^2 + Bxy(ru - st)^2 + Cy^2(ru - st)^2$$

elde edilir. $\det S = 1$ olduğundan

$$Q'|_{S^{-1}} = Ax^2 + Bxy + Cy^2 = Q(x, y)$$

bulunur.

Tanım 1.4.2. $Q' = Q|_S$ olacak şekilde bir $S \in SL_2(\mathbb{Z})$ matrisi varsa Q ve Q' formlarına denk formlar denir ve $Q' \sim Q$ ile gösterilir. Q formuna denk olan formların kümesine de Q formunun denklik sınıfı denir.

Tanım 1.4.3. Bir $Q = (A, B, C)$ kuadratik formunun matrisi

$$M(Q) = \begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} \text{ veya } m(Q) = \frac{1}{2}M(Q) = \begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}$$

şeklinde tanımlanır. Q formunun matrisi kullanılarak

$$4Q(x, y) = (x, y)M(Q)\begin{pmatrix} x \\ y \end{pmatrix} \text{ veya } Q(x, y) = (x, y)m(Q)\begin{pmatrix} x \\ y \end{pmatrix} \qquad \textbf{(1.4)}$$

şeklinde yazılabilir. Bu durumda $d(Q) = -\det M(Q) = -4d(m(Q))$ eşitliği elde edilir.

Önerme 1.4.4. $Q=(A,B,C)$ bir kuadratik form olsun. $S=\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ matrisi $SL_2(\mathbb{Z})$ modüler grubunun bir elemanı ve $Q'=(A',B',C')=Q|_S$ olsun. Bu takdirde;

1. $d(Q)=d(Q')$ dır,
2. $ebob(A,B,C)=ebob(A',B',C')$ dır,
3. $d<0$ ise A ve A' aynı işarete sahiptir,
4. $\begin{pmatrix} u_1 \\ v_1 \end{pmatrix}=\mathrm{S}^{-1}\begin{pmatrix} x \\ y \end{pmatrix}$ olmak üzere $Q(x,y)=Q'(u_1,v_1)$ dir,
5. Q ve Q' aynı tamsayıyı temsil ederler,
6. Q ve Q' formları tarafından öz temsil edilen tamsayılar aynıdır.

İspat: 1. $Q'=Q|_S$ kuadratik formunun matrisi $M(Q|_S)$, S^T matrisi S matrisinin transpozu olmak üzere, $M(Q|_S)=S^TM(Q)S$ aşağıdaki formülden elde edilir.

$$\begin{aligned} S^TM(Q)S &= \begin{pmatrix} r & t \\ s & u \end{pmatrix}\begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix}=\begin{pmatrix} r & t \\ s & u \end{pmatrix}\begin{pmatrix} 2Ar+Bt & 2As+Bu \\ Br+2Ct & Bs+2Cu \end{pmatrix} \\ &= \begin{pmatrix} 2Ar^2+2Brt+2Ct^2 & 2Ars+2Ctu+B(ru+st) \\ 2Ars+2Ctu+B(ru+st) & 2As^2+2Bsu+2Cu^2 \end{pmatrix} \\ &= M(Q') \\ &= M(Q|_S) \end{aligned}$$

olur. Bu durumda

$$d(Q')=-\det M(Q|_S)=-(\det S)^2\det M(Q)=(\det S)^2 d(Q)$$

eşitliği elde edilir. $S\in SL_2(\mathbb{Z})$ matrisinin determinantı 1 olduğundan $d(Q')=d(Q)$ olur.

2. $ebob(A,B,C)\,|\,ebob(A',B',C')$ olduğu kolayca görülür. $Q=Q'|_{S^{-1}}$ olduğundan benzer şekilde $ebob(A',B',C')\,|\,ebob(A,B,C)$ olur. Buradan $ebob(A,B,C)=ebob(A',B',C')$ elde edilir.

3. $d=B^2-4AC<0$ alınsın. $4AA'=4A^2r^2+4ABrt+4ACt^2=(2Ar+Bt)^2-dt^2\geq 0$ eşitliğinde $(2Ar+Bt)^2-dt^2=0$ alındığında eşitliği sağlayan tek durum $r=t=0$ olur, buradan $\det S=0$ elde edilir. Bu da $\det S=1$ olmasıyla çelişir. Buradan $4AA'=(2Ar+Bt)^2-dt^2>0$ olur. Yani $4AA'>0$ olup $AA'>0$ elde edilir. Bu da A ile A' nün aynı işarete sahip olması demektir.

4. Genelliği bozmaksızın $M=M(Q)$ yazılsın. n tamsayısı Q kuadratik formu tarafından temsil edilsin. (1.4)' e göre $4Q(x,y)=(x,y)M\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)$ dir. Buradan $4n=(x,y)M\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)$ olur. $M(Q|_S)=S^TMS$ ve $\left(\begin{smallmatrix}u_1\\v_1\end{smallmatrix}\right)=\mathrm{S}^{-1}\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)$ olduğundan $4n=4Q|_S\,(u_1,v_1)=(u_1,v_1)S^TMS\left(\begin{smallmatrix}u_1\\v_1\end{smallmatrix}\right)$ bulunur.

5. (x,y) tamsayıları için $n=Q(x,y)$ olsun. $S\in SL_2(\mathbb{Z})$ olduğundan $S^{-1}\in SL_2(\mathbb{Z})$ olur. Bu da u ve v' nin tamsayı olduğunu gösterir. 4' e göre $Q(x,y)=Q'(u_1,v_1)$ olduğundan aynı sayıyı temsil ederler.

6. $Q(x,y)$ formu n' nin bir öz temsili olsun. Bu durumda $ebob(x,y)=1$ dir. Ayrıca $\left(\begin{smallmatrix}u_1\\v_1\end{smallmatrix}\right)=\mathrm{S}^{-1}\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)$ den $ebob(x,y)\,|\,ebob(u_1,v_1)$ dir. Benzer şekilde $ebob(u_1,v_1)\,|\,ebob(x,y)$ dir. $1\,|\,ebob(u_1,v_1)$ ve $ebob(u_1,v_1)\,|\,1$ olduğundan $ebob(u_1,v_1)=1$ elde edilir. Bu da istenendir.

Örnek 1.4.5. $Q(x,y)=x^2+y^2$ kuadratik formu 5 tamsayısını $5=2^2+1^2$ olacak şekilde temsil eder. $S=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}\in SL_2(\mathbb{Z})$ matrisi alındığında $Q'=Q\mid_S$ olacak şekilde bir $S\in SL_2(\mathbb{Z})$ matrisi bulunduğu için Q ve Q' formları denktir.

$$\begin{aligned}Q\mid_S(x,y)&=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}=(2x+y,x+y)\\ &=(2x+y)^2+0(2x+y)(x+y)+(x+y)^2\\ &=5x^2+6xy+2y^2\end{aligned}$$

bulunur. Şimdi $S^{-1}=\begin{pmatrix}1 & -1\\ -1 & 2\end{pmatrix}$ olduğundan $S^{-1}\begin{pmatrix}2\\ 1\end{pmatrix}=\begin{pmatrix}1 & -1\\ -1 & 2\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}=\begin{pmatrix}1\\ 0\end{pmatrix}$ bulunur. Gerçekten de $Q\mid_S(1,0)=5$ tir.

Örnek 1.4.6. $Q=(1,0,5)$ ve $Q'(2,2,3)$ kuadratik formlarının ikisinin de diskriminantı $d=-20$ olmasına rağmen bu iki form denk değildir. Birinci form 1 sayısını temsil etsin. Bu formlar denk olmadığından ikinci kuadratik formun 1 sayısını temsil edemeyeceğini gösterelim. $1=2x^2+2xy+3y^2$ den $2=(2x+y)^2+5y^2$ olur. Bu da ikinci formun 1 sayısını temsil edemeyeceğini gösterir.

1.5. Otomorfizm ve Pell Denklemleri

Bir Q kuadratik formu verilsin. Q formunu kendine dönüştüren bütün $S\in SL_2(\mathbb{Z})$ matrislerinin kümesi dönüşümlerin bileşke işlemine göre bir grup oluşturur. Bu gruba, Q formunun otomorfları grubu denir. Bu

$$Aut^+(Q)=\{S\in SL_2(\mathbb{Z}):Q\mid_S=Q\}$$

şeklinde gösterilir [6].

$Q=(A,B,C)$, d diskriminantlı bir primitif kuadratik form olsun. $S=\begin{pmatrix} r & s \\ t & u \end{pmatrix}\in SL_2(\mathbb{Z})$ bu formun bir otomorfu olsun. $M(Q)=\begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix}$ matrisini kullanarak $Q=Q|_S$ eşitliğini $M(Q)=M(Q|_S)=S^TM(Q)S$ veya buna denk olacak şekilde

$$\begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix}=\begin{pmatrix} u & -t \\ -s & r \end{pmatrix}\begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix}$$

biçiminde yazılabilir. Buradan

$$\begin{pmatrix} 2Ar+Bt & 2As+Bu \\ Br+2Ct & Bs+2Cu \end{pmatrix}=\begin{pmatrix} 2Au-Bt & Bu-2Ct \\ -2As+Br & -Bs+2Cr \end{pmatrix}$$

elde edilir. Matrislerin eşitliğinden aşağıdaki eşitlikler

$$Bt=A(u-r),\qquad As=-Ct,\qquad Bs=C(r-u)$$

elde edilir.

İlk iki denklemden $A\mid Bt$ ve $A\mid Ct$ olduğu görülür. Q primitif olduğundan $ebob(A,ebob(B,C))=1$ olur. Buradan $A\mid t$ elde edilir. O halde $U=\frac{t}{A}$ olacak biçimde bir U tamsayısı vardır. $As=-Ct$ denkleminde $\frac{t}{A}$ yerine U yazıldığında

$s=-CU$, $t=AU$ ve $BU=u-r$ elde edilir. Bundan sonrasını iki farklı durumda inceleyelim.

$d=4m$ ise $B\equiv d(\bmod 2)$ olduğundan B çifttir. $A(r-u)\equiv C(r-u)\equiv 0(\bmod 2)$ ve (A,B,C) primitif olduğundan A ya da C den en az biri tektir . O halde $r\equiv u(\bmod 2)$ yazılabilir. $T\in\mathbb{Z}$ için $u+r=2T$ alınırsa Q formunun A,B,C katsayılarını ve r,s,t,u yu T,U cinsinden ifade edebiliriz. Bu denklemler

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}=\begin{pmatrix} T-\dfrac{B}{2} & -CU \\ AU & T+\dfrac{B}{2}U \end{pmatrix}$$

matris formlarıyla gösterilebilir.

Bu matris $SL_2(\mathbb{Z})$ kümesinin elemanı olduğundan $1=ru-st=T^2-mU^2$ bulunur. Bundan dolayı

$$T^2-mU^2=1$$

bulunur. Böylece her otomorf Pell denkleminin bir tamsayı çözümünden geldiği görülür. Aksine Pell denklemlerinin her tamsayı çözümü Q formunun bir otomorfunu verir.

$d=4m+1$ ise $B\equiv d(\bmod 2)$ olduğundan B tektir. Bu yüzden $u+r\equiv u-r=BU\equiv U(\bmod 2)$ olur. Böylelikle $r+u=2T+U$ olacak biçimde bir T tamsayısı vardır. Bu durumda $r=T+\dfrac{1-B}{2}U$, $u=T+\dfrac{1+B}{2}U$ olup

$$1 = ru - st = T^2 + TU + U^2\frac{1-B^2}{4} + ACU^2 = T^2 + TU - mU^2$$

elde edilir. Buradan

$$T^2 + TU - mU^2 = 1$$

olur. Dolayısıyla

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} T + \frac{1-B}{2}U & -CU \\ AU & T + \frac{1+B}{2}U \end{pmatrix}$$

dir.

BÖLÜM 2. KUADRATİK FORMLARIN İNDİRGENMESİ

Hangi tamsayıların bir Q kuadratik formu tarafından temsil edilebileceği sorusu bir çok matematikçi tarafından ele alınmıştır. Basit gibi görünen bu soru ile aslında cebirsel sayılar teorisinin resiprosite ve sınıf cisimleri alanında önemli gelişmeler sağlanmıştır ve sağlanmaya devam etmektedir. Literatürde bazı kaynaklarda, örneğin [14,16,17],

1. $p \equiv 1 (\mathrm{mod}\, 4)$
2. $x^2 \equiv -1 (\mathrm{mod}\, p)$ nin bir x tamsayı çözümü vardır. Yani $\left(\frac{-1}{p}\right) = 1$ dir.
3. $p = x^2 + y^2,\ x, y \in \mathbb{Z}$

ifadelerinin birbirine denk olduğu ispatlanmıştır. Fermat ve Euler de sonsuz azalan yöntemini kullanarak buna benzer ifadeleri ispatlamışlardır. Ayrıca Langrange, benzer sonuçları daha kolay elde edecek şekilde kuadratik formların indirgeme teorisini geliştirmiştir. $x^2 + ay^2$ biçimindeki formların asal bölenlerini ele almak Euler, Langrange ve Legendre' ın kuadratik resiprosite kurallarını bulmasını sağlamıştır. Aşağıda Euler, Langrange ve Legendre' nin elde ettiği temel sonuçlar bulunmaktadır.

Kongrüans	Şart	Form
$p \equiv 1 (\mathrm{mod}\, 4)$	$x^2 \equiv -1 (\mathrm{mod}\, p)$	$p = x^2 + y^2$
$p \equiv 1 (\mathrm{mod}\, 3)$	$x^2 \equiv -3 (\mathrm{mod}\, p)$	$p = x^2 + 3y^2$
$p \equiv \pm 1 (\mathrm{mod}\, 8)$	$x^2 \equiv +2 (\mathrm{mod}\, p)$	$p = x^2 - 2y^2$
$p \equiv 1, 3 (\mathrm{mod}\, 8)$	$x^2 \equiv -2 (\mathrm{mod}\, p)$	$p = x^2 + 2y^2$

Euler yukarıdaki tabloda durumların birbirine denk olduğunu bilmesine rağmen bunları tam olarak ispatlayamamıştır. Langrange ise bazı formların birbirleri cinsinden yazılabileceğini farkederek büyük katsayılı bir formu küçük katsayılı diğer formlara dönüştürerek Langrange indirgeme teorisinin temellerini atmıştır. Langrange indirgemesi olarak adlandırılan bu indirgeme yöntemi Bölüm 2.1' de verilecektir.

2.1. Langrange İndirgemesi

Verilen bir Q formunun katsayıları olabildiğince küçük olan bir Q' formuna denk olduğu gösterilmiştir. Bu da verilen bir denklik sınıfındaki bütün (A,B,C) formları için A nın mümkün olan en küçük değeri, bu sınıftaki formlar tarafından temsil edilen en küçük katsayı ile ilişkili olduğunu gösterir.

Tanım 2.1.1. $|B| \le |A| \le |C|$ şartını sağlayan bir $Q = (A,B,C)$ formuna Langrange indirgenmiş form denir [12].

Önerme 2.1.2. Bir n tamsayısının öz temsili Q formu ise $A' = n$ olmak üzere $Q \sim Q' = (A',B',C')$ olan bir Q' formu vardır [12].

İspat: n tamsayısının öz temsili Q formu olsun. Yani $Ax^2 + Bxy + Cy^2 = n$ olsun. Q formuna denk olan bir Q' formu olduğunu göstermek için bir $S \in SL_2(\mathbb{Z})$ matrisi bulunmalıdır. Bir $S = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ matrisi alınsın.

$$Q'(x,y) = Q\left(\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) = Q\left(rx + sy, tx + uy\right)$$

den $A' = Q(r,t) = Ar^2 + Brt + Ct^2$ olduğu görülür. $Q = (A,B,C) = n$ olduğundan $A' = n$ elde edilir. Ayrıca Q formu n'nin bir öz temsili olduğundan $ebob(r,t) = 1$ olur. Buradan $ru - st = 1$ olacak şekilde $u,s \in \mathbb{Z}$ vardır. Bu da istenen $S \in SL_2(\mathbb{Z})$ matrisini verir.

Önerme 2.1.3. İkili kuadratik formların her denklik sınıfı $|B| \le |A| \le |C|$ olacak biçimde bir (A,B,C) formu içerir.

İspat: $d = B^2 - 4AC$ diskriminantlı bir Q kuadratik formu verilsin. Bu form için uygun bir $S = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ matrisi alınsın. Bu durumda

$$\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = (x - ny, y) \Longrightarrow A(x-ny)^2 + B(x-ny)y + Cy^2$$
$$= Ax^2 + (B - 2An)xy + (An^2 - Bn + C)y^2$$

olup buradan yeni bir

$$Q = (A, B - 2An, An^2 - Bn + C)$$

formu elde edilir. Bu formun Langrange indirgenmiş olabilmesi için $|B - 2An| \le |A|$ şartını sağlaması gerekir. Buradan bu şartı sağlayacak şekilde uygun bir n tamsayısı seçilir. Bulunan form Langrange indirgenmiş ise işlem biter. Eğer bulunan form Langrange indirgenmiş form değilse bu forma bir $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ matrisi uygulanır. Böylece

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = (-y, x) \Rightarrow A(-y)^2 + Bx(-y) + Cx^2 = Ay^2 - Bxy + Cy^2$$

olup buradan da

$$Q = (C, -B, A)$$

formu elde edilir. Bulunan form indirgenmiş ise işlem sonlanır. Bulunan form indirgenmiş değilse yukarıda yapılan işlemler indirgenmiş form bulana kadar tekrar edilir.

Örnek 2.1.4. $(2,5,4)$ formu Langrange indirgenmiş form değildir. Aşağıdaki şekilde indirgenir.

$(2,5,4)$ formuna $S = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ matrisi uygulanırsa $Q = (2, 5-4n, 2n^2 - 5n + 4)$ formu elde edilir. Bu formun Langrange indirgenmiş olması için $|5-4n| \le |2|$ eşitsizliğini sağlayacak şekilde uygun bir n seçilir. Burada $n = 1$ olduğu görülür. Buradan $Q = (2,1,1)$ formu bulunur. Ancak bu form ingenmiş olmadığından bulduğumuz bu forma $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ matrisi uygulanır. Böylece yeni Q formu $Q = (1,-1,2)$ bulunur. Bu formda Langrange indirgenmiş formdur.

Önerme 2.1.5. Bir $Q = (A,B,C)$ Langrange indirgenmiş formunun katsayıları aşağıdaki eşitsizlikleri sağlar.

1. $d < 0$ ise $|B| \le \sqrt{\frac{-d}{3}}$, $|A| \le \sqrt{\frac{-d}{3}}$ ve $|C| \le \frac{1-d}{4}$,
2. $d > 0$ ise $|B| \le \sqrt{\frac{d}{5}}$, $|A| \le \sqrt{\frac{d}{2}}$ ve $|C| \le \frac{d}{4}$

dir.

İspat: 1. $d<0$ ise $B^2-4AC=d<0$ olur, böylece $AC>0$ elde edilir. (A,B,C) formu Langrange indirgemesini sağladığından $|B|\le|A|\le|C|$ dir. Buradan

$$-d=4AC-B^2\ge 4A^2-A^2=3A^2$$

olup $|A|\le\sqrt{\frac{-d}{3}}$ elde edilir. Ayrıca $|B|\le|A|$ olduğundan $|B|\le\sqrt{\frac{-d}{3}}$ bulunur. Bunlara ek olarak

$$|C|=\frac{B^2}{4|A|}-\frac{d}{4|A|}\le\frac{A^2}{4|A|}-\frac{d}{4|A|}=\frac{|A|}{4}-\frac{d}{4|A|}$$

elde edilir. $|A|$ bir fonksiyon ve d bir sabit sayı gibi düşünülürse sağ taraftaki ifade $\left[1,\sqrt{-d}\right]$ aralığında azalandır ve maksimum değerine $|A|=1$ sınırında ulaşılır. Böylece ispat tamamlanmış olur.

2. $d>0$ durumunu ele alınsın. Bu durumda $AC\ge B^2>4AC$ olduğundan $AC<0$ elde edilir. Böylece $d=B^2-4AC=B^2+4|AC|\ge 5B^2$ bulunur. Bu da $|B|\le\sqrt{\frac{d}{5}}$ eşitsizliğini verir. $B^2\ge 0$ ve $|C|\ge|A|$ eşitsizliklerinden $d=B^2+4|AC|\ge 4A^2$ olduğu görülür. Böylece $|A|\le\frac{1}{2}\sqrt{d}$ olur. Dolayısıyla $4|C|\le 4|AC|=d-B^2\le d$ olup $|C|\le\frac{d}{4}$ bulunur. Bu da bize son eşitsizliği verir.

Önerme 2.1.5' ten aşağıdaki sonuç verilebilir.

Sonuç 2.1.6. d diskriminantlı indirgenmiş formların sayısı sonludur.

Örnek 2.1.7. $d=-260$ diskriminantlı pozitif belirli Langrange indirgenmiş formları bulalım. Önerme 2.1.5' ten $|B| \le \sqrt{\frac{260}{3}} < 10$ olduğundan $-8 \le B \le 8$ bulunur. Ayrıca Langrange indirgenmiş formları aradığımızdan bu formların $|B| \le |A| \le |C|$ şartını sağlaması gerekir. Buradan $B \equiv 0 (\mathrm{mod}\, 2)$ olduğundan B değerleri $B = 0,\ \pm 2,\ \pm 4,\ \pm 6,\ \pm 8$ bulunur.

$B=0$ değeri için $-260 = 0^2 - 4AC \Rightarrow AC = 65$ elde edilir. Buradan $(1,0,65),\ (65,0,1),\ (5,0,13)$ ve $(13,0,5)$ formları elde edilir. Ancak bu formlardan $(1,0,65),\ (5,0,13)$ formları Langrange indirgenmiştir.

$B=\pm 2$ değeri için $AC=66$ olup buradan $(2,\pm 2,33),\ (3,\pm 2,22)$ ve $(6,\pm 2,11)$ Langrange indirgenmiş formları elde edilir.

$B=\pm 4$ değeri için $AC=69$ olup buradan $(1,\pm 4,69),\ (69,\pm 4,1),\ (3,\pm 4,23)$ ve $(23,\pm 4,3)$ formları bulunur. Ancak bu formların hiçbiri $|B| \le |A| \le |C|$ şartını sağlamadığından Langrange indirgenmiş değildir.

$B=\pm 6$ değeri için $AC=74$ olup hiçbir Langrange indirgenmiş form yoktur.

Son olarak $B=\pm 8$ değeri için $AC=81$ olup $(9,\pm 8,9)$ Langrange indirgenmiş formları elde edilir.

Böylece $d=-260$ diskriminantlı Langrange indirgenmiş formların sayısının 10 olduğu görülür.

Örnek 2.1.8. $d=13$ diskriminantlı belirsiz Langrange indirgenmiş formları bulalım. Önerme 2.1.5' ten $|B| \le \sqrt{\frac{13}{5}}$ olduğundan $-2 \le B \le 2$ bulunur. Buradan $B = 13 \equiv 1 (\mathrm{mod}\, 2)$ olup B değerleri ± 1 olarak elde edilir.

$B = \pm 1$ değerleri için $13 = 1 - 4AC$ olup $AC = 3$ bulunur. Buradan $(1, \pm 1, -3)$, $(-1, \pm 1, 3)$, $(3, \pm 1, -1)$ ve $(-3, \pm 1, 1)$ kuadratik formları elde edilir. Ancak bu formlardan $(1, \pm 1, -3)$ ve $(-1, \pm 1, 3)$ formları Langrange indirgenmiştir.

Tanım 2.1.9. $Q_0 = \begin{cases} (1,0,m), & d=-4m \\ (1,1,m), & d=1-4m \end{cases}$ olacak biçimde Langrange indirgemesine sahip, d diskriminantlı kuadratik forma temel form denir.

2.2. Pozitif Belirli Formların İndirgenmesi

Bu bölümde $A > 0$, $d = B^2 - 4AC < 0$ ve $ebob(A, B, C) = 1$ olmak üzere $Q = (A, B, C)$ primitif formları ele alınacaktır. Primitif kuadratik formların her denklik bağıntısı bir ya da daha fazla Langrange indirgenmiş form içerir.

Tanım 2.2.1. $Q = (A, B, C)$ pozitif belirli formu

$$-A < B \le A < C$$

veya

$$0 \le B \le A = C$$

şartlarını sağlıyorsa Q formuna indirgenmiş form denir.

Bundan sonra pozitif belirli formlarla çalışılacağı için $A > 0$ alınacaktır.

Önerme 2.2.2. $B > 0$ ve $Q = (A, B, C)$ indirgenmiş ise, Q formunun en küçük tamsayı öz temsilleri A, C ve $A - B + C$ dir. Daha açık şekilde $A = Q(\pm 1, 0)$, $C = Q(0, \pm 1)$, $A - B + C = Q(\pm 1, \mp 1)$ formlarının yanı sıra

$$(x, y) \neq (0,0),\ (\pm 1, 0) \Rightarrow Q(x, y) \geq A$$
$$(x, y) \neq (0,0),\ (\pm 1, 0),\ (0, \pm 1) \Rightarrow Q(x, y) \geq C$$
$$(x, y) \neq (0,0),\ (\pm 1, 0),\ (0, \pm 1),\ (\pm 1, \mp 1) \Rightarrow Q(x, y) \geq A - B + C$$

dir .

İspat: Bu sayıların Q tarafından öz temsil edilen en küçük sayılar olduğunu göstermek için $xy > 1$ olan x, y tamsayıları için $Q(x, y) \geq A - |B| + C$ olduğu gösterilmelidir. Bunu üç durumda inceleyelim.

1. $|x| = |y|$ ise $Q(x, y) = Ax^2 - |B|xx + Cx^2 = x^2(A - |B| + C) > A - |B| + C$ dir.
2. $|x| > |y|$ ise $Q(x, y) \geq Ax^2 - |B||xy| + Cy^2 > (A - |B|)|xy| + Cy^2$
$$\geq (A - |B| + C)y^2 > A - |B| + C$$

dir.

3. $|x| < |y|$ ise $Q(x, y) \geq (A - |B| + C)x^2 > A - |B| + C$ dir.

Buradaki A, C ve $A - |B| + C$ tamsayıları farklı olmak zorunda değildir. Yani eğer $Q = (1,1,1)$ ise $A = C = A - |B| + C = 1$ olur.

Önerme 2.2.2 özellikle, denk olan pozitif belirli iki formun birbirine eşit olduğunu ispatlamak için kullanılır.

Sonuç 2.2.3. 1 ile temsil edilen bir pozitif belirli kuadratik form temel forma denktir.

İspat: Q, 1 ile temsil edilen bir kuadratik form olsun. Bu durumda Q formu 1 tarafından temsil edilen indirgenmiş bir Q' formuna denk olur. Q' tarafından temsil edilen en küçük doğal sayı 1 olduğundan Önerme 2.2.2' ye göre $Q'=(A,B,C)$ formunda $A=1$ alabiliriz. Q' indirgenmiş olduğundan $|B|\le|A|=1$ olur. Böylece $Q'=(1,0,C)$ veya $Q'=(1,1,C)$ olur. Bu formlar da sırasıyla $d=-4C$, $d=1-4C$ diskriminantlarına sahip temel formlardır.

Teorem 2.2.4. Primitif pozitif belirli kuadratik formların her denklik sınıfı bir tek indirgenmiş form içerir.

İspat: $Q=(A,B,C)$ ve $Q'=(A',B',C')$ formları pozitif belirli ve indirgenmiş form olsun. Q ve Q' denk formlarının birbirine eşit olduğu gösterilmelidir. Q ve Q' formlarının temsil ettiği en küçük tamsayılar sırasıyla A ve A' olsun. $Q\sim Q'$ olduğundan aynı tamsayıları temsil ederler. Buradan $A=A'$ olur. Q indirgenmiş olduğundan $C\ge A$ dır. Burada iki durumla karşılaşılır:

1. $C>A$ olsun. $A=Q(\pm1,0)$ olduğundan A, Q tarafından iki kez temsil edilir. Aynı şekilde A, Q' tarafından da iki kez temsil edilir. Böylece $C'=Q'(0,\pm1)>A'=A$ olur. C, Q tarafından temsil edilen ikinci en küçük tamsayı olduğundan Q' tarafından da temsil edilen ikinci küçük tamsayı olur. Q ve Q' birbirine denk olduğundan $C=C'$ olur. Ayrıca $d(Q)=d(Q')$ olduğundan $|B|=|B'|$ olur. Eğer $B'=-B$ alırsak $(A,B,C)=Q\sim Q'=(A,-B,C)$ olur. $S=\begin{pmatrix} r & s \\ t & u \end{pmatrix}\in SL_2(\mathbb{Z})$ için $Q'=Q|_S$ olsun. Buradan da $A=A'=Ar^2+Brt+Ct^2$ olduğu görülür. $C>A$ olduğundan bu denklemin tek çözümü $r=\pm1,\ t=0$ dır. Böylece $S=\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ veya $S=\begin{pmatrix} -1 & s \\ 0 & -1 \end{pmatrix}$ olur. $-B=B'=2As+B$ ise $As=-B$ dir. $|B|\le A$ olduğundan $s=0$ alınabilir. Buradan da $B=0=-B=B'$ olur. Ya da $s=1$

alabiliriz. Ancak $s=1$ alındığında da $B=-A$ olur. Bu da Q formunun indirgenmiş olmasıyla çelişir. Bütün bu durumlarda da $Q=Q'$ olur.

2. $C=A$ olsun. Bu durumda $A=Q(\pm 1,0)=Q(0,\pm 1)$ olur. Bu da A nın Q tarafından en az dört kez temsil edildiğini gösterir, aynı zamanda Q' tarafından da dört kez temsil edildiğini gösterir. Bu durumda $C'=A$ olur ve böylece $C=C'$ bulunur. Birinci durumda olduğu gibi $B'=\pm B$ elde edilir. Ancak $(A,B,A)\sim(A,B',A)$ ve indirgenmiş olduğundan B ve B' pozitif olmalıdır. Buradan da $Q=Q'$ elde edilir.

Tanım 2.2.5. $d<0$ diskriminantlı primitif tam formların denklik sınıflarının sayısına d ' nin sınıf sayısı denir ve $h(d)$ ile gösterilir.

Örnek 2.2.6. $d=-20$ olmak üzere $h(-20)$ sınıf sayısını bulalım.

$d<0$ olduğundan Önerme 2.1.5' ten $B\le\sqrt{\frac{-20}{3}}$ olur. Buradan $B=0,1,2$ elde edilir.

$B=0$ değeri için $B^2-4AC=-20$ olup $AC=5$ bulunur. Böylece $(1,0,5)$, $(5,0,1)$ formları elde edilir. Ancak sadece $(1,0,5)$ indirgenmiş formdur.

$B=1$ değeri için uygun A ve C tamsayı değerleri yoktur.

$B=2$ değeri için $B^2-4AC=-20\Rightarrow AC=6$ bulunur. Buradan $(1,2,6)$, $(6,2,1)$, $(2,2,3)$ ve $(3,2,2)$ formları elde edilir. Ancak $(2,2,3)$ formu indirgenmiştir.

Böylece $d=-20$ diskriminantının sınıf sayısı $h(-20)=2$ bulunur.

2.3. Zagier İndirgemesi

Tanım 2.3.1. Tamkare olmayan pozitif d diskriminantına sahip bir $Q=(A,B,C)$ belirsiz formu

$$\begin{aligned}&\sqrt{d}<B<\sqrt{d}+2A,\\&\sqrt{d}<B<\sqrt{d}+2C\end{aligned} \qquad \textbf{(2.1)}$$

şartlarını sağlıyorsa bu forma Zagier indirgenmiş form veya kısaca Z-indirgenmiştir denir [12]. Zagier indirgemesi belirsiz formlarda kullanılır.

Tanım 2.3.1' e gore ilk katsayısı en küçük olacak şekilde $A>0$ olan bir form seçilsin. B modulo $2|A|$' ya göre seçilirse B, $2A$ uzunluğunda bir aralıkta değer alabilir. Buradan $B\in\left[\sqrt{d},\sqrt{d}+2A\right]$ olur. Bu seçimden $AC>0$ elde edilir. Q formu C' yi temsil etsin. A' nın en küçük oluşundan $A\le C$ bulunur. Böylece $B\in\left[\sqrt{d},\sqrt{d}+2C\right]$ de yazılabilir.

Teorem 2.3.2. $Q=(A,B,C)$, d diskriminantlı primitif belirsiz form olsun. $Q(x,-1)=Ax^2-Bx+C$ kuadratik denkleminin iki kökü $\xi_1=\dfrac{B+\sqrt{d}}{2A}$ ve $\xi_2=\dfrac{B-\sqrt{d}}{2A}$ olsun. Bu durumda aşağıdaki ifadeler birbirine dektir.

a) (A,B,C) Zagier indirgenmiştir.

b) (C,B,A) Zagier indirgenmiştir.

c) $0<B-\sqrt{d}<2A<B+\sqrt{d}$ dir.

d) $0 < B - \sqrt{d} < 2C < B + \sqrt{d}$ dir.

e) $0 < \xi_2 < 1 < \xi_1$ dir.

f) $A > 0,\ C > 0,\ B > A + C$ dir.

İspat: a)$\Rightarrow$b): olduğunu gösterelim. Zagier indirgemesi tanımına göre A ve C simetriktir. Böylece a) ve b) ifadeleri birbirine denk olur.

a)$\Rightarrow$c): (A,B,C) formu Zagier indirgenmiş ise (2.1)' e göre $0 < B - \sqrt{d} < 2A < B + \sqrt{d}$ dir. Ayrıca Zagier indirgenme tanımından $A > 0$ ve $C > 0$ dır. Bu da $B^2 + 4AC > d$ olmasını sağlar. Böylece $B > \sqrt{d}$ olur. Dolayısıyla $0 < B - \sqrt{d}$ yazılabilir. $B < \sqrt{d} + 2A$ eşitsizliğinden $B - \sqrt{d} < 2A$ bulunur. Zagier indergeme tanımına göre $B < \sqrt{d} + 2C$ olduğundan $2A = \dfrac{B^2 - d}{2C} < \dfrac{B^2 - d}{B - \sqrt{d}} = B + \sqrt{d}$ elde edilir.

a)$\Rightarrow$d): (A,B,C) formu Zagier indirgenmiş ise $0 < B - \sqrt{\Delta} < 2C < B + \sqrt{d}$ dir. Yukarıdaki ispatta (A,B,C) yerine (C,B,A) yazıldığında ispat biter.

c)$\Rightarrow$e): $0 < B - \sqrt{d} < 2A < B + \sqrt{d}$ eşitsizliğinde her taraf $2A$ ile bölünürse $0 < B - \sqrt{d} < 2A < B + \sqrt{d}$ ile $0 < \xi_2 < 1 < \xi_1$ ifadeleri birbirine denk olur.

e)$\Rightarrow$f): $\xi_1 - \xi_2 > 0$ olduğundan $A > 0$ bulunur. $\xi_1 = \dfrac{B + \sqrt{d}}{2A} > 1$ ve $\xi_2 = \dfrac{B - \sqrt{d}}{2A} < 1$ eşitsizliğinden $|B - 2A| < \sqrt{d}$ olur. Böylece

$$d-(B-2A)^2=4A(B-A-C) \qquad \textbf{(2.2)}$$

özdeşliğinden $B>A+C$ olduğu görülür. Sonuç olarak $C=\xi_1\xi_2>0$ elde edilir.

Şimdi d)$\Rightarrow$e) olduğunu gösterelim. $d-(B-2A)^2=4A(B-A-C)$ eşitsizliğinden $|B-2A|<\sqrt{d}$ sağlanır, bu da $\xi_1>1$ ve $\xi_2<1$ eşitsizliklerini verir. $0<C=\xi_1\xi_2$ olduğundan $\xi_2>0$ olur bu da ispatı tamamlar.

Önerme 2.3.3. d diskriminantlı $Z-$indirgenmiş formlar sonlu sayıdadır. Yani, $Q=(A,B,C)$ $Z-$indirgenmiş formların katsayıları $0<A,\ C\le\dfrac{d}{4}$ ve $\sqrt{d}<B\le\dfrac{d+1}{2}$ eşitsizliklerini sağlar.

İspat: (2.2)' den $\dfrac{d-(B-2A)^2}{4(B-A-C)}\le\dfrac{d}{4}$ eşitsizliği yazılabilir. Simetriden dolayı C için de aynı eşitsizlik geçerli olur. Sonuç olarak $B^2=d+4AC\le d+\dfrac{1}{4}(d-1)^2=\dfrac{1}{4}(d+1)^2$ bulunur. Bu da istenendir.

d diskriminantlı primitif formların F_d kümesi üzerinde indirgenmiş formların bazı notasyonlarını verelim. R_d, indirgenmiş formların alt kümesi olsun. Böyle bir durumda indirgeme özellikleri taşıyan bir

$$\rho: F_d\to F_d$$

indirgeme dönüşümü tanımlanabilir.

Herhangi bir $Q\in F_d$ formu verilsin. Bir $v\ge 0$ tamsayısı vardır öyle ki

$$\rho^{v}(Q) = \underbrace{(\rho \circ \rho \circ ... \circ \rho)}_{v \text{ kez}}(Q)$$

indirgenmiştir. Yani $\rho^{v}(Q) \in R_d$ olacak biçimde bir v pozitif tamsayısı vardır. Q indirgenmiş ise $\rho(Q)$ da indirgenmiştir. Yani ρ, R_d yi R_d ye dönüştürür.

Böyle bir durumda $\rho(Q)$ formuna Q formunun sağ komşuluğu denir ve ρ nin görüntüsündeki formlara da yarı indirgenmiş formlar denir.

Eğer $R_d = R_{zag}$, d diskriminantlı Zagier indirgenmiş formların kümesi ise aşağıdaki gibi bir indirgeme dönüşümü mevcuttur.

Bir $Q = (A, B, C)$ formunun $\rho(Q)$ sağ komşuluğu, $n > \dfrac{B + \sqrt{d}}{2A} > n - 1$ olmak üzere $S = S_n = \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$ için $Q' = Q|_S$ olan bir $Q' = (A', B', C')$ formudur. Burada $S_n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ Tanım 1.4.1 de verilen S ve T matrislerinden elde edilmektedir.

Lemma 2.3.4. $Q = (A, B, C)$ formunun sağ komşuluğu aşağıdaki şekilde hesaplanır.

$C' = A$

$B + B' \equiv 0 (\mathrm{mod}\, 2A)$ ve $\begin{cases} \sqrt{d} < B' < \sqrt{d} + 2A, & A > 0 \\ \sqrt{d} + 2A < B' < \sqrt{d}, & A < 0 \end{cases}$

$(B')^2 - 4A'C' = d$.

Bu durumlar sırasıyla C', B' ve A' sayılarını belirler.

İspat: n bir tamsayı olmak üzere, $B+B'=2An$ ve $S=\begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix}$ olsun. Buradan

$$\begin{aligned} Q' &= Q\left(\begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) = Q(nx+y,-x) \\ &= A(nx+y)^2 + B(nx+y)(-x) + C(-x)^2 \\ &= An^2x^2 + 2Anxy + Ay^2 - Bnx^2 - Bxy + Cx^2 \\ &= x^2\left(An^2 - bn + C\right) + xy(2An - B) + Ay^2 \end{aligned}$$

olur. Böylece $Q' = Q|_S$ olan $Q' = (A', B', C')$ formu $A' = An^2 - Bn + C$, $B' = 2An - B$ ve $C' = A$ olacak biçimde elde edilir. Eğer $A > 0$ için $2An > B + \sqrt{d} > 2A(n-1)$ olduğu ya da $A < 0$ için $2An < B + \sqrt{d} < 2A(n-1)$ olduğu gösterilebilirse $Q|_S = (A', B', C') = \rho(Q)$ eşitliği açıktır.

İlk eşitsizlik $2An - B > \sqrt{d}$ olmasına denktir ve $\sqrt{d} < B' = 2An - B$ seçildiğinde sağlanır. İkinci eşitsizlik de $2An - B < \sqrt{d} + 2A$ eşitsizliğine denktir ve $2An - B = B' < \sqrt{d} + 2A$ olduğundan sağlanır.

Son olarak da $(B')^2 - 4A'C' = d$ olduğunu gösterelim.

$$\begin{aligned} (B')^2 - 4A'C' &= (2An - B)^2 - 4\left(An^2 - Bn + C\right)A \\ &= 4A^2n^2 - 4nAB + B^2 - 4\left(An^2 - Bn + C\right)A \\ &= B^2 - 4AC \\ &= d \end{aligned}$$

elde edilir.

Örnek 2.3.5. $Q = (1,4,2)$ için $\rho(Q) = Q' = (2,4,1)$ ve $\rho(Q') = Q$ olduğunu gösterelim.

$Q=(A,B,C)=(1,4,2)$ olsun. Bu durumda $C'=A=1$ olup $B+B'\equiv 0(\mathrm{mod}\,2A)$ bulunur. Buradan $A>0$ ve $\sqrt{d}<B'<\sqrt{d}+2A$ olduğundan $B'\equiv -B\equiv -4\equiv 0(\mathrm{mod}\,2A)$ ve $\sqrt{8}<B'<\sqrt{8}+2$ için $B'=4$ olur. Sonuç olarak $d=(B')^2-4A'C'$ olup $A'=\dfrac{(B')^2-d}{4C'}=\dfrac{4^2-8}{4}=2$ bulunur.

Önerme 2.3.6. $Q=(A,B,C)$, $d>0$ diskriminantlı bir kuadratik form ve $Q'=(A',B',C')=\rho(Q)$ da bu kuadratik formun sağ komşuluğu olsun. Bu durumda aşağıdaki özellikler sağlanır.

1. $A<0$ ise $A'>A$ dır.
2. $A>0$ ise $A'>0$ dır.
3. $A'\geq A>0$ ise Q' formu Zagier indirgenmiştir.
4. Q Zagier indirgenmişse $n\geq 2$ olmak üzere, $S=S_n=\begin{pmatrix} n & 1\\ -1 & 0\end{pmatrix}$ için

   $\rho(Q)=Q|_S$ dir.

İspat: 2. θ bir reel sayı ve $0<\theta<1$ olmak üzere $\dfrac{B+\sqrt{d}}{2A}=n-\theta$ olsun. $A'=An^2-Bn+C$ eşitliğinde n yerine $\dfrac{B+\sqrt{d}}{2A}+\theta$ yazılırsa

$$A'=A\theta^2+\sqrt{d}\,\theta$$

elde edilir. Bu durumda hipotezin ikinci özelliği sağlanır.

1. $A<0$ ise A ve θ^2-1 negatif olduğundan $A'-A=A\left(\theta^2-1\right)+\sqrt{d}\,\theta>0$ elde edilir.

3. $A'\geq A>0$ olsun. Bu durumda

$$\begin{aligned} 0\leq A'-A&=\theta\sqrt{d}-A\left(1-\theta^2\right)\\ &<(1+\theta)\sqrt{d}-A\left(1-\theta^2\right)=(1+\theta)\left(\sqrt{d}-A(1-\theta)\right)\end{aligned}$$

$$= \frac{1+\theta}{1-\theta}\left(\sqrt{d}\,(1-\theta) - A(1-\theta)^2\right) = \frac{1+\theta}{1-\theta}\left(B' - A' - C'\right)$$

olur.

Ayrıca $A' \geq A > 0$, $C' = A > 0$ ve $B' > A' + C'$ olduğundan, Q' formunun Zagier indirgenmiş olduğu görülür.

4. Q formu Zagier indirgenmiş olsun. Buradan $\varepsilon_2 = \dfrac{B+\sqrt{d}}{2A} > 1$ olup bu da $n \geq 2$ olmasını sağlar.

Önerme 2.3.7. ρ dönüşümü bir indirgeme dönüşümüdür. Yani, $Q = (A, B, C)$ pozitif d diskriminantlı bir kuadratik form olmak üzere,

1. $\rho^v(Q)$ Zagier indirgenmiş olacak şekilde bir $v > 0$ tamsayısı vardır.
2. Q Zagier indirgenmişse $\rho(Q)$ da Zagier indirgenmiştir.

İspat: 1. A negatif ise Önerme 2.3.6' ya göre $A' > A$ olur. ρ yi tekrar tekrar uygulamak ilk katsayısı pozitif olan bir form verir. Önerme 2.3.6' nın ikinci özelliğine göre ilk katsayı pozitif ve $C' = A$ olduğundan ρ nin bir defa daha uygulanmasıyla elde edilen formun ilk ve son katsayısı pozitif olur. İlk katsayı pozitif kaldığından $A' \geq A$ olmalıdır. Ancak Önerme 2.3.6' nın ilk özelliğinden ρ nin birden fazla uygulaması bir Zagier indirgenmiş form üretir.

2. Eğer Q Zagier indirgenmişse bu durumda $\dfrac{\sqrt{d}}{A} = n - \theta - \dfrac{B-\sqrt{d}}{2A} > 1 - \theta$ olduğundan $A', C' > 0$ ve

$$B' - A' - C' = (1-\theta)\left(\sqrt{d} - A(1-\theta)\right) > 0$$

dir. Böylece $\rho(Q)=Q'$ Zagier indirgenmiştir.

Herhangi bir Q formunun bir $\rho(Q)$ sağ komşuluğu vardır. Genel olarak farklı formlar aynı sağ komşuluğa sahip olabilir. Ancak bu durum

$$\begin{cases}\sqrt{d}<B'<\sqrt{d}+2A, & A>0\\ \sqrt{d}+2A<B'<\sqrt{d}, & A<0\end{cases} \qquad \textbf{(2.3)}$$

şartlarını sağlayan $Q=(A,B,C)$ formu için sağlanmaz.

Tanım 2.3.8. (2.3) ile verilen şartları sağlayan formlara yarı indirgenmiş form denir.

Önerme 2.3.9. ρ dönüşümü yarı indirgenmiş formlar üzerinde birebirdir [12].

ρ indirgeme dönüşümünün tersinden $\lambda(Q)$ sol komşuluğunu tanımlayalım. $Q=(A,B,C)$ ve $Q'=(A',B',C')$ için $\rho(Q)=Q'$ olsun. Buradan $\lambda(Q')=Q$ olduğunu gösterelim. Bunun için

1. $A=C'$

2. $B+B'\equiv 0(\mathrm{mod}\,2C')$ ve $\begin{cases}\sqrt{d}<B<\sqrt{d}+2C', & C'>0\\ \sqrt{d}+2C'<B<\sqrt{d}, & C'<0\end{cases}$ **(2.4)**

3. $B^2-4AC=d$

olsun. Bu durumda A',B' ve C' den A,B ve C hesaplanabilir. Şimdi $\lambda(Q)$' nun bulunması için bir başka yöntemi Önerme 2.3.10 da verelim.

Önerme 2.3.10. $Q'=(A',B',C')$ bir primitif kuadratik form olsun. n, $n>\dfrac{B'+\sqrt{d}}{2C'}>n-1$ şartını sağlayan bir tamsayı olmak üzere, $S=\begin{pmatrix}0 & -1\\ 1 & n\end{pmatrix}$ için $\lambda(Q')=Q'|_S$ dir.

İspat: $B=-B'+2An$ olacak biçimde bir n tamsayısı olsun. Buradan

$$C=\frac{B^2-d}{4A}=A'-B'n+C'n^2$$

olur. Bundan dolayı $S=\begin{pmatrix}0 & -1\\ 1 & n\end{pmatrix}$ için $Q=\lambda(Q')=Q'|_S$ olur. Dolayısıyla $n=\frac{B'+B}{2A}=\frac{B'+B}{2C'}$ dir. Eğer $C'>0$ ise $B>\sqrt{d}$ ve $n>\frac{B'+\sqrt{d}}{2C'}>n-1$ dir. Eğer $C'<0$ ise $B<\sqrt{d}$ ve tekrar $n>\frac{B'+\sqrt{d}}{2C'}>n-1$ olur.

Önerme 2.3.11. Q yarı indirgenmişse, $(\lambda\circ\rho)(Q)=Q$ ve $(\rho\circ\lambda)(Q)=Q$ olur [12].

Önerme 2.3.11' den aşağıdaki sonuç verilebilir.

Sonuç 2.3.12. ρ indirgeme dönüşümü indirgenmiş formlar kümesinin permütasyonudur. Aynı sonuç λ için de geçerlidir.

İspat: ρ dönüşümü indirgenmiş formları indirgenmiş formlara dönüştürür. Q ve Q' indirgenmiş formlar ve $\rho(Q)=\rho(Q')$ olduğunu kabul edelim. Her iki tarafa λ uygulanırsa Önerme 2.3.11' den $Q=Q'$ elde edilir.

Tanım 2.3.13. Bir Q formunun kendisine denk olan $Q,Q_1,Q_2,...,Q_n$ biçimindeki sağ ya da sol komşuluklarından biri tekrar Q formuna denk oluyorsa Q formunun sağ komşuluklarına Q formunun bir devri denir. d diskriminantlı bir Q formunun sınıf sayısı $h(d)$, Q formunun devirlerinin sayısına eşittir.

Örnek 2.3.14. $d=5$ diskriminantlı kuadratik formun devirlerini bulalım. Önerme 2.3.3 teki $0<A,\ C\le\frac{d}{4}$ ve $\sqrt{d}<B\le\frac{d+1}{2}$ şartlarından ve $0<A,\ C\le\frac{5}{4}$ eşitsizliğinden $A=1,\ C=1$ ve $\sqrt{5}<B\le\frac{5+1}{2}$ olur. Buradan da $B=3$ bulunur. Bu şartlardan $Q=(1,3,1)$ formunu buluruz. (2.4)' e göre $C'=A$ olup dolayısıyla $C'=1$ bulunur. $A>0$ olduğundan $\sqrt{d}<B'<\sqrt{d}+2A$ dir. Ayrıca $B+B'\equiv 0(\mathrm{mod}\,2A)$ olduğundan $\sqrt{5}<B'<\sqrt{5}+2.1$ ve $3+B'\equiv 0\,\mathrm{mod}(2.1)$ ve böylece $B'=3$ buluruz. Diskriminanttan $A'=1$ bulunur. Yani Q nun komşuluğu olan Q' kendisine eşit olur. Burdan da Q nun devrinin bir olduğu görülür. Bu durumda Q formunun sınıf sayısı 1 olur. Yani $h(5)=1$ dir.

Örnek 2.3.15. $d=136$ diskriminantlı kuadratik formun devirlerini ve sınıf sayısını bulalım. Önerme 2.3.3 ten $0<A,\ C\le\frac{136}{4}$ ve $\sqrt{136}<B\le\frac{136+1}{2}$ yazılabilir. Diskriminant çift olduğundan $B=12,14,16,...,64,66,68$ değerlerini alır.

$B=12$ değeri için $d=B^2-4AC\Rightarrow AC=2$ ve böylece $Q=(1,12,2)$ kuadratik formu elde edilir. Bulunan Q formunun sağ komşuluklarını bulmak için Önerme 2.3.9' a göre $C'=1$ ve $A>0$ için $\sqrt{136}<B'<\sqrt{136}+2$ olup $12+B'\equiv 0(\mathrm{mod}\,2)$ den $B'=12$ olur. $d=(B')^2-4A'C'$ eşitliğinden $A'=2$ elde edilir. Q formunun sağ komşuluğu $Q'=(2,12,1)$ bulunur. Aynı işlemler tekrar edilerek Q' formunun sağ komşuluğunun kendisine eşit olduğu görülür.

$B=14$ değeri için $AC=15$ olup $(1,14,15),(15,14,1),(3,14,5),(5,14,3)$ kuadratik formları bulunur. Ancak bu formlardan $(1,14,15)$ ve $(15,14,1)$ formları indirgenmemiştir. Şimdi $(3,14,5)$ ve $(5,14,3)$ formlarının devirlerini bulalım.

$(3,14,5)$ formunun sağ komşulukları Önerme 2.3.9' a göre $C'=3$ ve $A>0$ için $\sqrt{136}<B'<\sqrt{136}+6$ olup $14+B'\equiv 0(\mathrm{mod}\,6)$ olduğundan $\mathrm{B}'=16$ olur. Diskriminanttan $A'=10$ bulunur. Bu şekilde devam edilirse $(3,14,5)$ formunun sağ komşulukları $(3,14,5)$, $(10,16,3)$, $(11,24,10)$, $(6,20,11)$, $(5,16,6)$ bulunur. En son bulunan $(5,16,6)$ formunun sağ komşuluğu $(3,14,5)$ olduğundan $(3,14,5)$ formunun $(3,14,5)$, $(10,16,3)$, $(11,24,10)$, $(6,20,11)$, $(5,16,6)$ devri elde edilir.

$(5,14,3)$ formunun sağ komşulukları yukarıdaki işlemler tekrar edilerek bulunur. Buradan $(5,14,3)$, $(6,16,5)$, $(11,20,6)$, $(10,24,11)$, $(3,16,10)$ devri elde edilir.

Son olarak $B=26$ değeri için $AC=135$ olur ve $0<A,C\leq 34$ olduğundan $(3,26,45)$, $(45,26,3)$, $(9,26,15)$, $(15,26,9)$, $(27,26,5)$, $(5,26,27)$ formları bulunur. Ancak bu formlardan sadece $(9,26,15)$ ve $(15,26,9)$ formları indirgenmiştir. Şimdi $(9,26,15)$ formunun sağ komşuluklarını bulalım.

Önerme 2.3.9' dan $C'=9$ ve $A>0$ için $\sqrt{136}<B'<\sqrt{136}+18$ olup $26+B'\equiv 0(\mathrm{mod}\,18)$ olduğundan $\mathrm{B}'=28$ olur. Diskriminanttan $A'=18$ bulunur. Benzer şekilde devam edilirse $(9,26,15)$ formunun sağ komşulukları $(9,26,15)$, $(18,28,9)$, $(25,44,18)$, $(30,56,25)$, $(33,64,30)$, $(34,68,33)$, $(33,68,34)$, $(30,64,33)$, $(25,56,30)$, $(18,44,25)$, $(9,28,18)$, $(15,26,9)$, $(17,34,15)$, $(15,34,17)$ şeklinde bulunur. $(15,34,17)$ formunun sağ komşuluğu $(9,26,15)$ olduğundan $(9,26,15)$ formunun

$(9,26,15)$, $(18,28,9)$, $(25,44,18)$, $(30,56,25)$, $(33,64,30)$, $(34,68,33)$, $(33,68,34)$, $(30,64,33)$, $(25,56,30)$, $(18,44,25)$, $(9,28,18)$, $(15,26,9)$, $(17,34,15)$, $(15,34,17)$

devri elde edilir.

Buradan $d=136$ diskriminantının sınıf sayısı $h(136)=4$ bulunur.

Önerme 2.3.16. $S=\begin{pmatrix} r & s \\ t & u \end{pmatrix}\in SL_2(\mathbb{Z})$ matrisi için $Q'=Q|_S$ olacak şekilde Q ve Q' formları Zagier indirgenmiş iki form olsun. Bu durumda $S=S_aS_b...S_h$ indirgenmiş matrislerin çarpımıdır ve $Q_1=Q|_{S_a}$, $Q_2=Q_1|_{S_b},...$ formlarının tümü Zagier indirgenmiştir [12].

Teorem 2.3.17. Q ve Q', d diskriminantlı iki primitif $Z-$ indirgenmiş formlar olsun. Q ve Q' nün denk olması için gerekli ve yeterli koşul aynı devire ait olmalarıdır.

İspat: $S=\begin{pmatrix} r & s \\ t & u \end{pmatrix}\in SL_2(\mathbb{Z})$ matrisi için $(A',B',C')=(A,B,C)|_S$ olduğunu varsayalım. Önerme 2.3.16' a göre Q ve Q' Zagier indirgenmiş formlar ise S matrisi $S=S_aS_b...S_h$ olacak biçimde indirgenmiş matrislerin çarpımı olarak yazılabilir. Fakat indirgenmiş formlara $S_a,S_b,...,S_h$ uygulanarak Q formu Q' formuna dönüştüğünden Q' formu ile Q formu aynı devirdedir.

2.4. Gauss İndirgemesi

$Q=(A,B,C)$, $d>0$ sıfır diskriminantlı belirsiz bir kuadratik form olsun. Q tarafından temsil edilen en küçük tamsayı $|A|$ olsun. B' yi $(\mathrm{mod}\,2A)$ da değiştirerek B' nin $2A$ uzunluğunda sabit bir aralıkta olduğunu söyleyebiliriz. $B\in[\sqrt{d}-|A|,\sqrt{d}+|A|]$ aralığı seçilebilir. Bu seçim $|B^2-d|$ değerini daha küçük yapar. $\sqrt{d}-2|A|<B<\sqrt{d}$ Gauss şartından özellikle $B<\sqrt{d}$ eşitsizliği tercih edilir. Bu eşitsizlikleri sağlayan formlara yarı indirgenmiş form denir. $|A|$ minimal alındığından $|A|\le|C|$ olur. Böylece Q formu

$$\begin{aligned}\sqrt{d}-2|A|<B<\sqrt{d}\\ \sqrt{d}-2|C|<B<\sqrt{d}\end{aligned} \qquad \textbf{(2.5)}$$

şartlarını sağlar.

Tanım 2.4.1. (2.5) ile verilen özellikleri sağlayan formlara Gauss indirgenmiş ya da kısaca indirgenmiş form denir [12].

Her indirgenmiş form yarı indirgenmiştir ve her $Q=(A,B,C)$ belirsiz formu için bir tane $Q'=(A,B',C')$ yarı indirgenmiş form vardır. Bir formun indirgenme şartlarının simetrisinden (A,B,C) formunun indirgenmiş olması için gerekli ve yeterli koşul (C,B,A) formunun da indirgenmiş olmasıdır.

Teorem 2.4.2. $Q=(A,B,C),\ d=B^2-4AC$ diskriminantlı primitif belirsiz bir form olsun. $Q(x,1)=Ax^2+Bx+C$ kuadratik denkleminin iki kökü ξ_1 ve $\xi_2=\xi_1'$ olsun. Bu durumda aşağıdaki ifadeler birbirine denktir [12].

a) (A,B,C) indirgenmiştir.
b) (C,B,A) indirgenmiştir.
c) $0<B-\sqrt{d}<2|A|<B+\sqrt{d}$ dir.
d) $0<B-\sqrt{d}<2|C|<B+\sqrt{d}$ dir.
e) $\xi_1\xi_2<0,\ |\xi_1|<1<|\xi_2|$ dir.
f) $AC<0,\ B>|A+C|$ dir.

Önerme 2.4.3. $Q=(A,B,C)$ belirsiz formu indirgenmiş ise

$$B>0,\ AC<0 \text{ ve } 0<|A|,\ B,\ |C|<\sqrt{d}$$

dir [12].

Önerme 2.4.4. Her pozitif d diskriminantı için B, $B < \sqrt{d}$ ve $B \equiv d \pmod 2$ şartlarını sağlayan en büyük tamsayı olmak üzere Q_0 temel formu bir tek $(1, B, C)$ indirgenmiş formuna denktir [12].

Tanım 2.4.5. Bir d diskriminantlı $Q = (A, B, C)$ formu verilsin.

1. $A' = C$,
2. $B + B' \equiv 0 \pmod{2A'}$ ve $\sqrt{d} - |2A'| < B' < \sqrt{d}$,
3. $(B')^2 - 4A'C' = d$.

şartlarını sağlayan bir $\rho(Q) = Q' = (A', B', C')$ formuna Q formunun sağ komşuluğu denir.

Bu şartlar sırasıyla A', B' ve C' katsayılarını belirler. Burada t, $B + B' = 2Ct$ olarak belirlenmek üzere $S = \begin{pmatrix} 0 & 1 \\ -1 & t \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}$ için $\rho(Q) = Q|_S$ dir.

Önerme 2.4.6. 1. Q bir primitif belirsiz form ise $\rho(Q)$ formu yarı indirgenmiştir.

2. Q indirgenmiş ise $\rho(Q)$ formu da indirgenmiştir [12].

Örnek 2.4.7. $d = 21$ diskriminantlı Gauss indirgenmiş formların devirlerini ve sınıf sayısını bulalım.

Önerme 2.4.3' e göre $B > 0$, $AC < 0$ ve $0 < |A|, B, |C| < \sqrt{21}$ olup $d = 21$ tek olduğundan $B = 1, 3$ olur.

$B=1$ değeri için $d=B^2-4AC$ olduğundan $AC=5$ olur. $AC<0$ ve $0<|A|,|C|<\sqrt{21}$ olduğundan $(-1,1,5),\ (1,1,-5),\ (5,1,-1)$ ve $(-5,1,1)$ formları bulunur. Ancak bu formların hiçbiri Gauss indirgenmiş form değildir.

$B=3$ değeri için $d=B^2-4AC \Rightarrow AC=3$ olur. Buradan da $(1,3,-3),(-1,3,3)$, $(3,3,-1)$ ve $(-3,3,1)$ formlarını elde ederiz. Bu formlar Gauss indirgenmiş formlardır. Şimdi bu formların sağ komşuluklarını bulalım.

$(1,3,-3)$ formunun sağ komşuluklarını bulalım. Önerme 2.4.4' e göre $A'=-3$ olur. $3+B'\equiv 0(\mathrm{mod}\,6)$ ve $\sqrt{21}-|6|<B'<\sqrt{21}$ olduğundan $B'=3$ bulunur. Diskriminant tanımından $C'=1$ elde edilir. $(1,3,-3)$ formunun sağ komşuluğunun $(-3,3,1)$ olduğu görülür. Benzer şekilde devam edilirse $(-3,3,1)$ formunun sağ komşuluğunun $(1,3,-3)$ olduğu bulunur. Buradan $(1,3,-3)$, $(-3,3,1)$ devri elde edilir.

$(-1,3,3)$ formunun sağ komşuluklarını bulalım. $A'=3$, $3+B'\equiv 0(\mathrm{mod}\,6)$ ve $\sqrt{21}-|6|<B'<\sqrt{21}$ olduğundan $B'=3$ olur. Diskriminanttan $C'=-1$ olduğu görülür. Bu durumda $(-1,3,3)$ formunun sağ komşuluğu $(3,3,-1)$ olarak bulunur. Benzer şekilde $(3,3,-1)$ formunun sağ komşuluğu $(-1,3,3)$ formudur. Buradan $(-1,3,3)$, $(3,3,-1)$ devri elde edilir.

Böylece $d=21$ diskriminantlı kuadratik formunun sınıf sayısı $h(21)=2$ olur.

BÖLÜM 3. BELİRSİZ KUADRATİK FORMLARLA TAMSAYILARIN TEMSİLİ

Tanım 3.1. d tamkare olmayan pozitif bir tamsayı ve $N \neq 0$ tamsayı olmak üzere

$$x^2 - dy^2 = N$$

Pell denklemi çözülebilir olsun. $x^2 - dy^2 = N$ denkleminin herhangi iki çözümü $u + v\sqrt{d}$ ve $u' + v'\sqrt{d}$ olsun. Eğer $x^2 - dy^2 = 1$ Pell denkleminin $u' + v'\sqrt{d} = (u + v\sqrt{d})(x + y\sqrt{d})$ eşitliğini sağlayan bir $x + y\sqrt{d}$ çözümü varsa $u + v\sqrt{d}$ ve $u' + v'\sqrt{d}$ aynı sınıftadır denir. Aynı sınıftaki tüm çözümlerin oluşturduğu kümeye ise çözüm sınıfı denir.

Ayrıca $u' + v'\sqrt{d} = (u + v\sqrt{d})(x + y\sqrt{d})$ eşitliğinden elde edilen $u' + v'\sqrt{d}$ çözümü ile $u + v\sqrt{d}$ çözümüne ilgilidir denir. $x^2 - dy^2 = N$ denkleminin bir çözüm sınıfındaki çözümlerin hepsi birbiriyle ilgilidir [1,13].

Teorem 3.2. d tamkare olmayan pozitif bir tamsayı olsun. Eğer

$$x^2 - dy^2 = N$$

Pell denkleminin bir K sınıfının temel çözümü $u + v\sqrt{d}$ ve

$$x^2 - dy^2 = 1$$

Pell denkleminin temel çözümü $x_1 + y_1\sqrt{d}$ ise

$$0 \le v \le \frac{y_1}{\sqrt{2(x_1+1)}}\sqrt{N} \tag{3.1}$$

ve

$$0 < |u| \le \sqrt{\frac{1}{2}(x_1+1)N} \tag{3.2}$$

eşitsizlikleri sağlanır.

Teorem 3.3. d tamkare olmayan pozitif bir tamsayı olsun. Eğer

$$x^2 - dy^2 = -N$$

Pell denkleminin bir K sınıfının temel çözümü $u + v\sqrt{d}$ ve

$$x^2 - dy^2 = 1$$

Pell denkleminin temel çözümü $x_1 + y_1\sqrt{d}$ ise

$$0 < v \le \frac{y_1}{\sqrt{2(x_1-1)}}\sqrt{N} \tag{3.3}$$

ve

$$0 \le |u| \le \sqrt{\frac{1}{2}(x_1-1)N} \tag{3.4}$$

eşitsizlikleri sağlanır.

Önerme 3.4. $x^2 - dy^2 = 1$ denkleminin temel çözümü (x_1, y_1) olsun. Her $n \in \mathbb{N}$ için

$$A_n = \sum_{k=0}^{\left\lfloor \frac{n}{2} \right\rfloor} (d)^k \binom{n}{2k} x_1^{n-2k} y_1^{2k} \tag{3.5}$$

ve

$$B_n = \sum_{k=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} (d)^k \binom{n}{2k+1} x_1^{n-1-2k} y_1^{2k+1} \tag{3.6}$$

olmak üzere, $(x_1 + y_1\sqrt{d})^n = A_n + B_n\sqrt{d}$ dir [8].

İspat: İspat tümevarım yoluyla rahatlıkla gösterilebilir.

Teorem 3.5. d tamkare olmayan pozitif bir tamsayı olmak üzere, $x^2 - dy^2 = N$ denkleminin bir K sınıfının temel çözümü $x + y\sqrt{d}$ olsun. $x^2 - dy^2 = 1$ denkleminin temel çözümü de $x_1 + y_1\sqrt{d}$ olsun. Bu durumda $x^2 - dy^2 = N$ denkleminin K sınıfın bütün tamsayı çözümleri $n \in \mathbb{N}$ olmak üzere $(x + y\sqrt{d})(x_1 + y_1\sqrt{d})^n$ biçimindedir [8].

Teorem 3.6. $Q = (A, B, C)$ belirsiz kuadratik formu tarafından temsil edilen m tamsayısı için $Au^2 + Buv + Cv^2 = m$ şartını sağlayan (u, v) ikilileri

$$(u, v) = \left(\frac{(x - By)A_n - (xB - yd)B_n}{2A}, xB_n + yA_n\right)$$

formülü ile verilir.

İspat: $Q(u,v)$, m tamsayısının $Au^2+Buv+Cv^2=m$ olacak biçimde bir temsili olsun. $Au^2+Buv+Cv^2=m$ formunun her iki tarafı 4A ile çarpılırsa

$$4Am=(2Au+Bv)^2-dv^2$$

elde edilir. $x=2Au+Bv,\ y=v$ ve $N=4Am$ alınırsa $d=B^2-4AC>0$ olduğundan $x^2-dy^2=N$ Pell denklemi elde edilir. Bu durumda $\sqrt{d}$ ' nin sürekli kesir açılımı kullanılırsa $x^2-dy^2=1$ denkleminin temel çözümü belirlenebilir. $x^2-dy^2=1$ denkleminin temel çözümü (x_1,y_1) olsun. $x^2-dy^2=N$ Pell denkleminin bir K sınıfının temel çözümü de $x+y\sqrt{d}$ olsun. Teorem 3.5' ten $x^2-dy^2=N$ Pell denkleminin genel çözümü $x_n+y_n\sqrt{d}=(x+y\sqrt{d})(x_1+y_1\sqrt{d})^n$ olur. Önerme 3.4' ten A_n ve B_n sırasıyla (3.5) ve (3.6) eşitliklerinde verildiği gibi $(x_1+y_1\sqrt{d})^n=A_n+B_n\sqrt{d}$ bulunur. Buradan da $x_n=xA_n+ydB_n$ ve $y_n=xB_n+yA_n$ olduğu görülür. Dolayısıyla

$$(u,v)=(\frac{(x-By)A_n-(xB-yd)B_n}{2A},xB_n+yA_n)$$

elde edilir.

Örnek 3.7. $Q=(1,-5,1)$ belirsiz kuadratik formu -3 tamsayısını temsil etsin. Buradan $Q(u,v)$, $u^2-5uv+v^2=-3$ olacak biçimde -3 tamsayısının bir temsili olsun. $u^2-5uv+v^2=-3$ kuadratik formunun her iki tarafı 4 ile çarpılırsa $4u^2-20uv+4v^2=-12$ kuadratik formu elde edilir. Buradan da $(2u-5v)^2-21v^2=-12$ denklemi bulunur. $x=2u-5v$ ve $y=v$ alınırsa $u^2-21v^2=-12$ Pell denklemi elde edilir. $u^2-21v^2=-12$ Pell denkleminin genel çözümlerini bulmak için öncelikle $u^2-21v^2=1$ denkleminin temel çözümü bulunmalıdır. $\sqrt{21}$ in sürekli kesir açılımı yapılırsa

$$a_0 = \sqrt{21},$$

$$a_1 = \frac{1}{a_0 - [\![a_0]\!]} = \frac{1}{\sqrt{21}-4} = \frac{\sqrt{21}+4}{5},$$

$$a_2 = \frac{1}{a_1 - [\![a_1]\!]} = \frac{1}{\frac{\sqrt{21}+4}{5}-1} = \frac{5}{\sqrt{21}-1} = \frac{\sqrt{21}+1}{4},$$

$$a_3 = \frac{1}{a_2 - [\![a_2]\!]} = \frac{1}{\frac{\sqrt{21}+1}{4}-1} = \frac{4}{\sqrt{21}-3} = \frac{\sqrt{21}+3}{4},$$

$$a_4 = \frac{1}{a_3 - [\![a_3]\!]} = \frac{1}{\frac{\sqrt{21}+3}{4}-1} = \frac{4}{\sqrt{21}-1} = \frac{\sqrt{21}+1}{5},$$

$$a_5 = \frac{1}{a_4 - [\![a_4]\!]} = \frac{1}{\frac{\sqrt{21}+1}{5}-1} = \frac{5}{\sqrt{21}-4} = \sqrt{21}+4,$$

$$a_6 = \frac{1}{a_5 - [\![a_5]\!]} = \frac{1}{\sqrt{21}+4-8} = \frac{1}{\sqrt{21}-4} = a_1$$

olup $\sqrt{21} = \left[4, \overline{1,1,2,1,1,8}\right]$ bulunur. Buradan $x^2 - dy^2 = 1$ denkleminin temel çözümü Teorem 1.1.5' ten (p_5, q_5) olur.

$$\frac{p_5}{q_5} = 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{1}}}}} = \frac{55}{12}$$

olup temel çözüm $55 + 12\sqrt{21}$ dir. Teorem 3.3' den $0 < v \le \frac{12}{\sqrt{2(55-1)}}\sqrt{21}$, $0 \le |u| \le \sqrt{\frac{1}{2}(55-1)21}$ dir. Böylece, $v = 1,2,3,4$ ve $u = 0,1,...,17,18$ elde ederiz. Buradan da $x^2 - 21y^2 = -12$ Pell denkleminin dört çözüm sınıfı olduğunu görürüz.

Bu sınıfların temel çözümleri $3+\sqrt{21},\ -3+\sqrt{21},\ 18+4\sqrt{21}$ ve $-18+4\sqrt{21}$ dir. Teorem 3.5' ten denklemin dört sınıfının bütün çözümleri de

$(3+\sqrt{21})(55+12\sqrt{21})^n,\ (-3+\sqrt{21})(55+12\sqrt{21})^n,\ (18+4\sqrt{21})(55+12\sqrt{21})^n$ ve $(-18+4\sqrt{21})(55+12\sqrt{21})^n$

dir. Önerme 3.4' ten

$$A_n = \sum_{k=0}^{\left\lfloor \frac{n}{2} \right\rfloor} (21)^k \binom{n}{2k} 55^{n-2k} 12^{2k}$$

Ve

$$B_n = \sum_{k=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} (21)^k \binom{n}{2k+1} 55^{n-1-2k} 12^{2k+1}$$

olmak üzere $(55+12\sqrt{21})^n = A_n + B_n\sqrt{21}$ olduğu kolayca görülür. Bu dört sınıfın bütün çözümleri de

$$(3+\sqrt{21})(A_n + B_n\sqrt{21}) = (3A_n + 21B_n) + \sqrt{21}(A_n + 3B_n),$$
$$(-3+\sqrt{21})(A_n + B_n\sqrt{21}) = (-3A_n + 21B_n) + \sqrt{21}(A_n - 3B_n),$$
$$(18+4\sqrt{21})(A_n + B_n\sqrt{21}) = (18A_n + 84B_n) + \sqrt{21}(4A_n + 18B_n)$$
ve
$$(-18+4\sqrt{21})(A_n + B_n\sqrt{21}) = (-18A_n + 84B_n) + \sqrt{21}(4A_n - 3B_n)$$

dir. Böylece $x = 2u - 5v$ ve $y = v$ aldığımızdan (u, v) tamsayı ikilileri de

$(4A_n + 18B_n, A_n + 3B_n)$, $(A_n + 3B_n, A_n - 3B_n)$, $(19A_n + 87B_n, 4A_n + 18B_n)$ ve $(A_n - 3B_n, 4A_n - 3B_n)$

olur.

BÖLÜM 4. SONUÇ VE ÖNERİLER

Bu tezde ilk olarak kuadratik formlar ve Pell denklemleri hakkında temel tanım ve teoremler verildi. Daha sonra tezin 2. Bölümünde ikili kuadratik formların indirgeme çeşitlerinden bahsedildi. Ayrıca bu bölümde $Q(x,y)=2x^2+2xy+y^2$ formunun $Q(x,y)=(x+y)^2+x^2$ şeklinde yazılabileceği de gösterilmiştir. Langrange bu gibi formlardan yola çıkarak her formun başka bir forma dönüşebileceğini keşfetmiştir. Biz de bu bölümde ilk olarak Langrange indirgemesinden, daha sonra Zagier ve Gauss indirgemelerinden bahsettik. Bu indirgemelerden yaralanarak bir kuadratik formun komşuluklarını elde ettik.

Bu tezde yapılan incelemeler sonucunda kuadratik formların karşılık geldiği eliptik eğriler incelenebilir. Ayrıca komşuluklarda elde edilen kuadratik formların karşılık geldiği eliptik eğriler de araştırılabilir. Bu konuyla ilgili [18,19,20] numaralı kaynaklara bakılabilir.

Ayrıca [8] de Andresscu, Andrica ve Cucurezonu $u^2-5uv+v^2=-3$ denkleminin tüm pozitif tamsayı çözümlerini Fermat' ın sonsuz azalan yöntemini kullanarak bulmuşlardır. Tezin 3. Bölümünde -3 tamsayısını temsil eden $Q=(1,-5,1)$ belirsiz kuadratik formu ele alınarak $Q(u,v)=-3$ şartını sağlayan tüm (u,v) tamsayı çiftleri araştırıldı. Daha sonra m tamsayısını temsil eden en genel $Q=(A,B,C)$ belirsiz formunu sağlayan tüm (u,v) tamsayı çiftlerini belirleme problemi ele alınıp, Pell denklemleri ve çözüm sınıfları kullanılarak tüm çözümler elde edilmiştir.

Bu tezden hareketle m tamsayısını temsil eden ve A, B, C katsayıları genelleştirilmiş Fibonacci ve Lucas sayıları olan $Q=(A,B,C)$ belirsiz kuadratik

formu için $Q(x, y) = m$ şartını sağlayan tüm (x, y) tamsayı çiftlerinin belirlenmesi problemleri üzerinde durulabilir.

KAYNAKLAR

[1] NAGELL,T., Introduction to Number Theory, AMS Chelsea Pub, New York, 2010.

[2] LANDAU, E., Elemantary Number Theory, Chelsea Pub, New York, 1958.

[3] REDMOND, D., Number Theory An Introduction, Marcel Dekker, New York, 1996.

[4] JACOBSON, M., WILLIAMS, H., Solving the Pell Equation, Canadian Math. Soc., Canada, 2009.

[5] BUCHMANN, J., VOLLMER, U., Binary Quadratic Forms, Springer, 2007.

[6] BUELL, D.A., Binary Quadratic Forms Classical Theory and Modern Com putations, Springer-Verlag, 1989.

[7] NIVEN, I., ZUCKERMAN, H.S., MONTGOMERY, H.L., An Introduction to the Theory of Numbers, John Wiley and Suns, Inc., USA, 1991.

[8] ANDREESCU, T., ANDRICA, T., CUCUREZEANU, I., An Introduction to Diophantine Equations, Birkhauser, 2010.

[9] HARDY, G.H., WRIGHT, E.M., An Introduction to the Theory of Numbers, Oxford Uni. Pres., Oxford, 1979.

[10] ROSEN, K.H., Elemantary Number Theory and Its Applications, Addison Wesley Pub. Com., 1986.

[11] BOSMA, W., KRAAIKMAP, C., Continued Fractions, http://www.math.ru.nl/~bosma/Students/CF.pdf, 2013.

[12] LEMMERMEYER, F., Binary Quadratic Forms,http://www.rzuser.uni-heidelberg.de, 2013.

[13] GÜNEY, M., Pell Denklemleri, Yüksek lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, 2012.

[14] MOLLIN, R. A., Quadratics, CRC Press, U.S.A, 1996.

[15] ROBERTSON, J. P., Solving the Generalized Pell Equation $x^2 - dy^2 = N$, www.jpr2718.org/pell.pdf, 2014.

[16] COX, D., A., Primes of the Form $x^2 + ny^2$: Fermat, Class Field theory, and Complex Multiplication, Wiley Pub., 2013.

[17] ALACA, Ş., WILLIAMS, K. S., Introductory Algebraic Number Theory, Cambridge University Press, 2003.

[18] WASHINGTON, L.C., Elliptic Curves, Number Theory and Cryptography, Chapman Hall/CRC, Boca London, New York, Washington DC, 2003.

[19] SILVERMAN, J.H., The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.

[20] TEKCAN, A., ÖZKOÇ, A., GEZER, B., BİZİM, O., Elliptic Curves, Conics and Cubic Congruencies Associated with Indefinite Binary Quadratic Forms, Novi Sad Journal of Mathematics 38(2)(2008).

[21] MOLLIN, R. A., Fundamental Number Theory with Applications, CRC Press, Boca Raton, New York-London-Tokyo, 1988.

ÖZGEÇMİŞ

Ece ÖZEL, 09.10.1988 de Hatay'da doğdu. İlk, orta ve lise eğitimini Hatay'da tamamladı. 2006 yılında Yüksel Acun Anadolu Lisesinden mezun oldu. 2011 yılında Eskişehir Osmangazi Üniversitesi Matematik bölümünden mezun oldu. 2011-2012 yılları arasında Eskişehir Osmangazi Üniversitesi'nde formasyon eğitimi aldı. 2012 yılından itibaren özel bir kurumda matematik öğretmenliği yapmaktadır. 2012 yılında Sakarya Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim dalında yüksek lisans eğitimine başladı.