T.C.

ULUDAĞ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KUADRATİK FORMLAR VE UYGULAMALARI

ARZU ÖZKOÇ

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

BURSA, 2009

T.C.

ULUDAĞ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KUADRATİK FORMLAR VE UYGULAMALARI

ARZU ÖZKOÇ

Doç. Dr. Osman BİZİM

(DANIŞMAN)

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

BURSA, 2009

T.C.

ULUDAĞ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KUADRATİK FORMLAR VE UYGULAMALARI

ARZU ÖZKOÇ

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

2009

Bu tez 12.08.2009 tarihinde aşağıdaki jüri tarafından oybirliği/oyçokluğu ile kabul edilmiştir.

....

Doç. Dr. Osman BİZİM (Danışman)

Doç.Dr. Muhittin AHMETOĞLU (Jüri Üyesi)

....

Doç.Dr. Ahmet TEKCAN (Jüri Üyesi)

ÖZET

Beş bölümden oluşan bu çalışmada kuadratik formlar ve bu formların eliptik eğriler, kübik kongrüanslar, kuadratik idealler, konikler ve modüler formlar ile olan ilişkileri ele alınmıştır.

Birinci bölümde tezin daha sonraki bölümlerinde kullanılacak olan bazı kavram ve notasyonlara yer verilmiştir.

İkinci bölümünde 73 determinatlı $F = (1,7,-6)$ kuadratik formunun devirleri ve has devirleri belirlenmiş ve bu devirdeki formlara karşılık gelen eliptik eğriler üzerindeki rasyonel noktaların sayısı $\mathbb{F}_{73}$ sonlu cisminde ele alınmıştır. Bu bölümde, ayrıca, $F = (1,7,-6)$ formunun devrindeki formlara karşılık gelen konikler üzerindeki rasyonel noktaların sayısı, ilk olarak $\mathbb{F}_{73}$ sonlu cisminde ele alınmış ve daha sonra elde edilen sonuçlar $\mathbb{F}_p$ sonlu cismine genelleştirilmiştir. Bu bölümde son olarak yine bu formlara karşılık gelen kübik kongrüansların çözümleri $\mathbb{F}_{73}$ de ele alınmıştır.

Üçüncü bölümünde pozitif tanımlı kuadratik formların özel bir ailesi tanımlanarak bu ailedeki formların özellikleri incelenmiş ve daha sonra bu ailedeki formlara karşılık gelen singüler eğriler üzerindeki rasyonel noktaların sayısı belirlenmiştir. Bu bölümde son olarak bu ailedeki formlara karşılık gelen kuadratik kongrüansların çözümleri ele alınmıştır.

Dördüncü bölümünde $F_1 = x_1^2+x_1x_2+8x_2^2$ ve $G_1= 2x_1^2+x_1x_2+4x_2^2$ kuadratik formları ve bu formların F_4, G_4, $F_3 \oplus G_1$, $F_2 \oplus G_2$ ve $F_1 \oplus G_3$ direkt toplamları ele alınmış, bu direkt toplamlar yardımıyla $S_4(\Gamma_0(31),\ 1)$ uzayı için baz oluşturulmuş ve daha sonra bu bazın elemanları kullanılarak tamsayıların yukarıdaki direkt toplamlar ile gösterilmesi ile ilgili formüller verilmiştir.

Son bölümünde $\delta = \sqrt{D}$ ve $\delta = \frac{1+\sqrt{D}}{2}$ değerleri için kuadratik irrasyoneller, kuadratik idealler ve kuadratik formlar arasındaki ilişki ele alınmış bununla ilgili sonuçlar verilmiştir.

Anahtar Kelimeler: Kuadratik formlar, eliptik eğriler, konikler, kuadratik idealler.

ABSTRACT

In this thesis, we consider quadratic forms, and the relationship between elliptic curves, cubic congruances, quadratic ideals, conics and moduler forms.

In the first section, we give some definitions, notations and properties which we need in later sections.

In the second section, we consider elliptic curves, conics and cubic congruencies over finite fields associated with indefinite binary quadratic forms in the proper cycle of $F=(1,7,-6)$. We will determine the number of rational points on elliptic curves and conics over $\mathbb{F}_{73}$. Moreover, we consider the number of integer solutions of cubic congruences associated with these forms.

In the third section, we consider some properties of positive definite binary quadratic forms in a special family. Also we determine the number of integer solutions of quadratic congruencies and determine the number of rational points on singular curves related to forms over finite fields.

In the fourth section, we consider the quadratic forms $F_1=x_1^2+x_1x_2+8x_2^2$ and $G_1=2x_1^2+x_1x_2+4x_2^2$ of discriminant -31, and their direct sums F_4, G_4, $F_3\oplus G_1$, $F_2\oplus G_2$, $F_1\oplus G_3$. We obtain some results concerning the modular forms. Using these, we construct a basis for the cusp form space $S_4(\Gamma_0(31),1)$, and then we give formulas for the number of representations of positive integer by these quadratic forms and their direct sums.

In the last section, for $\delta=\sqrt{D}$ and $\delta=\frac{1+\sqrt{D}}{2}$ values we obtain some results and connection between quadratic irrationals, quadratic ideals and quadratic forms.

Key Words: Quadratic forms, elliptic curves, conics, quadratic ideals.

İÇİNDEKİLER

SİMGELER DİZİNİ

$S_4(\Gamma_0(31), 1)$	-	cusp form uzayı
$\Delta(F)$	-	F kuadratik formunun determinantı
$z(F)$	-	F kuadratik formunun taban noktası
$\wp(\tau;Q,P_v)$	-	Genelleştirilmiş katlı teta serisi
$\overline{\Gamma}$	-	Genişletilmiş modüler grup
$I=[Q,\delta+P]$	-	İdeal
$F=(a,b,c)$	-	Kuadratik form
$\left(-\frac{k}{2},\ N,\ \mu(d)\right)$	-	k değişkenli, N seviyeli, $\mu(d)$ karakterli kuadratik form
$\Gamma_0(N)$	-	Γ homojen modüler grubunun özel denklik alt grubu
F_Γ	-	Γ nın temel bölgesi
$G_k(\Gamma_0,\mu)$	-	(k,Γ_0,μ) tipindeki modüler formların uzayı
$S_k(\Gamma_0,\mu)$	-	(k,Γ_0,μ) tipindeki cusp formların uzayı
$ord(F(\tau), i\infty, \Gamma_0)$	-	$F(\tau)\in G_k(\Gamma_0,\mu)$ nin $\xi=i\infty$ daki Γ_0 ya göre mertebesi
$r(n;Q)$	-	Pozitif n tamsayısının Q formu ile gösterilmesi sayısı
$\zeta(k)$	-	Riemann zeta fonksiyonu
$\wp(\tau;Q)$	-	Q formuna karşılık gelen teta serisi
$E(\tau;Q)$	-	Q formuna karşılık gelen Eisenstein serisi
$\mathbb{K}=\mathbb{Q}(\sqrt{D})$	-	Reel kuadratik sayı cismi
$\mathbb{U}$	-	Üst yarı düzlem

ŞEKİL VE TABLOLAR DİZİNİ

Sayfa

GİRİŞ

Bu çalışmanın amacı kuadratik formlar ile eliptik eğriler, kübik kongrüanslar, kuadratik idealler ve modüler formlar arasındaki ilişkileri incelemektir.

Bu amaca yönelik olarak tezin ön bilgiler kısmında kuadratik formlar, eliptik eğriler, ayrık gruplar, konikler ve idealler ile ilgili bazı temel kavramlara ve sonuçlara yer verilmiştir.

Tezin ikinci bölümünde 73 determinatlı $F=(1,7,-6)$ kuadratik formunun devirleri ve has devirleri ele alınmış ve bu devirdeki her bir forma karşılık gelen eliptik eğriler üzerindeki rasyonel noktaların sayısı sonlu $\mathbb{F}_{73}$ cisminde incelenmiştir. Daha sonra bu formun devrindeki formlara karşılık gelen konikler üzerindeki rasyonel noktaların sayısı yine $\mathbb{F}_{73}$ de ele alınmış ve bulunan bu sonuçlar $\mathbb{F}_p$ sonlu cisimlerine genelleştirilmiştir. Son olarak yine bu formlara karşılık gelen kübik kongrüansların çözümleri de mod 73 de ele alınmıştır.

Tezin üçüncü bölümünde pozitif tanımlı kuadratik formların özel bir ailesi tanımlanmış bu ailedeki formların özellikleri ele alınmıştır. Daha sonra bu ailedeki formlara karşılık gelen singüler eğriler üzerindeki rasyonel noktaların sayıları belirlenmiş ve bu ailedeki formlara karşılık gelen kuadratik kongrüansların çözümleri incelenmiştir.

Tezin dördüncü bölümünde -31 determinantlı $F_1{=}x_1^2{+}x_1x_2{+}8x_2^2$ ve $G_1{=}2x_1^2{+}x_1x_2{+}4x_2^2$ kuadratik formları ve bu formların F_4, G_4, $F_3\oplus G_1$, $F_2\oplus G_2$ ve $F_1\oplus G_3$ direkt toplamları ele alınmış olup bu direkt toplamlardan faydalanarak $S_4(\Gamma_0(31),1)$ uzayı için baz teşkil edilmiştir. Daha sonra ise bu bazın elemanları kullanılarak tamsayıların F_4, G_4, $F_3\oplus G_1$, $F_2\oplus G_2$ ve $F_1\oplus G_3$ formları ile gösterilmesi ile ilgili formüller verilmiştir.

Tezin son bölümünde kuadratik irrasyoneller, kuadratik idealler ve kuadratik formlar arasındaki ilişki ele alınmış ve $\delta = \sqrt{D}$ ve $\delta = \frac{1+\sqrt{D}}{2}$ değerleri için bazı sonuçlar verilmiştir.

1. BÖLÜM

ÖNBİLGİLER

Bu bölümde tezde kullanacağımız ayrık gruplar, ikinci dereceden kuadratik formlar, eliptik eğriler, konikler ve kuadratik idealler ile ilgili bazı temel kavramlara ve notasyonlara yer verilmiştir.

1.1 Ayrık Gruplar

Bu bölümde ayrık gruplar teorisinde çok önemli bir yere sahip olan modüler ve genişletilmiş modüler grup hakkında bazı temel kavramlar verilecektir.

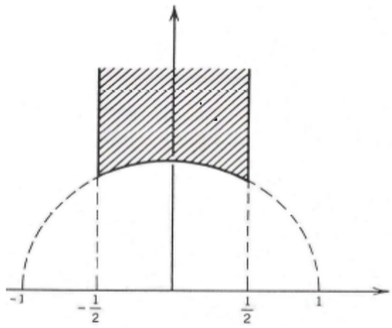
$PSL(2,\mathbb{R})$ nin bir ayrık alt grubu olan modüler grup

$$z \to \frac{az+b}{cz+d},\ a,b,c,d \in \mathbb{Z} \text{ ve } ad-bc=1$$

şeklindeki dönüşümlerden oluşan bir gruptur. Bu grubu Γ ile gösterirsek, Γ grubu mertebesi 2 olan $T(z)=\frac{-1}{z}$ ve mertebesi 3 olan $V(z)=1-\frac{1}{z}$ dönüşümleri ile üretilir ve $\Gamma=\left\langle T,\ V : T^2=V^3=I \right\rangle$ şeklinde bir gösterime sahiptir. Eğer $U=VT$ denirse $U(z)=z+1$ dönüşümü mertebesi ∞ olan bir parabolik dönüşüm olur. Γ nın temel bölgesi

$$F_\Gamma=\left\{z \in \mathbb{U} : |\operatorname{Re}(z)| \leq \frac{1}{2},\ |z| \geq 1\right\}$$

kümesi olup bu küme Şekil 1.1.1 de gösterilmiştir.



Şekil 1.1.1 Modüler grubun temel bölgesi

Genişletilmiş modüler grup ise $a,b,c,d \in \mathbb{Z}$ olmak üzere

$$z \to \frac{az+b}{cz+d},\ ad-bc=1 \text{ ve } z \to \frac{a\bar{z}+b}{c\bar{z}+d},\ ad-bc=-1$$

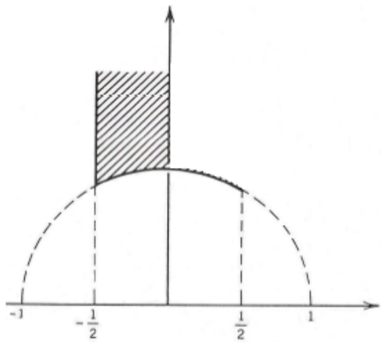
şeklindeki dönüşümlerden oluşan bir gruptur ve bu grup $\overline{\Gamma}$ ile gösterilmektedir. $R(z)=-\bar{z}$ sanal eksene göre yansıma dönüşümü olmak üzere, modüler grup ile genişletilmiş modüler grup arasındaki ilişki $\overline{\Gamma}=\Gamma \cup R\Gamma$ eşitliği ile verilir. $T(z)=\frac{-1}{z}$, $U(z)=z+1$ ve $W(z)=(TU)(z)=-\frac{1}{z+1}$ dönüşümleri için

$$\overline{\Gamma}=\left\langle R,\ T,\ W : R^2=T^2=W^3=I \right\rangle$$

dır. Üstelik $[\overline{\Gamma}:\Gamma]=2$ olduğundan Γ, $\overline{\Gamma}$ nın bir normal alt grubudur. $\overline{\Gamma}$ nın temel bölgesi ise

$$F_{\overline{\Gamma}}=\left\{ z \in \mathbb{U} : \frac{-1}{2} \le \mathrm{Re}(z) \le 0,\ \ |z| \ge 1 \right\}$$

kümesi olup bu küme Şekil 1.1.2 de gösterilmiştir.



Şekil 1.1.2 Genişletilmiş Modüler grubun temel bölgesi

1.2 Kuadratik Formlar

$a,b,c \in \mathbb{R}$ olmak üzere

$$F(X,Y) = aX^2 + bXY + cY^2$$

şeklindeki polinomlara kuadratik (ikinci dereceden) form denir ve bu form kısaca katsayıları yardımıyla $F = (a, b, c)$ ile gösterilir. F nin determinantı $\Delta(F) = b^2 - 4ac$ olarak tanımlanır. Üstelik "$F = (a, b, c)$ formu için F tamdır $\Leftrightarrow$ $a,b,c \in \mathbb{Z}$ dir", "F pozitif tanımlıdır $\Leftrightarrow$ $\Delta(F) < 0,\ a,c > 0$ dır" ve "F indefinite formdur $\Leftrightarrow$ $\Delta(F) > 0$ dır."

$F = (a, b, c)$ kuadratik formu

$$F(X,Y) = (X \ \ Y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}$$

biçiminde yazılır. Burada $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ matrisine F formunun matrisi denir ve $M(F)$ ile gösterilir. Üstelik formun determinantının $\Delta(F) = -4\det(M(F))$ olduğu görülür. Bu formun özdeğerleri ise $M(F) - \lambda I_2$ matrisi için $|M(F) - \lambda I_2| = 0$ denkleminin kökleridir. Buna göre

$$\begin{vmatrix} a-\lambda & b/2 \\ b/2 & c-\lambda \end{vmatrix} = (a-\lambda)(c-\lambda) - \frac{b^2}{4} = 0$$

denkleminden

$$\lambda_1 = \frac{a+c+\sqrt{a^2+b^2+c^2-2ac}}{2} \quad \text{ve} \quad \lambda_2 = \frac{a+c-\sqrt{a^2+b^2+c^2-2ac}}{2}$$

elde edilir. Üstelik

$$\begin{aligned} a^2+b^2+c^2-2ac &= a^2+b^2+c^2-4ac+2ac \\ &= b^2-4ac+a^2+c^2+2ac \\ &= \Delta+(a+c)^2 \\ &= \Delta+Tr^2(M(F)) \end{aligned}$$

olduğundan F formunun özdeğerleri

$$\lambda_1 = \frac{Tr(M(F))+\sqrt{\Delta+Tr^2(M(F))}}{2} \quad \text{ve} \quad \lambda_2 = \frac{Tr(M(F))-\sqrt{\Delta+Tr^2(M(F))}}{2}$$

dir.

$g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} = [r;s;t;u] \in \overline{\Gamma}$ için gF formu

$$\begin{aligned} gF(X,Y) = (ar^2+brs+cs^2)X^2 + (2art+bru+bts+2csu)XY \\ +(at^2+btu+cu^2)Y^2 \end{aligned}$$

olarak tanımlanır. Bu tanıma göre genişletilmiş modüler grup, formlar kümesi üzerine grup etkisi yapmaktadır, yani her $g,h \in \overline{\Gamma}$ için $(gh)F = g(hF)$ ve $IF = F$ dir. Üstelik her $g \in \overline{\Gamma}$ için $\Delta(gF) = \Delta(F)$ dir, yani F ile gF aynı determinantlıdır. Ayrıca F pozitif tanımlı, indefinite veya tam ise gF de pozitif tanımlı, indefinite veya tamdır. gF nin bu tanımına dikkat edilirse F formunda $X \rightarrow rX+tY$ ve $Y \rightarrow sX+$

uY değişken değişimi yapılmak suretiyle gF formu elde edilmiştir. F formunun yukarıdaki matrisini kullanarak gF nin

$$gF(X,Y) = (X \quad Y)gM(F)g^t \begin{pmatrix} X \\ Y \end{pmatrix}$$

şeklinde olduğu görülür.

F ve G iki form olsun. Eğer $gF = G$ olacak şekilde en az bir $g \in \overline{\Gamma}$ varsa F ve G formlarına denktir denir. Eğer $\det(g) = 1$ ise bu iki forma has denk, eğer $\det(g) = -1$ ise bu iki forma has olmayan denk denir. Denk formlar aynı determinantlı iken aynı determinantlı formların denk olması gerekmez. Eğer bir F formu kendisine has olmayan denk ise bu forma ambiguous form denir. $g \in \overline{\Gamma}$ için $gF = F$ oluyorsa g ye F formunun bir otomorfizmi denir. Eğer $\det(g) = 1$ ise g ye has otomorfizm, $\det(g) = -1$ ise g ye has olmayan otomorfizm denir. F nin has otomorfizmleri kümesi $Aut(F)^+$ ile has olmayan otomorfizmleri kümesi ise $Aut(F)^+$ ile gösterilir (Kuadratik formlarla ilgili daha fazla bilgi için Buchmann ve Vollmer 2007, Buell 1989 ve Flath 1989 kaynaklarına bakılabilir).

1.2.1 Pozitif tanımlı formlar

$F = (a, b, c)$ kuadratik formu için $\Delta(F) < 0$ ve $a, c > 0$ ise bu forma pozitif tanımlı form denildiği bilinmektedir. $F = (a, b, c)$ pozitif tanımlı bir form olsun. Bu takdirde belli bir $z \in \mathbb{U}$ kompleks sayısı için bu form

$$F(X,Y) = a(X + zY)(X + \bar{z}Y)$$

şeklinde yazılabilir. Bu şekildeki z sayısına F formunun taban noktası denir ve $z = z(F)$ ile gösterilir. Eğer $z = x + iy$ olarak alınırsa yukarıdaki eşitlik

$$F(X,Y)=a(X+zY)(X+\bar{z}Y)=aX^2+2axXY+a|z|^2Y^2$$

haline gelir. Bu son eşitlikten $2ax=b$ ve $a|z|^2=c$ olup

$$x=\frac{b}{2a} \quad \text{ve} \quad y=\frac{\sqrt{-\Delta(F)}}{2a}$$

elde edilir. y pozitif olduğundan $z=\dfrac{b+i\sqrt{-\Delta(F)}}{2a}\in\mathbb{U}$ dur.

Tersine herhangi bir $z\in\mathbb{U}$ karmaşık sayısı verildiğinde taban noktası z olan pozitif tanımlı bir form vardır. Gerçekten de $z=x+iy$ için $a=\dfrac{1}{|z|^2}$, $b=\dfrac{2x}{|z|^2}$ ve $c=1$ olarak alınırsa taban noktası z olan $\Delta(F)=\dfrac{-4y^2}{|z|^4}<0$ determinantlı

$$F=(a,\,b,\,c)=\left(\frac{1}{|z|^2},\ \frac{2x}{|z|^2},\ 1\right)$$

formu elde edilir. Dolayısıyla $\varphi:F\rightarrow z(F)$ dönüşümü, sabit determinantlı pozitif tanımlı formlar ile $\mathbb{U}$ nun noktaları arasında birebir bir dönüşümdür.

Buna göre F ve G formlarının denk olması için gerek ve yeter şart bu formların taban noktalarının genişletilmiş modüler grubun aynı yörüngesinde olmasıdır. $F=(a,\,b,\,c)$ pozitif tanımlı bir formu için $|b|\leq a\leq c$ şartı sağlanıyor ise F ye indirgenebilir form denir. F formunun z taban noktası için z ve $\bar{z}$ simetrik roller oynadığından $\mathrm{Im}(z)>0$ kabul edilebilir. Bu durumda $|b|\leq a$ şartı $|z+\bar{z}|\leq 1$ ye yani $|\mathrm{Re}(z)|\leq 1/2$ şartına, benzer şekilde $a\leq c$ şartı ise $z\bar{z}\geq 1$ ye yani $|z|\geq 1$ şartına denktir. Dolayısıyla bir $F=(a,\,b,\,c)$ formunun indirgenebilir olması için gerek ve yeter şart F nin taban noktasının modüler grubun temel bölgesinde olmasıdır (Tekcan ve Bizim 2003).

1.2.2 İndefinite formlar

$F=(a,b,c)$ kuadratik formu için $\Delta(F)>0$ ise bu forma indefinite form denildiği bilinmektedir. $F=(a,b,c)$ indefinite formu için eğer

$$\left|\sqrt{\Delta}-2|a|\right|<b<\sqrt{\Delta}$$

şartı sağlanıyorsa bu forma indirgenebilirdir denir. Eğer bir form indirgenebilir değilse aşağıdaki indirgeme algoritması kullanılarak bu form indirgenebilir hale getirilir. İndirgenemeyen F formu için

$$s_i=s_i(F)=\begin{cases} \operatorname{sgn}(c_i)\left\lfloor \dfrac{b_i}{2|c_i|}\right\rfloor & |c_i|\geq\sqrt{\Delta}\ ise \\ \operatorname{sgn}(c_i)\left\lfloor \dfrac{b_i+\sqrt{\Delta}}{2|c_i|}\right\rfloor & |c_i|<\sqrt{\Delta}\ ise \end{cases}$$

tanımlansın. Bu takdirde F nin indirgenmişi $i\geq 0$ için

$$\rho^{i+1}(F)=(c_i,-b_i+2c_is_i,c_is_i^2-b_is_i+a_i)$$

dir. Eğer elde edilen $\rho^1(F)$ formu indirgenebilir değilse bu forma bir kez daha indirgeme algoritması uygulanır ve bu şekilde devam edilerek sonlu bir adımda F nin indirgenmişi elde edilir.

Şimdi F formu için $\tau(F)=(-a,b,-c)$ dönüşümü tanımlansın. $k>0$ olsun. $G=(k,n,m)$, F ye denk olan bir form olmak üzere F nin devri pozitif i tamsayısı için $((\tau\rho)^i(G))$ dizisidir. Eğer G formu F ye has denk ise F nin has devri de $(\rho^i(\text{G}))$ dizisidir. F nin devri ve has devri $F_0\sim F_1\sim\cdots\sim F_{l-1}$ ile gösterilir ve aşağıdaki gibi elde edilir.

1.2.2.1 Teorem. $F=(a,b,c)$ indirgenebilir bir form olsun.

$$s_i=|s(F_i)|=\left\lfloor \frac{b_i+\sqrt{\Delta}}{2|c_i|}\right\rfloor \tag{1.1}$$

olmak üzere $0\leq i\leq l-2$ için

$$F_{i+1} = (a_{i+1}, b_{i+1}, c_{i+1}) = (|c_i|, -b_i + 2s_i|c_i|) \tag{1.2}$$

dır. Bu takdirde F nin devri $F_0 \sim F_1 \sim \cdots \sim F_{l-1}$ olup bu devrin uzunluğu l dir. Eğer l tek ise F nin has devri $2l$ uzunlukludur ve

$$F_0 \sim \tau(F_1) \sim F_2 \sim \tau(F_3) \sim \cdots \sim \tau(F_{l-2}) \sim F_{l-1} \sim \tau\,(F_0) \sim F_1 \sim \tau(F_2) \sim \cdots \sim F_{l-2} \sim \tau(F_{l-1})$$

şeklindedir. Eğer ve l çift ise F nin has devri l uzunlukludur ve

$$F_0 \sim \tau(F_1) \sim F_2 \sim \tau(F_3) \sim \cdots \sim F_{l-2} \sim \tau(F_{l-1})$$

şeklindedir (Buchmann ve Vollmer 2007).

1.3 Kuadratik İdealler

$D \neq 1$ pozitif tam kare olmayan bir tamsayı olmak üzere $D \equiv 1 \pmod 4$ için $r = 2$ ve diğer hallerde $r = 1$ olmak üzere $\mathbb{K} = \mathbb{Q}\,(\sqrt{D})$, diskriminantı $\Delta = \frac{4D}{r^2}$ olan bir kuadratik sayı cismidir. $O_{\mathbb{K}}$ ile $\mathbb{K}$ cisminin tamsayılarının halkası gösterilir. O halde $w_\Delta = \frac{r-1+\sqrt{D}}{r}$ olmak üzere $O_{\mathbb{K}} = [1, w_\Delta] = \mathbb{Z}\,[w_\Delta]$ dır. Bu taktirde $\{1, w_\Delta\}$, $\mathbb{K}$ cismi için bir tam baz olur.

Teorem 1.3.1 $I = [a, b + cw_\Delta]$ olsun. Bu taktirde I nın bir ideal olması için gerek ve yeter şart $c \mid b, c \mid a$ ve $ac \mid N(b + cw_\Delta)$ olmasıdır (Mollin 1996).

$a, b, c \in \mathbb{Z}$ olmak üzere $I = [a, b + cw]$ idealinin normu $N(I) = |ac|$ olarak tanımlanır. Bu ideal için a ve c sayıları bir tektir ve a sayısı I daki en küçük pozitif tamsayıdır. Bu sayı $L(I)$ ile gösterilir. Eğer $L(I) = N(I)$ ise I idealine ilkel ideal denir. Bu durumda $c = 1$ olup I ilkel ideali standart gösterimi $I = [a, b + w]$ şeklindedir. Bu idealin eşleniği $\bar{I}=[a,\overline{b+w}]$ dır. Eğer $I=\bar{I}$ ise (Diğer bir ifade ile $\frac{2P}{Q}\in\mathbb{Z}$ ise) I ya ambiguous ideal denir. $P,Q\in\mathbb{Z}$ için $\alpha=\frac{P+\sqrt{D}}{Q}$ bir kuadratik irrasyonel, yani $P^2\equiv D \pmod{Q}$ olsun. Bu takdirde $I=[Q,P+\sqrt{D}]$ bir ilkel ideal olur. Bu ideal için

$$P+\sqrt{D}>Q \text{ ve } -Q<P-\sqrt{D}<0$$

şartı sağlanıyor ise I ya indirgenebilir ideal denir.

1.4 Eliptik Eğriler ve Konikler

Bu bölümde eliptik eğriler teorisinden bahsedilmektedir. q pozitif bir tamsayı ve $\mathbb{F}_q$ sonlu bir cisim olmak üzere $\mathbb{F}_q$ deki bir E eliptik eğrisi $a_1,a_2,a_3,a_4,a_6\in\mathbb{F}_q$ olmak üzere

$$E: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

denklemiyle verilen bir eğridir ve bu eğriye Weierstrass uzun form denir. Burada

$$b_2=a_1^2+4a_2,\qquad b_4=2a_4+a_1a_3,\qquad b_6=a_3^2+4a_6,$$
$$b_8=a_1^2+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2\,,\ c_4=b_2^2-24b_4$$

olmak üzere eğrinin diskriminantı $\Delta=-b_2^2b_8-8\,b_4^3-27b_6^2+9b_2b_4b_6$ ve $j-$invaryantı ise $j=j(E)=\frac{c_4^3}{\Delta}$ dır. Eğer $\Delta=0$ ise bu E ye singüler eğri denir. İki eliptik eğrinin denk olması için gerek ve yeter şart aynı $j-$invaryantına sahip olmasıdır.

Eğer E nin uzun formunda $a_1=0,\ a_2=a, a_3=0, a_4=b,\ a_6=0$ olarak alınırsa $b_2=4a,\ b_4=2b,\ b_6=0,\ b_8=-b^2,\ c_4=16a^2-48b$ olup E eğrisi

$$E: y^2=x^3+ax^2+bx$$

haline gelir. Bu eğri için $\Delta = 16b^2(a^2-4b)$ ve $j = j(E) = \dfrac{256(a^2-3b)^3}{b^2(a^2-4b)}$ dir. O sonsuzdaki ideal nokta olmak üzere E üzerindeki rasyonel noktaların kümesi

$$E(\mathbb{F}_q) = \left\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = x^3 + ax^2 + bx\right\} \cup \{O\}$$

ile gösterilir ve bu küme aşağıdaki gibi tanımlanan toplama işlemine göre bir grup oluşturur. $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$, E de herhangi iki nokta olmak üzere bu iki noktanın toplamı $P_3 = P_1 + P_2 = (x_3, y_3)$ ile gösterilir ve aşağıdaki gibi tanımlanır: $x_1 \neq x_2$ ise $m = \dfrac{y_2 - y_1}{x_2 - x_1}$ olmak üzere $x_3 = m^2 - x_1 - x_2$ ve $y_3 = m(x_1 - x_3) - y_1$ dir. Eğer $x_1 = x_2$ fakat $y_1 \neq y_2$ ise $P_1 + P_2 = O$ dur. Eğer $P_1 = P_2$ ve $y_1 \neq 0$ ise $m = \dfrac{3x_1^2 + a}{2y_1}$ için $x_3 = m^2 - 2x_1$ ve $y_3 = m(x_1 - x_3) - y_1$ dir ve eğer $P_1 = P_2$ ve $y_1 = 0$ ise $P_1 + P_2 = O$ dur.

$E(\mathbb{F}_q)$ grubunun mertebesi $\# E(\mathbb{F}_q)$ ile gösterilir ve $(\frac{x}{q})$ Legendre sembolü olmak üzere

$$\# \, E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax^2 + bx}{\mathbb{F}_q} \right)$$

olarak tanımlanır. (Washington 2003, Silverman 1986, Silverman ve Tate 1992).

a, b, c, d, e, f ler keyfi reel sayılar olmak üzere

$$C: ax^2 + bxy + cy^2 + dx + ey + f = 0$$

şeklindeki denklemlere konik denir. Bu koniğin diskriminantı $\Delta(C) = b^2 - 4ac$ olarak tanımlanır. Bu konik, $\Delta(C) < 0$ için bir elips, $\Delta(C) = 0$ için bir parabol ve $\Delta(C) > 0$ için bir hiperbol belirtir.

2. BÖLÜM

İNDEFİNİTE KUADRATİK FORMLAR, ELİPTİK EĞRİLER, KONİKLER VE KÜBİK KONGRÜANSLAR

Çalışmanın bu bölümünde 73 determinatlı $F = (1,7,-6)$ formu ele alınacaktır. Bu formun devrini ve has devrini teşkil ettikten sonra bu forma karşılık gelen eliptik eğrilerin üzerindeki rasyonel noktaların sayısı $\mathbb{F}_{73}$ de ele alınıp daha sonra bu formlara karşılık gelen koniklerin üzerindeki rasyonel noktaların sayısı belirlenecektir. Bu bölümün sonunda ise yine bu formlara karşılık gelen kübik kongrüansların çözümleri ele alınacaktır.

2.1 $\boldsymbol{F = (1,7,-6)}$ Formunun Devirleri

Bu bölümde, $F = (1,7,-6)$ formunun devri ve has devri elde edilecektir.

2.1.1 Teorem. $F = (1,7,-6)$ formunun devri 9 uzunlukludur ve

$$F_0 = (1,7,-6) \sim F_1 = (6,5,-2) \sim F_2 = (2,7,-3) \sim F_3 = (3,5,-4) \sim F_4 = (4,3,-4)$$

$$\sim F_5 = (4,5,-3) \sim F_6 = (3,7,-2) \sim F_7 = (2,5,-6) \sim F_8 = (6,7,-1)$$

şeklindedir. Dolayısıyla bu formun has devri ise 18 uzunlukludur ve

$$F_0 = (1,7,-6) \sim F_1 = (-6,5,2) \sim F_2 = (2,7,-3) \sim F_3 = (-3,5,4) \sim F_4 = (4,3,-4)$$

$$\sim F_5 = (-4,5,3) \sim F_6 = (3,7,-2) \sim F_7 = (-2,5,6) \sim F_8 = (6,7,-1) \sim F_9 = (-1,7,6)$$

$$\sim F_{10} = (6,5,-2) \sim F_{11} = (-2,7,3) \sim F_{12} = (3,5,-4) \sim F_{13} = (-4,3,4)$$

$$\sim F_{14} = (4, 5, -3) \sim F_{15} = (-3, 7, 2\,) \sim F_{16} = (2, 5, -6) \sim F_{17} = \ (-6, 7, 1)$$

şeklindedir.

İspat. $F = F_0 = (1, 7, -6)$ olsun. Bu takdirde (1.1) den $s_0 = 1$ olup (1.2) den

$$F_1 = (a_1, b_1, c_1) = \big(|c_0\,|, -b_0 + 2s_0|c_0\,|, -(a_0 + b_0 s_0 + c_0 s_0^2)\big) = \ (6, 5, -2)$$

elde edilir. Benzer şekilde devam edilirse aşağıdaki tablo elde edilir.

i	0	1	2	3	4	5	6	7	8
a_i	1	6	2	3	4	4	3	2	6
b_i	7	5	7	5	3	5	7	5	7
c_i	−6	−2	−3	−4	−4	−3	−2	−6	−1
s_i	1	3	2	1	1	2	3	1	7

Tablo 2.1.1 $F = (1,7,-6)$ formunun devri

Bu tabloya göre F nin devri

$$F_0 = (1,7,-6) \sim F_1 = (6, 5, -2) \sim F_2 = (2, 7, -3) \sim F_3 = (3, 5, -4) \sim F_4 = \ (4, 3, -4)$$

$$\sim F_5 = (4, 5, -3) \sim F_6 = (3, 7, -2) \sim F_7 = (2, 5, -6) \sim F_8 = \ (6, 7, -1)$$

dir. F nin bu devri 9 uzunluklu olup Teorem 1.2.2.1 gereği F nin has devri 18 uzunlukludur ve

$$F_0 = (1,7,-6) \sim F_1 = (-6, 5, 2) \sim F_2 = (2,7,-3) \sim \ F_3 = (-3,5,4) \sim F_4 = \ (4,3,-4)$$

$$\sim F_5 = (-4, 5, 3) \sim F_6 = (3,7,-2) \sim F_7 = (-2, 5, 6) \sim F_8 = \ (6, 7, -1) \sim F_9 = (-1, 7, 6)$$

$$\sim F_{10} = (6,5,-2) \sim F_{11} = (-2, 7, 3) \sim F_{12} = (3, 5, -4) \sim F_{13} = \ (-4, 3, 4)$$

$$\sim F_{14} = (4, 5, -3) \sim F_{15} = (-3, 7, 2\,) \sim F_{16} = (2, 5, -6) \sim F_{17} = \ (-6, 7, 1)$$

şeklindedir.

2.2 Eliptik Eğriler Üzerindeki Rasyonel Noktalar

Bu bölümde bir önceki bölümde elde edilen $F = (1,7,-6)$ formunun has devrindeki formlara karşılık gelen eliptik eğriler üzerindeki rasyonel noktaların sayıları $\mathbb{F}_{73}$ sonlu cismi üzerinde ele alınacaktır. Önbilgiler kısmında eliptik eğriler teorisinden kısaca bahsedilmişti. Problem ele alınmadan önce eliptik eğriler ile kuadratik formlar arasındaki ilişki incelenecektir. $F = (a, b, c)$ formu $\Delta(F) = b^2 - 4ac$ diskriminantlı bir form olsun. Bu forma karşılık gelen eliptik eğri

$$E_F\colon y^2 = ax^3 + bx^2 + cx$$

olarak tanımlansın. Bu eliptik eğride $x \to \frac{x}{\sqrt[3]{a}}$ değişken değişimi yapılırsa

$$E_F\colon y^2 = ax^3 + bx^2 + cx = x^3 + ba^{-2/3}x^2 + ca^{-1/3}x$$

eliptik eğrisi elde edilir. Bu eğrinin diskriminantı ise $\Delta(E_F) = 16c^2a^{-2}\,\Delta(F)$ dır.

Bu bölümde bir önceki alt bölümde elde ettiğimiz F nin has devrindeki $0 \le i \le 17$ için $F_i = (a_i, b_i, c_i)$ formlarına karşılık gelen

$$E_{F_i}\colon y^2 = a_ix^3 + b_ix^2 + c_ix \tag{2.1}$$

eliptik eğrileri üzerindeki rasyonel noktaların sayısı $\mathbb{F}_{73}$ sonlu cisminde ele alınacaktır. Bu eğrilerin rasyonel noktaları kümesi

$$E_{F_i}(\mathbb{F}_{73}) = \{(x, y) \in \mathbb{F}_{73} \times \mathbb{F}_{73} : y^2 = a_ix^3 + b_ix^2 + c_ix\} \cup \{O\}$$

ile gösterilsin. Bu takdirde aşağıdaki teorem verilebilir.

2.2.1 Teorem. E_{F_i} yukarıdaki eliptik eğriler olmak üzere

$$\#E_{F_i}(\mathbb{F}_{73}) = \begin{cases} 73 & i = 4, 13 \text{ için} \\ 75 & \text{diğerler hallerde} \end{cases}$$

dir.

İspat. $i = 4, 13$ olsun. $\mathbb{F}_{73}$ üzerinde $E_{F_i} : y^2 = a_i x^3 + b_i x^2 + c_i x$ eliptik eğrisi dikkate alınsın. Eğer $y = 0$ ise $x(a_i x^2 + b_i x + c_i) \equiv 0 \pmod{73}$ olup buradan

$$x \equiv 0 \pmod{73} \quad \text{ve} \quad a_i x^2 + b_i x + c_i \equiv 0 \pmod{73} \qquad (2.2)$$

elde edilir. Buradan açıkça görülür ki (2.2) denkleminin bir çözümü $x = 0$ ve

$$x = \begin{cases} 27 & i = 4 \\ 46 & i = 13 \end{cases}$$

dir, yani $i = 4$ için E_{F_4} eliptik eğrisi üzerinde (0, 0) ve (27, 0) ve $i = 13$ için $E_{F_{13}}$ eliptik eğrisi üzerinde (0, 0) ve (46, 0) rasyonel noktaları bulunmaktadır. Q_p, kuadratik rezidülerin kümesini göstermek üzere

$$Q_{73} = \{\, 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 19, 23, 24, 25, \mathbf{27}, 32, 35, 36, 37, 38, 41, \mathbf{46},$$
$$48, 49, 50, 54, 55, 57, 61, 64, 65, 67, 69, 70, 71, 72 \,\}$$

dır. Dikkat edilirse $27, 46 \in Q_{73}$ dür. Şimdi

$$Q_{73}^{x} = Q_{73} - \begin{cases} \{27\} & i = 4 \\ \{46\} & i = 13 \end{cases}$$

olsun. Bu takdirde Q_{73}^{x} ün her bir x elemanı, $a_i x^3 + b_i x^2 + c_i x$ ifadesini bir tam kare yapar (yukarıda $x = 27$ ve $x = 46$ nın bu ifadeyi sıfır yaptığı görülmüştür). Belli bir $t \in \mathbb{F}_{73}^{*}$ elemanı için $a_i x^3 + b_i x^2 + c_i x = t^2$ olsun. Bu takdirde $y^2 \equiv t^2 \pmod{73} \Leftrightarrow y \equiv \pm t \pmod{73}$ olduğundan E_{F_i} üzerinde (x, t) ve $(x, -t)$ gibi iki rasyonel nokta vardır. Yani her bir $x \in Q_{73}^{x}$ için E_{F_i} üzerinde iki tane nokta vardır. Q_{73}^{x} de 35 tane eleman olduğundan E_{F_i} üzerinde toplam $2 \cdot 35 = 70$ tane rasyonel nokta vardır. Üstelik (0, 0) ve $(x, 0)$ da bu eğri üzerinde iki nokta olup sonsuz noktasını da ilave edersek E_{F_i} de toplam $70 + 2 + 1 = 73$ tane rasyonel nokta vardır.

Şimdi $i \neq 4, 13$ kabul edilsin. Bu takdirde $y = 0$ ise (2.2) denkleminin bir çözümü $x = 0$ ve

$$x = \begin{cases} 33 & i=0 \\ 43 & i=1 \\ 53 & i=2 \\ 13 & i=3 \\ 28 & i=5 \\ 11 & i=6 \\ 56 & i=7 \\ 42 & i=8 \end{cases} \qquad x = \begin{cases} 40 & i=9 \\ 30 & i=10 \\ 20 & i=11 \\ 60 & i=12 \\ 45 & i=14 \\ 62 & i=15 \\ 17 & i=16 \\ 31 & i=17 \end{cases}$$

dir. Yani x yukarıdaki gibi olmak üzere E_{F_i} de $(0, 0)$ ve $(x, 0)$ gibi iki nokta vardır. Dikkat edilirse yukarıda elde edilen bu x değerleri Q_{73} ün elemanları değildir. Üstelik Q_{73} ün her bir x elemanı $a_i x^3 + b_i x^2 + c_i x$ ifadesini tam kare yapmaktadır. O halde belli bir $t \neq 0$ için $a_i x^3 + b_i x^2 + c_i x = t^2$ denilirse $y^2 \equiv t^2 \pmod{73}$ olup buradan $y \equiv \pm t \pmod{73}$ elde edilir. Yani E_{F_i} de (x, t) ve $(x, -t)$ gibi iki rasyonel nokta vardır. Bu ise Q_{73} deki her bir x değeri için E_{F_i} de iki tane noktanın olması demektir. Q_{73} de 36 tane eleman olduğundan E_{F_i} de $2 \cdot 36 = 72$ tane rasyonel nokta vardır. $(0, 0)$, $(x, 0)$ ve sonsuz noktalarını da ilave edersek E_{F_i} de toplam $72 + 2 + 1 = 75$ tane rasyonel nokta bulunur.

2.3 Konikler Üzerindeki Rasyonel Noktalar

Bu bölümde $F = (1, 7, -6)$ formunun has devrindeki her bir forma karşılık gelen konikler üzerindeki rasyonel noktaların sayıları belirlenecektir. $N \in \mathbb{F}_{73}^*$ belli bir sayı olmak üzere $F = (1, 7, -6)$ formunun has devrindeki $F_i = (a_i, b_i, c_i)$ formlarına karşılık gelen konik

$$C_{F_i} : a_i x^2 + b_i xy + c_i y^2 - N = 0 \tag{2.3}$$

olsun. Bu konik için

$$C_{F_i}(\mathbb{F}_{73}) = \{(x, y) \in \mathbb{F}_{73} \times \mathbb{F}_{73} : \ a_i x^2 + b_i xy + c_i y^2 - N \equiv 0 \pmod{73}\}$$

tanımlansın. Bu takdirde aşağıdaki teorem verilebilir.

2.3.1 Teorem. Yukarıda tanımlanan C_{F_i} koniği için

$$\#C_{F_i}(\mathbb{F}_{73}) = \begin{cases} 2\cdot 73 & N \in Q_{73} \text{ ise} \\ 0 & N \notin Q_{73} \text{ ise} \end{cases}$$

dir.

İspat. Teoremin ispatı iki durumda ele alınacaktır.

1. Durum. $N \in Q_{73}$ olsun. Bu takdirde belli bir $t \neq 0$ için $N = t^2$ dir. Eğer $y = 0$ ise

$$a_i x^2 \equiv t^2 \pmod{73} \Leftrightarrow x \equiv \pm\frac{t}{\sqrt{a_i}} \pmod{73} \tag{2.4}$$

olur. Burada $\frac{t}{\sqrt{a_i}} \equiv m \pmod{73}$ olsun. Bu takdirde (2.4) denkleminin m ve $73 - m$ gibi farklı iki çözümü vardır. Dolayısıyla C_{F_i} koniği üzerinde $(m, 0)$ ve $(73 - m, 0)$ gibi iki tane rasyonel nokta vardır. Eğer $x = 0$ ise

$$c_i y^2 \equiv t^2 \pmod{73} \Leftrightarrow y \equiv \pm\frac{t^2}{\sqrt{c_i}} \pmod{73} \tag{2.5}$$

olur. Benzer şekilde $\frac{t^2}{\sqrt{c_i}} \equiv k \pmod{73}$ denilsin. Bu takdirde (2.5) denkleminin k ve $73 - k$ gibi iki çözümü ve dolayısıyla C_{F_i} üzerinde $(0, k)$ ve $(0, 73 - k)$ gibi iki rasyonel nokta vardır. Üstelik belli bir $x = h \in \mathbb{F}_{73}^*$ için

$$a_i h^2 + b_i h y + c_i y^2 \equiv t^2 \pmod{73}$$

kongrüansının $y = y_1$ çözümü ve $x = 73 - h$ için

$$a_i(73 - h)^2 + b_i(73 - h)y + c_i y^2 \equiv t^2 \pmod{73}$$

kongrüansının da $y = y_2$ çözümü vardır. Böylece C_{F_i} üzerinde $(m, 0)$, $(73 - m, 0)$, $(0, k)$, $(0, 73 - k)$, (h, y_1) ve $(73 - h, y_2)$ gibi altı tane rasyonel nokta vardır. Şimdi $G_{73} = \mathbb{F}_{73} - \{0, m, h\}$ diyelim. Bu takdirde her bir $x \in G_{73}$ için $a_i x^2 + b_i xy + c_i y^2 \equiv t^2 \pmod{73}$ kongrüansının iki tane çözümü vardır. Dolayısıyla C_{F_i} üzerinde iki tane rasyonel nokta vardır. G_{73} de $73-3=70$ tane x noktası bulunduğundan C_{F_i} de toplam $2{\cdot}70=140$ tane rasyonel nokta vardır. Yukarıda C_{F_i} de $(m,\,0)$, $(73-m,0)$, $(0,\,k)$, $(0,73-k)$, (h,y_1) ve $(73-h,y_2)$ gibi altı nokta olduğunu gösterilmişti. Dolayısıyla C_{F_i} üzerinde $140+6=146$ tane rasyonel nokta vardır.

2. Durum. $N\notin Q_{73}$ olsun. Eğer $y=0$ ise $a_ix^2\equiv N$ (mod 73) denkleminin çözümü yoktur. Çünkü $\frac{N}{a_i}$ ifadesi mod 73 de bir tam kare değildir. Eğer $x=0$ ise $\frac{N}{c_i}$ bir tam kare olmadığından $c_iy^2\equiv N$ (mod 73) denkleminin çözümü yoktur. Üstelik $a_ix^2+b_ixy+c_iy^2\equiv N$ (mod 73) kongrüansının her bir $x\in\mathbb{F}_{73}-\{0\}$ için y çözümü yoktur. O halde C_{F_i} de hiç bir rasyonel nokta yoktur.

2.3.2 Not. Yukarıdaki teoremde C_{F_i} deki rasyonel noktaların sayısını sadece $\mathbb{F}_{73}$ de ele alınmıştır. Eğer problem diğer sonlu $\mathbb{F}_p$ cisimlerinde ele alınırsa aşağıdaki genel teorem verilebilir.

2.3.3 Teorem. C_{F_i} yukarıdaki gibi olmak üzere $p\equiv 1$ (mod 4) ise

$$\#C_{F_i}(\mathbb{F}_p)=\begin{cases}2p & N\in Q_p\\ 0 & N\notin Q_p\end{cases}$$

ve $p\equiv 3$ (mod 4) ise

$$\#C_{F_i}(\mathbb{F}_p)=p+1$$

dir.

İspat. Teorem 2.3.1 in ispatına benzer şekilde yapılabilir.

2.4 Kübik Kongrüansların Çözümleri

p bir asal sayı ve $a, b, c \in \mathbb{F}_p$ için

$$x^3 + ax^2 + bx + c \equiv 0 \pmod{p}$$

şeklindeki denkliklere kübik kongrüans denir. Bu bölümde $F = (1, 7, -6)$ formunun has devrindeki formlara karşılık gelen kübik kongrüansların çözümleri $\mathbb{F}_{73}$ sonlu cisminde ele alınacaktır. $F_i = (a_i, b_i, c_i)$, F nin has devrinde herhangi bir form olmak üzere bu forma karşılık gelen kübik kongrüans

$$K^3_{\mathrm{F_i}} : x^3 + a_i x^2 + b_i x + c_i \equiv 0 \pmod{73}$$

olsun. Bu kongrüansın çözümlerinin kümesi

$$K^3_{F_i}(\mathbb{F}_{73}) = \{x \in \mathbb{F}_{73} : x^3 + a_i x^2 + b_i x + c_i \equiv 0 \pmod{73}\}$$

ile gösterilirse aşağıdaki teorem verilebilir.

2.4.1 Teorem. $K^3_{F_i}$ kübik kongrüansı için

$$\# K^3_{F_i} = \begin{cases} 3 & i = 5, 6, 8, 14, 15, 17 \\ 1 & i = 0, 4, 9, 13 \\ 0 & i = 1, 2, 3, 7, 10, 11, 12, 16 \end{cases}$$

dir.

İspat. $i = 5$ için $F_5 = (-4, 5, 3)$ kuadratik formuna karşılık gelen kübik kongrüans $K^3_{\mathrm{F_5}} : x^3 - 4x^2 + 5x + 3 \equiv 0 \pmod{73}$ olup bu kongrüansının $x = 32, 54$ ve 64 gibi üç tane çözümü vardır. Benzer şekilde aşağıdaki tablo elde edilebilir.

i	F_i	$K^3_{\mathrm{F_i}}$	$K^3_{F_i}(\mathbb{F}_{73})$	$\#K^3_{F_i}(\mathbb{F}_{73})$
0	F_0	$x^3 + x^2 + 7x - 6$	$\{41\}$	1
1	F_1	$x^3 - 6x^2 + 5x + 2$	$\{\}$	0

2	F_2	x^3+2x^2+7x-3	$\{\}$	0
3	F_3	x^3-3x^2+5x+4	$\{\}$	0
4	F_4	x^3+4x^2+3x-4	$\{12\}$	1
5	F_5	x^3-4x^2+5x+3	$\{32, 54, 64\}$	3
6	F_6	x^3+3x^2+7x-2	$\{3, 32, 35\}$	3
7	F_7	x^3-2x^2+5x+6	$\{\}$	0
8	F_8	x^3+6x^2+7x-1	$\{24, 55, 61\}$	3
9	F_9	x^3-x^2+7x+6	$\{32\}$	1
10	F_{10}	x^3+6x^2+5x-2	$\{\}$	0
11	F_{11}	x^3-2x^2+7x+3	$\{\}$	0
12	F_{12}	x^3+3x^2+5x-4	$\{\}$	0
13	F_{13}	x^3-4x^2+3x+4	$\{61\}$	1
14	F_{14}	x^3+4x^2+5x-3	$\{9, 19, 41\}$	3
15	F_{15}	x^3-3x^2+7x+2	$\{38, 41, 70\}$	3
16	F_{16}	x^3+2x^2+5x-6	$\{\}$	0
17	F_{17}	x^3-6x^2+7x+1	$\{12, 18, 49\}$	3

Tablo 2.4.1 $K_{F_i}^3$ kübik kongrüansının çözümleri

Bu tabloya göre teorem ispatlanmıştır.

3. BÖLÜM

POZİTİF TANIMLI KUADRATİK FORMLAR, KUADRATİK KONGRÜANSLAR VE SİNGÜLER EĞRİLER

Tezin bu kısmında pozitif tanımlı F_j kuadratik formlarının bir Ω ailesi tanımlanıp bu ailedeki formların bazı özellikleri incelenecektir. Daha sonra bu ailedeki formlara karşılık gelen C_{F_j} kuadratik kongrüanslarının tamsayı çözümlerinin sayısını ve son olarak $E_{F_{\frac{p-1}{2}}}$ singüler eğrisinin sonlu $\mathbb{F}_p$ cismi üzerindeki rasyonel noktalarının sayısı belirlenecektir.

3.1 Pozitif Tanımlı Formlar Ailesi

Bu alt bölümde pozitif tanımlı formlar ailesini ve bu ailedeki formların bazı temel özellikleri incelenecektir. $p \geq 5$ asalı ve $1 \leq j \leq \frac{p-1}{2}$ için $\Delta = 4j^2 - 2j(p-1)$ diskriminantlı

$$F_j = (a_j, b_j, c_j) = \left(1, 2j, \frac{p-1}{2}j\right) \tag{3.1}$$

formlarını ele alınsın. Bu formların ailesi

$$\Omega = \left\{F_j : F_j = \left(1, 2j, \ \frac{p-1}{2}j\right), 1 \leq j \leq \frac{p-1}{2}\right\} \tag{3.2}$$

ile gösterilsin. Dikkat edilirse $j = \frac{p-1}{2}$ için F_j formunun diskriminantı 0 olduğundan bu form pozitif tanımlı değildir. Dolayısıyla j nin bu değeri ihmal edilecektir. İlk olarak bu ailedeki F_j formlarının indirgenebilirliği ele alınsın. (3.1) de tanımlanan F_j pozitif tanımlı formları için $|b_j| > a_j$ olduğundan bu formlar indirgenebilir değildir. Ancak indirgenemeyen pozitif tanımlı bir form aşağıdaki indirgeme algoritması kullanılarak indirgenebilir hale getirilebilir. Bunun için $F = F_0 = (a_0, b_0, c_0)$ olsun. Bu takdirde $i \geq 0$ olmak üzere

$$s_i = \left\lfloor \frac{b_i + c_i}{2c_i} \right\rfloor \tag{3.3}$$

için F nin indirgenmişi

$$\rho^{i+1}(F) = (c_i,\ -b_i + 2c_i s_i,\ c_i s_i^2 - b_i s_i + a_i) \tag{3.4}$$

şeklindedir. Eğer $\rho^1(F)$ formu indirgenebilir değilse bu forma tekrar indirgeme algoritması uygulanır ve $\rho^2(F)$ elde edilir. Bu şekilde devam edilirse sonlu bir $k \geq 1$ adımda indirgenmiş $\rho^k(F)$ formu elde edilir.

3.1.1 Teorem. $1 \leq j \leq \frac{p-3}{2}$ için F_j pozitif tanımlı formunun indirgenmişi

$$\rho^2(F_j) = \begin{cases} (1,0,1) & p = 5 \\ \left(1, 0, -j^2 + \dfrac{p-1}{2} j\right) & p > 5 \end{cases} \tag{3.5}$$

dir.

İspat. $p = 5$ olsun. O halde $F_1 = (1, 2, 2)$ olup ve $F_0 = F_{1_0} = (a_0, b_0, c_0) = (1, 2, 2)$ için (3.3) den $s_0 = 1$ ve böylece (3.4) den $\rho^1(F_1) = (a_1, b_1, c_1) = (2, 2, 1)$ elde edilir. $|b_1| > c_1$ olduğundan bu form indirgenebilir değildir. Bu forma tekrar indirgeme algoritması uygulanırsa $s_1 = 1$ olup $\rho^2(F_1) = (a_2, b_2, c_2) = (1, 0, 1)$ olur. Bu form indirgenebilir olduğundan $p = 5$ için F_j nin indirgenmişi $\rho^2(F_1) = (1, 0, 1)$ formudur.

Şimdi $p > 5$ olsun. $i = 0$ için $s_0 = 0$ olup $\rho^1(F_j) = \left(\frac{p-1}{2}j, -2j,\ 1\right)$ formu elde edilir. Bu form indirgenmiş değildir. Benzer şekilde devam edilirse $s_1 = -j$ olup $\rho^2(F_j) = \left(1, 0, -j^2 + \frac{p-1}{2}j\right)$ formu elde edilir ki bu form indirgenebilir olduğundan F_j formunun indirgenmişi $\rho^2(F_j)$ formudur.

3.1.2 Teorem. F_j ve $\rho^2(F_j)$ sırasıyla (3.1) ve (3.5) de tanımlı formlar olsun. Bu takdirde $1 \leq j \leq \frac{p-3}{2}$ özelliğindeki her j için

$$\# Aut(F_j)^+ = \# Aut(F_j)^- = \# Aut(\rho^2(F_j))^+ = \# Aut(\rho^2(F_j))^- = \begin{cases} 4 & p = 5 \text{ ise} \\ 2 & p > 5 \text{ ise} \end{cases}$$

dir.

İspat. $p = 5$ ve $F_1 = (1, 2, 2)$ formu için $g = [r; s; t; u] \in \overline{\Gamma}$ olmak üzere

$$r^2 + 2rs + 2s^2 = 1$$

$$2rt + 2ru + 2ts + 4su = 2$$

$$t^2 + 2tu + 2u^2 = 2$$

denklem sisteminin $detg = 1$ için $g = \pm[1; 0; 0; 1], \pm[1; -1; 2; -1]$ ve $detg = -1$ için $g = \pm[1; -1; 0; -1], \pm[1; 0; 2; -1]$ çözümleri vardır. Dolayısıyla $Aut(F_1)^+ = \pm\{[1; 0; 0; 1], [1; -1; 2; -1]\}$ ve $Aut(F_1)^- = \pm\{[1;\ -1;\ 0; -1], [1; 0; 2; -1]\}$ dir. Benzer şekilde $p > 5$ için $Aut(F_j)^+ = \{\pm[1; 0; 0; 1]\}$ ve $Aut(F_j)^- = \{\pm[1; 0; 2j; -1]\}$ dir. $p = 5$ için

$$Aut(\rho^2(F_1))^+ = \pm\{[1; 0; 0; 1], [0; -1; 1; 0]\}$$

$$Aut(\rho^2(F_1))^- = \pm\{[1; 0; 0; -1], [1; 0; 0; -1]\}$$

ve $p > 5$ için ise $Aut(\rho^2(F_j))^+ = \{\pm[1; 0; 0; 1]\}$ ve $Aut(\rho^2(F_j))^- = \{\pm[1; 0; 0; -1]\}$

olduğu görülür.

3.1.3 Not. Dikkat edilirse yukarıdaki teoremde sadece $1 \leq j \leq \frac{p-3}{2}$ değerleri için F_j ve $\rho^2(F_j)$ formlarının otomorfizmleri ele alınmıştır. $j = \frac{p-1}{2}$ için $F_{\frac{p-1}{2}}$ ve $\rho^2(F_{\frac{p-1}{2}})$ nin diskriminantı $\Delta = 0$ olduğundan bu formlar pozitif tanımlı değildir. Ancak bu formların has ve has olmayan otomorfizmleri grubu sonsuz mertebelidir.

3.1.4 Teorem. 3.1.2 Teoreminde geçen F_j ve $\rho^2(F_j)$ formları için $1 \leq j \leq \frac{p-3}{2}$ olmak üzere $Aut(F_j)^+ \cong C_{Aut(F_j)^+}$ ve $Aut(\rho^2(F_j))^+ \cong C_{Aut(\rho^2(F_j))^+}$ dir.

İspat. $p = 5$ ve $Aut(F_1)^+ = \pm\{[1;0;0;1],[1;-1;2;-1]\}$ için

$$[1;-1;2;-1].[1;-1;2;-1] = [1-2;-1+1;2-2;-2+1] = [-1;0;0;-1]$$

$$[-1;0;0;-1].[1;-1;2;-1] = [-1+0;1;-2;1] = [-1;1;-2;1]$$

$$[-1;1;-2;1].[1;-1;2;-1] = [-1+2;0;-2+2;2-1] = [1;0;0;1]$$

$$[1;0;0;1].[1;-1;2;-1] = [1;-1;2;-1]$$

olduğundan

$$Aut(F_1)^+ \cong \langle[1;-1;2;-1]\rangle \cong C_4 \cong \langle[-1;1;-2;1]\rangle$$

dir. Benzer şekilde

$$Aut(F_j)^+ \cong C_2,\ Aut(\rho^2(F_1))^+ \cong C_4 \text{ ve } Aut(\rho^2(F_j))^+ \cong C_2$$

olduğu görülür.

3.1.5 Teorem. Her $1 \leq j \leq \frac{p-1}{2}$ için F_j ve $\rho^2(F_j)$ formları ambiguousdur.

İspat. F_j ve $\rho^2(F_j)$ nin has olmayan otomorfizmlerinin kümesi boş olmadığından belli bir $g_1 \in Aut(F_j)^-$ ve $g_2 \in Aut(\rho^2(F_j))^-$ için $g_1F_j = F_j$ ve $g_2\rho^2(F_j) = \rho^2(F_j)$ dir, yani F_j ve $\rho^2(F_j)$ formları ambiguousdur.

3.2 Kuadratik Kongrüanslar

Bu bölümde bir önceki bölümde tanımlanan F_j ve $\rho^2(F_j)$ formları için $F_1, F_{\frac{p-1}{2}}$ ve bu formların $\rho^2(F_1)$ ve $\rho^2(F_{\frac{p-1}{2}})$ indirgenmişlerine karşılık gelen kuadratik kongrüansların $\mathbb{F}_p$ deki tamsayı çözümleri ele alınacaktır. $F = (a, b, c)$ herhangi bir kuadratik form ve $C_F: ax^2 + bxy + cy^2 \equiv 1(\operatorname{mod} p)$ bu forma karşılık gelen kuadratik kongrüans olsun. Buna göre F_1, $F_{\frac{p-1}{2}}$ ve $\rho^2(F_1)$, $\rho^2(F_{\frac{p-1}{2}})$ formlarına karşılık gelen kuadratik kongrüanslar sırasıyla

$$C_{F_1}: x^2+2xy+\frac{p-1}{2}y^2 \equiv 1(\operatorname{mod} p) \tag{3.6}$$

$$C_{F_{\frac{p-1}{2}}}: x^2+(p-1)xy+\left(\frac{p-1}{2}\right)^2 y^2 \equiv 1(\operatorname{mod} p) \tag{3.7}$$

$$C_{\rho^2(F_1)}: x^2+\frac{p-3}{2}y^2 \equiv 1(\operatorname{mod} p) \tag{3.8}$$

$$C_{\rho^2(F_{\frac{p-1}{2}})}: x^2 \equiv 1(\operatorname{mod} p) \tag{3.9}$$

dır. Bu kongrüansların çözüm kümeleri de sırasıyla

$$C_{F_1}(\mathbb{F}_p) = \left\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p: x^2 + 2xy + \frac{p-1}{2}y^2 \equiv 1(\operatorname{mod} p)\right\}$$

$$C_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \left\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p: x^2 + (p-1)xy + \left(\frac{p-1}{2}\right)^2 y^2 \equiv 1(\operatorname{mod} p)\right\}$$

$$C_{\rho^2(F_1)}(\mathbb{F}_p) = \left\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p: x^2 + \frac{p-3}{2}y^2 \equiv 1(\operatorname{mod} p)\right\}$$

$$C_{\rho^2\left(F_{\frac{p-1}{2}}\right)}(\mathbb{F}_p) = \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p: x^2 \equiv 1(\operatorname{mod} p)\}$$

olsun. Bu takdirde aşağıdaki teorem verilebilir.

3.2.1 Teorem. C_{F_1}, $C_{F_{\frac{p-1}{2}}}$, $C_{\rho^2(F_1)}$ ve $C_{\rho^2(F_{\frac{p-1}{2}})}$ yukarıda tanımlanan kuadratik kongrüanslar olmak üzere her $p \geq 5$ asalı için

$$\# \, C_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \# \, C_{\rho^2(F_{\frac{p-1}{2}})}(\mathbb{F}_p) = 2p$$

ve

$$\# \, C_{F_1}(\mathbb{F}_p) = \# \, C_{\rho^2(F_1)}(\mathbb{F}_p) = \begin{cases} p-1 & p \equiv 1, 5, 19, 23 \ (\mathrm{mod}\ 24) \text{ ise} \\ p+1 & p \equiv 7, 11, 13, 17 (\mathrm{mod}\ 24) \text{ ise} \end{cases}$$

dir.

İspat. $C_{F_{\frac{p-1}{2}}}$ kongrüansı için $y = 0$ ise $x^2 \equiv 1(\mathrm{mod}\, p) \Leftrightarrow x \equiv \pm 1 \ (\mathrm{mod}\, p)$ dır. Benzer şekilde $x = 0$ ise $\left(\frac{p-1}{2}\right)^2 (\pm 2)^2 \ \equiv p^2 - 2p + 1 \equiv 1(\mathrm{mod}\, p)$ olduğundan

$$\left(\frac{p-1}{2}\right)^2 y^2 \ \equiv 1(\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm 2(\mathrm{mod}\, p)$$

dir. Üstelik (1, 4) ve $(p-1, p-4)$ de $C_{F_{\frac{p-1}{2}}}$ nin bir çözümüdür. Şu halde kongrüansın $(1,0), (p-1,0), (0,2), (0,p-2), (1,4)$ ve $(p-1,p-4)$ gibi altı tane tamsayı çözümü vardır. Ayrıca $p^2 - 2p + 1 \equiv 1(\mathrm{mod}\, p)$ ve $(p-1)^2 | 2((1-p)x \pm 1)$ dir. $x \in H_p = \mathbb{F}_p - \{0, 1, p-1\}$ için kongrüans y ye göre çözülürse

$$\left(\frac{p-1}{2}\right)^2 y^2 + (p-1)xy + x^2 - 1 = 0 \tag{3.10}$$

olur. (3.10) un diskriminantı

$$\Delta = ((p-1)x)^2 - 4\left(\frac{p-1}{2}\right)^2 (x^2 - 1) = p^2 - 2p + 1 \equiv 1(\mathrm{mod}\, p)$$

olup çözümleri

$$y_{1,2} = \frac{-(p-1)x \pm \sqrt{p^2 - 2p + 1}}{2\left(\frac{p-1}{2}\right)^2} \equiv \frac{2[-(p-1)x \pm 1]}{(p-1)^2} (\mathrm{mod}\, p)$$

dir. Burada $(p-1)^2|2((1-p)x \pm 1)$ olduğundan her bir $x \in H_p$ için bu kongrüansın iki tane y çözümü vardır. H_p de $p-3$ tane x değeri olup bunların her biri için iki tane y çözümü olduğundan kongrüansın toplam $2(p-3) = 2p-6$ tane çözümü vardır. Ayrıca $(1,0), (p-1,0), (0,2), (0,p-2), (1,4)$ ve $(p-1,p-4)$ değerleri de çözüm olduğundan toplam $2p-6+6 = 2p$ tane çözüm vardır.

Diğer üç kongrüansta benzer şekilde çözülür.

3.3 Singüler Eğriler

Bu bölümde (3.1) de tanımlanan F_j formuna karşılık gelen singüler eğriler üzerindeki rasyonel noktaların sayısı ele alınacaktır. Hatırlanacağı üzere kuadratik formlar ile eliptik eğriler arasında bir ilişki vardır. Dolayısıyla $\Delta(F) = a^2 - 4b$ determinantlı $F = (1, a, b)$ formuna karşılık gelen eliptik eğri

$$E_F: y^2 = x^3 + ax^2 + bx \tag{3.11}$$

dir. Bu eğri için $\Delta(E_F) = 16b^2(a^2 - 4b) = 16b^2\,\Delta(F)$ dir. Buna göre eğer F formunun diskriminantı 0 ise E_F nin de diskriminantı 0 olacağından bu bir singüler eğri olur. Dolayısıyla da bu eğrinin bir singüler noktası vardır. Gerçekten de (3.11) eşitliğini açarsak $x^2 + ax + b = 0$ ikinci dereceden denklemin diskriminantı $\Delta = a^2 - 4b = 0$ olduğundan bu denklemin çakışık iki kökü vardır ve bu kök $\frac{-a}{2}$ dir. Dolayısıyla (3.11) eşitliği

$$E_F: y^2 = x^3 + ax^2 + bx = x(x^2 + ax + b) = x\left(x - \left(\frac{-a}{2}\right)\right)^2$$

haline gelir. $1 \leq j \leq \frac{p-1}{2}$ için

$$E_{F_j}: y^2 = x^3 + 2jx^2 + \left(\frac{p-1}{2}\right)jx$$

eğrileri F_j formuna karşılık gelen eliptik eğri olsun. E_{F_j} nin bu tanımına dikkat edilirse $1 \leq j \leq \frac{p-3}{2}$ için bu eğrinin diskriminantı sıfırdan farklı olduğundan bu eğri bir eliptik eğri belirtir. Ancak $j = \frac{p-1}{2}$ formun diskriminantı 0 olduğundan bu forma karşılık gelen eğrinin diskriminantı olacağından bu bir singüler eğridir, yani $E_{F_{\frac{p-1}{2}}}$ singülerdir. Şimdi

$$E_{F_{\frac{p-1}{2}}}: y^2 = x^3+(p-1)x^2 + \frac{(p-1)^2}{4}x = x(x - \frac{1-p}{2})^2 \tag{3.12}$$

singüler eğrisi ele alınsın. Bu eğrinin rasyonel noktalarının kümesi

$$E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \left\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x\right\} \cup \{O\}$$

ile gösterilirse aşağıdaki teorem verilebilir.

3.3.1 Teorem. (3.12) de tanımlı $E_{F_{\frac{p-1}{2}}}$ singüler eğrisi için

$$\# E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \begin{cases} p & p \equiv 1,7 \pmod 8 \text{ ise} \\ p+2 & p \equiv 3,5 \pmod 8 \text{ ise} \end{cases}$$

dir.

İspat. $p \equiv 1,7 (\mathrm{mod}\ 8)$ olsun. Eğer $y = 0$ ise

$$x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x \equiv 0 (\mathrm{mod}\ p) \Leftrightarrow x\left[x^2 + (p-1)x + \frac{(p-1)^2}{4}\right] \equiv 0 (\mathrm{mod}\ p)$$

$$\Leftrightarrow x \equiv 0 (\mathrm{mod}\ p) \text{ veya } x^2 + (p-1)x + \frac{(p-1)^2}{4} \equiv 0 (\mathrm{mod}\ p)$$

olur. Buradan kolayca görüleceği üzere $x = 0$ ve $x = \frac{1-p}{2}$ yukarıdaki kongrüansın birer çözümüdür, yani $E_{F_{\frac{p-1}{2}}}$ de $(0,0)$ ve $(\frac{1-p}{2}, 0)$ gibi iki rasyonel nokta vardır. Üstelik p nin bu değerleri için $\frac{1-p}{2}$ bir kuadratik rezidü, yani $\frac{1-p}{2} \in Q_p$ dir. Şimdi kabul edelim ki $x \in Q_p$ olsun. Bu takdirde yukarıdaki eşitlikten

$$\left(\frac{x^3+(p-1)x^2+\frac{(p-1)^2}{4}x}{p}\right)=\left(\frac{x-\frac{1-p}{2}}{p}\right)$$

elde edilir. Eğer $x=\frac{1-p}{2}$ ise $\left(\frac{x-\frac{1-p}{2}}{p}\right)=0$ olduğundan $y^2\equiv 0(\mathrm{mod}\,p)$ nin $y=0$ gibi bir çözümü vardır. Eğer $x\neq\frac{1-p}{2}$ ise $\left(\frac{x-\frac{1-p}{2}}{p}\right)=1$ olduğundan $x^3+(p-1)x^2+\frac{(p-1)^2}{4}x$ ifadesi $\mathrm{mod}\,p$ de bir tam karedir. $u\in\mathbb{F}_p^*$ için $x^3+(p-1)x^2+\frac{(p-1)^2}{4}x=u^2$ olsun. Bu takdirde

$$y^2\equiv u^2(\mathrm{mod}\,p)\Leftrightarrow y\equiv\pm u\ (\mathrm{mod}\,p)$$

olduğundan $E_{F_{\frac{p-1}{2}}}$ de (x,u) ve $(x,p-u)$ gibi iki rasyonel nokta vardır. Bu ise her bir x değeri için iki tane y değerinin olması demektir. Şu halde $x^3+(p-1)x^2+\frac{(p-1)^2}{4}x$ bir tam kare olacak şekilde $\frac{p-1}{2}-1=\frac{p-3}{2}$ tane x değeri vardır (kuadratik rezidülerin sayısı $\frac{p-1}{2}$ olduğundan bu sayıdan 1 çıkartılır, çünkü $\frac{1-p}{2}$ bir kuadratik rezidü iken bu değere karşılık bir tane y değeri elde edilir). O halde $E_{F_{\frac{p-1}{2}}}$ de $2\left(\frac{p-3}{2}\right)=p-3$ nokta rasyonel nokta vardır. Üstelik yukarıda $E_{F_{\frac{p-1}{2}}}$ de $(0,0)$ ve $(\frac{1-p}{2},0)$ rasyonel noktalarının da olduğu görüldü. Sonsuz noktasını da ilave edersek $E_{F_{\frac{p-1}{2}}}$ de toplam $p-3+2+1=p$ tane rasyonel nokta olduğu görülür.

$p\equiv 3,5(\mathrm{mod}\ 8)$ olması hali de benzer şekilde gösterilebilir.

3.3.2 Not. Yukarıdaki teoremde sadece singüler eğriler üzerindeki rasyonel noktaların sayısı belirlendi. Daha önceden de söylediğimiz gibi $1\leq j\leq\frac{p-3}{2}$ değerleri için E_{F_j} ler birer eliptik eğridir. Fakat j nin bu değerleri için E_{F_j} eliptik eğrileri üzerindeki rasyonel noktaların sayısı düzenli olmadığı için bir formül elde edilememiştir.

3.3.3 Sonuç. $p \equiv 1,7 (\mathrm{mod}\ 8)$ veya $p \equiv 3,5 (\mathrm{mod}\ 8)$ olması hallerinde her $x \notin Q_p$ için $\left(\frac{x^3+(p-1)x^2+\frac{(p-1)^2}{4}x}{p}\right) = -1$ olduğundan x in bu değerleri için $E_{F_{\frac{p-1}{2}}}$ üzerinde rasyonel nokta yoktur.

3.3.4 Örnek 1. $p = 23$ olsun. Bu takdirde $\mathbb{F}_{23}$ de $E_{F_{11}}: y^2 = x^3+22x^2+6x$ singüler eğrisi üzerindeki rasyonel noktaların kümesi

$$E_{F_{11}}(\mathbb{F}_{23}) = \left\{ \begin{array}{c} (\mathbf{0}, \mathbf{0}), (1, \pm 11), (2, \pm 4), (3, \pm 6), (4, \pm 7), (6, \pm 3), \\ (8, \pm 6), (9, \pm 9), (\mathbf{12}, \mathbf{0}), (13, \pm 6), (16, \pm 7), (18, \pm 2) \end{array} \right\} \cup \{O\}$$

dir.

2. $p = 37$ için $\mathbb{F}_{37}$ de $E_{F_{18}}: y^2 = x^3+36x^2+28x$ eğrisi üzerindeki rasyonel noktaların kümesi

$$E_{F_{18}}(\mathbb{F}_{37}) = \left\{ \begin{array}{c} (\mathbf{0}, \mathbf{0}), (1, \pm 18), (3, \pm 18), (4, \pm 7), (7, \pm 3), (9, \pm 7), \\ (10, \pm 12), (11, \pm 1), (12, \pm 12), (16, \pm 12), (\mathbf{19}, \mathbf{0}), \\ (21, \pm 11), (25, \pm 7), (26, \pm 4), (27, \pm 10), (28, \pm 14), \\ (30, \pm 2), (33, \pm 17), (34, \pm 18), (36, \pm 9) \end{array} \right\} \cup \{O\}$$

dir.

Şimdi $E_{F_{\frac{p-1}{2}}}$ singüler eğrisi üzerindeki (x, y) rasyonel noktalarının $x-$ ve $y-$ koordinatları toplamı ele alınsın. Bunun için

$$E^x_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \{x \in \mathbb{F}_p : (x, y) \in E_{F_{\frac{p-1}{2}}}\} \text{ ve } E^y_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \{y \in \mathbb{F}_p : (x, y) \in E_{F_{\frac{p-1}{2}}}\}$$

tanımlansın. Buna göre

$$\sum_{[x]} E^x_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) \text{ ve } \sum_{[y]} E^y_{F_{\frac{p-1}{2}}}(\mathbb{F}_p)$$

toplamları ile ilgili aşağıdaki teorem verilebilir.

3.3.5 Teorem. $E_{F_{\frac{p-1}{2}}}$ eğrisi için

$$\sum_{[x]} E^{x}_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \begin{cases} \frac{p^3+5p-6}{12} & p \equiv 1,7 (\text{mod } 8) \text{ ise} \\ \frac{p^3-7p+6}{12} & p \equiv 3,5 (\text{mod } 8) \text{ ise} \end{cases}$$

ve

$$\sum_{[y]} E^{y}_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \begin{cases} \frac{p^2-3p}{2} & p \equiv 1,7 (\text{mod } 8) \text{ ise} \\ \frac{p^2-p}{2} & p \equiv 3,5 (\text{mod } 8) \text{ ise} \end{cases}$$

dir.

İspat. $\mathbb{F}_p$ deki birimlerin kümesi $U_p = \{1, 2, \ldots, p-1\}$ olmak üzere bu kümedeki her bir elemanın karesinin alınması suretiyle kuadratik rezidülerin Q_p kümesi elde edilmiş olur. Q_p deki tüm elemanların toplamı ise

$$\sum_{x \in Q_p} x = \frac{p^3 - p}{24}$$

dir. Şimdi $p \equiv 1,7 (\text{mod } 8)$ olsun. Bu takdirde Teorem 3.3.1 gereği $\frac{1-p}{2} \in Q_p$ olup $x = \frac{1-p}{2}$ için $E_{F_{\frac{p-1}{2}}}$ singüler eğrisi üzerinde sadece bir nokta bulunmaktadır. $H_p = Q_p - \left\{\frac{1-p}{2}\right\}$ olsun. Bu takdirde

$$\sum_{x \in H_p} x = \sum_{x \in Q_p} x - \frac{1-p}{2} = \frac{p^3 + 11p - 12}{24}$$

dir. Ayrıca H_p deki her bir x elemanı $x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x$ ifadesini bir tam kare yapar. $x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x = t^2$ olsun. Buradan $y^2 \equiv t^2 (\text{mod } p)$ elde edilir. Bu ise eğride (x, t) ve $(x, p-t)$ gibi iki rasyonel noktanın olması demektir. Şu halde her bir $x \in H_p$ için iki rasyonel nokta vardır ve bu rasyonel noktaların $x-$

koordinatlarının toplamı $2x$ dir. O halde $E_{F_{\frac{p-1}{2}}}$ deki tüm rasyonel noktaların $x-$ koordinatları toplamı

$$2\sum_{x\in H_p} x = \frac{p^3+11p-12}{12}$$

dır. Ayrıca $\left(\frac{1-p}{2}, 0\right)$ noktası da $E_{F_{\frac{p-1}{2}}}$ singüler eğrisi üzerindedir. O halde sonuç olarak $E_{F_{\frac{p-1}{2}}}$ deki tüm rasyonel noktaların x −koordinatları toplamı

$$\sum_{[x]} E^{x}_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \frac{1-p}{2} + 2\sum_{x\in H_p} x = \frac{p^3+5p-6}{12}$$

dir. Benzer şekilde $p \equiv 3, 5 (\mathrm{mod}\ 8)$ için

$$\sum_{[x]} E^{x}_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \frac{p^3-7p+6}{12}$$

olduğu görülür.

Şimdi y −koordinatları toplamı ele alınsın. $p \equiv 1, 7 (\mathrm{mod}\ 8)$ için Teorem 3.3.1 den $x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x$ ifadesini tam kare yapan $\frac{p-3}{2}$ tane x noktasının olduğu bilinmektedir. Keyfi bir $t \neq 0$ tamsayısı için $x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x = t^2$ olsun. Bu takdirde $y^2 \equiv t^2 (\mathrm{mod}\ p) \Leftrightarrow y \equiv \pm t (\mathrm{mod}\ p)$ nin $y = t$ ve $y = -t = p - t$ gibi iki çözümü vardır, yani $E_{F_{\frac{p-1}{2}}}$ singüler eğrisi üzerinde (x, t) ve $(x, p-t)$ gibi iki rasyonel nokta vardır. Bunların $y-$ koordinatları toplamı p dir. $x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x$ ifadesini tam kare yapan H_p de $\frac{p-3}{2}$ tane x değerinin olduğu bilinmektedir. O halde $E_{F_{\frac{p-1}{2}}}$ deki tüm (x, y) rasyonel noktaların y −koordinatları toplamı

$$\sum_{[y]} E^{y}_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = p\left(\frac{p-3}{2}\right) = \frac{p^2-3p}{2}$$

dir. Benzer şekilde $p \equiv 3, 5 (\mathrm{mod}\ 8)$ ise bu toplamın $\frac{p^2-p}{2}$ olduğu görülür.

4. BÖLÜM

POZİTİF TAMSAYILARIN KUADRATİK FORMLAR İLE GÖSTERİMİ

Bu bölümde pozitif tamsayıların kuadratik formlar ve bu formların direkt toplamları ile gösterilmesi problemi ele alınacaktır. Tamsayıların kuadratik formlar ile gösterimi kuadratik formlar teorisinde çok önemli bir yere sahip olup bir çok matematikçi tarafından ele alınmıştır. Probleme başlamadan önce aşağıdaki teoremler ve notasyonlar verilecektir.

$k > 2,\ 2|k$ pozitif tamsayı ve b_{rs} ler de tamsayı olmak üzere

$$F = F(x_1, x_2, ..., x_k) = \sum_{1 \le r \le s \le k} b_{rs} x_r x_s \tag{4.1}$$

formuna k −değişkenli ikinci dereceden form denir. Bu formun determinantı Δ ile gösterilir ve bu F formuna karşılık gelen

$$M(F) = \begin{pmatrix} b_{11} & b_{12}/2 & b_{13}/2 & \dots & b_{1k}/2 \\ b_{21}/2 & b_{22} & b_{23}/2 & \dots & b_{2k}/2 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ b_{k1}/2 & b_{k2}/2 & b_{k3}/2 & \dots & b_{kk} \end{pmatrix}$$

matrisin determinantı olarak tanımlanır, yani $\Delta = |M(F)|$ dir. Şimdi yukarıdaki formdan faydalanarak D determinantlı

$$2F = \sum_{r,s=1}^{k} a_{rs} x_r x_s,\ \ (a_{rr} = 2b_{rr},\ a_{rs} = a_{sr} = b_{rs},\ r < s) \tag{4.2}$$

kuadratik formu tanımlansın. Bu takdirde Δ determinantlı F ile D determinantlı $2F$ formunun determinantları arasındaki ilişki $\Delta = (-1)^k D$ şeklindedir. A_{rs} ile (4.2) deki a_{rs} elemanlarının kofaktörleri gösterilsin. $\delta = obeb\left(\frac{A_{rr}}{2},\, A_{rs}\right)$ olsun. Bu takdirde $N = \frac{D}{\delta}$ ye F formunun seviyesi denir. F nin karakteri $\mu(d)$ ile gösterilir ve aşağıdaki gibi tanımlanır: Eğer Δ tam kare ise $\mu(d) = 1$; eğer Δ tam kare değil ve $2 \nmid \Delta$ ise $d > 0$ için $\mu(d) = \left(\frac{d}{|\Delta|}\right)$ve $d < 0$ için $\mu(d) = (-1)^{k/2}\mu(-d)$ dir. Burada $\left(\frac{d}{|\Delta|}\right)$ genelleştirilmiş Jakobi sembolüdür. k değişkenli, N seviyeli ve $\mu(d)$ karakterli bir F kuadratik formu $\left(-\frac{k}{2},\, N,\, \mu(d)\right)$ tipinde kuadratik form diye adlandırılır.

N doğal sayı ve $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ olmak üzere $a \in \mathbb{Z}$ nin mod N ye göre kalan sınıfı a_N ile gösterilirse $\begin{pmatrix} a_N & b_N \\ c_N & d_N \end{pmatrix}$ şeklindeki matrislerin oluşturduğu küme de Γ_N ile gösterilir. mod N ye göre tüm kalan sınıfların halkası $\mathbb{Z}_N$ olmak üzere $\mathbb{Z} \to \mathbb{Z}_N$, $r \to r_N$ halka homomorfizmi Γdan Γ_N içine

$$\sigma : \Gamma \to \Gamma_N ,\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a_N & b_N \\ c_N & d_N \end{pmatrix}$$

grup homomorfizmini indirger. Bu grup homomorfizminin çekirdeği

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\operatorname{mod} N) \right\} \tag{4.3}$$

Γnin bir normal alt grubudur. Üstelik Γnin σ homomorfizmi altındaki resmi $\sigma(\Gamma) \approx \Gamma / \Gamma(N) \approx \Gamma_N$ dir. Bu normal alt gruba N seviyeli temel denklik alt grubu denir. N doğal sayısı için Γ homojen modüler grubunun özel denklik alt grubu

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 (\operatorname{mod} N) \right\}$$

dır. $G_k(\Gamma_0,\mu)$ ve $S_k(\Gamma_0,\mu)$ sırasıyla (k,Γ_0,μ) tipindeki modüler ve cusp formların uzayını göstermek üzere $F(\tau)\in G_k(\Gamma_0,\mu)$ için $\xi=i\infty$ cuspının komşuluğunda $F(\tau)$

$$F(\tau)=\sum_{m=m_0\geq 0}^{\infty} a_m z^m\,,\ a_{m_0}\neq 0 \tag{4.4}$$

şeklinde yazılabilir. Bu takdirde $F(\tau)\in G_k(\Gamma_0,\mu)$ nin $\xi=i\infty$ daki Γ_0 ya göre mertebesi

$$ord\left(F(\tau),\ i\infty,\ \Gamma_0\right)=m_0 \tag{4.5}$$

dır. (4.4) deki a_{m_0} sayısına mertebenin katsayısı denir ve $a_{m_0}(F(\tau))$ ile gösterilir. (Lang 1976)

F kuadratik formu için

$$\wp\left(\tau;F(x),\ P_\nu(x),h\right)=\sum_{n_i\equiv h_i\ (\mathrm{mod}\ N)} P_\nu(n_1,n_2,\ldots,n_k)\,z_N^{\frac{1}{N}F(n_1,n_2,\ldots,n_k)} \tag{4.6}$$

ve

$$\wp\left(\tau;F(x),\ P_\nu(x)\right)=\sum_{n=1}^{\infty}\left(\sum_{F(x)=n}P_\nu(x)\right)z^n \tag{4.7}$$

tanımlansın. Burada $F(x)=\frac{1}{2}\sum_{r,s=1}^{k}a_{rs}x_r x_s$, $\left(\frac{k}{2},\ N,\ \mu\right)$ tipinde bir kuadratik form ve $P_\nu(x)$ de bu forma karşılık gelen ν mertebeden küresel fonksiyonlardır. Üstelik $n_1,n_2,\ldots,n_k$ tamsayıları için $h=(h_1,h_2,\ldots,h_k)$ tamsayısı

$$\sum_{s=1}^{k}a_{rs}h_s\equiv 0\ (\mathrm{mod}\,N),\quad (r=1,\ 2,\ldots,\ k)$$

özelliğinde bir tamsayıdır.

n pozitif bir tamsayı olmak üzere $r(n;F)$, $F=F(x_1,x_2,\ldots,x_k)=n$ denkleminin çözümlerinin sayısını göstersin. Bu takdirde F kuadratik formuna belli bir

$$\wp(\tau;F)=1+\sum_{n=1}^{\infty} r(n;F)z^n \tag{4.8}$$

teta serisi karşılık gelir. Şimdi q tek asal sayı olmak üzere aşağıdaki lemmalar verilebilir.

4.1 Lemma. $k>2$ için $(-k,q,1)$ tipindeki F kuadratik formuna belli bir

$$E(\tau;F)=1+\sum_{n=1}^{\infty}(\alpha\sigma_{k-1}(n)z^n+\beta\sigma_{k-1}(n)z^{qn}) \tag{4.9}$$

Eisenstein serisi karşılık gelir. Burada $\alpha=\frac{i^k}{\rho_k}\frac{q^{k/2}-i^k}{q^k-1}$, $\beta=\frac{1}{\rho_k}\frac{q^k-i^kq^{k/2}}{q^k-1}$ ve $\zeta(k)$ Riemann zeta fonksiyonu olmak üzere $\rho_k=(-1)^{k/2}\frac{(k-1)!}{(2\pi)^k}\zeta(k)$ ve $\sigma_{k-1}(n)=\sum_{d|n}d^{k-1}$ dir (Hecke 1970).

4.2 Lemma. $k>2$ çift tamsayısi için F formu $(-k,q,1)$ tipinde bir form ise

$$\wp(\tau;F)-E(\tau;F)$$

farkı da $(-k,q,1)$ tipinde bir cusp formdur (Hecke 1970).

4.3 Lemma. k değişkenli

$$\varphi_{rs}=x_rx_s-\frac{1}{k}\frac{A_{rs}}{D}2F \quad (r,s=1,2,\ldots,k) \tag{4.10}$$

kuadratik polinomları, F formuna karşılık gelen ikinci mertebeden küresel fonksiyonlardır (Hecke 1970).

4.4 Lemma. F formu $\left(-\frac{k}{2},\, N,\, \mu\right)$ tipinde bir kuadratik form ve $P_v(x)$ de bu forma karşılık gelen v mertebeli küresel fonksiyonlar olmak üzere genelleştirilmiş katlı

$$\wp(\tau; F, P_v) = \sum_{n=1}^{\infty}\left(\sum_{F=n} P_v\right) z^n \tag{4.11}$$

teta serisi de $\left(-\left(\frac{k}{2}+v\right), \Gamma_0(N),\, \mu\right)$ tipinde bir cusp formdur. (Hecke 1970)

4.5 Lemma. F_1 ve F_2 sırasıyla $(k_1,\, N,\, \mu_1)$ ve $k_2,\, N,\, \mu_2$ tipinde formlar ise bunların $F_1 \oplus F_2$ direkt toplamları da $(k_1+k_2,\, N,\, \mu_1\mu_2)$ tipinde bir kuadratik formdur (Hecke 1970).

Bu açıklamalar yardımıyla, bu bölümde tamsayıların -31 determinantlı $F_1 = x_1^2 + x_1x_2 + 8x_2^2$ ve $G_1 = 2x_1^2 + x_1x_2 + 4x_2^2$ kuadratik formlar ve bu formların direkt toplamları ile gösterimi problemi üzerinde durulacaktır. Daha sonra $S_4(\Gamma_0(31), 1)$ uzayı için baz oluşturup bu bazın elemanları kullanılarak tamsayıların $F_4,\ G_4,\ F_3 \oplus G_1,\ F_2 \oplus G_2$ ve $F_1 \oplus G_3$ formları ile gösterilmesi ile ilgili formüller verilecektir.

Hatırlanacağı üzere 4.5 Lemması gereği F_i ve G_j formları $N = N_i = N_j$ seviyeli ve sırasıyla $\chi_i(d)$ ve $\chi_j(d)$ karakterli iki form ise bunların $F_i \oplus G_j$ direkt toplamları da N seviyeli ve $\chi_1(d)\chi_2(d)$ karakterli bir formdur. Dolayısıyla $i + j = k$ için

$$\wp(\tau; F_k) = \wp^k(\tau; F_1) = \wp(\tau; F_i)\wp(\tau; F_j)$$

$$\wp(\tau; G_k) = \wp^k(\tau; G_1) = \wp(\tau; G_i)\wp(\tau; G_j)$$

$$\wp(\tau; F_i \oplus G_j) = \wp(\tau; F_i)\wp(\tau; G_j) = \wp^i(\tau; F_1)\wp^j(\tau; G_1)$$

dir. Bu tanıma göre

$$F_2(x_1, x_2, x_3, x_4) = (x_1^2 + x_3^2) + (x_1x_2 + x_3x_4) + 8(x_2^2 + x_4^2)$$

$$G_2(x_1, x_2, x_3, x_4) = 2(x_1^2 + x_3^2) + (x_1x_2 + x_3x_4) + 4(x_2^2 + x_4^2)$$

$$F_1 \oplus G_1(x_1, x_2, x_3, x_4) = x_1^2 + x_1x_2 + 8x_2^2 + 2x_3^2 + x_3x_4 + 4x_4^2$$

dir. O halde aşağıdaki teoremler verilebilir.

4.6 Teorem. F_2 kuadratik formu için

(1) $\varphi_{11} = x_1^2 - \frac{8}{31}F_2$, F_2 ye karşılık gelen ikinci mertebeden küresel fonksiyondur.

(2) $\wp(\tau; F_2, \varphi_{11}) = \frac{30}{31}z + \frac{60}{31}z^2 + \frac{120}{31}z^4 + \frac{300}{31}z^5 + \cdots \in S_4(\Gamma_0(31), 1)$ dir.

(3) $ord(\wp(\tau; F_2, \varphi_{11})) = 1$ dir.

İspat. $F_1 = x_1^2 + x_1x_2 + 8x_2^2$ kuadratik formu için tanım gereği $b_{11} = 1, b_{12} = b_{21} = 1/2$ ve $b_{22} = 8$ olup $a_{11} = 2$, $a_{12} = a_{21} = b_{12} = 1/2$ ve $a_{22} = 16$ dır. Dolayısıyla $A_{11} = 16$ ve $A_{22} = 2$ dir. Üstelik $D = 31$ olup $\delta = 1$ ve $N = \frac{D}{\delta} = 31$ olduğundan F_1, $(-1, \Gamma_0(31), \chi)$ tipinde bir kuadratik formdur. Eğer $k = 4$, $F = F_2$ ve $r = s = 1$ olarak alınırsa Lemma 4.3 gereği $\varphi_{11} = x_1^2 - \frac{8}{31}F_2$ fonksiyonu F_2 ye karşılık gelen ikinci mertebeden küresel fonksiyon olur. Şimdi pozitif n tamsayısı için

$$F_1(x_1, x_2) = x_1^2 + x_1x_2 + 8x_1x_2 + x_2^2 = n$$

denklemi ele alınsın. Bu denklemin $n = 1$ için $(\pm 1, 0)$ iki çözümü vardır, $n = 2, 3$ ve 5 için çözümü yoktur ve $n = 4$ için $(\pm 2, 0)$ iki çözümü vardır. Dolayısıyla (4.8) den

$$\wp(\tau; F_1) = 1 + 2z + 2z^4 + \cdots \tag{4.12}$$

dir. Benzer şekilde $F_2(x_1, x_2, x_3, x_4) = n$ denkleminin ise $n = 1$ için $(\pm 1, 0, 0, 0)$, $(0, 0, \pm 1, 0)$ dört çözümü vardır, $n = 2$ için $(-1, 0, \pm 1, 0)$, $(1, 0, \pm 1, 0)$ dört çözümü vardır, $n = 3$ için çözümü yoktur, $n = 4$ için $(\pm 2, 0, 0, 0), (0, 0, \pm 2, 0)$ dört çözümü vardır ve $n = 5$ için $(-2, 0, \pm 1, 0)$, $(-1, 0, \pm 2, 0)$, $(1, 0, \pm 2, 0)$, $(2, 0, \pm 1, 0)$ sekiz çözümü vardır. Böylece (4.8) den

$$\wp(\tau; F_2) = \wp^2(\tau; F_1) = 1 + 4z + 4z^2 + 4z^4 + 8z^5 + \cdots \qquad (4.13)$$

elde edilir. Buna göre Lemma 4.3 gereği

$$\wp(\tau; F_2, \varphi_{11}) = \frac{1}{31}((31 \cdot 1 \cdot 2 - 8 \cdot 1 \cdot 4)z + (31 \cdot 1 \cdot 4 - 8 \cdot 2 \cdot 4)z^2 + (31 \cdot 4 \cdot 2 - 8 \cdot 4 \cdot 4)z^4 + (31 \cdot 4 \cdot 4 + 31 \cdot 1 \cdot 4 - 8 \cdot 5 \cdot 8)z^5 + \cdots)$$

$$= \frac{30}{31}z + \frac{60}{31}z^2 + \frac{120}{31}z^4 + \frac{300}{31}z^5 + \cdots \in S_4(\Gamma_0(31),1) \qquad (4.14)$$

fonksiyonu $(-4, \Gamma_0(31), \chi)$ tipinde bir cusp form olup mertebesi 1 dir.

4.7 Teorem. G_2 kuadratik form için

(1) $\varphi_{11} = x_1^2 - \frac{4}{31}G_2$ ve $\varphi_{22} = x_2^2 - \frac{2}{31}G_2$, G_2 ye karşılık gelen ikinci mertebeden küresel fonksiyonlardır.

(2) $\wp(\tau; G_2, \varphi_{11}) = \frac{30}{31}z^2 - \frac{4}{31}z^4 - \frac{18}{31}z^5 + \cdots \in S_4(\Gamma_0(31), 1)$ dir.

(3) $\wp(\tau; G_2, \varphi_{22}) = -\frac{16}{31}z^2 - \frac{2}{31}z^4 + \frac{22}{31}z^5 + \cdots \in S_4(\Gamma_0(31), 1)$ dir.

(4) $ord(\wp(\tau; G_2, \varphi_{11})) = ord(\wp(\tau; G_2, \varphi_{22})) = 2$ dir.

İspat. $G_1 = 2x_1^2 + x_1x_2 + 4x_2^2$ formu için $b_{11} = 2$, $b_{12} = b_{21} = 1/2$ ve $b_{22} = 4$ olup $a_{11} = 4$, $a_{12} = a_{21} = 1/2$ ve $a_{22} = 8$ dir. Dolayısıyla $A_{11} = 8$ ve $A_{22} = 4$ dür. Üstelik $D = 31$ olup $\delta = 1$ ve $N = \frac{D}{\delta} = 31$ olduğundan G_1, $(-1, \Gamma_0(31), \chi)$ tipinde bir kuadratik formdur. Eğer $k = 4$, $F = G_2$ ve $r = s = 1$ ve $r = s = 2$ olarak alınırsa $\varphi_{11} = x_1^2 - \frac{4}{31}G_2$ ve $\varphi_{22} = x_2^2 - \frac{2}{31}G_2$ nin G_2 ye karşılık gelen ikinci mertebeden küresel fonksiyonlar olduğu görülür. n pozitif tamsayısı için

$$G_1(x_1, x_2) = 2x_1^2 + x_1x_2 + 4x_2^2 = n$$

denkleminin $n=1$ ve 3 için çözümü yoktur, $n=2$ için $(\pm 1{,}0)$ iki çözümü vardır, $n=4$ için $(0,\pm 1)$ iki çözümü vardır ve $n=5$ için $(-1{,}1)$, $(1,-1)$ iki çözümü vardır. Dolayısıyla (4.8) den

$$\wp(\tau;G_1)=1+2z^2+2z^4+2z^5+\cdots \tag{4.15}$$

olur. Benzer şekilde $G_2(x_1,x_2,x_3,x_4)=n$ denkleminin ise $n=1$ ve $n=3$ için çözümü yoktur, $n=2$ için $(\pm 1,0,0,0)$, $(0{,}0,\ \pm 1,0)$ dört çözümü vardır, $n=4$ için $(-1,0,\pm 1,0)$, $(0,\pm 1,0,0)$, $(0,0,0,\pm 1)$, $(1{,}0,\ \pm 1,0)$ sekiz çözümü vardır ve $n=5$ için $(0,0,1,-1)$, $(1,-1,0,0)$ dört çözümü vardır. Böylece (4.8) den

$$\wp(\tau;G_2)=\wp^2(r;G_1)=1+4z^2+8z^4+4z^5+\cdots \tag{4.16}$$

elde edilir. Buna göre

$$\begin{aligned}\wp(\tau;G_2,\varphi_{11})&=\tfrac{1}{31}((31\cdot 1\cdot 2-4\cdot 2\cdot 4)z^2+(31\cdot 1\cdot 4-4\cdot 4\cdot 8)z^4+\\&\quad(31\cdot 1\cdot 2-4\cdot 5\cdot 4)z^5\ldots)\\&=\tfrac{30}{31}z^2-\tfrac{4}{31}z^4-\tfrac{18}{31}z^5+\cdots\ \in S_4(\Gamma_0(31),1)\end{aligned} \tag{4.17}$$

ve

$$\begin{aligned}\wp(\tau;G_2,\varphi_{22})&=\tfrac{1}{31}((31\cdot 0\cdot 4-2\cdot 2\cdot 4)z^2+(31\cdot 1\cdot 2-2\cdot 4\cdot 8)z^4+\\&\quad(31\cdot 1\cdot 2-2\cdot 5\cdot 4)z^5\ldots)\\&=-\tfrac{16}{31}z^2-\tfrac{2}{31}z^4+\tfrac{22}{31}z^5+\cdots\ \in S_4(\Gamma_0(31),1)\end{aligned} \tag{4.18}$$

G_2 formu için $(-4,\Gamma_0(31),\chi)$ tipinde cusp formlardır. (4.17) ve (4.18) den her iki fonksiyonun da mertebesinin 2 olduğu görülür.

4.8 Teorem. $F_1\oplus G_1$ kuadratik formu için

(1) $\varphi_{11}=x_1^2-\frac{8}{31}F_1\oplus G_1$ ve $\varphi_{22}=x_2^2-\frac{1}{31}F_1\oplus G_1$, bu forma karşılık gelen ikinci mertebeden küresel fonksiyonlardır.

(2) $\wp(\tau; F_1 \oplus G_1, \varphi_{11}) = \frac{46}{31}z - \frac{32}{31}z^2 + \frac{28}{31}z^3 + \frac{120}{31}z^4 - \frac{116}{31}z^5 + \cdots \in S_4(\Gamma_0(31),\ 1)$ dir.

(3) $\wp(\tau; F_1 \oplus G_1, \varphi_{22}) = -\frac{2}{31}z - \frac{4}{31}z^2 - \frac{12}{31}z^3 - \frac{16}{31}z^4 - \frac{30}{31}z^5 + \cdots \in S_4(\Gamma_0(31),\ 1)$ dir.

(4) $ord(\wp(\tau; F_1 \oplus G_1, \varphi_{11})) = ord(\wp(\tau; F_1 \oplus G_1, \varphi_{22})) = 1.$

İspat. F_1 formunun $(-1, \Gamma_0(31),\ \chi)$ tipinde kuadratik form olduğu bilinmektedir. Eğer $k = 4,\ F = F_1 \oplus G_1$ ve $r = s = 1$ ve $r = s = 2$ ise φ_{11} ve φ_{22} nin $F_1 \oplus G_1$ e karşılık gelen ikinci mertebeden küresel fonksiyonlar olduğu görülür. n pozitif tamsayısı için $F_1 \oplus G_1(x_1, x_2) = x_1^2 + x_1x_2 + 8x_2^2 + 2x_3^2 + x_3x_4 + 4x_4^2 = n$ denkleminin $n = 1$ için $(\pm 1, 0, 0, 0)$ iki çözümü, $n = 2$ için $(0, 0, \pm 1, 0)$ iki çözümü, $n = 3$ için $(-1, 0, \pm 1, 0),\ (1, 0, \pm 1, 0)$ dört çözümü, $n = 4$ için $(\pm 2, 0, 0, 0),\ (0, 0, 0, \pm 1)$ dört çözümü ve $n = 5$ için $(-1, 0, 0, \pm 1),\ (0, 0, -1, 1),\ (0, 0, 1, -1),\ (1, 0, 0, \pm 1)$ altı çözümü vardır. Dolayısıyla (4.8) den

$$\wp(\tau; F_1 \oplus G_1) = 1 + 2z + 2z^2 + 4z^3 + 4z^4 + 6z^5 + \cdots \tag{4.19}$$

olup

$$\wp(\tau; F_1 \oplus G_1, \varphi_{11}) = \frac{1}{31}((31 \cdot 1 \cdot 2 - 8 \cdot 1 \cdot 2)z + (31 \cdot 0 \cdot 2 - 8 \cdot 2 \cdot 2)z^2 + (31 \cdot 1 \cdot 48 \cdot 3 \cdot 4)z^3 + (31 \cdot 4 \cdot 2 - 8 \cdot 4 \cdot 4)z^4 + (31 \cdot 1 \cdot 4 - 8 \cdot 5 \cdot 6)z^5 + \cdots)$$

$$= \frac{46}{31}z - \frac{32}{31}z^2 + \frac{28}{31}z^3 + \frac{120}{31}z^4 - \frac{116}{31}z^5 + \cdots\ S_4(\Gamma_0(31), 1) \tag{4.20}$$

ve

$$\wp(\tau; F_1 \oplus G_1, \varphi_{22}) = \frac{1}{31}((31 \cdot 0 \cdot 2 - 1 \cdot 1 \cdot 2)z + (31 \cdot 0 \cdot 2 - 1 \cdot 2 \cdot 2)z^2 + (31 \cdot 0 \cdot 41 \cdot 3 \cdot 4)z^3 + (31 \cdot 0 \cdot 4 - 1 \cdot 4 \cdot 4)z^4 + (31 \cdot 0 \cdot 6 - 1 \cdot 5 \cdot 6)z^5 + \cdots)$$

$$= -\frac{2}{31}z - \frac{4}{31}z^2 - \frac{12}{31}z^3 - \frac{16}{31}z^4 - \frac{30}{31}z^5 + \cdots\ S_4(\Gamma_0(31), 1) \tag{4.21}$$

nin $(-4, \Gamma_0(31), \chi)$ tipinde cusp form oldukları görülür. Buna göre bu iki fonksiyonun mertebesi 1 dir.

4.9 Teorem. F_2, G_2, ve $F_1 \oplus G_1$ kuadratik formları için

$$\wp(\tau; F_2, \varphi_{11}) = \frac{1}{31}\sum_{n=1}^{\infty}\left(\sum_{F_2=n} 31x_1^2 - 8n\right)z^n$$

$$\wp(\tau; G_2, \varphi_{11}) = \frac{1}{31}\sum_{n=1}^{\infty}\left(\sum_{G_2=n} 31x_1^2 - 4n\right)z^n$$

$$\wp(\tau; G_2, \varphi_{22}) = \frac{1}{31}\sum_{n=1}^{\infty}\left(\sum_{G_2=n} 31x_2^2 - 2n\right)z^n \tag{4.22}$$

$$\wp(\tau; F_1 \oplus G_1, \varphi_{11}) = \frac{1}{31}\sum_{n=1}^{\infty}\left(\sum_{F_1\oplus G_1=n} 31x_1^2 - 8n\right)z^n$$

$$\wp(\tau; F_1 \oplus G_1, \varphi_{22}) = \frac{1}{31}\sum_{n=1}^{\infty}\left(\sum_{F_1\oplus G_1=n} 31x_2^2 - n\right)z^n$$

genelleştirilmiş teta serileri $(-4, \Gamma_0(31), 1)$ tipinde $S_4(\Gamma_0(31), 1)$ uzayı için bir bazdır.

İspat. (4.14), (4.17), (4.18), (4.20) ve (4.21) de sırasıyla

$$\wp(\tau; F_2, \varphi_{11}) = \tfrac{30}{31}z + \tfrac{60}{31}z^2 + \tfrac{120}{31}z^4 + \tfrac{300}{31}z^5 + \cdots$$

$$\wp(\tau; G_2, \varphi_{11}) = \tfrac{30}{31}z^2 - \tfrac{4}{31}z^4 - \tfrac{18}{31}z^5 + \cdots$$

$$\wp(\tau; G_2, \varphi_{22}) = -\tfrac{16}{31}z^2 - \tfrac{2}{31}z^4 + \tfrac{22}{31}z^5 + \cdots$$

$$\wp(\tau; F_1 \oplus G_1, \varphi_{11}) = \tfrac{46}{31}z - \tfrac{32}{31}z^2 + \tfrac{28}{31}z^3 + \tfrac{120}{31}z^4 - \tfrac{116}{31}z^5 + \cdots$$

$$\wp(\tau; F_1 \oplus G_1, \varphi_{22}) = -\tfrac{2}{31}z - \tfrac{4}{31}z^2 - \tfrac{12}{31}z^3 - \tfrac{16}{31}z^4 - \tfrac{30}{31}z^5 + \cdots$$

olduğu görüldü. Üstelik yukarıdaki bu eşitlikler birbirinden bağımsızdır. Diğer yandan $|S_4(\Gamma_0(31),1)| = 5$ olduğundan bu denklem sistemi $(-4,\Gamma_0(31),1)$ tipinde cusp formların $S_4(\Gamma_0(31),1)$ uzayı için bir baz teşkil eder.

Bu bazın elemanları kullanılarak tamsayıların F_4, G_4, $F_1 \oplus G_3$, $F_2 \oplus G_2$ ve $F_3 \oplus G_1$ kuadratik formları ile gösterilmesi ile ilgili formüller verilebilir.

4.10 Teorem. $\sigma_3(n)$, 4.1 Lemmasındaki gibi olmak üzere

$$\sigma_3^* = \begin{cases} \sigma_3(n) & 31 \ n \ yi \ bölmez \ ise \\ \sigma_3(n) + 31^2 \sigma_3\left(\dfrac{n}{31}\right) & 31 \ n \ yi \ böler \ ise \end{cases}$$

olsun. Bu takdirde

$$r(n;F_4) = \frac{120}{481}\sigma_3^*(n) - \frac{1745176}{33910 \cdot 31}\left(\sum_{F_2=n} 31x_1^2 - 8n\right)$$

$$+\frac{2600640}{22607 \cdot 31}\left(\sum_{G_2=n} 31x_1^2 - 4n\right) + \frac{3477232}{22607 \cdot 31}\left(\sum_{G_2=n} 31x_2^2 - 2n\right)$$

$$+\frac{145168}{22607 \cdot 31}\left(\sum_{F_1 \oplus G_1=n} 31x_1^2 - 8n\right) - \frac{1122160}{22607 \cdot 31}\left(\sum_{F_1 \oplus G_1=n} 31x_2^2 - n\right)$$

$$r(n;G_4) = \frac{120}{481}\sigma_3^*(n) + \frac{1058092}{339105 \cdot 31}\left(\sum_{F_2=n} 31x_1^2 - 8n\right)$$

$$-\frac{1378192}{22607 \cdot 31}\left(\sum_{G_2=n} 31x_1^2 - 4n\right) - \frac{2581444}{22607 \cdot 31}\left(\sum_{G_2=n} 31x_2^2 - 2n\right)$$

$$-\frac{35688}{22607\cdot 31}\left(\sum_{F_1\oplus G_1=n}31x_1^2-8n\right)+\frac{324688}{22607\cdot 31}\left(\sum_{F_1\oplus G_1=n}31x_2^2-n\right)$$

$$r(n;F_1\oplus G_3)=\frac{120}{481}\sigma_3^*(n)-\frac{224254}{339105\cdot 31}\left(\sum_{F_2=n}31x_1^2-8n\right)$$

$$+\frac{548213}{22607\cdot 31}\left(\sum_{G_2=n}31x_1^2-4n\right)+\frac{812492}{22607\cdot 31}\left(\sum_{G_2=n}31x_2^2-2n\right)$$

$$+\frac{26361}{22607\cdot 31}\left(\sum_{F_1\oplus G_1=n}31x_1^2-8n\right)-\frac{231348}{22607\cdot 31}\left(\sum_{F_1\oplus G_1=n}31x_2^2-n\right)$$

$$r(n;F_2\oplus G_2)=\frac{120}{481}\sigma_3^*(n)-\frac{224254}{339105\cdot 31}\left(\sum_{F_2=n}31x_1^2-8n\right)$$

$$+\frac{570820}{22607\cdot 31}\left(\sum_{G_2=n}31x_1^2-4n\right)+\frac{767278}{22607\cdot 31}\left(\sum_{G_2=n}31x_2^2-2n\right)$$

$$+\frac{48968}{22607\cdot 31}\left(\sum_{F_1\oplus G_1=n}31x_1^2-8n\right)-\frac{412204}{22607\cdot 31}\left(\sum_{F_1\oplus G_1=n}31x_2^2-n\right)$$

$$r(n;F_3\oplus G_1)=\frac{120}{481}\sigma_3^*(n)-\frac{224254}{339105\cdot 31}\left(\sum_{F_2=n}31x_1^2-8n\right)$$

$$+\frac{1000353}{22607\cdot 31}\left(\sum_{G_2=n}31x_1^2-4n\right)+\frac{1309846}{22607\cdot 31}\left(\sum_{G_2=n}31x_2^2-2n\right)$$

$$+\frac{71575}{22607\cdot 31}\left(\sum_{F_1\oplus G_1=n}31x_1^2-8n\right)-\frac{593060}{22607\cdot 31}\left(\sum_{F_1\oplus G_1=n}31x_2^2-n\right)$$

dir.

İspat. F_4, G_4, $F_1 \oplus G_3$, $F_2 \oplus G_2$ ve $F_3 \oplus G_1$ kuadratik formlarının $(-4, \Gamma_0(31), 1)$ tipinde kuadratik formlar olduğu bilinmektedir. $k = 4$ için $\rho_4 = \frac{1}{240}$ olduğundan $\alpha = \frac{120}{481}$ ve $\beta = \frac{120 \cdot 31^2}{481}$ elde edilir. Dolayısıyla (4.9) dan

$$E(\tau; F_4) = E(\tau; G_4) = E(\tau; F_3 \oplus G_1) = E(\tau; F_2 \oplus G_2) = E(\tau; F_1 \oplus G_3)$$

$$= 1 + \sum_{n=1}^{\infty} (\alpha\sigma_3(n) z^n + \beta\sigma_3(n) z^{qn}) \tag{4.23}$$

$$= 1 + \frac{120}{481} \sum_{n=1}^{\infty} \sigma_3(n)(z^n + 31^2 z^{31n})$$

$$= 1 + \frac{120}{481} z + \frac{1080}{481} z^2 + \frac{3360}{481} z^3 + \frac{8760}{481} z^4 + \frac{15120}{481} z^5 + \ldots$$

olur. Lemma 4.3 gereği $\wp(\tau; F) - E(\tau; F)$ farkı, $(-4, \Gamma_0(31), 1)$ tipinde bir cusp formdur. Teorem 4.9 gereği

$$\wp(\tau; F_2, \varphi_{11}), \wp(\tau; G_2, \varphi_{11}), \wp(\tau; G_2, \varphi_{22}), \wp(\tau; F_1 \oplus G_1, \varphi_{11}) \text{ ve } \wp(\tau; F_1 \oplus G_1, \varphi_{22})$$

nin $S_4(\Gamma_0(31), 1)$ uzayı için bir baz olduğu biliniyor. O halde

$$\begin{aligned} \wp(\tau; F_4) - E(\tau; F_4) &= c_1\wp(\tau; F_2, \varphi_{11}) + c_2\wp(\tau; G_2, \varphi_{11}) + c_3\wp(\tau; G_2, \varphi_{22}) \\ &\quad + c_4\wp(\tau; F_1 \oplus G_1, \varphi_{11}) + c_5\wp(\tau; F_1 \oplus G_1, \varphi_{22}) \end{aligned} \tag{4.24}$$

olacak şekilde c_1, c_2, c_3, c_4, c_5 tamsayıları bulunabilir. (4.14), (4.17), (4.18), (4.20) ve (4.21) eşitlikleri kullanılırsa

$$\begin{aligned} \wp(\tau; F_4) - E(\tau; F_4) &= c_1\left(\frac{30}{31} z + \frac{60}{31} z^2 + \frac{120}{31} z^4 + \frac{300}{31} z^5\right) + c_2\left(\frac{30}{31} z^2 - \frac{4}{31} z^4 - \frac{18}{31} z^5\right) \\ &\quad + c_3\left(\frac{-16}{31} z^2 - \frac{2}{31} z^4 + \frac{22}{31} z^5\right) + c_4\left(\frac{46}{31} z - \frac{32}{31} z^2 + \frac{28}{31} z^3 + \frac{120}{31} z^4 - \frac{116}{31} z^5\right) \\ &\quad + c_5\left(\frac{-2}{31} z - \frac{4}{31} z^2 - \frac{12}{31} z^3 - \frac{16}{31} z^4 - \frac{30}{31} z^5\right) \end{aligned}$$

olur. Bu denklem sisteminin katsayılar matrisinin determinantı

$$\begin{vmatrix} 30/31 & 0 & 0 & 46/31 & -2/31 \\ 60/31 & 30/31 & -16/31 & -32/31 & -4/31 \\ 0 & 0 & 0 & 28/31 & -12/31 \\ 120/31 & -4/31 & -2/31 & 120/31 & -16/31 \\ 300/31 & -18/31 & 22/31 & -116/31 & -30/31 \end{vmatrix} = \frac{-45120}{29791} \neq 0$$

olduğundan bu denklem sistemi çözülebilirdir.

$$\wp(\tau; F_4) = 1 + 8z + 24z^2 + 32z^3 + 24z^4 + 48z^5 + \cdots \tag{4.25}$$

olduğu hatırlanırsa (4.23) ve (4.25) den

$$\wp(\tau; F_4) - E(\tau; F_4) = \frac{3728}{481} z + \frac{10464}{481} z^2 + \frac{12032}{481} z^3 + \frac{2784}{481} z^4 + \frac{7968}{481} z^5 + \ldots$$

elde edilir. Buna göre

$$\frac{30}{31}c_1 + \frac{46}{31}c_4 - \frac{2}{31}c_5 = \frac{3728}{481}$$

$$\frac{60}{31}c_1 + \frac{30}{31}c_2 - \frac{16}{31}c_3 - \frac{32}{31}c_4 - \frac{4}{31}c_5 = \frac{10464}{481}$$

$$\frac{28}{31}c_4 - \frac{12}{31}c_5 = \frac{12032}{481}$$

$$\frac{120}{31}c_1 - \frac{4}{31}c_2 - \frac{2}{31}c_3 + \frac{120}{31}c_4 - \frac{16}{31}c_5 = \frac{2784}{481}$$

$$\frac{300}{31}c_1 - \frac{18}{31}c_2 + \frac{22}{31}c_3 - \frac{116}{31}c_4 - \frac{30}{31}c_5 = \frac{7968}{481}$$

denklem sistemi elde edilmiş olur. Bu denklem sistemin bir çözümü

$$c_1 = -\frac{1745176}{339105},\ c_2 = \frac{2600640}{22607},\ c_3 = \frac{3477232}{22607},\ c_4 = \frac{145168}{22607},\ c_5 = -\frac{1122160}{22607}$$

olup (4.2) den

$$\wp(\tau;F_4)-E(\tau;F_4)=-\frac{1745176}{339105}\wp(\tau;F_2,\varphi_{11})+\frac{2600640}{22607}\wp(\tau;G_2,\varphi_{11})+\frac{3477232}{22607}$$
$$\wp(\tau;G_2,\varphi_{22})+\frac{145168}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{11})-\frac{1122160}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{22})$$

olur. Benzer şekilde

$$\wp(\tau;G_4)-E(\tau;G_4)=\frac{1058092}{339105}\wp(\tau;F_2,\varphi_{11})-\frac{1378192}{22607}\wp(\tau;G_2,\varphi_{11})-\frac{2581444}{22607}$$
$$\wp(\tau;G_2,\varphi_{22})-\frac{35688}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{11})+\frac{324688}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{22})$$

$$\wp(\tau;F_1\oplus G_3)-E(\tau;F_1\oplus G_3)=-\frac{224254}{339105}\wp(\tau;F_2,\varphi_{11})+\frac{548213}{22607}\wp(\tau;G_2,\varphi_{11})+\frac{812492}{22607}$$
$$\wp(\tau;G_2,\varphi_{22})+\frac{26361}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{11})-\frac{231348}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{22})$$

$$\wp(\tau;F_2\oplus G_2)-E(\tau;F_2\oplus G_2)=-\frac{224254}{339105}\wp(\tau;F_2,\varphi_{11})+\frac{570820}{22607}\wp(\tau;G_2,\varphi_{11})+\frac{767278}{22607}$$
$$\wp(\tau;G_2,\varphi_{22})+\frac{48968}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{11})-\frac{412204}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{22})$$

$$\wp(\tau;F_3\oplus G_1)-E(\tau;F_3\oplus G_1)=-\frac{224254}{339105}\wp(\tau;F_2,\varphi_{11})+\frac{1000353}{22607}\wp(\tau;G_2,\varphi_{11})+\frac{1309846}{22607}$$
$$\wp(\tau;G_2,\varphi_{22})+\frac{71575}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{11})-\frac{593060}{22607}\wp(\tau;F_1\oplus G_1,\varphi_{22})$$

olduğu da gösterilebilir.

5.BÖLÜM

KUADRATİK İRRASYONELLER, KUADRATİK İDEALLER VE KUADRATİK FORMLAR

Bu bölümde kuadratik irrasyonellerin, kuadratik ideallerin ve indefinite kuadratik formların bazı özellikleri ele alınacaktır. $D \neq 1$ pozitif, tam kare olmayan bir tamsayı iken $\delta = \sqrt{D}$ veya $\delta = \frac{1+\sqrt{D}}{2}$ bir kuadratik irrasyonel olsun. Bu irrasyonelin izi ve normu sırasıyla $t = \delta + \bar{\delta}$ ve $n = \delta\bar{\delta}$ dır. P ve Q, $P^2 \equiv D(\text{mod } Q)$ özelliğinde iki tamsayı olmak üzere

$$\alpha = \frac{P+\delta}{Q} \tag{5.1}$$

bir kuadratik irrasyonel olup

$$I_\alpha = [Q, P+\delta] \tag{5.2}$$

bir kuadratik ideal ve

$$\begin{aligned} F_\alpha(x,y) &= Q(x-\alpha y)(x-\overline{\alpha}y) \\ &= Qx^2 - Qxy(\alpha+\overline{\alpha}) + Q(\alpha\overline{\alpha})y^2 \\ &= Qx^2 - Q\left(\frac{P+\delta}{Q} + \frac{P+\overline{\delta}}{Q}\right)xy + Q\left(\frac{(P+\delta)(P+\overline{\delta})}{Q^2}\right)y^2 \\ &= Qx^2 - (t+2P)xy + \left(\frac{n+tP+P^2}{Q}\right)y^2 \end{aligned} \tag{5.3}$$

ise $\Delta = t^2 - 4n$ diskriminantlı bir indefinite formdur.

I_α nin eşleniği $\overline{I}_\alpha = [Q, P+\overline{\delta}]$ ve dolayısıyla F_α nın eşleniği de

$$\overline{F}_\alpha(x,y) = Qx^2 + (t+2P)xy + \left(\frac{n+tP+P^2}{Q}\right)y^2 \qquad (5.4)$$

dir. Eğer $\delta = \sqrt{D}$ olarak alınırsa $t = 0$ ve $n = -D$ olup ve $\Delta = 4D$ dir. Eğer $\delta = \frac{1+\sqrt{D}}{2}$ ise $t = 1$ ve $n = \frac{1-D}{4}$ olup $\Delta = D$ dir. α, I_α ve F_α arasındaki ilişki aşağıdaki diagramdaki gibidir. (Mollin 1999)

$$\alpha = \frac{P+\delta}{Q} \quad \rightarrow \quad I_\alpha = [Q,\ P+\delta]$$

$$\downarrow$$

$$F_\alpha(x,y) = Q(x-\alpha y)(x-\overline{\alpha}y)$$

5.1 $\boldsymbol{\delta = \sqrt{D}}$ hali

Bu alt bölümde $\delta = \sqrt{D}$ olması halinde yukarıda tanımladığımız α, I_α ve F_α nın bazı özellikleri verilecektir. $\delta = \sqrt{D}$ için $Q=1$ olarak alalım. $p \equiv 1, 5 (\mathrm{mod}\ 6)$ asal sayısı için $P = \frac{-p}{2}$ olsun. Bu takdirde

$$\alpha_1 = -\frac{p}{2} + \sqrt{D} \qquad (5.5)$$

bir kuadratik irrasyonel ve böylece

$$I_{\alpha_1} = [1,\ \frac{-p}{2} + \sqrt{D}] \qquad (5.6)$$

bir kuadratik ideal ve

$$F_{\alpha_1}(x,y) = x^2 + pxy + \left(\frac{p^2-4D}{4}\right)y^2 \qquad (5.7)$$

ise $4D$ diskriminantlı bir indefinite formdur.

5.1.1 Teorem. Her $p \equiv 1,5(\text{mod } 6)$ asalı için α_1 kendisinin $\bar{\alpha}_1$ eşleniğine denktir.

İspat. α ve β reel sayıları için $g\alpha = \beta$ olacak şekilde en az bir $g = [r;s;t;u] \in \overline{\Gamma}$ varsa α ve β elemanlarına denk denildiği bilinmektedir. α_1 in eşleniği $\bar{\alpha}_1 = \frac{-p}{2} - \sqrt{D}$ olup $g = [-1;-p;\ 0;1] \in \overline{\Gamma}$ elemanı için

$$g\bar{\alpha}_1 = \frac{-1\left(\frac{-p}{2} - \sqrt{D}\right) + (-p)}{0\left(-\frac{-p}{2} - \sqrt{D}\right) + 1} = \frac{\frac{-p}{2} + \sqrt{D}}{1} = \alpha_1$$

dir. Dolayısıyla α_1 eşleniğine denktir.

5.1.2 Teorem. Her $p \equiv 1,5(\text{mod } 6)$ asalı için I_{α_1} ideali ambiguousdur.

İspat. I_{α_1} ideali için $\frac{t+2P}{Q} = -p \in \mathbb{Z}$ olduğundan tanım gereği I_{α_1}ambiguousdur.

5.1.3 Sonuç. Her $p \equiv 1,5(\text{mod } 6)$ asalı için F_{α_1} indefinite formu $\bar{F}_{\alpha_1}$ eşleniğine denktir ve ambiguousdur.

İspat. 5.1.1 Teoreminde her $p \equiv 1,5(\text{mod } 6)$ asalı α_1 in $\bar{\alpha}_1$ eşleniğine denk olduğu görüldü. Dolayısıyla da F_{α_1} indefinite formu da kendisinin $\bar{F}_{\alpha_1}$ eşleniğine denktir. Diğer yandan yukarıdaki teorem gereği I_{α_1} ideali ambiguous olduğundan F_{α_1} indefinite formu her $p \equiv 1,5(\text{mod } 6)$ asalı için ambiguousdur.

5.1.4 Teorem. F_{α_1} indefinite formu için

1) $p \equiv 1(\text{mod } 6)$ ise $k \geq 1$ pozitif tamsayısı için $p = 1 + 6k$ olsun. Bu takdirde

$$F_{\alpha_1} \text{ indirgenebilirdir } \Leftrightarrow D \in [9k^2 + 3k + 1, 9k^2 + 9k + 2] - \{9k^2 + 6k + 1\}$$

dir.

2) $p \equiv 5(\text{mod } 6)$ ise $k \geq 1$ pozitif tamsayısı için $p = 5 + 6k$ olsun. Bu takdirde

$$F_{\alpha_1} \text{ indirgenebilirdir} \Leftrightarrow D \in [9k^2 + 15k + 7, 9k^2 + 21k + 12] - \{9k^2 + 18k + 9\}$$

dir.

Her iki durumda da bu indirgenmiş formların sayısı p dir.

İspat. 1) $p \equiv 1(\text{mod } 6), p = 1 + 6k$ için F_{α_1} indirgenebilir olsun. Bu takdirde tanımdan dolayı

$$\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta} \Leftrightarrow \left|\sqrt{4D} - 2|1|\right| < p < \sqrt{4D}$$
$$\Leftrightarrow 2\sqrt{D} - 2 < p < 2\sqrt{D} \qquad (5.8)$$

dır. Buradan

$$D > \frac{p^2}{4} = \frac{1}{4} + 3k + 9k^2 \Leftrightarrow D \geq 1 + 3k + 9k^2$$

ve

$$D < \frac{(p+2)^2}{4} = \frac{9}{4} + 9k + 9k^2 \Leftrightarrow D \leq 2 + 9k + 9k^2$$

elde edilir. Bu son iki eşitsizlikten $9k^2 + 3k + 1 \leq D \leq 9k^2 + 9k + 2$ bulunur. Ancak $D = 9k^2 + 6k + 1 = (3k + 1)^2$ tam kare olduğu için bu değer alınmamaktadır. O halde $D \in [9k^2 + 3k + 1, 9k^2 + 9k + 2] - \{9k^2 + 6k + 1\}$ dir.

Tersine $D \in [9k^2 + 3k + 1, 9k^2 + 9k + 2] - \{9k^2 + 6k + 1\}$ ise F_{α_1} indirgenebilir olduğu açıktır. Yukarıdaki son eşitsizlikten bu indirgenmiş formların sayısı $9k^2 + 9k + 2 - (9k^2 + 3k + 1) = 6k + 1 = p$ olarak elde edilir.

2) $p \equiv 5(\text{mod } 6), p = 5 + 6k$ için F_{α_1} indirgenebilir olsun. Bu takdirde (5.8) den

$$D > \frac{25}{4} + 15k + 9k^2 \Leftrightarrow D \geq 7 + 15k + 9k^2$$

ve

$$D < \frac{49}{4} + 21k + 9k^2 \Leftrightarrow D \leq 12 + 21k + 9k^2$$

olup $9k^2 + 15k + 7 \leq D \leq 9k^2 + 21k + 12$ elde edilir. Fakat $D = 9k^2 + 18k + 9 = (3k+3)^2$ tam kare olduğu için bu değer de ihmal edilmelidir. Sonuçta $D \in [9k^2 + 15k + 7, 9k^2 + 21k + 12] - \{9k^2 + 18k + 9\}$ dir.

Tersine $D \in [9k^2 + 15k + 7, 9k^2 + 21k + 12] - \{9k^2 + 18k + 9\}$ için F_{α_1} in indirgenebilir olduğu görülür. İndirgenebilir bu formların sayısı ise $9k^2 + 21k + 12 - (9k^2 + 15k + 7) = 6k + 5 = p$ dir.

5.1.5 Örnek 1. $p = 13 \equiv 1 \pmod 6$ olsun. Bu takdirde $k = 2$ olup $g = [-1; -13; 0; 1] \in \overline{\Gamma}$ elemanı için $\alpha_1 = \frac{-13}{2} + \sqrt{D}$ eşleniğine denktir. Ayrıca $I_{\alpha_1} = \left[1, \frac{-13}{2} + \sqrt{D}\right]$ ideali ambiguousdur ve $D \in [43, 56] - \{49\}$ için $F_{\alpha_1}(x, y) = x^2 + 13xy + \left(\frac{169-4D}{4}\right)y^2$ indefinite formu indirgenebilirdir. İndirgenebilir bu formların sayısı 13 dür.

2. $p = 23 \equiv 5 \pmod 6$ için $k = 3$ olup $g = [-1; -23; 0; 1] \in \overline{\Gamma}$ için $\alpha_1 = \frac{-23}{2} + \sqrt{D}$ eşleniğine denktir. $I_{\alpha_1} = \left[1, \frac{-23}{2} + \sqrt{D}\right]$ ambiguousdur ve $D \in [133, 156] - \{144\}$ için $F_{\alpha_1}(x, y) = x^2 + 23xy + \left(\frac{529-4D}{4}\right)y^2$ formu indirgenebilirdir. İndirgenebilir bu formların sayısı ise 23 dür.

5.2 $\delta = \frac{1+\sqrt{D}}{2}$ hali

Bu alt bölümde $\delta = \frac{1+\sqrt{D}}{2}$ için α, I_α ve F_α nın bazı özellikleri verilecektir. δ nın bu değeri için $t = 1$ ve $n = \frac{1-D}{4}$ olur. $p \equiv 1, 5 \pmod 6$ asal sayısı için $P = \frac{-(p+1)}{2}$ olsun. Q=1 özel hali için

$$\alpha_2 = \frac{-p+\sqrt{D}}{2} \tag{5.9}$$

bir kuadratik irrasyonel olup

$$I_{\alpha_2} = [1,\ \frac{-p+\sqrt{D}}{2}] \tag{5.10}$$

bir kuadratik ideal ve

$$F_{\alpha_2}(x,y) = x^2 + pxy + \left(\frac{p^2-D}{4}\right)y^2 \tag{5.11}$$

ise determinantı D olan bir indefinite kuadratik formdur.

5.2.1 Teorem. Her $p \equiv 1, 5 (\mathrm{mod}\ 6)$ asalı için α_2 kendisinin $\bar{\alpha}_2$ eşleniğine denktir.

İspat. α_2 nin eşleniği $\bar{\alpha}_2 = \frac{-p-\sqrt{D}}{2}$ olup $g = [-1; -p; 0; 1] \in \overline{\Gamma}$ için

$$g\bar{\alpha}_2 = \frac{-1\left(\frac{-p-\sqrt{D}}{2}\right) + (-p)}{0\left(\frac{-p-\sqrt{D}}{2}\right) + 1} = \frac{\frac{-p+\sqrt{D}}{2}}{1} = \alpha_2$$

olduğundan α_2 eşleniğine denktir.

5.2.2 Teorem. Her $p \equiv 1, 5 (\mathrm{mod}\ 6)$ asalı için I_{α_2} ideali ambiguousdur.

İspat. I_{α_2} ideali için $\frac{t+2P}{Q} = -p \in \mathbb{Z}$ olduğundan ambiguousdur.

5.2.3 Sonuç. Her $p \equiv 1, 5 (\mathrm{mod}\ 6)$ asalı için F_{α_2} indefinite formu kendisinin $\bar{F}_{\alpha_2}$ eşleniğine denktir ve ambiguousdur.

5.2.4 Teorem. D diskriminantlı F_{α_2} formu için

1) $p \equiv 1(\text{mod } 6)$ ise $k \geq 1$ pozitif tamsayısı için $p = 1 + 6k$ olsun. Bu takdirde F_{α_2}indirgenebilirdir$\Leftrightarrow D \in [36k^2 + 12k + 2, 36k^2 + 36k + 8] - \{36k^2 + 24k + 4\}$ dir.

2) $p \equiv 5(\text{mod } 6)$ ise $k \geq 1$ pozitif tamsayısı için $p = 5 + 6k$ olsun. Bu takdirde F_{α_2} indirgenebilirdir$\Leftrightarrow D \in [36k^2 + 60k + 26, 36k^2 + 84k + 48] - \{36k^2 + 72k + 36\}$ dir.

Her iki durumda da bu indirgenmiş formların sayısı $4p + 2$ dir.

İspat. 1) $p \equiv 1(\text{mod } 6)$, $p = 1 + 6k$ için F_{α_2} indirgenebilir olsun. Bu takdirde

$$\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta} \Leftrightarrow \left|\sqrt{D} - 2|1|\right| < p < \sqrt{D}$$

$$\Leftrightarrow \sqrt{D} - 2 < p < \sqrt{D} \tag{5.12}$$

dir. Buradan

$$D > p^2 = 1 + 12k + 36k^2 \Leftrightarrow D \geq 2 + 12k + 36k^2$$

ve

$$D < (p + 2)^2 = 9 + 36k + 36k^2 \Leftrightarrow D \leq 8 + 36k + 36k^2$$

olup $36k^2 + 12k + 2 \leq D \leq 36k^2 + 36k + 8$ elde edilir. Fakat $D = 36k^2 + 24k + 4 = (6k + 2)^2$ tam kare olduğundan bu değer ihmal edilmelidir. O halde $D \in [36k^2 + 12k + 2, 36k^2 + 36k + 8] - \{36k^2 + 24k + 4\}$ olur.

Tersine $D \in [36k^2 + 12k + 2, 36k^2 + 36k + 8] - \{36k^2 + 24k + 4\}$ olsun. Bu takdirde F_{α_2} indefinite formu indirgenebilirdir. Üstelik bu formların sayısı $36k^2 + 36k + 8 - (36k^2 + 12k + 2) = 24k + 6 = 4(6k + 1) + 2 = 4p + 2$ dir.

2) $p \equiv 5(\text{mod } 6)$, $p = 5 + 6k$ için F_{α_2} indefinite formu indirgenebilir olsun. Bu takdirde (5.12) den

$$D > 25 + 60k + 36k^2 \Leftrightarrow D \geq 26 + 60k + 36k^2$$

ve

$$D < 49 + 84k + 36k^2 \Leftrightarrow D \leq 48 + 84k + 36k^2$$

olup bu iki eşitsizlikten $36k^2 + 60k + 26 \leq D \leq 36 \quad k^2 + 84k + 48$ elde edilir. Fakat $D = 36k^2 + 72k + 36 = (6k + 6)^2$ tam kare olduğundan bu ihmal edilirse $D \in [36k^2 + 60k + 26, 36k^2 + 84k + 48] - \{36k^2 + 72k + 36\}$ dır.

Tersine D nin bu değerleri için F_{α_2} indirgenebilirdir ve üstelik indirgenebilir bu formların sayısı $4p + 2$ dir.

KAYNAKLAR

ATKIN, A. O. L. ve F. MORALIN. 2003. Elliptic Curves and Primality Proving. Math. Comp. 61(203)(1993), 29-68.

BUCHMANN, J. ve U. VOLLMER. 2007. Binary Quadratic Forms: An Algorithmic Approach. Springer-Verlag, Berlin, Heidelberg.

BUELL, D. A. 1989. Binary Quadratic Forms, Clasical Theory and Modern Computations. Springer-Verlag, New York.

FLATH, D. E. 1989. Introduction to Number Theory. Wiley.

HECKE, E. 1970. Mathematische Werke. Zweite Auflage, Vandenhoeck u. Ruprecht, Göttingen.

LANG, S. 1976. Introduction to Modular Forms. Springer-Verlag.

MOLLIN, R. A. 1996. Quadratics. CRS Press, Boca Raton, New York, London, Tokyo.

MOLLIN, R. A and CHENG K. 1999. Palindromy and Ambiguous Ideals Revisited. Journal of Number Theory 74(1999), 98-110.

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

SILVERMAN, J.H. ve J. TATE. 1992. Rational Points on Elliptic Curves. Springer.

TEKCAN, A. ve O. BİZİM. 2003. The Connection between Quadratic Forms and the Extended Modular Group. Mathematica Bohemica 128(3)(2003), 225-236.

TEKCAN, A. ve A. ÖZKOÇ. 2009. Quadratic Irrationals, Quadratic Ideals and Indefinite Quadratic Forms II. Int. Jour. of Comp. and Math. Sci. 3(2)(2009), 56-59.

TEKCAN, A. ve A. ÖZKOÇ. 2009. Positive Definite Binary Quadratic Forms, Quadratic Congruences and Singular Curves. Comptes ren.math.Math.Rep. 31(2) (2009), 53-64.

TEKCAN, A., A. ÖZKOÇ, B. GEZER ve O.BİZİM. Representations of Positive Integers by Positive Quadratic Forms. South East Asian Bulletin of Mathematics dergisinde yayına kabul edildi.

TEKCAN, A., A. ÖZKOÇ, B. GEZER ve O.BİZİM. Elliptic Curves, Conics and Cubic Congruencies associated with Indefinite Binary Quadratic Forms. Novi Sad Journal of Mathematics dergisinde yayına kabul edildi.

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

ÖZGEÇMİŞ

1984 yılında Antalya' da doğan Arzu ÖZKOÇ; ilk, orta ve lise öğrenimini Antalya' da tamamladıktan sonra 2003 yılında Uludağ Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümünde lisans öğrenimine başlamıştır. 2007 yılında bu bölümden MATEMATİKÇİ olarak mezun olmuştur. Eylül 2007 de Uludağ Üniversitesi Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı, Analiz ve Fonksiyonlar Teorisi bilim dalında yüksek lisans öğrenimine başlamıştır.

TEŞEKKÜR

Yüksek lisans çalışmam esnasında bana yol gösteren, bilgi ve deneyimleri ile katkıda bulunan saygıdeğer danışman hocam Doç.Dr. Osman BİZİM'e, ayrıca bu çalışmanın planlanması, yürütülmesi ve sonuçlandırılması aşamalarında bilgi, tecrübe ve hoşgörüsüyle öncülük eden değerli hocam Doç.Dr. Ahmet TEKCAN'a, maddi ve manevi desteklerini hiç bir zaman esirgemeyen babam Mehmet Emin ÖZKOÇ'a, annem Şerife ÖZKOÇ'a ve abim Cihan ÖZKOÇ'a sonsuz teşekkür ederim.

Yüksek lisans hayatım boyunca 2228 kodlu Son Sınıf Lisans Öğrencileri için Yurt İçi Lisansüstü Burs Programı ile beni destekleyen Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na teşekkür ederim.