

**YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**KUADRATİK SAYI CİSİMLERİNDE ÇARPANLARA
AYIRMA, İDEAL SINIF GRUBU ve L-FONKSİYONLARI**

Matematikçi Bülent KÖKLÜCE

**FBE Matematik Anabilim Dalı Matematik Programında
Hazırlanan**

DOKTORA TEZİ

Tez Savunma Tarihi: 8 Aralık 2005

Tez Danışmanı : Doç. Dr. Ömer GÖK (YTÜ)

Jüri Üyeleri : Prof. Dr. Göksel AĞARGÜN (YTÜ)

: Doç. Dr. Mustafa BAYRAM (YTÜ)

: Prof. Dr. Mehmet BAYRAMOĞLU (YTÜ)

: Prof. Dr. Elimhan MAHMUDOV (İÜ)

İSTANBUL, 2005

İÇİNDEKİLER

	Sayfa
SİMGE LİSTESİ	iv
KISALTMA LİSTESİ	vi
ÇİZELGE LİSTESİ	vii
ÖNSÖZ	viii
ÖZET	ix
ABSTRACT	x
1. GİRİŞ	1
2. CEBİRSEL SAYI CİSİMLERİ ve KUADRATİK SAYI CİSİMLERİ	6
2.1 Cebirsel Sayı Cisimleri	6
2.2 Kuadratik Sayı Cisimlerine Giriş	10
2.3 Kuadratik Sayı Cisimlerinin Tamlık Halkası ve Diskriminantı	13
2.4 Kuadratik Sayı Cisimlerinde Birimseller Grubu	17
2.5 Bölümle İlgili Pari Komut ve Programları	31
3. KUADRATİK SAYI CİSİMLERİNDE ÇARPANLARA AYIRMA ve İDEALLER	35
3.1 Tek Türlü Çarpanlara Ayrılabilme Özelliği Üzerine	35
3.2 Euclid Bölgeleri	42
3.3 Kuadratik sayı Cisimlerinin İdealleri	45
3.4 İdeal Sınıf Grubu	53
3.5 Asalların Parçalanışı	58
3.5.1 Bölümle İlgili Pari Komut ve Programları	75
3.5.2 Bölümle İlgili Maple Komut ve Programları	77
4. İKİLİ KUADRATİK FORMLAR ve KUADRATİK SAYI CİSİMLERİYLE BAĞLANTISI	81
4.1 İkili Kuadratik Formlar	81
4.2 İkili Kuadratik Formlar ve Kuadratik Sayı Cisimlerinin İdealleri Arasındaki Bağlantı	87
4.3 Bölümle İlgili Pari Komut ve Programları	93
5. ZETA ve L-FONKSİYONLARI	98
5.1 Dirichlet Karakterleri	98
5.2 Zeta ve L-Fonksiyonları	104
5.3 Kuadratik Sayı Cisimlerinin Zeta ve L-Fonksiyonları	108
5.4 Bölümle İlgili Pari Komut ve Programları	123

6.	SONUÇLAR.....	127
	KAYNAKLAR.....	128
	ÖZGEÇMİŞ.....	130

SİMGE LİSTESİ

$a b$	a böler b
$a \equiv b \pmod{n}$	a denktir $b \pmod{n}$
$\left(\frac{a}{p}\right)$	Legendre sembolü
$\left(\frac{a}{n}\right)$	Kronecker sembolü
$\mathfrak{a} = (\alpha, \beta)$	O_K 'nın α ve β tarafından üretilen ideali
$\mathfrak{a}'$	$\mathfrak{a}$ 'nın eşleniği
$\mathfrak{a} b$	$\mathfrak{a}$ ideali b 'yı böler veya $b \subseteq \mathfrak{a}$
$\mathfrak{a}^{-1}$	$\mathfrak{a}$ kesirsel idealinin tersi
$\mathfrak{a} \sim b$	$\mathfrak{a}$ ve b idealleri denk idealler
$[\mathfrak{a}]$	$\mathfrak{a}$ 'nın denklik sınıfı
B_n	n . Bernoulli sayısı
$\mathbb{C}$	Kompleks sayılar
$\mathcal{C}$	K 'nın ideal sınıf grubu
$\text{çek } f$	f 'nin çekirdeği
$\text{der}_{P_F}(\alpha, x)$	α 'nın F üzerindeki derecesi
$\text{ebob}(\mathfrak{a}, \mathfrak{b})$	$\mathfrak{a}, \mathfrak{b}$ ideallerinin en büyük ortak böleni
$\text{ekok}(\mathfrak{a}, \mathfrak{b})$	$\mathfrak{a}, \mathfrak{b}$ ideallerinin en küçük ortak katı
d_K	K 'nın diskriminantı
d_Q	Q ikili kuadratik formunun diskriminantı
$\mathbf{F}_K$	K 'nın sıfırdan farklı kesirsel ideallerinin kümesi
h_K	K 'nın sınıf sayısı
$[K : \mathbb{Q}]$	K sayı cisminin $\mathbb{Q}$ rasyonel sayı cismi üzerindeki boyutu
$K = \mathbb{Q}(\sqrt{d})$	d kare-bağımsız tamsayı olmak üzere, $\sqrt{d}$ 'yi içeren kuadratik sayı cismi
$L(s, \chi)$	χ Dirichlet karakteri ile s 'de Dirichlet L-fonksiyonu
$L(1, \chi)$	χ Dirichlet karakteri ile 1 'de Dirichlet L-fonksiyonu
M_K	Minkowski sınırı
$\mathbb{N}$	Doğal sayılar kümesi
$N(\alpha)$	α 'nın normu
$N(\mathfrak{a})$	$\mathfrak{a}$ idealinin normu
O_K	$K = \mathbb{Q}(\sqrt{d})$ 'nin tamlık halkası
$P_F(\alpha, x)$	$\alpha \in E$ cebirsel sayısının $p(x) \in F[X]$ minimal polinomu
$\mathfrak{p}, \mathfrak{q}$	O_K 'nın asal idealleri
$\mathfrak{P}$	O_K 'nın temel kesirsel ideallerinin kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
$Q(x, y)$	x, y değişkenli ikili kuadratik form
$Q \sim Q'$	Denk kuadratik formlar
R	Regülatör
$\mathbb{R}$	Reel sayılar kümesi

$\mathbf{R}[x]$	$\mathbf{R}$ halkası üzerinde polinom halkası
r_1	$K \rightarrow \mathbf{C}$ reel otomorfizmaların sayısı
r_2	$K \rightarrow \mathbf{C}$ sanal otomorfizmaların yarı sayısı
$SL_2(\mathbf{R})$	2×2 'lik determinantı 0 'dan farklı olan reel sayı bileşenli matrislerin kümesi
$SL_2(\mathbf{Z})$	2×2 'lik determinantı 1 olan tamsayı bileşenli matrislerin oluşturduğu grup
$Tr(\alpha)$	α 'nın izi
u	O_K 'nın birimsel elemanı
U_K	O_K 'nın birimsel elemanlarının grubu
$\mathbf{Z}[x]$	$\mathbf{Z}$ halkası üzerinde polinom halkası
$\mathbf{Z}$	Tamsayılar kümesi
$\{1, \omega_d\}$	O_K 'nın tamlık tabanı
(α)	α tarafından üretilen temel ideal
α'	α 'nın eşleniği
$\chi(n)$	Dirichlet karakteri
ε_K	$K = \mathbf{Q}(\sqrt{d})$ 'nin temel birimi
$\sigma_i(\alpha)$	K 'dan $\mathbf{C}$ 'ye $\sigma_i : K \rightarrow \mathbf{C}$ otomorfizması
ω_d	Kuadratik sayı cismi $K = \mathbf{Q}(\sqrt{d})$ 'de $d \equiv 2,3(\bmod 4)$ ise $\omega_d = \sqrt{d}$; $d \equiv 1(\bmod 4)$ ise $\omega_d = \frac{1+\sqrt{d}}{2}$ biçiminde tanımlanan kompleks sayı
w	K sanal kuadratik sayı cismindeki birimsellerin sayısı
ζ_n	1 'in n . dereceden kökü
$\zeta(s)$	Riemann zeta fonksiyonu
$\zeta_K(s)$	K sayı cismi üzerindeki zeta fonksiyonu
$\Delta(\alpha_1, \dots, \alpha_n)$	$\alpha_1, \dots, \alpha_n \in K$ 'nın diskriminantı

KISALTMA LİSTESİ

ALP	Ayrık Logaritma Problemi
DB	Dedekind Bölgesi
EB	Euclid Bölgesi
FST	Fermat'ın Son Teoremi
İKİF	İkili Kuadratik Form
İTS	İndirgenmiş Tam Temsilciler Sistemi
TB	Tamlık Bölgesi
TÇAB	Tek Türlü Çarpanlara Ayrılabilen Bölge
TİB	Temel(Esas) İdeal Bölgesi

ÇİZELGE LİSTESİ

Sayfa

Çizelge 2.1	$K = \mathbb{Q}(\sqrt{34})$ 'de temel birimin hesaplanması.....	24
Çizelge 2.2	Sürekli kesirler kullanılarak temel birimin bulunması.....	25
Çizelge 2.3	Bazı reel kuadratik sayı cisimlerinin temel birimleri $d = 1, 2, \dots, 370$ kare-bağımsız d ler için, $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cisimlerinde temel birimlerin, $(\varepsilon_K = a + b\omega_d)$ listesi.....	27
Çizelge 2.4	$d = 2, \dots, 32050$ için temel birimi küçük olan bazı $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cisimlerinde temel birimlerin örnek bir listesi.....	29
Çizelge 2.5	Bazı $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cisimlerinin regülatörleri ($R = \log(\varepsilon_K)$)..	30
Çizelge 3.1	TÇAB olmayan tamlık halkası bazı $\mathbb{Z}[\omega_d]$ 'lerde çarpanlara ayrılmanın tek türlü olmadığına dair örnekler (Stewart ve Tall, 2002).....	40
Çizelge 3.2.	$ d \leq 70$ olan kare bağımsız d 'ler için $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisimlerine karşılık gelen Minkowski sınırlarının (M_K) değerleri.....	57
Çizelge 3.3	$d = 1, 2, \dots, 226$ için TİB olmayan reel kuadratik sayı cisimlerinde $K = \mathbb{Q}(\sqrt{d})$ 'nin ideal sınıf gruplarının yapıları.....	71
Çizelge 3.4	Kare-bağımsız d ($d < 870$) değerleri için $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cisimlerinin sınıf sayıları ($h = h_K$)	73
Çizelge 3.5	Kare-bağımsız $d = -1, -2, \dots, -718$ değerleri için $K = \mathbb{Q}(\sqrt{d})$ sanal kuadratik sayı cisimlerinin sınıf sayıları ($h = h_K$)	74
Çizelge 4.1	$K = \mathbb{Q}(\sqrt{-119})$ sanal kuadratik sayı cismi için indirgenmiş kuadratik formlar.	87
Çizelge 4.2	$K = \mathbb{Q}(\sqrt{-71})$ sanal kuadratik sayı cismi için indirgenmiş kuadratik formlar...	89
Çizelge 4.3	$d = -1, -2, \dots, -100$ için, TİB olmayan sanal kuadratik sayı cisimleri $K = \mathbb{Q}(\sqrt{d})$ 'lerde ideal sınıf gruplarının yapıları.....	91
Çizelge 5.1	mod 5 Dirichlet karakterleri.....	101
Çizelge 5.2	$ d < 12$ ve $1 \leq n \leq 45$ için $\chi(n)$ 'nin değerleri. Eğer $d \equiv 1 \pmod{4}$ ise χ , mod $ d $ Dirichlet karakteri, $d \equiv 2, 3 \pmod{4}$ ise χ , mod $ 4d $ Dirichlet karakteridir.....	103
Çizelge 5.3	$n = 0, 1, 2, \dots, 50$ için Bernoulli sayıları	107
Çizelge 5.4	Zeta fonksiyonunun bazı tamsayı değerleri.....	108
Çizelge 5.5	$d = 2 \dots 443$ için $K = \mathbb{Q}(\sqrt{d})$ 'lere karşılık gelen $L(1, \chi)$ fonksiyonlarının değerleri	121
Çizelge 5.6	$d = -1 \dots -443$ için $K = \mathbb{Q}(\sqrt{d})$ sanal kuadratik sayı cisimlerine karşılık gelen $L(1, \chi)$ fonksiyonlarının değerleri	122

ÖNSÖZ

Bu tez çalışması sırasında yaptığı değerli katkılarından ötürü öncelikle danışman hocam Doç. Dr. Ömer Gök'e sonsuz teşekkür ederim.

Beni, sayılar teorisiyle ve özellikle de kuadratik sayı cisimleriyle tanıştıran Fatih Üniversitesi Öğretim Üyesi Prof. Dr. Barış Kendirli'ye teşekkürlerimi belirtmek istiyorum.

Ayrıca tez izleme komitemin diğer değerli üyelerinden Prof. Dr. Göksel Ağargün'e değerli tavsiyeleriyle yol göstermesinden dolayı ve Doç. Dr. Mustafa Bayram'a tezimi dikkatli bir şekilde okuyup onun gelişmesi konusunda faydalı tavsiyelerde bulunmasından dolayı çok teşekkür ederim.

Son olarak, doktora çalışmalarım boyunca büyük bir sabırla benden sevgi ve desteklerini hiç esirgemeyen ve beni sürekli cesaretlendiren başta ailem olmak üzere dost, akraba, arkadaşlarım ve ümidimi yitirdiğim anlarda beni hayat dolu sözleriyle ümitlendiren ama bugün aramızda olmayan sevgili ablama sonsuz şükranlarımı belirtmek istiyorum.

ÖZET

$K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisminin tamsayılar halkası O_K TÇAB olduğunda sayılar teorisinde tamsayılar için yapılan birçok işlem bu tamlık halkalarına transfer edilebilir. Fakat maalesef cebirsel sayı cisimlerinin tamlık halkalarında her zaman çarpanlara ayrılma tamsayılardaki gibi tek türlü olmayabiliyor. Bu özelliğin yokluğunun ölçüsü sınıf sayısı olarak adlandırılır. Sayılar teorisiyle uğraşanların bu özelliğin olmayabileceğini fark etmesinden sonra bu problemin üstesinden gelebilmek için epeyce çaba harcamışlardır. Bu çalışmalar yeni bir alanı, ideal teorisini doğurmuştur. Ondan beri ideal teorisi ve sınıf sayısı hesaplama problemi üzerine çok sayıda çalışmalar yapılmıştır. Sınıf sayısının hesaplanmasının zorluğu kriptografik uygulamalarda kuadratik sayı cisimlerinin kullanılmasını sonuç vermiştir.

Bu tezde $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisimlerinde çarpanlara ayırma ve ideal teorisi genişçe ele alınmıştır. İdeal sınıf gruplarının yapısı ve sınıf sayısı diye adlandırılan mertebeleri incelenmiştir. İki tane cebirsel birisi analitik olan üç farklı sınıf sayısı bulma metodu ele alınmıştır. Dirichlet karakterleri ve bir kuadratik sayı cismine karşılık gelen kuadratik formlar, ζ ve L-fonksiyonları çalışılmış ve kuadratik sayı cisimleriyle bağlantılarına dair sonuçlar elde edilmiştir. Pari programının cebirsel sayı cisimleri paketinin geniş bir kısmını kaplayan kuadratik sayı cisimleriyle ilgili bölümü tanıtıldı. Her bir bölümün sonunda bölümle ilgili Pari kodları ve tezde çözülen problemlerde ve çizelgelerin oluşturulmasında kullanılan Pari programları verildi.

Anahtar kelimeler: Kuadratik sayı cisimleri, tamsayılar halkası, temel birim, Euclid bölgesi, tek türlü çarpanlara ayrılabilen bölge, idealler, temel ideal bölgesi, ideal sınıf grubu, ikili kuadratik formlar, indirgenmiş formlar, sınıf sayısı, Dirichlet karakterleri, zeta fonksiyonları, L-fonksiyonları, Pari GP.

ABSTRACT

When the ring of integers O_K of a quadratic number field $K = \mathbb{Q}(\sqrt{d})$ is UFD, then most of the applications can be transferred from ordinary integers to this rings which can be done in ordinary number theory. But unfortunately the factorization is not always unique for the ring of integers of an algebraic number field as in the case of ordinary integers. The size of non-existence of this property is called the class number. After realizing the failure of unique factorization property in most of such rings, number theorists has been expended a great amount of effort to overcome this problem. Such works has given rise to a new field, the ideal theory. Since then there has been done so many works on ideal theory and the class number computation problem. The difficulty of computing the class number has given rise to cryptographic algorithms based on arithmetic in quadratic fields.

In this thesis the factorization and ideal theory in a quadratic field $K = \mathbb{Q}(\sqrt{d})$ has been studied, widely. The structure and index of ideal class groups is investigated. Three different class number computation method has been studied, two of which are based on algebraic and one is on analytic methods. The Dirichlet characters, binary quadratic forms, ζ and L-functions of quadratic number fields has been studied and some results are obtained from this subjects. Quadratic number fields part of the algebraic number fields package of Pari program is introduced. At the end of each chapter related Pari codes and scripts are given which are used for solving some problems and preparing the figures in the thesis.

Keywords: Quadratic fields, ring of integers, fundamental unit, Euclidean domain, unique factorization domain, ideals, principal ideal domain, ideal class group, binary quadratic forms, reduced forms, class number, Dirichlet characters, zeta functions, L-functions, Pari GP.

1. GİRİŞ

Fermat'ın(1601-1665) Son Teoremi (FST) kısaca; $x^n + y^n = z^n$ denkleminin $n > 2$ için tamsayı çözümünün olmadığını ifade eder. Yaklaşık 350 yıl aradan sonra 1994 yılında Andrew Wiles(1953-) tarafından ispatlanan bu teorem üzerinde yapılan çalışmalar sayılar teorisinin gelişmesine önemli katkıda bulunmuştur. Kummer'ın(1810-1893) FST üzerindeki çalışmalarından beri sayılar teorisi birçok matematikçi için büyük bir ilgi alanı olmuştur. Cebirsel sayı cisimleri ve özellikle de kuadratik sayı cisimleri üzerinde o tarihlerden bu yana epeyce çaba sarf edilmiştir. Kuadratik sayı cisimleri Kummer, Dedekind (1831-1916) ve diğerleri tarafından sonraları daha yüksek dereceli sayı cisimlerine genişletilmiştir. Onların başarılı çalışmaları matematiğin önemli branşlarından olan cebirsel sayılar teorisinin temelini de oluşturmaktadır. Kummer'ın cebirsel sayı cisimleri ile ilgili çalışmaları onun FST üzerindeki en başarılı sonuçları elde etmesinde rol oynamıştır öyle ki, onun kullandığı metotlar modern matematiğin yapıtaşları haline gelmiştir.

Cebirsel sayı cisimlerinin iyi bilinen örneklerinden bazıları; ζ_n , 1'in n . dereceden kökü olmak üzere $\mathbb{Q}(\zeta_n)$ biçiminde gösterilen cyclotomik cisimler, θ , 3. dereceden indirgenemez bir polinomun kökü olmak üzere $\mathbb{Q}(\theta)$ biçiminde gösterilen kübik sayı cisimleri ve d kare-bağımsız bir tamsayı olmak üzere $\mathbb{Q}(\sqrt{d})$ biçiminde gösterilen ve tezimin konusu olan kuadratik sayı cisimleridir. Genel olarak θ , n . dereceden tamsayı katsayılı bir minimal polinomun kökü ise $\mathbb{Q}(\theta)$ cismi n . dereceden bir cebirsel sayı cismi diye adlandırılır. Bu bağlamda ikinci dereceden bir indirgenemez polinomun kökü olan θ 'nın $\mathbb{Q}$ 'ya katılmasıyla oluşturulan kuadratik sayı cisimleri $\mathbb{Q}(\sqrt{d})$, 2. dereceden cebirsel sayı cisimleridir. Burada eğer $d > 0$ ise $\mathbb{Q}(\sqrt{d})$ 'yi reel, $d < 0$ ise $\mathbb{Q}(\sqrt{d})$ 'yi sanal kuadratik sayı cismi diye isimlendirerek ayırt ederiz. Her iki tür sayı cisminde çalışma da Gauss'un tanıttığı $ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}$ biçimindeki ikili kuadratik formların teorisiyle oldukça yakından bağlantılıdır.

K sayı cismindeki monik, tamsayı katsayılı bir polinomun kökü olan sayılar (cebirsel tamsayılar) bir halka oluşturur, bu halkaya K 'nın tamlık halkası adı verilir ve O_K biçiminde gösterilir.

O_K 'da terslenebilir elemanların oluşturduğu $K^\times$ 'ın alt grubu olan U_K birim grubu şeklinde isimlendirilir. $\mathbb{Q}(\sqrt{d})$ kuadratik sayı cisminin birim grubu $d < 0$ iken sonlu, $d > 0$ olduğunda

ise sonsuz devirli bir gruptur. Kübik sayı cisimlerinde ise birim grubu, rankın 1 veya 2 olmasına bağlı olarak değişir.

FST'nin $n=3$ ve $n=5$ gibi özel haller için ispatında kullanılan yöntem ve malzemeler kuadratik sayı cisimlerinin rasyonel tamsayılar teorisi üzerine ilk uygulamalarını oluşturmaktadır. Euler 1770'te $K = \mathbb{Q}(\sqrt{-3})$ sanal kuadratik sayı cisminin tamlık halkası $O_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, yi FST'nin $n=3$ özel hali, Dirichlet(1805-1859) ve Legendre(1752-

1833)'de 1825'te, $K = \mathbb{Q}(\sqrt{5})$ reel kuadratik sayı cisminin tamlık halkası $O_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, yi

$n=5$ özel hali için teoremin doğru olduğunu ispatlamada kullanmışlardır. Ama bu alanda ilk önemli adımlar 1830'larda Gauss'un(1777-1855) bikuadratik rezidüler üzerinde çalışmaları sırasında $\mathbb{Z}[i]$ için sayılar teorisi geliştirmekle başlamıştır. Bugün $\mathbb{Z}[i]$ halkası Gauss'un kuadratik sayı cisimlerinde öncü çalışmalarından ötürü onun onuruna Gauss tamsayıları diye adlandırılmaktadır. Gauss'un ardından, onun gözde öğrencisi Eisenstein(1823-1852), $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, yi kübik rezidülerle ilgili sayılar teorisiyle bağlantılı sonuçlar elde etmek için kullanmıştır. O yüzden bu sayılar da Eisenstein sayıları olarak isimlendirilirler.

Kummer, cebirsel sayı cisimleri üzerinde çalışmaları sırasında FST'ni ispatladığını zannetmiştir ama cyclotomic cisimlerde tamsayılardan farklı olarak tek türlü çarpanlara ayrılma özelliğinin olmayabileceği gerçeğini göz ardı etmiştir. O yüzden bu problem üzerindeki çalışmaları başarısızlıkla sonuçlanmıştır. Daha sonraları tek türlü çarpanlara ayrılma özelliğinin olabilmesi için gerek ve yeter şartın K sayı cisminin sınıf sayısının 1 olması gerektiği sonucuna varacaktır. Kummer tek türlü çarpanlara ayrılma özelliğinin eksikliği probleminin üstesinden gelebilmek için de ideal kompleks sayıları geliştirerek yeni bir çıkış açmıştır. İlerleyen yıllarda FST'nin bütün düzgün asal sayılar ($p: p, k = \mathbb{Q}(\zeta_p)$ sayı cisminin sınıf sayısını bölmez şartını sağlayan asal sayı) için doğru olduğunu ispatlamıştır. Kummer'dan sonra Dedekind, onun ideal kompleks sayılarında karşılaştığı problemlerin üstesinden gelebilmek için onların üzerine ideal teorisini geliştirmiş ve Kummer'ın ideal kompleks sayılar diye tarif ettiği sayıların ismini idealler diye değiştirmiştir. Sonuç olarak 1800'lerin sonlarına doğru Kronecker(1823-1891)'in de katkısıyla cebirsel sayılar için bir bütün teori ortaya çıkmıştır.

O_K 'nın bütün ideallerinin kümesi, idealler arası tanımlanan çarpma işlemi altında bir yarı-grup oluşturur. Bu yarı grubu gruba çevirmek için kesirsel idealleri hesaba katmak gereklidir. K 'nın bütün kesirsel ideallerinin grubu $\mathbf{F}$, O_K 'nın idealleri tarafından üretilen serbest değişmeli bir gruptur. $\mathbf{F}$ 'nin bütün temel kesirsel idealleri onun bir $\mathcal{P}$ alt grubunu oluşturur. $\mathbf{F}/\mathcal{P}$ bölüm grubu K sayı cisminin *sınıf grubu* diye adlandırılır ve $\mathbf{Cl} = \mathbf{Cl}(O_K)$ biçiminde gösterilir. Minkowsky teoremi bu grubun eleman sayısının sonlu olduğunu belirtir. Bu sonlu grubun derecesi K 'nın sınıf sayısı olarak isimlendirilir ve h_K ile gösterilir.

İkili kuadratik formlarla bağlantılı olan kuadratik sayı cisimleri, cebirsel sayı cisimleriyle uğraşanlar için her zaman iyi bir test alanı olmuştur. Kuadratik sayı cisimleri, cebirsel sayı cisimleri arasında en anlaşılır teoriye sahip olmasına rağmen hala çok sayıda zor ve çözülmemiş problem vardır. Mesela sınıf sayısı 1 olan reel kuadratik sayı cisimlerinin sonlu olup olmadığı henüz çözülmemiş bir problemdir. Zengin geçmişi ile birlikte hala cebirsel sayılar teorisinde kayda değer önemli çalışmalar yapılmaktadır. Bunlardan birisi 1966'da H. M. Stark'ın TÇAB olan sanal kuadratik sayı cisimlerinin 9 taneden ibaret olduğunu göstermesiyle bu problemin çözümüne son noktayı koymasındır. Günümüzde sınıf sayısı problemi, sınıf sayısının belli sayılar tarafından bölünebilirliği ve kriptografik uygulamalar üzerinde çok sayıda yeni çalışmalar yapılmaktadır.

Gauss, aynı $d(d = b^2 - 4ac)$ diskriminantlı kuadratik formları hesaba katarak formların denkliğini tanımladı. Belli bir diskriminantta sahip formların sınıf sayılarını onların denklik sınıflarının sayısı olarak tanımladı. Bu sınıf sayısı ile aynı diskriminantlı kuadratik sayı cisimlerinin sınıf sayıları arasında basit bir bağlantı vardır. Aslında K 'nın içindeki ideal sınıfları ile ikili kuadratik formların denklik sınıfları arasında birebir bir eşleme vardır. Bu bize $d < 0$ iken sınıf sayısının hesaplanmasında en kolay metotlardan birini verir. Kuadratik formların bileşkesi diyebileceğimiz bir bileşke kuralı vardır ve bu kural ideal sınıflarının çarpımı işlemine karşılık gelir.

$ax^2 + bxy + cy^2$ İKF'una karşılık gelen ideal sınıf sayısını hesaplamak için b 'nin $b \leq \sqrt{\frac{-d}{3}}$ şartını sağlayan bütün idealleri dolaşmasını ve d 'ye bağlı olarak onun da tek veya çift sayı olmasını isteriz. Bu tipte her b için $ac = \frac{1}{4}(b^2 - d)$ yi çarpanlarına ayırırız ve $a \geq b > -a$, $c \geq a$ ve $a = c$ ise $b \geq 0$ şartını sağlayan (a, b, c) üçlülerini hesaplarız. Burada, h , K 'nın sınıf sayısı olmak üzere tam olarak h tane bu biçimde üçlü vardır.

Hem reel hem de sanal kuadratik sayı cisimlerinin sınıf grubu ve sınıf sayılarının belirlenmesi çoğu zaman zor olabilmektedir. Kuadratik sayı cisimlerinde sınıf sayılarının hesaplanmasında kullanılan metot ve materyaller oldukça karmaşık olmasına rağmen sınıf grubu ve sayısının hesaplanmasının zorluğu kriptografik protokollerin güvenliğinde pratik kullanımından dolayı bu alanda kriptografik çalışmaların başlamasını beraberinde getirmiştir. Örneğin, anahtar değişim protokolleri hem sanal hem de reel sayı cisimlerinin kullanımlarını içermektedir. Bu projelerde güvenlik cismin seçimine bağlıdır, dolayısıyla kuadratik sayı cisminin yapısının bilinmesine ihtiyaç vardır.

Günümüz popüler krypto sistemleri genellikle tamsayılar üzerinde ya çarpanlara ayırmanın ya da Ayrık Logaritma Problemi (ALP)'nin çözümünün zorluğu üzerine inşa edilmiştir. Modulo n tamsayılar üzerine inşa edilmeyen bir anahtar değişim problemi tamsayı sistemi kırıldığında hala güvenli kalabileceği için daha kullanışlı hale gelir. İşte bu maksatla Buchmann ve Hugh Williams sanal kuadratik sayı cisimlerinin sınıf grubu üzerine kurulu bir anahtar değişim tanımlamışlardır. Bu çalışma daha sonra reel kuadratik sayı cisimlerine, kübik sayı cisimlerine ve fonksiyon cisimlerine de genişletilmiştir.

Çalışmamızın birinci ve ikinci bölümü kuadratik sayı cisimleri ile ilgili temel tanım ve teoremlere ayrılmıştır. Üçüncü bölümde, kuadratik sayı cisimlerinde çarpanlara ayırma üzerinde duruldu. Çarpanlara ayırmanın tek türlü olmadığı durumlarda ideallerin nasıl bu problemin üstesinden gelmede kullanılabileceği anlatıldı ve ideal teorisi geniş bir şekilde ele alındı. Dördüncü bölümde öncelikle kuadratik formlar tanıtıldı daha sonra ideallerle kuadratik formlar arasındaki bağlantı üzerinde duruldu. Her ikisi için de ideal sınıf grubunun yapısı ve mertebesi değişik tanım ve teoremlerle ele alındı. Bu grupların mertebelerinin hesaplanması için iki cebirsel metot gösterilmiş ve grubun üreticinin elde edilmesi örneklerle açıklanmıştır.

Beşinci bölümde öncelikle genel manada Dirichlet karakterleri tanıtılarak bir kuadratik sayı cismine karşılık gelen Dirichlet karakterleri ele alındı. Daha sonra Riemann ζ ve L fonksiyonları tanıtılarak kuadratik sayı cisimlerine karşılık gelen ζ ve L fonksiyonları ele alındı. Bazı kuadratik sayı cisimlerine karşılık gelen Dirichlet karakterleri hesaplanarak $L(1, \chi)$ fonksiyonlarının değerleri elde edildi. Bu fonksiyonların değerleriyle sınıf sayısı arasındaki bağlantı üzerinde duruldu. $L(1, \chi)$ fonksiyonun değerlerinin hesaplanması için farklı metotlar verildi ve gösterilen bu metotlarla sınıf sayısının analitik yolla hesaplanmasının ne kadar kolay olduğu örneklerle gösterildi. Hemen her bölümle bağlantılı olarak oldukça yeni olan ayrıca henüz kullanımı çok yaygınlaşmayan ve cebirsel sayılar

teorisi üzerine geniş bir altyapısı olan Pari programı kullanıldı. Bölüm sonlarına, ilgili bölümlerle bağlantılı Pari komutları eklenmiş, açıklamaları yapılmış ve örnek olarak verilen problemlerin çözümü ve tabloların hazırlanmasında kullanılan Pari programları eklenmiştir.

2. CEBİRSEL SAYI CİSİMLERİ ve KUADRATİK SAYI CİSİMLERİ

2.1 Cebirsel Sayı Cisimleri

Tanım 2.1. E ve F iki cisim olmak üzere $F \leq E$ (Yani F , E 'nin bir alt cismi) ise E 'ye F 'nin bir *genişlemesi* adı verilir.

Tanım 2.2. E , F 'nin bir genişlemesi olmak üzere eğer $[E:F]$ sonlu ise E 'ye *sonlu genişleme* denir.

Tanım 2.3. E , F 'nin bir genişlemesi olsun. Eğer $\alpha \in E$ için $f(\alpha) = 0$ olacak şekilde sıfırdan farklı bir $f(x) = a_0 + a_1x + \dots + a_nx^n \in F[X]$ polinomu varsa α 'ya F üzerinde *cebirsel eleman* denir. α , F üzerinde cebirsel değilse α 'ya *transandantal eleman* denir.

Örnek 2.1. $\mathbb{C}$ (kompleks sayılar kümesi) ve $\mathbb{Q}$ 'nun (rasyonel sayılar kümesi) her ikisi de toplama ve çarpma işlemi altında birer cisimdirler. $\mathbb{Q} \subset \mathbb{C}$ olduğu için $\mathbb{C}$, $\mathbb{Q}$ 'nun bir cisim genişlemesidir. $\sqrt{-5} \in \mathbb{C}$ sayısı $\mathbb{Q}$ üzerinde cebirseldir. Çünkü kolayca görüleceği üzere $\sqrt{-5}$, $f(x) = x^2 + 5 \in \mathbb{Q}[X]$ polinomunun bir köküdür.

Örnek 2.2. π sayısı $\mathbb{Q}$ rasyonel sayı cismi üzerinde transandanttır ama $\mathbb{R}$ (reel sayılar cismi) üzerinde cebirseldir. Çünkü $\mathbb{Q}[X]$ 'te π 'yi kök kabul eden herhangi bir polinom bulunmamasına rağmen π sayısı, $f(x) = x - \pi \in \mathbb{R}[X]$ polinomunun bir köküdür.

Tanım 2.4. $\mathbb{C}$ 'nin $\mathbb{Q}$ üzerindeki cebirsel olan elemanlarına *cebirsel sayı* denir. $\mathbb{C}$ 'nin $\mathbb{Q}$ üzerinde cebirsel olmayan elemanlarına da *transandantal sayı* denir.

Örnek 2.3. $\sqrt[3]{2} - i \in \mathbb{C}$ sayısı $\mathbb{Q}$ üzerinde cebirseldir. Çünkü eğer $\alpha = \sqrt[3]{2} - i$ alırsak α sayısı, $(\alpha + i)^3 = 2$ denkleminin bir kökü olduğu açıktır. Buradan $3i(\alpha^2 - 1) = 2 + 3\alpha - \alpha^3$. Her iki tarafın karesi alınırsa $\sqrt[3]{2} - i$ 'nin $x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5 \in \mathbb{Q}[X]$ polinomunun bir kökü olduğu görülür.

Benzer şekilde $3 - \sqrt{11}$, $x^2 - 6x - 2 \in \mathbb{Q}[X]$ polinomunun kökü, $i + \sqrt{2}$ de $x^4 - 2x^2 + 9 \in \mathbb{Q}[x]$ polinomunun kökü olduğu için cebirsel sayıdırlar.

Tanım 2.5. Eğer $\alpha \in E$ cebirsel ise aşağıdaki şartları sağlayan bir $p(x) \in F[X]$ polinomu vardır ve bu polinoma α 'nın sağladığı *minimal polinom (minipol)* denir. α 'nın F

üzerindeki minimal polinomu $P_F(\alpha, x)$ biçiminde gösterilir.

- $p \neq 0$ ve $p(\alpha) = 0$,
- $p(x)$ monik (baş katsayısı 1 olan) polinomdur,
- $p(x)$, $F[x]$ 'in indirgenemez polinomudur.

Diğer yandan bu $p(x)$ polinomu α 'yı kök kabul eden muhtemel diğer bütün polinomları da böler.

Tanım 2.6. Tanım 2.5 ile tanımlanan polinomun derecesine α 'nın F üzerindeki derecesi denir ve $derP_F(\alpha, x)$ biçiminde gösterilir.

Tanım 2.7. $F \leq E$ ve $\alpha \in E$ olmak üzere $F(\alpha)$, $F \leq F(\alpha)$ ve $\alpha \in F(\alpha)$ şartlarını sağlayan en küçük cisim olarak tanımlanır. $F(\alpha)$ cismine F 'ye α katmakla elde edilen *basit cisim* denir.

Teorem 2.1. Eğer $\alpha \in E$ cebirsel ve $n = derP_F(\alpha, x)$ ise $[F(\alpha) : F] : n$ 'dir . Ayrıca $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$, $F(\alpha)/F$ 'nin bir bazıdır.

Örnek 2.4. $[Q(\sqrt[3]{11}) : Q] = derP_Q(\sqrt[3]{11}, x)$ 'dir. Burada $P_Q(\sqrt[3]{11}, x) = x^3 - 11$ 'dir ve $p = 11$ alınırsa Eisenstein kriterine göre $x^3 - 11$ polinomu indirgenemezdir. Bu durumda $\{1, \sqrt[3]{11}, (\sqrt[3]{11})^2\}$, $Q(\sqrt[3]{11})$ cismi için bir bazdır. O halde $Q(\sqrt[3]{11})$ 'nin elemanları $a_0 + a_1(\sqrt[3]{11}) + a_2(\sqrt[3]{11})^2 : a_0, a_1, a_2 \in Q$ biçiminde sayılardır.

Tanım 2.8. E , F 'nin bir genişlemesi ve eğer $\forall \alpha \in E$ sayısı F üzerinde cebirsel ise E 'ye F 'nin bir *cebirsel genişlemesi* adı verilir.

Teorem 2.2. Eğer $[E : F] < \infty \Rightarrow E/F$ cebirseldir.

Teorem 2.3. $\alpha_1, \alpha_2 \in E$ cebirsel iseler $\alpha_1 \pm \alpha_2, \alpha_1 \cdot \alpha_2$ sayıları da cebirseldirler. Ayrıca eğer, $\alpha_2 \neq 0 \Rightarrow \alpha_1 / \alpha_2$ 'de F üzerinde cebirseldir.

Tanım 2.9. Q rasyonel sayılar cisminin sonlu genişlemelerine *cebirsel sayı cismi* denir.

Örnek 2.5. Cebirsel sayı cisimlerinin en bilinen örneklerinden bazıları;

i-) d kare-bağımsız bir tamsayı olmak üzere $Q(\sqrt{d})$ şeklinde belirtilen kuadratik sayı

cisimleri,

ii-) ζ_n , 1'in n . dereceden kökü olmak üzere $Q(\zeta_n)$ biçiminde gösterilen cyclotomik cisimler ve

iii-) θ , 3. dereceden indirgenemez bir polinomun kökü olmak üzere $Q(\theta)$ biçiminde gösterilen kübik sayı cisimleridir.

Örnek 2.4'te verdiğimiz $Q(\sqrt[3]{11})$ cismi Q 'nun bir sonlu genişlemesidir ve bir kübik sayı cisimidir.

Tanım 2.10. Özel olarak eğer $\alpha \in \mathbb{C}$, katsayıları tamsayı olan bir monik polinomun kökü ise α 'ya *cebirsel tamsayı* denir. Bir cebirsel sayı cisminde cebirsel tamsayıların kümesi bir halka oluşturur. Bu halkaya *tamlık halkası* denir ve O_K sembolü ile gösterilir.

Örnek 2.6. $\theta = \frac{3 + \sqrt{-3}}{2}$ sayısı tamsayı katsayılı $f(x) = x^2 - 3x + 3$ monik polinomun kökü

olduğu için cebirsel bir tamsayıdır. Buna rağmen $\gamma = 13/5$ cebirsel tamsayı değildir. $13/5$ sayısı, $f(x) = 5x - 13$ polinomunun bir köküdür fakat bu polinom monik değildir. Öte yandan $13/5$, $g(x) = x - 13/5$ monik polinomunun bir köküdür ama bu polinomun da katsayıları tamsayı değildir. Aslında $\gamma = 13/5$ 'in kökü olduğu tamsayı katsayılı bir polinom bulunamaz. Dolayısıyla bir cebirsel tamsayı değildir fakat cebirsel sayıdır. Her cebirsel tamsayının bir cebirsel sayı olduğu açıktır. Ama tersi doğru değildir.

Bölüm 2.3'te $Q(\sqrt{d})$ 'nin tamlık halkasının $d \equiv 1 \pmod{4}$ olduğunda $\mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right]$ ve

$d \equiv 2, 3 \pmod{4}$ olduğunda ise $\mathbb{Z}[\sqrt{d}]$ olduğu ispatlayacağız. $Q(\zeta_n)$ cisminin tamlık halkası ise $\mathbb{Z}[\zeta_n]$ dir.

Teorem 2.4. $K = Q(\alpha)$, Q üzerinde n . dereceden bir sayı cismi olsun. Bu durumda $\alpha \in K$ olmak üzere K 'dan $\mathbb{C}$ 'ye n -tane farklı $\sigma_i : K \rightarrow \mathbb{C}, \sigma_i(\alpha) = \alpha_i, (i = 1 \dots n)$ olacak şekilde otomorfizma vardır. Burada $P_Q(\alpha, x) = \prod_{i=1}^n (x - \alpha_i)$, α 'nın minimal polinomunun kompleks sayılar üzerindeki parçalanışını göstermek üzere, $\sigma_i(\alpha) = \alpha_i$ 'ler, $P_Q(\alpha, x)$ 'in $\mathbb{C}$ 'deki n -farklı köküdür.

$P_Q(\alpha, x)$ 'in reel köklerinin sayısı için r_1 , kompleks kök çiftlerinin sayısı için r_2 sembolleri kullanılır. Burada $n = r_1 + 2r_2$ eşitliği mevcuttur.

Tanım 2.11. Teorem 2.4'te verilen α_i 'lerin her birine $\alpha \in K$ 'nın eşlenikleri denir. Bu α_i 'lerin her biri cebirsel sayılardır ve her birinin minimal polinomları $P_Q(\alpha, x)$ 'tir . $\forall \alpha \in K$ için kendisi ile birlikte n farklı eşlenik vardır.

Örnek 2.7. $\alpha = \sqrt[4]{3}$ ve $K = \mathbb{Q}(\alpha)$ olsun. α 'nın minimal polinomu 4. dereceden $P_Q(\alpha, x) = x^4 - 3$ polinomudur. Bu polinom iki tane reel köke $(\pm \sqrt[4]{3})$, iki tane de kompleks köke $(\pm i\sqrt[4]{3})$ sahiptir. Buradan $r_1 = 2, r_2 = 1$ olduğu anlaşılmaktadır. $\sigma_i : K \rightarrow \mathbb{C}$ omorfizmalar aşağıdaki gibidir.

$$\begin{aligned}\sigma_1(\alpha) &= \sqrt[4]{3} \\ \sigma_2(\alpha) &= -\sqrt[4]{3} \\ \sigma_3(\alpha) &= i\sqrt[4]{3} \\ \sigma_4(\alpha) &= -i\sqrt[4]{3}\end{aligned}$$

Tanım 2.12. $K = \mathbb{Q}(\alpha)$, $\mathbb{Q}$ üzerinde n . dereceden bir sayı cismi ve $\sigma_1, \sigma_2, \dots, \sigma_n$, K 'dan $\mathbb{C}$ 'ye otomorfizmalar olmak üzere, $\beta \in K$ 'nın normu ve iz(trace)'i sırasıyla aşağıdaki gibi tanımlanır.

$$N_{K/\mathbb{Q}}(\beta) = \prod_{i=1}^n \sigma_i(\beta), \quad (2.1)$$

$$Tr_{K/\mathbb{Q}}(\beta) = \sum_{i=1}^n \sigma_i(\beta). \quad (2.2)$$

Tanım 2.13. K , n . dereceden bir sayı cismi olmak üzere $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n \in K$ 'ların diskriminantı,

$$\Delta(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n) = (\det(\sigma_i(\alpha_j)))^2$$

biçiminde verilir.

Örnek 2.8. $K = \mathbb{Q}(\sqrt{3})$, olmak üzere $P_Q(\alpha, x) = P_Q(\sqrt{3}, x) = x^2 - 3$. Bu polinomun kökleri $\sqrt{3}$, ve $-\sqrt{3}$ 'tür. Yani iki tane reel kök vardır ve otomorfizmalar;

$$\sigma_1(\sqrt{3}) = \sqrt{3}, \quad \sigma_2(\sqrt{3}) = -\sqrt{3}$$

şeklinde iki tanedir. $\alpha_1 = 3, \alpha_2 = 2 + \sqrt{3}$ olmak üzere,

$$\Delta(3, 2 + \sqrt{3}) = \begin{vmatrix} 3 & 3 \\ 2 + \sqrt{3} & 2 - \sqrt{3} \end{vmatrix}^2 = (3(2 - \sqrt{3}) - 3(2 + \sqrt{3}))^2 = 108.$$

Teorem 2.5. K , n . dereceden bir sayı cismi ve $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n \in K$ olmak üzere $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n \in K$ 'nın diskriminantı $\Delta(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n) = \det(\text{Tr}_{K/Q}(\alpha_i \alpha_j))$ şeklindedir.

Teorem 2.6. $\Delta(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n) \in \mathbb{Q}$ dur. Özel olarak eğer α_i 'ler cebirsel tamsayı ise $\Delta(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n) \in \mathbb{Z}$ 'dir.

Tanım 2.14. K sayı cisminin diskriminantı, O_K 'nın bir tamlık tabanı $\alpha_1, \alpha_2, \dots, \alpha_n$ diskriminantı $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)$ olarak tanımlanır.

Tanım 2.15. Bir cebirsel sayı cismi K 'da O_K 'nın bütün idealleri ideal çarpma işlemine göre bir semi-grup oluşturmaktadır. Bu semi-grubu, gruba dönüştürmek için kesirsel idealler hesaba katılabilir. Bir kesirsel α ideali $\alpha \in O_K$ için $\alpha \alpha \subset O_K$ şartını sağlayan O_K 'nın bir alt modülüdür. K 'nın bütün kesirsel ideallerin grubu $\mathbf{F}$, O_K 'nın asal idealleri tarafından üretilmiş olan serbest değişmeli gruptur. $\mathbf{F}$ 'nin bütün temel kesirsel ideallerinin kümesi $\mathbf{P}$ ile gösterilen $\mathbf{F}$ 'nin bir alt grubudur. $\mathbf{Cl} = \mathbf{F}/\mathbf{P}$ kesrine K 'nın sınıf grubu adı verilir, bu grubun mertebesi $|\mathbf{Cl}|$ 'ye ise K sayı cisminin sınıf sayısı adı verilir bu da h_K sembolüyle gösterilir.

Bu bölümde cebirsel sayılar ve cebirsel sayı cisimlerinin bazı temel tanım ve özellikleri verildi. Sonraki bölümden itibaren tezin esas konusu olan kuadratik sayı cisimleri ele alındı.

2.2 Kuadratik Sayı Cisimlerine Giriş

Tanım 2.16. K/Q bir cebirsel genişleme olmak üzere özel olarak, $[K:Q] = 2$ ise K cebirsel sayı cismine *kuadratik sayı cismi* denir.

Teorem 2.7. d , kare-bağımsız (bölenleri arasında 1'den başka tam-kare içermeyen) bir tamsayı olmak üzere kuadratik sayı cisimleri, $\mathbb{Q}(\sqrt{d})$ biçimindedirler.

İspat: K bir kuadratik sayı cismi ve $\{1, \alpha\}$, K 'nin $\mathbb{Q}$ üzerindeki bir bazı olsun. Bu durumda $K = \mathbb{Q}(\alpha)$ ve $\exists b, c \in \mathbb{Z} : \alpha^2 = c + b\alpha$ dir. α ,

$$f(x) = x^2 - bx - c \quad (2.3)$$

polinomunun bir köküdür. Diğer taraftan (2.3) denklemiyle verilen f 'nin kökleri $\frac{b \pm \sqrt{b^2 + 4c}}{2}$, dir. d kare-bağımsız bir tamsayı olmak üzere $b^2 + 4c = a^2 d$ olacak şekilde

$a \in \mathbb{Q}$ vardır. Böylece $\frac{b \pm \sqrt{b^2 + 4c}}{2} = \frac{b}{2} \pm \frac{a}{2} \sqrt{d}$ dir. Dolayısıyla $\alpha \in \mathbb{Q}(\sqrt{d})$ ve $\sqrt{d} \in \mathbb{Q}(\alpha)$.

Yani d kare-bağımsız bir sayı olmak üzere $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$ $\{1, \sqrt{d}\}$ bir baz olduğu için $\mathbb{Q}(\sqrt{d})$ 'nin elemanları $p + q\sqrt{d} : p, q \in \mathbb{Q}$ şeklindedir. Böylece d , kare-bağımsız olmak üzere,

$$\mathbb{Q}(\sqrt{d}) = \{p + q\sqrt{d} : p, q \in \mathbb{Q}\}. \quad (2.4)$$

biçiminde verilir.

Tanım 2.17. $K = \mathbb{Q}(\sqrt{d})$ bir kuadratik sayı cismi olmak üzere eğer $d > 0$ ise K 'ya *reel kuadratik sayı cismi*, $d < 0$ ise K 'ya *sanal (imajiner) kuadratik sayı cismi* denir.

Örnek 2.9. $\mathbb{Q}(\sqrt{105})$ reel, $\mathbb{Q}(\sqrt{-23})$ ise sanal kuadratik sayı cisimleridir. Bununla birlikte (2.4)'ten $\frac{2 - \sqrt{-23}}{2} \in \mathbb{Q}(\sqrt{-23})$ fakat $i \notin \mathbb{Q}(\sqrt{-23})$ olduğu da anlaşılmaktadır.

Teorem 2.8. Kuadratik sayı cisimlerinde iki tane otomorfizma $\sigma_1, \sigma_2 : \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{C}$ vardır. Bu otomorfizmalar $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ olmak üzere; $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$ özdeşlik dönüşümü ve $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$ şeklinde verilen dönüşümlerden oluşan otomorfizmalardır.

İspat: $P_{\mathbb{Q}}(\sqrt{d}, x) = f(x) = x^2 - d$ olduğu açıktır. $f(x)$ 'in $\mathbb{C}$ 'deki kökleri ise $\sqrt{d}$ ve $-\sqrt{d}$ olmak üzere iki tanedir. Buradan otomorfizmaların $\sigma_1 : \sqrt{d} \rightarrow \sqrt{d}, \sigma_2 : \sqrt{d} \rightarrow -\sqrt{d}$ olduğu görülmektedir. O halde $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ olmak $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$ özdeşlik dönüşümü ve $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$ dönüşümleri mevcuttur.

Diğer yandan eğer, K reel kuadratik sayı cismi ise $r_1 = 2, r_2 = 0$, sanal kuadratik sayı cismi ise $r_1 = 0, r_2 = 1$ olduğu da açıktır.

Tanım 2.18. $K = \mathbb{Q}(\sqrt{d})$ bir kuadratik sayı cismi olsun. $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ 'nin eşleniği (α') , normu $(N_{K/\mathbb{Q}}(\alpha))$ ve iz'i $(Tr_{K/\mathbb{Q}}(\alpha))$ sırasıyla aşağıdaki gibi tanımlanır.

- $\alpha' = a - b\sqrt{d}$,
- $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^2 \sigma_i(\alpha) = \sigma_1(a + b\sqrt{d})\sigma_2(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2d$,
- $Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^2 \sigma_i(\alpha) = \sigma_1(a + b\sqrt{d}) + \sigma_2(a + b\sqrt{d}) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$.

Bu tanımda (2.1) ve (2.2) denklemleri kullanılarak norm ve iz tanımları verilmiş daha sonra formüller kuadratik sayı cisimleri için daha basit hale getirilmiştir. Bundan böyle α 'nın normu ve iz'i için genel kullanıma uyarak sırasıyla kısaca $N(\alpha)$ ve $Tr(\alpha)$ sembollerini kullanacağız. $N(\alpha) = \alpha\alpha'$ ve $Tr(\alpha) = \alpha + \alpha'$ olduğu açıktır. İlerde görüleceği üzere norm, $\mathbb{Q}(\sqrt{d})$ 'deki çarpma ve bölünebilme ile ilgili problemleri $\mathbb{Z}$ 'ye transfer etmede oldukça yararlıdır.

Örnek 2.10. $\mathbb{Q}(\sqrt{-11})$ 'de $\alpha = 3 - 2\sqrt{-11}$ alalım. Bu durumda;

$$\alpha' = 3 + 2\sqrt{-11},$$

$$N(\alpha) = (3 - 2\sqrt{-11})(3 + 2\sqrt{-11}) = 9 + 4.11 = 53,$$

$$Tr(\alpha) = (3 - 2\sqrt{-11}) + (3 + 2\sqrt{-11}) = 2.3 = 6$$

elde edilir.

Teorem 2.9. $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ olmak üzere norm ve iz'in aşağıdaki özellikleri vardır.

$$i-) (\alpha \pm \beta)' = \alpha' \pm \beta', (\alpha\beta)' = \alpha'\beta',$$

$$ii) N(\alpha.\beta) = N(\alpha).N(\beta),$$

$$iii-) Tr(\alpha \pm \beta) = Tr(\alpha) \pm Tr(\beta),$$

$$\text{iv-)} N(\alpha), Tr(\alpha) \in \mathbb{Q},$$

$$\text{v-)} \alpha \in \mathbb{Q}(\sqrt{d}), f(x) = x^2 - Tr(\alpha)x + N(\alpha) \text{ polinomunun bir köküdür.}$$

İspat: $\alpha = a + b\sqrt{d}, \beta = e + f\sqrt{d}$ olsun.

$$\begin{aligned} \text{i-)} (\alpha \pm \beta)' &= (a + b\sqrt{d} \pm e + f\sqrt{d})' = ((a \pm e) + (b \pm f)\sqrt{d})' = (a \pm e) - (b \pm f)\sqrt{d} \\ &= (a - b\sqrt{d}) \pm (e - f\sqrt{d}) = \alpha' \pm \beta' \end{aligned}$$

$$\begin{aligned} (\alpha\beta)' &= ((a + b\sqrt{d})(e + f\sqrt{d}))' = ((ae + bfd) + (af + eb)\sqrt{d})' = ((ae + bfd) - (af + eb)\sqrt{d}) \\ &= (a - b\sqrt{d})(e - f\sqrt{d}) = (a + b\sqrt{d})'(e + f\sqrt{d})' = \alpha'\beta'. \end{aligned}$$

$$\text{ii-)} \text{Özellik (i) kullanılırsa, } N(\alpha.\beta) = (\alpha\beta)(\alpha\beta)' = \alpha\beta\alpha'\beta' = \alpha\alpha'\beta\beta' = N(\alpha)N(\beta) \text{ elde edilir.}$$

iii) Benzer şekilde;

$$Tr(\alpha \pm \beta) = (\alpha \pm \beta) + (\alpha \pm \beta)' = \alpha \pm \beta + \alpha' \pm \beta' = (\alpha + \alpha') \pm (\beta + \beta') = Tr(\alpha) \pm Tr(\beta).$$

$$\text{iv-)} a, b \in \mathbb{Q}, d \in \mathbb{Z} \text{ olduğu için } N(\alpha) = a^2 - b^2d \in \mathbb{Q} \text{ ve } Tr(a) = 2a \in \mathbb{Q} \text{ olduğu açıktır.}$$

$$\text{v-)} f(\alpha) = \alpha^2 - Tr(\alpha)\alpha + N(\alpha) = \alpha^2 - (\alpha + \alpha')\alpha - \alpha\alpha' = \alpha^2 - \alpha^2 - \alpha'\alpha + \alpha\alpha' = 0 \text{ olduğu}$$

için aşıkardır.

2.3 Kuadratik Sayı Cisimlerinin Tamlık Halkası ve Diskriminantı

$K = \mathbb{Q}(\sqrt{d})$ bir kuadratik sayı cismi olmak üzere, K 'da bulunan cebirsel tamsayıların kümesini O_K ile göstereceğiz. Herhangi bir kuadratik sayı cismi K 'da $O_K \subset K$ olacak şekilde $\mathbb{Q}$ 'nun $\mathbb{Z}$ ile ilişkisine benzer bir ilişki kurabileceğimiz bir tamsayılar kümesi vardır. Eğer a ve b birer tamsayı iseler $N(a + b\sqrt{d}) = a^2 - b^2d$ ve $Tr(a + b\sqrt{d}) = 2a$ değerleri tamsayı oldukları için $a + b\sqrt{d}$ sayısı tamsayı katsayılı, $f(x) = x^2 - Tr(x)x + N(x)$ monik polinomunun bir kökü olduğunu Teorem 2.9'un beşinci özelliğinden dolayı biliyoruz. Dolayısıyla, eğer $a, b \in \mathbb{Z}$ ise $\alpha = a + b\sqrt{d}$ sayısı cebirsel bir tamsayıdır. Yani O_K 'nın bir elemanıdır. Fakat K 'da başka cebirsel sayılar da vardır. Aşağıdaki teoremle K 'da cebirsel sayıları içeren en geniş kümeyi elde edeceğiz.

Teorem 2.10.

$$\omega_d = \begin{cases} \sqrt{d}; & d \equiv 2,3(\text{mod } 4) \\ \frac{1+\sqrt{d}}{2}; & d \equiv 1(\text{mod } 4) \end{cases} \quad (2.5)$$

olmak üzere,

$$O_K = \{m + n\omega_d : m, n \in \mathbb{Z}\} \quad (2.6)$$

dir.

İspat: $\alpha = m + n\sqrt{d} \in \mathbb{Q}(\sqrt{d}) : m, n \in \mathbb{Q}$ olsun.

Eğer $n = 0$ ise $\alpha = m \in \mathbb{Q}$ cebirsel tamsayıdır $\Leftrightarrow m \in \mathbb{Z}$ 'dir.

$n \neq 0$ olduğunu varsayalım. α 'nın $\mathbb{Q}$ üzerindeki minimal polinomu $X^2 - \text{Tr}(\alpha)X + N(\alpha)$, yani $X^2 - 2mX + m^2 - dn^2$ 'dir. O halde,

$$\alpha = m + n\sqrt{d} \in O_K \Leftrightarrow$$

$$2m \in \mathbb{Z} \text{ ve } m^2 - dn^2 \in \mathbb{Z} \quad (2.7)$$

olmalıdır.

$2m \in \mathbb{Z} \Rightarrow \exists a \in \mathbb{Z} : m = \frac{a}{2}$ 'dir. Diğer taraftan (2.6)'dan $d(2n)^2 \in \mathbb{Z}$ elde edilir. Çünkü

$$2m \in \mathbb{Z} \Rightarrow 4m^2 \in \mathbb{Z} \text{ ve}$$

$m^2 - dn^2 \in \mathbb{Z} \Rightarrow 4(m^2 - dn^2) = 4m^2 - 4dn^2 \in \mathbb{Z} \Rightarrow 4dn^2 = d(2n)^2 \in \mathbb{Z}$ elde edilir. Fakat d kare-bağımsız olduğu için $(2n)^2 \in \mathbb{Z}$. Dolayısıyla $2n \in \mathbb{Z}$ 'dir. O halde $\exists b \in \mathbb{Z} : n = \frac{b}{2}$ 'dir.

Dolayısıyla $m^2 - dn^2 \in \mathbb{Z} \Leftrightarrow a^2 - db^2 \equiv 0(\text{mod } 4)$ 'tür. Fakat tam kare sayıların mod 4 'e göre 0 veya 1'e denk oldukları göz önüne alınırsa iki durum ortaya çıkar;

Eğer,

$$d \equiv 2,3(\text{mod } 4) \Rightarrow a^2 \equiv b^2 \equiv 0(\text{mod } 4). \text{ Yani } a \text{ ve } b \text{ çift sayılardır.}$$

Eğer $d \equiv 1(\text{mod } 4) \Rightarrow a^2 \equiv b^2 \equiv 0(\text{mod } 4)$ ya da $a^2 \equiv b^2 \equiv 1(\text{mod } 4)$ 'tür.

$a^2 \equiv b^2 \equiv 0 \pmod{4} \Rightarrow a, b$ çift sayı $\Rightarrow m, n \in \mathbb{Z}$ 'dir.

$a^2 \equiv b^2 \equiv 1 \pmod{4} \Rightarrow a, b$ tek sayı olacakları için $\exists s \in \mathbb{Z} : m, n, s + \frac{1}{2}$ tipindedir.

Bu sonuçlar birleştirilirse istenen elde edilmiş olur.

(2.6) ile belirtilen O_K 'yı aşağıdaki gibi yazmakta mümkündür.

$$O_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2,3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod{4} \end{cases} \quad (2.8)$$

İlerleyen kısımlarda K kuadratik sayı cisminin cebirsel tamsayılarını ifade etmek için O_K , veya $\omega = \omega_d$ (2.5)'te belirtildiği gibi olmak üzere $\mathbb{Z}[\omega]$ sembollerinden birini kullanacağız.

Örnek 2.11. $K = \mathbb{Q}(\sqrt{-79})$ alınırsa $-79 \equiv 1 \pmod{4}$ olduğundan (2.5)'ten dolayı

$\omega_{-79} = \frac{1+\sqrt{-79}}{2}$ 'dir. Dolayısıyla K 'nın cebirsel tamsayılarının kümesi (2.6)'dan

$O_{-79} = \left\{ m + n \left(\frac{1+\sqrt{-79}}{2} \right) : m, n \in \mathbb{Z} \right\}$ olduğu kolayca görülür. Örnek olarak;

$\frac{3-\sqrt{-79}}{2} = 2 - 1 \cdot \left(\frac{1+\sqrt{-79}}{2} \right)$ ve $2, 1 \in \mathbb{Z}$ olduğu için $K = \mathbb{Q}(\sqrt{-79})$ cisminin cebirsel bir

tamsayıdır. Fakat $\frac{1}{2} + \sqrt{3} = m + n\sqrt{3}$ olacak şekilde $m, n \in \mathbb{Z}$ bulunamayacağı için

$\frac{1}{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{3})$ olduğu halde cebirsel bir tamsayı değildir.

Teorem 2.11. O_K cebirsel tamsayılar kümesi $K = \mathbb{Q}(\sqrt{d})$ 'nin bir alt halkasıdır.

İspat: O_K 'nın K 'nın alt halkası olduğunu göstermek için $\forall \alpha, \beta \in O_K$ için $\alpha - \beta, \alpha\beta \in O_K$ olduğunu göstermeliyiz. $\alpha = m_1 + n_1\omega_d, \beta = m_2 + n_2\omega_d$ olmak üzere;

$\alpha - \beta = (m_1 - m_2) + (n_1 - n_2)\omega_d \in O_K$ 'dır, çünkü $(m_1 - m_2), (n_1 - n_2) \in \mathbb{Z}$ 'dir.

$d \equiv 2,3 \pmod{4} \Rightarrow \omega_d = \sqrt{d} \Rightarrow \omega_d^2 = d \Rightarrow \alpha\beta = m_1m_2 + n_1n_2d + (m_1n_2 + m_2n_1)\omega_d \in O_K$ 'dır.

$$d \equiv 1 \pmod{4} \Rightarrow \omega_d^2 = \omega_d + \frac{d-1}{4} : \left(\frac{d-1}{4} \in \mathbb{Z} \right), \text{dir.}$$

$$\Rightarrow \alpha\beta = m_1m_2 + n_1n_2 \left(\frac{d-1}{4} \right) + (m_1n_2 + m_2n_1 + n_1n_2)\omega_d \in O_K \text{ 'dır.}$$

Dolayısıyla O_K bir alt halkadır.

Ayrıca $\alpha = m_1 + n_1\omega_d \in O_K$ için eğer $d \equiv 2,3 \pmod{4} \Rightarrow \omega_d = \sqrt{d}$ olduğundan

$$\alpha' = m_1 - n_1\sqrt{d} = m_1 - n_1\omega_d \in O_K \text{ dir. Yine, eğer } d \equiv 1 \pmod{4} \Rightarrow \omega_d = \frac{1+\sqrt{d}}{2} \text{ olur ki bu}$$

$$\text{durumda da } \alpha' = m_1 + n_1 \frac{1-\sqrt{d}}{2} = (m_1 + n_1) - n_1 \frac{1+\sqrt{d}}{2} = (m_1 + n_1) - n_1\omega_d \in O_K \text{ 'dır. Yani}$$

her iki durumda da $\alpha' \in O_K$ elde ederiz.

Özel olarak $\mathbb{Z}[i]$ tamlık halkasına Gauss sayıları, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ tamlık halkasına da Eisenstein sayıları adı verilir.

Tanım 2.19. O_K 'ya $\mathbb{Q}(\sqrt{d})$ 'nin *tamlık halkası* denir, ve $\{1, \omega_d\}$ 'ye de O_K tamlık halkasının *tamlık tabanı* adı verilir. $\{1, \omega_d\}$ tamlık tabanı olduğu için $a, b \in \mathbb{Z}$ olmak üzere O_K 'nın her bir elemanı $a.1 + b.\omega_d$ biçiminde ifade edilebilir.

Bölüm 1'de bir K sayı cisminin diskriminantını onun tamlık halkasının tamlık tabanının diskriminantı olarak tanımlamıştık. O halde $\mathbb{Q}(\sqrt{d})$ 'nin diskriminantını artık belirleyebiliriz.

Teorem 2.12. $K = \mathbb{Q}(\sqrt{d})$ bir kuadratik sayı cismi olmak üzere K 'nın diskriminantı;

$$d_K = \begin{cases} d, & d \equiv 2, 3 \pmod{4} \\ 4d, & d \equiv 1 \pmod{4} \end{cases} \quad (2.9)$$

dir.

İspat: $d \equiv 2, 3 \pmod{4}$ olsun. Bu durumda O_K 'nın tamlık tabanı $\{1, \sqrt{d}\}$ 'dir. Dolayısıyla;

$$d_K = \Delta(1, \sqrt{d}) = \begin{vmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d} - \sqrt{d})^2 = (-2\sqrt{d})^2 = 4d,$$

$d \equiv 1 \pmod{4}$ olsun. O_K 'nin tamlık tabanı $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ 'dir. O halde;

$$d_K = \Delta\left(1, \frac{1+\sqrt{d}}{2}\right) = \left|\frac{1}{\frac{1+\sqrt{d}}{2}} - \frac{1}{\frac{1-\sqrt{d}}{2}}\right|^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2}\right)^2 = (-\sqrt{d})^2 = d.$$

2.4 Kuadratik Sayı Cisimlerinde Birimseller Grubu

Tanım 2.20. $u \in O_K$ olmak üzere eğer $u^{-1} \in O_K$ ise u 'ya O_K 'da *birimsel eleman* veya kısaca *birimsel* denir. K sayı cisminin tamlık halkası O_K 'daki birimsel elemanların kümesini U_K ile göstereceğiz. Bazı kaynaklarda U_K yerine $O_K^\times$ kullanılmıştır.

Teorem 2.13. $u \in O_K$ olsun. $u \in U_K \Leftrightarrow N(u) = \pm 1$ 'dir.

İspat: $\Rightarrow$ u birimsel ise $u^{-1} \in O_K$ 'dır, dolayısıyla $N(u), N(u^{-1}) \in \mathbb{Z}$ 'dir. Diğer yandan

$$1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1}) \text{ 'dir. } 1\text{'in bölenleri } \mp 1 \text{ 'den ibaret olduğu için } N(u) = \pm 1 \text{ 'dir.}$$

$\Leftarrow$ $N(u) = \pm 1$ ise $uu' = \pm 1$ 'dir. Dolayısıyla $u^{-1} = \pm u'$. Teorem 2.11 in sonucunda gösterildiği üzere eğer $u \in O_K$ ise $u' \in O_K$ olacağı açıktır. Böylece $u^{-1} \in O_K$ 'dır. O halde $u \in U_K$.

Örnek 2.12. $O_K = \{1, \sqrt{3}\}$ alırsak $2 + \sqrt{3} \in U_K$ 'dır. Çünkü;

$$u^{-1} = \frac{1}{2 + \sqrt{3}} = 2 - \sqrt{3} \in O_K \text{ 'dır. Fakat ,}$$

$$\frac{1}{3 + \sqrt{3}} = \frac{3 - \sqrt{3}}{6} = \frac{1}{2} - \frac{\sqrt{3}}{6} \notin O_K$$

olacağından $3 + \sqrt{3} \notin U_K$ 'dır.

Teorem 2.14. $u = x + y\omega_d : x, y \in \mathbb{Z}$ olmak üzere $u \in U_K$ 'dır ancak ve ancak

$$\begin{aligned} x^2 - dy^2 &= \pm 1, & d &\equiv 2, 3 \pmod{4} \text{ ise} \\ x^2 + xy + \frac{1-d}{4}y^2 &= \pm 1, & d &\equiv 1 \pmod{4} \text{ ise} \end{aligned}$$

İspat: O_K 'nın her bir elemanının $x + y\omega_d$ biçiminde olduğu ve (2.5)'te verildiği gibi

$$\omega_d = \begin{cases} \sqrt{d}, & d \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod{4} \end{cases}$$

olduğu göz önüne alınıp Teorem 2.13 ile birleştirildiğinde istenen elde edilmiş olur.

Teorem 2.15. $d < 0$ ise O_K 'da sadece sonlu sayıda birimsel vardır ve $d = -1$, $d = -3$ halleri dışında birimseller ± 1 olmak üzere iki taneden ibarettir.

- $d = -1$ ise birimseller $\pm 1, \pm i$ olmak üzere dört tanedir.
- $d = -3$ ise birimseller $\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}$ olmak üzere altı tanedir.

İspat: $\alpha = m + n\sqrt{d} \in O_K$ 'nın birimsel olması için $N(\alpha) = \pm 1$ olmalıdır. Fakat $d < 0$ olduğunda $N(\alpha) \geq 0$ olur. O halde $d < 0$ durumunda $\alpha \in O_K$ 'nın birimsel olması için $N(\alpha) = 1$ olmalıdır.

(2.6)'dan $d \equiv 2, 3 \pmod{4}$ ise $\alpha \in O_K$ 'nın $m + n\sqrt{d} : m, n \in \mathbb{Z}$ biçiminde olduğunu biliyoruz. Dolayısıyla $N(m + n\sqrt{d}) = m^2 - dn^2 = m^2 + |d|n^2$ 'dir.

Eğer $d = -1$ ise

$$m^2 + n^2 = 1 \tag{2.10}$$

denkleminin çözümleri $\mathbb{Z}[i]$ 'nin (Gauss Sayılarının) birimsellerini verir. Kolayca gösterileceği üzere (2.10) ile belirtilen denklemin tamsayı çözümleri $(m, n) = (\pm 1, 0), (0, \pm 1)$ olmak üzere dört taneden ibarettir. Bunlara karşılık gelen $m + n\sqrt{-1}$ 'ler ise $\pm 1, \pm i$ 'dir. O halde; $K = \mathbb{Q}(\sqrt{-1})$ ise $U_K = \{\pm 1, \pm i\}$.

Eğer $d \equiv 2, 3 \pmod{4}$ ve $d < -1 \Rightarrow m^2 + |d|n^2 = 1$ denkleminin bütün çözümleri $(\pm 1, 0)$ den ibarettir. Çünkü, $m^2 + |d|n^2 \geq 0$ olduğundan $n = 0$ olmalıdır. Eğer $n = 0$ alınırsa $m^2 = 1$ elde edilir ki bu da $m = \pm 1$ demektir. Dolayısıyla da birimseller ± 1 olmak üzere iki tanedir.

Şimdi, $d \equiv 1 \pmod{4}$ olduğunu varsayalım. $\alpha \in O_K$, $m + n\frac{1+\sqrt{d}}{2} : m, n \in \mathbb{Z}$ biçimindedir.

$$N\left(m+n\left(\frac{1+\sqrt{d}}{2}\right)\right)=m^2+mn+\left(\frac{1-d}{4}\right)n^2=m^2+mn+\left(\frac{1+|d|}{4}\right)n^2 \quad (2.11)$$

dir.

Burada $|d| \equiv 3 \pmod{4}$ olduğundan $\frac{1+|d|}{4} \in \mathbb{Z}$ 'dir. Şimdi $r = \left(\frac{1+|d|}{4}\right)$ alalım, bu durumda

(2.11) denklemi,

$$m^2 + mn + rn^2 = 1 \quad (2.12)$$

denklemine dönüşür. Bu denklemi negatif olmayan $(m-n)^2$ ve $(m+n)^2$ terimleri cinsinden yazarsak;

$$(m-n)^2 = 1 - 3mn - (r-1)n^2 \geq 0 \quad (2.13)$$

$$(m+n)^2 = 1 + mn - (r-1)n^2 \geq 0 \quad (2.14)$$

denklemlerini elde ederiz.

Özel olarak $d = -3$ ise $r = 1$ olur. Bu durumda (2.13) ve (2.14) yerine $1 - 3mn \geq 0$ ve $1 + mn \geq 0$ denklemleri gelir ki, bunları bir tek denklemde birleştirirsek $-1 \leq mn \leq \frac{1}{3}$

elde ederiz. Bu şartı ve (2.12)'yi sağlayan (m, n) ikilileri ise,

$$(m, n) = (1, 0), (0, 1), (-1, 0), (0, -1), (1, -1), (-1, 1) \text{ 'dir.}$$

Bunlar $\alpha = m + n\left(\frac{1+\sqrt{d}}{2}\right)$ 'de yerine yazılırsa, $\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}$ olmak üzere altı tane birimsel

elde edilir.

Özetle; $K = \mathbb{Q}(\sqrt{-3})$ ise $U_K = \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\}$ 'dir.

Eğer $d < -3 \Rightarrow r > 1$ 'dir. Bu durumda da $n = 0$ ise $m = \pm 1$ 'dir. $n > 0$ ise (2.13) ve (2.14)'ten $(r-1)n^2 \geq 1$ 'dir ve $-3mn \geq 0$ ve $mn \geq 0$ elde ederiz ki bu durumda çözüm olmadığı açıktır.

Sonuç olarak $d < 0$ olması halinde birimselleri belirlemiş olduk. $d > 0$ olması durumunda ise

teori oldukça farklıdır. Bu durumda O_K 'daki birimsellerin sayısı sonlu değildir ve bunların belirlenmesi her zaman kolay olmayabilir.

Teorem 2.16. $d > 0$ ise O_K 'nın sonsuz sayıda birimsel elemanı vardır.

İspat: Öncelikle $\forall x, y \in \mathbb{Z}$ için $u = x + y\sqrt{d} \in O_K$ olduğunu gösterelim. (2.5) ve (2.6)'dan $d \equiv 2,3 \pmod{4}$ ise $\omega_d = \sqrt{d}$ dir ve $u = x + y\sqrt{d} \in O_K$ olduğu açıktır. Eğer $d \equiv 1 \pmod{4}$ ise yine $x + y\sqrt{d} = (x - y) + (2y)\omega_d$ biçiminde yazılabilir. O halde her iki durumda da $u = x + y\sqrt{d} \in O_K$ 'dır. $u = x + y\sqrt{d} \in U_K$ olması içinse $N(u) = x^2 - dy^2 = \pm 1$ olmalıdır. Diğer yandan bilindiği üzere eğer $d > 0$ kare-bağımsız ise,

$$N(u) = x^2 - dy^2 = 1 \quad (2.15)$$

Pell(1611-1683) denkleminin her zaman çözümü vardır ve sonsuz sayıdadır, (Silverman, 2001).

Eğer (x, y) ikilisi (2.15) denklemin bir çözümü ise $u = x + y\sqrt{d} \in U_K$ birimsel elemandır. Ayrıca $\forall n \in \mathbb{Z}$ için $u^n = (x + y\sqrt{d})^n = x_n + y_n\sqrt{d}$ olmak üzere (x_n, y_n) ikilileri de bu Pell denkleminin çözümüdür, dolayısıyla $u^n \in U_K$ 'dır. Bu durumda sonsuz sayıda birimsel vardır ve anlaşılacağı üzere bunların saptanması (2.15) ile verilen Pell denkleminin çözümü ile doğrudan bağlantılıdır.

Teorem 2.17. (Adams ve Goldstein, 1976) $u \in O_K$ birimsel ise $-u$ ve $\frac{1}{u}$ birimseldirler.

Ayrıca $u_1, u_2 \in U_K$ ise $u_1 \cdot u_2 \in U_K$ 'dır.

İspat: u birimsel ise $N(u) = \pm 1$ dir. Normun çarpımsallık özelliğinden

$$N(-u) = N(-1)N(u) = \pm 1 \quad \text{ve} \quad N\left(\frac{1}{u}\right) = \frac{N(1)}{N(u)} = \frac{1}{\pm 1} = \pm 1 \quad \text{olduğundan} \quad -u, \frac{1}{u} \in U_K \quad \text{olduğu}$$

açıktır.

Yine $u_1, u_2 \in U_K$ ise $N(u_1) = \pm 1$ ve $N(u_2) = \pm 1$ dir. O halde $N(u_1 u_2) = N(u_1)N(u_2) = \pm 1$.

Yani $u_1 u_2 \in U_K$.

Birimsellerin kümesi çarpma işlemi altında grup özelliklerini sağladığı için bir grup oluşturur. Bu gruba K kuadratik sayı cisminin *birim grubu* adı verilir.

Teorem 2.18. (Adams ve Goldstein, 1976) $B > 1$ olmak üzere $1 < u < B$ şartını sağlayan sadece sonlu sayıda $u \in O_K$ vardır.

İspat: $u \in O_K$ bir birimsel olsun. O_K 'nın herhangi bir elemanı u 'nun, tamsayı katsayılı $X^2 - \text{Tr}(u)X + N(u) = 0$ denkleminin kökü olduğunu biliyoruz. u , birimsel olduğundan $N(u) = \pm 1$ 'dir, dolayısıyla;

$$X^2 - \text{Tr}(u)X \pm 1 = 0 \text{ 'dır. } u > 1, \quad N(u) = uu' = \pm 1 \Rightarrow |u'| = \left| \frac{1}{u} \right| < 1 \text{ 'dir.}$$

Böylece, $|\text{Tr}(u)| = |u + u'| \leq |u| + |u'| < B + 1$ 'dir.

Bu durumda $|a| \leq B + 1$ olmak üzere u , $X^2 + aX \pm 1 = 0$ denklem çiftinden birinin köküdür. Bu şekilde sadece sonlu sayıda denklem vardır ve bu denklemler kuadratik olduğundan her biri en fazla iki tane çözüme sahiptir. Dolayısıyla sadece sonlu sayıda $1 < u < B$ şartını sağlayan $u \in O_K$ vardır.

Bunu sağlayan sonlu sayıda eleman olduğundan bunların en küçüğünden rahatlıkla söz edebiliriz.

Tanım 2.21. O_K 'nın 1 'den büyük en küçük birimsel elemanına *temel birim* denir ve ε_K ile gösterilir.

Teorem 2.19. $d > 0$ ve $O_K = \{1, \omega_d\}$ olsun. Bu durumda;

$$U_K = \{\pm \varepsilon_K^n : n \in \mathbb{Z}\} \quad (2.16)$$

dir

İspat: $u \geq 1$ O_K 'nın bir birimseli olsun. $\varepsilon_K > 1$ olduğundan $n \rightarrow \infty$ iken $\varepsilon_K^n \rightarrow \infty$ dir. O halde $n \geq 0$ olacak şekilde $\exists n \in \mathbb{Z}$ bulunabilir öyle ki,

$$\varepsilon_K^n \leq u < \varepsilon_K^{n+1} \quad (2.17)$$

dir. (2.17) ile verilen eşitsizliğin her iki yanı ε_K^n ile bölünürse $1 \leq u\varepsilon_K^{-n} < \varepsilon_K$ elde edilir. Fakat ε_K 'nın tanımından onun 1 'den büyük en küçük birimsel olduğunu biliyoruz. O halde $u\varepsilon_K^{-n} = 1$ olmalıdır. Bu da $u = \varepsilon_K^n$ olduğunu gösterir.

Fakat başta $u \geq 1$ olduğunu kabul etmiştik. Aslında $u \in U_K$ ise $u, u^{-1}, -u, (-u)^{-1}$ den en az biri ≥ 1 olacağından $n \geq 0$ olmak üzere ε_K^n biçimindedir. Dolayısıyla bütün birimseller temel birimin tamsayı kuvvetlerinden oluşmaktadır.

Teorem 2.20. (Adams ve Goldstein, 1976) $d > 0$ ve $u = x + \omega_d y > 1$, O_K 'nin birimsel elemanı olmak üzere $d = 5$ ve $u = \frac{1+\sqrt{5}}{2}$ dışında $x > 0, y > 0$ dir.

İspat: $\omega_d - \omega_d' > 0$ 'dır. Ayrıca $N(u) = uu' = \pm 1 \Rightarrow u^{-1} = \pm u'$ olduğundan $u - u' = u \pm \frac{1}{u} > 0$

$$u - u' = (\omega_d - \omega_d')y > 0 \Rightarrow y > 0.$$

Diğer taraftan $u > 1$ ve $uu' = \pm 1$ olduğundan

$$|u'| = |x + \omega_d' y| < 1$$

Bununla birlikte $\omega_d' < 0$ olduğundan $x \neq 0$ ise $x > 0$ olmalıdır. Eğer $x = 0$ olsaydı $N(u) = \pm 1$ olduğu için $y^2 \omega_d \omega_d' = \pm 1$ olur. Ama (2.5)'teki tanımından dolayı $\omega_d \omega_d' = -d$ veya $(1-d)/4$ 'tür. $d > 1$ olduğundan birincisi mümkün değil. O halde $d \equiv 1 \pmod{4}$ 'tür. Eğer $d > 5$ ise $|y^2 \omega_d \omega_d'| > 1$ 'dir. Eğer $d = 5$ ve $y^2 = 1 \Rightarrow y = \pm 1$. Böylece $u > 1$ ve $u = \frac{1+\sqrt{5}}{2}$ 'dir.

Teorem 2.21. (Adams ve Goldstein, 1976) $d > 0$ olmak üzere $u = x + \omega_d y$, O_K 'nin bir birimsel elemanı olsun. $u > 1$ ve $x \neq 0$ olduğunu varsayalım. Bu durumda x , $-\omega_d' y$ irrasyonel sayısına en yakın tamsayıdır.

İspat: Teorem 2.20'de $x > 0, y > 0$ olduğunu gösterdik, x ve y tamsayı olduğundan $x \geq 1$, $y \geq 1$ 'dir. Ayrıca $\omega_d > 1$ olduğundan $x + \omega_d y > 2$ 'dir.

$$N(u) = uu' = \pm 1 \Rightarrow |u'| = \frac{1}{u} < \frac{1}{2} \text{ 'dir.}$$

$$u' = x + \omega_d' y \Rightarrow \left| x + \omega_d' y \right| < \frac{1}{2}. \quad (2.18)$$

Denlem (2.18) bize x tamsayısının $-\omega_d' y$ 'ye en yakın tamsayı olduğunu belirtmektedir. ω_d' 'nin tanımını kullanırsak aşağıdakini elde ederiz.

$$-\omega_d' y = \begin{cases} \sqrt{d} y, & d \equiv 2, 3(\text{mod } 4) \\ \frac{\sqrt{d}-1}{2} y, & d \equiv 1(\text{mod } 4) \end{cases} \quad (2.19)$$

tür.

Teorem 2.22. (Adams ve Goldstein, 1976) $d > 0$ ve $u = x + \omega_d y > 1$, O_K 'nin bir birimsel elemanı olsun. $n \geq 1$ olan her bir tamsayı için $u^n = x_n + \omega_d y_n$ yazarsak $0 < x = x_1 < x_2 < \dots$ ve $0 < y = y_1 < y_2 < \dots$.

İspat:

$$\begin{aligned} u^n &= uu^{n-1} = (x_1 + \omega_d y_1)(x_{n-1} + \omega_d y_{n-1}) \\ &= \begin{cases} (x_1 x_{n-1} + d y_1 y_{n-1}) + \omega_d (x_1 y_{n-1} + y_1 x_{n-1}), & d \equiv 2, 3(\text{mod } 4) \\ \left(x_1 x_{n-1} + \frac{d-1}{4} y_1 y_{n-1} \right) + \omega_d (x_1 y_{n-1} + y_1 x_{n-1} + y_1 y_{n-1}), & d \equiv 1(\text{mod } 4) \end{cases} \end{aligned}$$

Böylelikle x_n ve y_n için x_1, x_{n-1} ve y_1, y_{n-1} 'e bağlı olan bir formül elde ettik.

Teorem 2.21 ve 2.22'yi temel birimi belirlemek için kullanabiliriz, öyle ki x tamsayısı $-\omega_d' y$ 'ye en yakın tamsayı olmak üzere $y = 1, 2, 3, \dots$ için $x + \omega_d y$ 'leri hesaplarız. Normu ± 1 olan elde ettiğimiz ilk eleman aradığımız temel birimdir.

Aşağıdaki örnekte bu metodu kullanarak $K = \mathbb{Q}(\sqrt{34})$ kuadratik sayı cismindeki temel birimi belirledik. $y = 6$ için $x + \omega_d y$ 'nin normu 1 olduğu için 6. adımda temel birimi elde etmiş olduk.

Örnek 2.13. $K = \mathbb{Q}(\sqrt{34})$ olsun $d = 34 \equiv 2(\text{mod } 4) \Rightarrow \omega_d = \sqrt{34}$ 'tür. (2.19) kullanılırsa

$$-\omega_{34}' y = -\sqrt{34}' y = \sqrt{34} y$$

olduğu görülür. Buna göre çizelgeyi oluşturarak temel birimi belirleyebiliriz.

Çizelge 2.1 $K = \mathbb{Q}(\sqrt{34})$ 'de temel birimin hesaplanması

y	$-\omega_{34}' y = -\sqrt{34}' y = \sqrt{34}y$	x	$N(x + y\sqrt{34}) = x^2 - 34y^2$
1	5.83	6	2
2	11.66	12	8
3	17.49	17	-17
4	23.32	23	-15
5	29.15	29	-9
6	34.99	35	1

Böylelikle $K = \mathbb{Q}(\sqrt{34})$ cisminin temel birimini $\varepsilon_K = 35 + 6\sqrt{34}$ olarak elde etmiş olduk. O halde K 'nın birim grubunu (2.16) denklemini kullanarak;

$$U_K = \left\{ \pm (35 + 6\sqrt{34})^n : n \in \mathbb{Z} \right\}$$

olarak elde ederiz. Sırasıyla $n = 2, 3, 4, 5$ değerlerini alırsak her birinin normu bir olan,

$2449 + 420\sqrt{34}$, $171395 - 29394\sqrt{34}$, $11995201 + 2057160\sqrt{34}$, $839492675 + 143971806\sqrt{34}$ birimsellerini elde ederiz. Yine $n = -1, -2$, için de $35 - 6\sqrt{34}$, $2449 - 420\sqrt{34}$ biçiminde farklı birimseller elde edilir.

Fakat metodun işleyişinden anlaşılacağı üzere ne kadar büyük y değeri için temel birim elde edilmişse o kadar çok adımdan sonra sonuca varılmıştır. Reel kuadratik sayı cisimlerinin temel birimleri sık sık şaşırtıcı şekilde büyük olabilmektedir. Örneğin; $d = 2005$ için temel birim $\varepsilon_K = 197 + 9\frac{1 + \sqrt{2005}}{2}$ olmasına rağmen $d = 1999$ için $\omega = \omega_d$ daha önceden tanımlandığı gibi olmak üzere temel birim,

$4027701399389138208695911951306886478800 + 90084665203202024260494303744425250249\omega$ olarak elde edilmektedir. Kolayca görüleceği üzere böyle bir temel birimi elde etmede bu algoritma oldukça kullanışsızdır, çünkü bu temel birim bu yolla ancak

$90084665203202024260494303744425250249$. adımda hesaplanır. Bu tip temel birimlerin elde edilmesinde bu algoritmayı baz alarak yapılan programların bilgisayarda bile sonuçlanması oldukça uzun süre almaktadır. Çizelge 2.3'te kare-bağımsız $d = 1, \dots, 370$ değerleri için $\mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cisimlerinin temel birimlerinin listesi verilmiştir.

Aşağıdaki ε_K 'yı hesaplamak için vereceğim algoritma sürekli kesirler yöntemini kullanmaktadır. Bu yöntemle temel birimi büyük olan kuadratik sayı cisimlerinde temel birimin hesaplanması bilgisayar programlarıyla çok daha kısa sürede gerçekleştirilebilmektedir.

$K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cismi ve $\alpha_0 = \alpha = -\omega_d'$ olsun. Biz öncelikle α 'nın sürekli kesre açılımını $[a_0, \overline{a_1, \dots, a_m}]$ 'yi hesaplamak istiyoruz. Bunun için de $\forall n \geq 0$ için $a_n = \lfloor \alpha_n \rfloor$ ve $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$ olarak alalım. Burada her n için $a_n \geq 1$ 'dir. Bu prosedürü $\alpha_{m+1} = \alpha_1$ elde edene ve bu noktadan sonra da dizinin buraya kadar olan terimleri tekrar ettiğini görene kadar devam ettiririz.

Daha sonra α_n 'nin yakınsaklığını, yani;

$p_n / q_n = [a_0, a_1, \dots, a_n]$: $\text{ebob}(p_n, q_n) = 1$ ve $q_n \geq 1$ olacak şekilde p_n, q_n değerlerini

$$\begin{aligned} p_n &= p_{n-1}a_n + p_{n-2} \\ q_n &= q_{n-1}a_n + q_{n-2} \end{aligned} \tag{2.20}$$

formüllerini kullanarak ve Çizelge 2.2'nin benzeri oluşturarak hesaplarız.

Çizelge 2.2 Sürekli kesirler kullanılarak temel birimin bulunması

n	-2	-1	0	1	2	3	4
a_n			a_0	a_1	a_2	a_3	a_4
p_n	0	1					
q_n	1	0					

Bu durumda $K = \mathbb{Q}(\sqrt{d})$ 'nin temel birimi $\varepsilon_K = p_{m-1} + q_{m-1}\omega$ 'dur.

Teorem 2.23. (Mollin,1999)

$K = \mathbb{Q}(\sqrt{d})$ bir reel kuadratik sayı cismi, $\sqrt{d}$ 'nin periyot uzunluğu m ve $m-1$. yaklaşımı

$\frac{p}{q}$ olsun. Bu durumda;

$$\begin{cases} \varepsilon_K = p + q\sqrt{d}, & d \equiv 2,3(\bmod 4) \text{ veya } d \equiv 1(\bmod 8) \text{ ise} \\ \varepsilon_K = p + q\sqrt{d} \text{ veya } \varepsilon_K^{-3} = p + q\sqrt{d}, & d \equiv 5(\bmod 8) \text{ ise} \end{cases}$$

Ayrıca m çift ise $N(\varepsilon_K) > 0$, m tek ise $N(\varepsilon_K) < 0$ 'dır.

Tanım 2.22. $R = \log(\varepsilon_K)$ değerine $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cisminin regülatörü denir.

Sanal kuadratik sayı cisimlerinde $R = 1$ 'dir.

Çizelge 2.5'te reel kuadratik sayı cisimlerinin regülatörlerinin bir listesi verilmiştir.

Çizelge 2.3 Bazı reel kuadratik sayı cisimlerinin temel birimleri

$d = 1, 2, \dots, 370$ kare-bağımsız d ler için, $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cisimlerinde temel birimlerin, $(\varepsilon_K = a + b\omega_d)$ listesi.

d	ε_K	d	ε_K	d	ε_K
2	$1 + w$	73	$943 + 250 w$	149	$28 + 5 w$
3	$2 + w$	74	$43 + 5 w$	151	$1728148040 + 140634693 w$
5	w	79	$80 + 9 w$	154	$21295 + 1716 w$
6	$5 + 2 w$	77	$4 + w$	155	$249 + 20 w$
7	$8 + 3 w$	79	$80 + 9 w$	157	$98 + 17 w$
10	$3 + w$	82	$9 + w$	158	$7743 + 616 w$
11	$10 + 3 w$	83	$82 + 9 w$	159	$1324 + 105 w$
13	$1 + w$	85	$4 + w$	161	$10847 + 1856 w$
14	$15 + 4 w$	87	$28 + 3 w$	163	$64080026 + 5019135 w$
15	$4 + w$	89	$447 + 106 w$	165	$6 + w$
17	$3 + 2 w$	91	$1574 + 165 w$	166	$1700902565 + 132015642 w$
19	$170 + 39 w$	93	$13 + 3 w$	167	$168 + 13 w$
21	$2 + w$	94	$2143295 + 221064 w$	170	$13 + w$
22	$197 + 42 w$	95	$39 + 4 w$	173	$6 + w$
23	$24 + 5 w$	97	$5035 + 1138 w$	174	$1451 + 110 w$
26	$5 + w$	101	$9 + 2 w$	177	$57731 + 9384 w$
29	$2 + w$	102	$101 + 10 w$	178	$1601 + 120 w$
30	$11 + 2 w$	103	$227528 + 22419 w$	179	$4190210 + 313191 w$
31	$1520 + 273 w$	105	$37 + 8 w$	181	$604 + 97 w$
33	$19 + 8 w$	107	$962 + 93 w$	182	$27 + 2 w$
34	$35 + 6 w$	109	$118 + 25 w$	183	$487 + 36 w$
35	$6 + w$	110	$21 + 2 w$	185	$63 + 10 w$
37	$5 + 2 w$	111	$295 + 28 w$	186	$7501 + 550 w$
38	$37 + 6 w$	113	$703 + 146 w$	187	$1682 + 123 w$
39	$25 + 4 w$	114	$1025 + 96 w$	190	$52021 + 3774 w$
41	$27 + 10 w$	115	$1126 + 105 w$	191	$8994000 + 650783 w$
43	$3482 + 531 w$	118	$306917 + 28254 w$	193	$1637147 + 253970 w$
47	$48 + 7 w$	119	$120 + 11 w$	194	$195 + 14 w$
51	$50 + 7 w$	122	$11 + w$	195	$14 + w$
53	$3 + w$	123	$122 + 11 w$	197	$13 + 2 w$
55	$89 + 12 w$	127	$4730624 + 419775 w$	199	$16266196520 + 1153080099 w$
57	$131 + 40 w$	129	$15371 + 2968 w$	201	$478763 + 72664 w$
58	$99 + 13 w$	131	$10610 + 927 w$	202	$3141 + 221 w$
59	$530 + 69 w$	133	$79 + 15 w$	203	$57 + 4 w$
61	$17 + 5 w$	134	$145925 + 12606 w$	205	$20 + 3 w$
62	$63 + 8 w$	137	$1595 + 298 w$	206	$59535 + 4148 w$
65	$7 + 2 w$	139	$77563250 + 6578829 w$	209	$43331 + 6440 w$
66	$65 + 8 w$	141	$87 + 16 w$	210	$29 + 2 w$
67	$48842 + 5967 w$	142	$143 + 12 w$	211	$278354373650 + 19162705353 w$
69	$11 + 3 w$	143	$12 + w$	213	$34 + 5 w$
70	$251 + 30 w$	145	$11 + 2 w$	214	$695359189925 + 47533775646 w$
71	$3480 + 413 w$	146	$145 + 12 w$	215	$44 + 3 w$

d	ε_K	d	ε_K
215	44 + 3 w	291	290 + 17 w
217	3583111 + 521904 w	293	8 + w
218	251 + 17 w	295	2024999 + 117900 w
219	74 + 5 w	298	409557 + 23725 w
221	7 + w	299	415 + 24 w
222	149 + 10 w	301	10717 + 1311 w
223	224 + 15 w	302	4276623 + 246092 w
226	15 + w	303	2524 + 145 w
227	226 + 15 w	305	461 + 56 w
229	7 + w	307	88529282 + 5052633 w
230	91 + 6 w	309	2379 + 287 w
231	76 + 5 w	310	848719 + 48204 w
233	21639 + 3034 w	311	16883880 + 957397 w
235	46 + 3 w	313	119691683 + 14341370 w
237	36 + 5 w	314	443 + 25 w
238	11663 + 756 w	317	42 + 5 w
239	6195120 + 400729 w	318	107 + 6 w
241	66436843 + 9148450 w	319	12901780 + 722361 w
246	88805 + 5662 w	321	203 + 24 w
247	85292 + 5427 w	322	323 + 18 w
249	8011739 + 1084152 w	323	18 + w
251	3674890 + 231957 w	326	325 + 18 w
253	872 + 117 w	327	217 + 12 w
254	255 + 16 w	329	2245399 + 262032 w
255	16 + w	330	109 + 6 w
257	15 + 2 w	331	2785589801443970 + 153109862634573 w
258	257 + 16 w	334	63804373719695 + 3491219999244 w
259	847225 + 52644 w	335	604 + 33 w
262	104980517 + 6485718 w	337	960491695 + 110671282 w
263	139128 + 8579 w	339	97970 + 5321 w
265	5699 + 746 w	341	131 + 15 w
266	685 + 42 w	345	6397 + 728 w
267	2402 + 147 w	346	93 + 5 w
269	77 + 10 w	347	641602 + 34443 w
271	115974983600 + 7044978537 w	349	8717 + 986 w
273	683 + 88 w	353	67471 + 7586 w
274	1407 + 85 w	354	258065 + 13716 w
277	1228 + 157 w	355	954809 + 50676 w
278	2501 + 150 w	357	9 + w
281	1000087 + 126890 w	358	176579805797 + 9332532726 w
282	2351 + 140 w	359	360 + 19 w
283	138274082 + 8219541 w	362	19 + w
285	8 + w	365	9 + w
286	561835 + 33222 w	366	907925 + 47458 w
287	288 + 17 w	367	19019995568 + 992835687 w
290	17 + w	370	327 + 17 w

Çizelge 2.4 $d = 2, \dots, 32050$ için temel birimi küçük olan bazı $K = Q(\sqrt{d})$ reel kuadratik sayı cisimlerinde temel birimlerin örnek bir listesi.

d	ε_K	d	ε_K	d	ε_K	d	ε_K	d	ε_K
2	1+w	1226	35+w	5183	72+w	11237	105+2w	20735	144+w
3	2+w	1295	36+w	5185	71+2w	11663	108+w	20737	143+2w
5	w	1297	35+2w	5330	73+w	11665	107+2w	21026	145+w
10	3+w	1370	37+w	5477	73+2w	11882	109+w	21317	145+2w
15	4+w	1443	38+w	5626	75+w	12099	110+w	21610	147+w
17	3+2w	1522	39+w	5777	75+2w	12101	109+2w	21905	147+2w
26	5+w	1599	40+w	5930	77+w	12322	111+w	22202	149+w
35	6+w	1601	39+2w	6083	78+w	12543	112+w	22499	150+w
37	5+2w	1763	42+w	6085	77+2w	12545	111+2w	22501	149+2w
65	7+2w	1765	41+2w	6242	79+w	12770	113+w	22802	151+w
82	9+w	1937	43+2w	6401	79+2w	12995	114+w	23105	151+2w
101	9+2w	2026	45+w	6562	81+w	12997	113+2w	23410	153+w
122	11+w	2117	45+2w	6890	83+w	13226	115+w	23717	153+2w
143	12+w	2210	47+w	7055	84+w	13457	115+2w	24026	155+w
145	11+2w	2305	47+2w	7057	83+2w	14162	119+w	24335	156+w
170	13+w	2402	49+w	7226	85+w	14401	119+2w	24337	155+2w
195	14+w	2501	49+2w	7395	86+w	14642	121+w	24963	158+w
197	13+2w	2602	51+w	7397	85+2w	14885	121+2w	24965	157+2w
226	15+w	2703	52+w	7570	87+w	15130	123+w	25282	159+w
255	16+w	2705	51+2w	7743	88+w	15377	123+2w	25599	160+w
257	15+2w	2810	53+w	7745	87+2w	15626	125+w	25601	159+ 2w
290	17+w	2915	54+w	7922	89+w	15877	125+2w	25922	161+w
323	18+w	2917	53+2w	8099	90+w	16130	127+w	26243	162+w
362	19+w	3026	55+w	8101	89+2w	16383	128+w	26245	161+ 2w
399	20+w	3135	56+w	8282	91+w	16385	127+2w	26570	163+w
401	19+2w	3137	55+2w	8463	92+w	16642	129+w	26895	164+w
442	21+w	3363	58+w	8465	91+2w	16899	130+w	26897	163+ 2w
483	22+w	3365	57+2w	8835	94+w	16901	129+2w	27226	165+w
485	21+2w	3482	59+w	8837	93+2w	17162	131+w	27555	166+w
530	23+w	3599	60+w	9026	95+w	17423	132+w	27557	165+ 2w
577	23+2w	3601	59+2w	9215	96+w	17690	133+w	27890	167+w
626	25+w	3722	61+w	9217	95+2w	17957	133+2w	28562	169+w
677	25+2w	3845	61+2w	9410	97+w	18226	135+w	28901	169+ 2w
730	27+w	3970	63+w	9605	97+2w	18497	135+2w	29242	171+w
785	27+2w	4097	63+2w	10001	99+2w	18770	137+w	29585	171+ 2w
842	29+w	4226	65+w	10202	101+w	19043	138+w	29930	173+w
899	30+w	4355	66+w	10403	102+w	19045	137+2w	30277	173+ 2w
901	29+2w	4357	65+2w	10405	101+2w	19322	139+w	30626	175+w
962	31+w	4490	67+w	10610	103+w	19599	140+w	30977	175+ 2w
1023	32+w	4623	68+w	10815	104+w	19601	139+2w	31330	177+w
1090	33+w	4762	69+w	10817	103+2w	19882	141+w	31683	178+w
1155	34+w	4899	70+w	11026	105+w	20163	142+w	31685	177+ 2w
1157	33+2w	5042	71+w	11235	106+w	20165	141+2w	32042	179+w

Çizelge 2.5 Bazı $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cisimlerinin regülatörleri ($R = \log(\varepsilon_K)$).

d	R	d	R	d	R	d	R	d	R
2	0.8813736	74	4.454482	149	4.111143	221	2.703576	298	13.615979
3	1.316958	77	2.184644	151	21.963463	222	5.697082	299	6.721424
5	0.4812118	78	4.663350	154	10.659375	223	6.104788	301	10.032101
6	2.292432	79	5.075135	155	6.210596	226	3.402307	302	15.961821
7	2.768659	82	2.893444	157	5.361314	227	6.113677	303	8.526747
10	1.818446	83	5.099829	158	9.647692	229	2.712465	305	6.885509
11	2.993223	85	2.209348	159	7.881560	230	5.203976	307	18.991991
13	1.194763	86	9.943189	161	10.066881	231	5.023837	309	8.526153
14	3.400084	87	4.025033	163	18.668790	233	10.743156	310	14.344631
15	2.063437	89	6.907756	165	2.558979	235	4.521670	311	17.335017
17	2.094713	91	8.054523	166	21.947572	237	4.343637	313	19.351761
19	5.828937	93	3.366105	167	5.817102	238	10.057324	314	6.786718
21	1.566799	94	15.271002	170	3.259573	239	16.332420	317	4.488763
22	5.976344	95	4.356544	173	2.570815	241	18.771493	318	5.365954
23	3.870767	97	9.324383	174	7.973155	246	12.087345	319	17.066023
26	2.312438	101	2.998223	177	11.734836	247	12.046983	321	6.063780
29	1.647231	102	5.308243	178	8.071531	249	16.655035	322	6.470797
30	3.088970	103	13.028175	179	15.941409	251	15.810181	323	3.582746
31	8.019613	105	4.406570	181	7.173959	253	7.528869	326	6.476970
33	3.828168	106	8.988446	182	3.988641	254	6.234407	327	6.073039
34	4.248291	107	7.562161	183	6.881410	255	3.464758	329	15.374251
35	2.477889	109	5.564535	185	4.912709	257	3.466711	330	5.384474
37	2.491780	110	3.737102	186	9.615939	258	6.242219	331	36.256383
38	4.303882	111	6.380120	187	8.120886	259	14.342869	334	32.479990
39	3.911623	113	7.347300	190	11.552550	262	19.162433	335	7.096721
41	4.159127	114	7.625595	191	16.705215	263	12.536297	337	21.432116
42	3.256614	115	7.719574	193	15.076317	265	9.404591	339	12.185564
43	8.848509	118	13.327480	194	5.966140	266	7.222565	341	5.624004
46	10.792818	119	5.480622	195	3.330927	267	8.477204	345	9.512073
47	4.564240	122	3.093102	197	3.333478	269	5.099904	346	5.225776
51	4.605070	123	5.497151	199	24.205502	271	26.169788	347	14.064871
53	1.965720	127	16.062714	201	13.845254	273	7.282073	349	9.821192
55	5.181752	129	10.425550	202	8.745444	274	7.942362	353	11.867294
57	5.710416	130	4.736275	203	4.736121	277	7.868254	354	13.154114
58	5.288293	131	9.962699	205	3.760659	278	8.517593	355	14.462414
59	6.966023	133	5.153258	206	11.687467	281	14.570253	357	2.941657
61	3.664218	134	12.583995	209	11.441451	282	8.455743	358	26.590186
62	4.836219	137	8.157084	210	4.060146	283	19.437896	359	6.579249
65	2.776472	138	4.543182	211	27.045308	285	2.829735	362	3.638278
66	4.867475	139	18.859751	213	4.290272	286	13.932111	365	2.947198
67	11.489493	141	5.246996	214	27.960842	287	6.356105	366	14.412064
69	3.217272	142	5.655980	215	4.477208	290	3.527224	367	24.361904
70	6.218596	143	3.176313	217	15.855188	291	6.363025	370	6.483110
71	8.847935	145	3.179785	218	6.218604	293	2.836656	371	8.128585
73	7.666690	146	5.669869	219	4.997167	295	15.214227	373	9.233666

2.5 Bölümle İlgili Pari Komut ve Programları

`contfrac(x)`: x sayısının sürekli kesre açılımını bulur (Burada sx , rasyonel sayı, reel sayı veya rasyonel fonksiyon olabilir).

Örnek 2.14. `contfrac(sqrt(1327))` yazarak $\sqrt{1327}$ nin sürekli kesre açılımını bulabiliriz.

`core(n, {flag=0})`: n sıfırdan farklı bir tamsayı, d kare-bağımsız bir tamsayı ve $n = df^2$ biçiminde yazılabiliyorsa sonuç olarak d sayısını verir. Eğer **flag** değeri 1 alınırsa sonuçta f değeri de elde edilebilir. Buradan eğer n kare-bağımsız değilse $Q(\sqrt{n})$ kuadratik sayı cisminin aslında hangi kuadratik sayı cismi $Q(\sqrt{d})$ 'yi belirttiğini elde edebiliriz.

`coredisc(n, {flag=0})`: `core(n, {flag=0})` den farkı, sonuç olarak diskriminantı vermesidir.

`fibonacci(n)`: n . Fibonacci sayısını verir.

`isfundamental(d)`: d 'nin bir kuadratik sayı cisminin diskriminantı olup olmadığını bulur. Eğer d , bir kuadratik sayı cisminin diskriminantı ise 1, değilse 0 sonucunu verir.

Örnek 2.15. $375 \equiv 3 \pmod{4}$ olduğundan diskriminantı 375 olan bir kuadratik sayı cismi yoktur. Bunu `isfundamental(375)` ile görebiliriz. Ama, eğer `isfundamental(375*4)` yazılırsa sonucun 1 olacağı yani bunun bir diskriminant olacağı anlaşılır. Alında $375.4 = 1500$, $Q(\sqrt{375})$ reel kuadratik sayı cisminin diskriminantıdır.

`issquarefree(x)`: Verilen x sayısının kare-bağımsız olup olmadığını tespit eder.

`quaddisc(d)`: d kare-bağımsız bir tamsayı olmak üzere $Q(\sqrt{d})$ kuadratik sayı cisminin diskriminantını verir. Aynı diskriminantı bulmak için, nf ilerde belirteceğimiz sayı cisimleri hakkında bilgi veren komut olmak üzere, `nfdisc(nf)` de kullanılabilir. Aslında n kare-bağımsız değilse de komut çalışmaktadır. Bu durumda $n = s^2d$ biçiminde ve d kare-bağımsız olacak şekilde $Q(\sqrt{n})$ 'in denk olduğu $Q(\sqrt{d})$ kuadratik sayı cisminin diskriminantını verecektir.

Örnek 2.16. `quaddisc(17)`, `quaddisc(17*4)`, `quaddisc(17*25*16*36)` komutlarının hepsi $Q(\sqrt{17})$ kuadratik sayı cisminin diskriminantı 17 yi sonuç verecektir. Çünkü $Q(\sqrt{68})$ ve $Q(\sqrt{244800})$ aynı sayı cismi $Q(\sqrt{17})$ 'ye karşılık gelmektedir.

`quadgen(dk)`: $Q(\sqrt{d})$ kuadratik sayı cisminin de $\{1, \omega\}$, O_K 'nin tamlık tabanı olacak şekilde

Teorem 2.10’da elde ettiğimiz ω kuadratik sayısını oluşturur. Bundan sonra artık cisim içinde bu eleman kullanılarak çalışılabilir.

Örnek 2.17. $Q(\sqrt{517})$ de $517 \equiv 1 \pmod{4}$ olduğundan $\omega_{517} = \omega = \frac{1 + \sqrt{517}}{2}$ olmak üzere $\omega^3 - 11\omega^2 + 1$ işlemini yaptırmak için $w = \text{quadgen}(\text{quaddisc}(517))$; $w^3 - 11w^2 + 1$ yazmak yeterlidir. Sonucun $-1289 + 119w$ olduğunu görürüz. Yine $N(3 + 2\omega)$ yu hesaplatmak için $\text{norm}(3 + 2w)$ yazmak gerekir. Bunda da sonuç -501 çıkacaktır. $\frac{17 - 2\omega}{2 - 7\omega}$ işlemi için $(17 - 2w)/(2 - 7w)$ yazıldığında sonucun $1891/6331 - 115/6331w$ olduğu yani $\frac{1891}{6331} - \frac{115}{6331}\omega$ olduğu görülecektir.

Aşağıda verdiğim program bir sanal kuadratik sayı cisminde normu, belli bir pozitif tamsayı değerinden küçük olan bütün sayıları bulur. Fakat sonuçta çıkan kuadratik tamsayılardan bazıları birbirlerinin eşlenikleri olabilir. Yaptığım bu programı çalıştırmak için bu kodlar Pari’ye aktarıldıktan sonra $\text{normsinir}(d,m)$ kodunun girilmesi gerekir. Burada d değeri çalışılan $Q(\sqrt{d})$ kuadratik sayı cismini m değeri ise sınır değerini belirtmektedir. Aynı program reel kuadratik sayı cisimlerinde çalıştırıldığında bütün sonuçları vermeyecektir. Çünkü aynı norma sahip olan sonsuz tane kuadratik tamsayı olabileceği gibi reel kuadratik sayı cisimlerinde norm negatif değer de almaktadır.

```
{normsinir(d,m)=
local(i,j,w);\
w=quadgen(quaddisc(d));
for(i=0,round(sqrt(abs(m))),
for(j=0,round(sqrt(abs(m))),
if(norm(i+j*w)<m,print(norm(i+j*w)," ",i,"+",j," ",w," ",i,"-",j," ",w))))
}
```

$\text{quadpoly}(dk)$: d_K diskriminantlı kuadratik sayı cismine karşılık gelen x değişkenli minimal polinomu verir. Eğer $\text{quadpoly}(dk,v)$ biçiminde kullanılırsa polinom v değişkenli olarak elde edilir.

Örnek 2.18. $Q(\sqrt{42879873})$ kuadratik sayı cisminin minimal polinomunun $x^2 - x - 10719968$ olduğunu `quadpoly(42879873)` yazarak görebiliriz. Aşağıdaki program $d = 1, \dots, 100$ olan kare-bağımsız d ’ler için $Q(\sqrt{d})$ kuadratik sayı cisimlerinin minimal polinomlarını vermektedir.

```
for(i=2,100,if(issquarefree(i)==1,print(i," ",quadpoly(quaddisc(i))))))
```

Bu da aynı şeyi sanal kuadratik sayı cisimleri için yapar.

```
for(i=1,100,if(issquarefree(i)==1,print(-i," ",quadpoly(quaddisc(-i))))))
```

`quadregulator(dk)`: d_K diskriminantlı reel kuadratik sayı cisminin regülatörünü bulur. Eğer d , bir kuadratik sayı cisminin disriminantı değilse hata verir.

Örnek 2.19. Çizelge 2.5’i oluşturmak için,

```
for(i=2,200, if(issquarefree(i),\
write("regulator.doc",i," ",quadregulator(quaddisc(i))))))
```

kullanılmıştır. Burada sonuç, “regulator.doc” isimli Microsoft Word dokümanına yazılacaktır.

`quadunit(dk)`: d_K diskriminantlı reel kuadratik sayı cisminin temel birimini verir. Burada w yine Teorem 2.10’da belirttiğimiz kare-bağımsız d ’ye karşılık gelen ω_d ’yi belirtmektedir.

Örnek 2.20. $Q(\sqrt{2005})$ kuadratik sayı cisminin temel birimini belirlemek için `quadunit(quaddisc(2005))` komutunu kullandığımızda onun $197 + 9\omega$ olduğunu görürüz.

$2005 \equiv 1 \pmod{4}$ olduğundan $197 + 9\omega = 197 + 9 \frac{1 + \sqrt{2005}}{2}$ dir.

Çizelge 2.3’ü oluşturmak için aşağıdaki programı yazdım.

```
for(i=2,377,if(issquarefree(i)==1,\
write("temelbirimler.doc",i," ",quadunit(quaddisc(i))))))
```

Burada sonuçlar “temelbirimler.doc” isimli dokümana kaydedilecektir.

Daha önce, bazı kuadratik sayı cisimlerinde temel birimlerin d değerinin büyüklüğüne nazaran şaşırtıcı derecede büyük veya küçük olabileceğini belirtmiştim. Eğer d kare-bağımsız sayısı için $d - 1$ veya $d + 1$ den birisi tam kare ise $Q(\sqrt{d})$ kuadratik sayı cisminin

temel biriminin bileşenleri mutlak değer olarak oldukça küçük sayılardan oluşmaktadır. Aşağıdaki program $d = 500000, \dots, 505000$ değerlerine karşılık gelen bu tür temel birimleri hesaplamaktadır. Sonuçta bu aralıktaki kare-bağımsız d' lerden en azından

$d = 501263, 501265, 502682, 504101$ için temel birimlerin sırasıyla $708 + \omega, 707 + 2\omega, 709 + \omega, 709 + 2\omega$, şeklinde küçük sayılar olduğunu görmekteyiz.

```
for(i=500000,505000,if(issquarefree(i),\
if(issquare(i-1) || (issquare(i+1)),\
print(i,"",quadunit(quaddisc(i)),"",))))
```

Fakat bu değerlere inat `quadunit(quaddisc(500001))` komutuyla $\mathbb{Q}(\sqrt{500001})$ kuadratik sayı cisminin $a + b\omega$ biçimindeki temel biriminde bulunan a ve b 'deki toplam rakam sayısının 630 olduğunu görmekteyiz.

3. KUADRATİK SAYI CİSİMLERİNDE ÇARPANLARA AYIRMA ve İDEALLER

3.1 Tek Türlü Çarpanlara Ayrılabilme Özelliği Üzerine

Tanım 3.1. Sıfır bölensiz değişmeli ve birimsel elemanı olan halkaya tamlık bölgesi (TB) adı verilir

Özel olarak eğer, $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cismi ise, O_K bir tamlık bölgesidir.

Teorem 2.11’de O_K ’nın halka olduğunu ispatladık. Ayrıca O_K , çarpma işlemine göre değişmelidir. Birimsel elemanların varlığını da Teorem 2.15 ve Teorem 2.16’da ispatladık. $\alpha, \beta \in O_K$ için eğer $\alpha\beta = 0$ ise α veya β ’dan en az birinin sıfır olduğu açıktır. Eğer $\alpha\beta = 0$ ve $\alpha \neq 0 \Rightarrow \frac{1}{\alpha}(\alpha\beta) = \frac{1}{\alpha}\alpha\beta = 1 \cdot \beta = 0 \Rightarrow \beta = 0$, yani diğer çarpan sıfırdır. Bu da O_K ’nın sıfır bölensiz olduğunu gösterir. Böylelikle O_K tamlık bölgesidir. Bu da bize O_K da tamsayılardaki gibi bölünebilme, kongrüanslar, tek türlü çarpanlara ayrılabilen bölge gibi tanımlardan söz etme imkanı tanımaktadır.

Tanım 3.2. $\alpha, \beta \in O_K$ olmak üzere $\beta = \gamma\alpha$ olacak şekilde $\gamma \in O_K$ varsa α , β ’yi böler denir ve $\alpha|\beta$ şeklinde gösterilir, diğer durumda α , β ’yi bölmez denir ve $\alpha \nmid \beta$ şeklinde gösterilir.

Tanım 3.3. $\alpha, \beta, \gamma \in O_K$ olsun. $\alpha \equiv \beta \pmod{\gamma} \Leftrightarrow \gamma|\alpha - \beta$ dir. Bu durumda α ve β , modülo γ kongrüent (denk) tir denir.

O_K da bölünebilme ve kongrüanslar $\mathbb{Z}$ ’tekine benzer özelliklere sahiptirler.

Tanım 3.4. $u \in O_K$ olmak üzere $u|1 \Leftrightarrow u$ birimsel elemandır.

Tanım 3.5. $\alpha, \beta \in O_K$ olmak üzere, eğer $\alpha = u\beta$ olacak şekilde $u \in U_K$ var ise α ile β ilgilidir denir.

Örnek 3.1. $K = \mathbb{Q}(\sqrt{7})$ olmak üzere O_K ’da $-13 + 5\sqrt{7}$ ile $1 + \sqrt{7}$ elemanları ilgilidirler. Gerçekten bölme işlemi yapılırsa,

$$-13 + 5\sqrt{7} = (8 - 3\sqrt{7})(1 + \sqrt{7}) \quad (3.1)$$

elde edilir. Burada gösterilmesi gereken $8 - 3\sqrt{7}$ ’nin birimsel eleman olup olmadığıdır. Bunu göstermek için birimsel elemanın için verdiğimiz Tanım 3.4’ü kullanalım.

$$\frac{1}{8-3\sqrt{7}} = \frac{1}{8-3\sqrt{7}} \cdot \frac{8+3\sqrt{7}}{8+3\sqrt{7}} = \frac{8+3\sqrt{7}}{1} = 8+3\sqrt{7} \in O_K \Rightarrow 8-3\sqrt{7} \mid 1$$

dir. Yani $8-3\sqrt{7} \in U_K$ 'dır.

Teorem 3.1. $\alpha, \beta \in O_K$ ilgilidirler $\Leftrightarrow |N(\alpha)| = |N(\beta)|$.

İspat: α ile β ilgilidir $\Leftrightarrow \exists u \in U_K : \alpha = u\beta$.

$$\Rightarrow |N(\alpha)| = |N(u\beta)| = |N(u)N(\beta)| = |N(u)||N(\beta)| = 1 \cdot |N(\beta)| = |N(\beta)|.$$

Bu özelliği (3.1) eşitliğini pekiştirmek için kullanırsak $|N(-13+5\sqrt{7})| = 6 = |N(1+\sqrt{7})|$ şeklinde eşit normlar elde ederiz.

Teorem 3.2. $\alpha, \beta \in O_K$ olsun. Eğer $\alpha \mid \beta$ ise Z 'de $N(\alpha) \mid N(\beta)$ 'dır.

İspat: $\alpha \mid \beta \Rightarrow \exists \gamma \in O_K$ öyle ki $\beta = \gamma\alpha$ dir. O halde $N(\beta) = N(\gamma)N(\alpha)$,

$$N(\gamma), N(\alpha) \in Z \text{ olduğundan } N(\alpha) \mid N(\beta).$$

Fakat bu teoremin tersi her zaman doğru değildir. Yani $N(\alpha) \mid N(\beta)$ ise $\alpha \mid \beta$ olması gerekmez.

Örnek 3.2. $K = \mathbb{Q}(\sqrt{-2})$ olsun. $N(1+\sqrt{-2}) = 3$, $N(2+\sqrt{-2}) = 6$ 'dır. Burada $3 \mid 6$ olmasına rağmen $1+\sqrt{-2} \nmid 2+\sqrt{-2}$ dir, çünkü $\frac{2+\sqrt{-2}}{1+\sqrt{-2}} = \frac{4-\sqrt{-2}}{3} \notin O_K$ dir.

Teorem 3.2'nin doğal sonucu olarak $\alpha \in O_K$ 'nın muhtemel bölenleri, normları $N(\alpha)$ 'nın bölenleri arasında olan sayılar arasındadır diyebiliriz. Yine Teorem 3.2'nin karşıt tersi doğru olacağından, eğer $N(\alpha)$, $N(\beta)$ 'nın bir böleni değilse α 'da β 'nın bir böleni olamaz.

Tanım 3.6. $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cismi olmak üzere $\alpha \in O_K$ aşağıdaki şartları sağlıyorsa α 'ya indirgenemez eleman denir.

- $\alpha \neq 0$ ve $\alpha \notin U_K$,
- Eğer $\beta, \gamma \in O_K$ için $\alpha = \beta\gamma$ ise β veya γ birimseldir.

Örnek 3.3. $\alpha = 2 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ in indirgenemez olduğunu gösterelim. $\alpha \neq 0$ olduğu açıktır. Diğer yandan $N(\alpha) = N(2 + \sqrt{-5}) = 9 \neq \pm 1$ olduğundan α birimsel değildir. $\beta = x + y\sqrt{-5} \in O_K$ 'nin α 'nın bir böleni olduğunu varsayalım. O halde $N(\beta) \mid N(\alpha) = N(2 + \sqrt{-5}) = 9$ dur. $N(\beta) = x^2 + 5y^2 \geq 0$ olduğundan $N(\beta) = 1, 3$ ya da 9 olmalıdır.

$N(\beta) = 1 \Rightarrow \beta \in U_K$ ' dir.

$N(\beta) = 3 \Rightarrow x^2 + 5y^2 = 3$ olmalı, fakat bunu sağlayan $x, y \in \mathbb{Z}$ yoktur. Yani bu ihtimal mümkün değildir.

$N(\beta) = 9 \Rightarrow N\left(\frac{2 + \sqrt{-5}}{\beta}\right) = 1$ olacağı için $\frac{2 + \sqrt{-5}}{\beta} \in U_K$, dolayısıyla diğer çarpan birimseldir.

O halde $2 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ indirgenemezdir.

Not: Bir tamsayı herhangi bir kuadratik sayı cisminde indirgenemez olup başka birinde indirgenebilir olabilir. Örneğin 3, $\mathbb{Z}[\sqrt{-5}]$ 'te indirgenemezdir, fakat $\mathbb{Z}[\sqrt{3}]$ 'te $3 = \sqrt{3} \cdot \sqrt{3}$ şeklinde her biri birimsel elemandan farklı iki sayının çarpımı olarak çarpanlara ayrılabilirdiği için indirgenemez değildir.

Teorem 3.3. Eğer $|N(\alpha)| \in \mathbb{Z}$ asal ise $\alpha \in O_K$ indirgenemezdir.

İspat: $|N(\alpha)| = p$ ise $\alpha \neq 0$ olduğu açıktır. Bununla birlikte $|N(\alpha)| \neq \pm 1$ olacağı için α birimsel değildir. $\alpha = \pi\gamma$ şeklinde O_K da çarpanlara ayrıldığını varsayalım.

$$p = |N(\alpha)| = |N(\pi\gamma)| = |N(\pi)| |N(\gamma)|$$

dir. Fakat $p \in \mathbb{Z}$ 'nin pozitif bölenleri 1 ve p olduğundan ya $|N(\pi)| = 1$ dir ki bu da π 'nin birimsel olması demektir veya $|N(\gamma)| = 1$ 'dir, bu durumda da γ birimseldir. O halde ya π veya γ birimseldir. Yani $\alpha \in O_K$ indirgenemezdir.

Teorem 3.4. $K = \mathbb{Q}(\sqrt{d})$ bir kuadratik sayı cismi olsun. $\alpha \in O_K$, sıfırdan ve birimselden farklı bir eleman ise, $\pi_1, \pi_2, \dots, \pi_t \in O_K$ indirgenemez elemanlar olmak üzere $\alpha = \pi_1 \pi_2 \dots \pi_t$ şeklinde indirgenemez elemanların çarpımı olarak yazılabilir. Yani sıfırdan ve birimselden

farklı her bir cebirsel tamsayı bir takım indirgenemez elemanların çarpımı olarak yazılabilir.

İspat : $|N(\alpha)|$ üzerinde induksiyonla göstereceğiz. $\alpha \neq 0$ ve $\alpha \notin U_K$ olduğundan $|N(\alpha)| \geq 2$ 'dir. Eğer α 'nın kendisi indirgenemez ise $t = 1$ ve $\pi_1 = \alpha$ alırsak, bu durumda iddia doğrudur. α 'nın kendisi indirgenemez değilse $\pi_1, \pi_2 \in O_K$, $\pi_1, \pi_2 \notin U_K$ olmak üzere $\alpha = \pi_1 \cdot \pi_2$ yazabiliriz. $|N(\pi_1)|, |N(\pi_2)| > 1$ ve $|N(\alpha)| = |N(\pi_1)| |N(\pi_2)|$ olduğundan

$|N(\pi_1)|, |N(\pi_2)| < |N(\alpha)|$ dır. Burada $|N(\pi_1)| < |N(\pi_2)| < |N(\alpha)|$ olarak alabiliriz (Normu küçük olanı π_1 olarak aldık). $|N(\alpha)|, |N(\pi_1)|, |N(\pi_2)|, \dots$ tamsayıların azalan bir dizisi olduğu için bir π_n indirgenemez elemanı vardır çünkü $|N(\gamma)| = 0 \Leftrightarrow \gamma = 0$ dır. Fakat $\alpha_n | \alpha$ dır. Bunu α 'nın α_n 'e bölümünden elde edilen sayı ve aynı şekilde diğerleri için de sürdürürsek α 'nın birtakım indirgenemezlerin çarpımı olarak yazılabileceği sonucuna varırız.

Tanım 3.7. $K = \mathbb{Q}(\sqrt{d})$ olmak üzere eğer O_K aşağıdaki özellikleri sağlıyorsa O_K 'ya *tek türlü çarpanlara ayrılabilen bölge* denir ve kısaca TÇAB ile gösterilir.

i-) O_K 'nın sıfırdan ve birimsel elemandan farklı her bir elemanı birtakım indirgenemez elemanların çarpımı olarak yazılabilir.

ii-) $\pi_1, \pi_2, \dots, \pi_m, \delta_1, \delta_2, \dots, \delta_n$ 'den her biri indirgenemez elemanlar olmak üzere eğer,

$$\alpha = \pi_1 \cdot \pi_2 \dots \pi_m = \delta_1 \cdot \delta_2 \dots \delta_n \quad (3.2)$$

biçiminde iki türde çarpanlara ayrılıyorsa (3.2) denklemi için $m = n$ 'dir ve yeniden sıraya konulduğunda her i için $\pi_i = \delta_i$ olduğu görülür. Yani indirgenemez elemanların çarpımı olarak yazılışı tek türdür.

Diğer bir ifadeyle O_K 'nın elemanları için eğer aritmetiğin temel teoremi doğruysa O_K , TÇAB'dir.

Burada dikkat edilecek bir husus, eğer π indirgenemez ise $u \in U_K$ olmak üzere $\pi \cdot u$ 'nun indirgenemez olduğu ve π ile aynı indirgenemez eleman olarak kabul edilebileceğidir. Örneğin; π_1, π_2 indirgenemez elemanlar ise $\alpha = \pi_1 \cdot \pi_2 = (u\pi_1)(u^{-1}\pi_2)$ aslında α 'nın aynı parçalanışı olarak kabul edilir.

Bilindiği üzere $\mathbb{Z}$ bir TÇAB'dir. TÇAB olan kuadratik sayı cisimlerinin belirlenmesi öteden

beri cebirsel sayılar teorisi ile uğraşanların ilgisini çekmiştir. 1840'lı yıllara kadar çarpanlara ayrılmanın tek türlü olmayabileceği hiç hesaba katılmayan bir problemdir. Bu yüzden Fermat'ın son teoreminin ispatı üzerine iki meşhur çalışma, yazarları o yıllarda tek türlü çarpanlara ayrılmanın varlığını kesin kabul ettikleri için başarısızlıkla sonuçlanmıştır. Hala, reel kuadratik sayı cisimlerinin tamlık halkalarından TÇAB olanlarının sonsuz sayıda olup olmadığı henüz ispatlanmamış bir problemdir. Gauss sonsuz sayıda olduğunu iddia etmiştir, çeşitli hesaplamalar da bunun doğruluğuna dair ipuçları vermektedir. Örneğin; $d < 50$ için TÇAB olan reel kuadratik sayı cisimleri $d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29,$

$31, 33, 37, 38, 41, 43, 46, 47$ 'ye karşılık gelen $Q(\sqrt{d})$ 'lerdir. Sanal kuadratik sayı cisimlerinde durum daha belirgindir. Baker ve Stark 1967 de TÇAB olan sanal kuadratik sayı cisimlerinin sonlu sayıda olduğunu ve bunların $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ kare-bağımsız tamsayılara karşılık gelen sadece 9 tane sanal kuadratik sayı cismi $Q(\sqrt{d})$ 'den ibaret olduğunu ispatlayarak sanal kuadratik sayı cisimleri için bu problemin çözümünü tamamlamıştır, (Kato, Kurokawa, ve Saito, 2000). Gauss sınıf sayısı n problemi olarak bilinen ve belli bir sınıf sayısına sahip olan bütün sanal kuadratik sayı cisimlerinin elde edilmesini öngören problem üzerinde günümüze kadar epeyce çalışma yapılmıştır. Oesterle sınıf sayısı 3 problemini çözdükten sonra 1985 yılında Serre onun kullandığı metodu kastederek "Aynı metot 100 kadar bütün küçük değerler için çalışır" diye yazmıştır. Fakat 10 yıl sonra Wagner problemin 5,6,7 için çözümünden sonra 8 için o kadar kolay olmadığı sonucuna varmıştır. İlerleyen yıllarda bu değerler için de problem çözülmüştür.

Örnek 3.4. $K = Q(\sqrt{-6})$ alınırsa $O_K = Z[\sqrt{-6}]$ TÇAB değildir. Bunu göstermek için 10'un O_K 'daki;

$$10 = 5 \cdot 2 = (2 + \sqrt{-6})(2 - \sqrt{-6}) \quad (3.3)$$

parçalanışını ele alalım.

Burada 10'un iki farklı çarpanlara ayrılışı vardır. Bu çarpanlardan her biri indirgenemezdir ve sol taraftaki çarpanlarla sağ taraftaki çarpanların hiçbirisi birbirleriyle ilgili değildir.

Bu çarpanlardan 5'in indirgenemez olduğunu gösterelim. $5 = \alpha \cdot \beta$ olsun. $\alpha \in O_K$ olduğundan $\exists x, y \in \mathbb{Z} : \alpha = x + y\sqrt{-6}$. $\alpha | 5 \Rightarrow N(\alpha) | N(5) = 25$.

$$N(\alpha) = x^2 + 6y^2 \geq 0 \Rightarrow N(\alpha) = 1, 5 \text{ ya da } 25 \text{ olmalıdır.}$$

$$N(\alpha) = 1 \Rightarrow \alpha \in U_K \text{ 'dır.}$$

$N(\alpha) = 5$ olması mümkün değildir, çünkü $x^2 + 6y^2 = 5$ denkleminin tamsayı çözümleri yoktur.

$$N(\alpha) = 25 \Rightarrow N\left(\frac{5}{\alpha}\right) = 1 \text{ olacağı için } \beta = \frac{5}{\alpha} \text{ birimsel elemandır. Buradan } 5 \in O_K$$

indirgenemez elemandır. (3.3)'teki diğer çarpanlardan $2, 2 + \sqrt{-6}, 2 - \sqrt{-6}$ 'nın her birinin indirgenemez olduğu kolayca gösterilebilir. Diğer yandan,

$$\frac{2 \pm \sqrt{-6}}{5} \notin O_K \text{ olduğu için } 5 \text{ ne } 2 + \sqrt{-6} \text{ ile ne de } 2 - \sqrt{-6} \text{ ile ilgili olabilir. Aynı şekilde}$$

$$\frac{2 \pm \sqrt{-6}}{2} \notin O_K \text{ dır ve } 2 \text{ 'de bu elemanlarla ilgili değildir.}$$

Sonuç olarak $Z[\sqrt{-6}]$ 'da 10 'un iki farklı çarpanlara ayrılışının varlığını ispatlamış olduk. Dolayısıyla $Z[\sqrt{-6}]$ TÇAB değildir.

Aşağıdaki çizelge TÇAB olmayan O_K 'larda bu özelliği bozan elemanlardan örnekler içermektedir.

Çizelge 3.1 TÇAB olmayan tamlık halkası bazı $Z[\omega_d]$ 'lerde çarpanlara ayrılmanın tek türlü olmadığına dair örnekler (Stewart ve Tall, 2002)

d	Bir sayının $Z[\omega_d]$ 'de çarpanlara ayrılışı	d	Bir sayının $Z[\omega_d]$ 'de çarpanlara ayrılışı
10	$6 = 2.3 = (4 + \sqrt{10})(4 - \sqrt{10})$	-14	$15 = 3.5 = (1 + \sqrt{-14})(1 - \sqrt{-14})$
15	$10 = 2.5 = (5 + \sqrt{15})(5 - \sqrt{15})$	-15	$4 = 2.2 = ((1 + \sqrt{-15})/2)((1 - \sqrt{-15})/2)$
26	$10 = 2.5 = (6 + \sqrt{26})(6 - \sqrt{26})$	-17	$18 = 2.3.3 = (1 + \sqrt{-17})(1 - \sqrt{-17})$
30	$6 = 2.3 = (6 + \sqrt{30})(6 - \sqrt{30})$	-21	$22 = 2.11 = (1 + \sqrt{-21})(1 - \sqrt{-21})$
-5	$21 = 3.7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$	-22	$26 = 2.13 = (2 + \sqrt{-22})(2 - \sqrt{-22})$
-6	$55 = 5.11 = (1 + 3\sqrt{-6})(1 - 3\sqrt{-6})$	-23	$6 = 2.3 = ((1 + \sqrt{-23})/2)((1 - \sqrt{-23})/2)$
-10	$14 = 2.7 = (2 + \sqrt{-10})(2 - \sqrt{-10})$	-29	$30 = 2.3.5 = (1 + \sqrt{-29})(1 - \sqrt{-29})$
-13	$14 = 2.7 = (1 + \sqrt{-13})(1 - \sqrt{-13})$	-30	$34 = 2.17 = (2 + \sqrt{-30})(2 - \sqrt{-30})$

Tanım 3.8. $\alpha, \beta \in O_K$ olmak üzere aşağıdaki şartları sağlayan bir $\gamma \in O_K$ varsa buna α ile β 'nin *en büyük ortak böleni* denir ve kısaca $ebob(\alpha, \beta)$ şeklinde gösterilir.

i-) $\gamma | \alpha, \gamma | \beta$,

ii-) Eğer $\delta | \alpha, \delta | \beta$ şeklinde $\delta \in O_K$ varsa $\delta | \gamma$ dır.

Tamsayılardan farklı olarak bazen içinde çalışılan O_K 'ya göre iki elemanın ebob'u bulunmayabilir.

Teorem 3.5. $\alpha, \beta, \gamma \in O_K$ ve $ebob(\alpha, \beta) = \gamma$ ve $\lambda \in O_K$, γ ile ilgili bir eleman olsun. Bu durumda λ 'da α ile β 'nin bir *ebob*'udur.

İspat: $u \in U_K$ olmak üzere $\lambda = u\gamma$ dır. Eğer γ i,ii yi sağlıyorsa $u\gamma$ 'nın da bunları sağladığı açıktır. Dolayısıyla $u\gamma = \lambda$ 'da α ile β 'nin bir *ebob*'udur

Tanım 3.9. $\pi \in O_K$ aşağıdaki şartları sağlıyorsa π 'ye asal sayı denir.

i-) $\pi \neq 0$ ve $\pi \notin U_K$,

ii-) $\alpha, \beta \in O_K$ olmak üzere $\pi | \alpha\beta$ ise $\pi | \alpha$ veya $\pi | \beta$ dır.

Teorem 3.6. K bir kuadratik sayı cismi olmak üzere eğer $\pi \in O_K$ asal ise indirgenemezdir.

İspat: π asal ve $\alpha, \beta \in O_K$ olmak üzere $\pi = \alpha\beta$ olsun. π 'nin asallığından $\pi | \alpha\beta \Rightarrow \pi | \alpha$ ya da $\pi | \beta$ 'dir. Genelliği kaybetmeden $\pi | \alpha$ alalım. Diğer yandan $\alpha | \pi$ 'den dolayı $\beta = \frac{\pi}{\alpha}$ birimsel elemandır. Dolayısıyla π indirgenemezdir.

Bu teoremin tersi her zaman doğru değildir. Yani her indirgenemeyen asal olması gerekmez.

Örnek 3.5. $5 \in O_{Q(\sqrt{-6})}$ 'nin indirgenemez olduğunu gösterdik. Diğer yandan,

$5 | 10 = (2 + \sqrt{-6})(2 - \sqrt{-6})$ olduğu açıktır. Fakat $\frac{2 + \sqrt{-6}}{5}, \frac{2 - \sqrt{-6}}{5} \notin O_K$ olduğundan

$5 | 2 + \sqrt{-6}$ ve $5 | 2 - \sqrt{-6}$. Buradan 5'in, $O_{Q(\sqrt{-6})}$ 'da indirgenemez olduğu halde asal

olmadığı ortaya çıkar.

3.2 Euclid Bölgeleri

Tanım 3.10. Sıfırdan farklı her $\alpha \in O_K$ için $\phi(\alpha) \geq 0$ olacak şekilde aşağıdaki şartları sağlayan bir ϕ fonksiyonu varsa O_K 'ya *Euclid bölgesi* denir ve kısaca EB şeklinde gösterilir.

- Eğer $\alpha|\beta$ ise $\phi(\alpha) \leq \phi(\beta)$. (3.4)

- Eğer $\alpha\beta \neq 0$ ise $\exists \gamma, \delta \in O_K$ öyle ki $\alpha = \beta\gamma + \delta$ ve $0 \leq \phi(\delta) \leq \phi(\beta)$ dır. (3.5)

Tanım 3.11. Eğer O_K Euclid bölgesi ise K sayı cismi *Euclidsel*'dir denir.

$N(\alpha)$, Tanım 2.18 ile tanımladığımız norm fonksiyonu olmak üzere, (3.4) ve (3.5) şartlarını sağlamaya aday bir fonksiyon, $\phi(\alpha) = |N(\alpha)|$ fonksiyonudur, öyle ki;

$d < 0$ olmak üzere $K = \mathbb{Q}(\sqrt{d})$ sanal kuadratik sayı cismi için,

$$\phi: O_K \rightarrow \mathbb{N}, \phi(a + b\sqrt{d}) = |N(a + b\sqrt{d})| = a^2 + |d|b^2 \quad (3.6)$$

normu (3.4) şartını sağlayan çarpımsal bir normdur. $d > 0$ olduğunda ise $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cismi ve

$$\phi(a + b\sqrt{d}) = |N(a + b\sqrt{d})| = |a^2 - db^2| \quad (3.7)$$

normu yine (3.4) şartını sağlayan çarpımsal bir normdur.

O halde ϕ fonksiyonu (3.5) şartı sağlıyorsa O_K bir EB olmaktadır. Ama bu şart her zaman sağlanmayabilir.

Örnek 3.6. $K = \mathbb{Q}(\sqrt{3})$ olmak üzere O_K 'nın EB olup olmadığını araştıralım. K reel kuadratik sayı cismi olduğundan norm olarak (3.7) ile tanımlanan normu kullanacağız.

$\phi: O_K \rightarrow \mathbb{N}: \phi(a + b\sqrt{d}) = |a^2 - 3b^2|$ normu daha önce belirtildiği üzere (3.4)'ü sağlandığı açıktır. (3.5)'in sağlandığını gösterelim. Yani $\forall \alpha, \beta \in O_K$ için $\exists \gamma, \delta \in O_K$ bulmalıyız öyle ki $\alpha = \beta\gamma + \delta: \phi(\delta) < \phi(\beta)$ şartı sağlansın. Burada $\phi(\delta) < \phi(\beta)$ olduğunu göstermek yerine $\phi\left(\frac{\alpha}{\beta} - \gamma\right) < 1$ olduğunu da gösterebiliriz. Çünkü $\phi(\delta) = \phi(\beta)\phi\left(\frac{\alpha}{\beta} - \gamma\right) < \phi(\beta)$ 'dir. Yani bu

ikisi aynı şeydir. Diğer yandan $\frac{\alpha}{\beta} = \frac{\alpha\beta'}{\beta\beta'}$ ve $\beta\beta' \in \mathbb{Z}$ ve $\alpha\beta' \in O_K$ olduğundan,

$\frac{\alpha}{\beta} = x + y\sqrt{3} : x, y \in \mathbf{Q}$ şeklinde yazabiliriz. $m, n \in \mathbf{Z}$ olmak üzere $\gamma = m + n\sqrt{3}$ ise

$$\phi\left(\frac{\alpha}{\beta} - \gamma\right) = \left|N\left(\frac{\alpha}{\beta} - \gamma\right)\right| = |(x-m)^2 - 3(y-n)^2|. \quad (3.8)$$

Burada (3.8) ile verilen mutlak değer $(x-m)$ olabildiğince küçük ve $(y-n)$ olabildiğince büyük seçildiğinde en büyük değerini alır. m ile n yi sırasıyla x ile y 'ye en yakın tamsayılar olarak alırsak $(x-m)$ 'nin en küçük değeri 0, $(y-n)$ 'nin en büyük değeri ise $\frac{1}{2}$ olur. O

halde $\phi\left(\frac{\alpha}{\beta} - \gamma\right) = \left|N\left(\frac{\alpha}{\beta} - \gamma\right)\right| \leq \left|\frac{-3}{4}\right| < 1$ 'dir.

Dolayısıyla (3.5) şartı da sağlanıyor. Yani $\mathbf{Z}[\sqrt{3}]$ EB'dir.

Örnek 3.7. $K = \mathbf{Q}(\sqrt{-3})$ olsun. Şimdi K sayı cismi sanal kuadratik sayı cismidir. O halde (3.6) ile verilen normu kullanabiliriz.

$$\phi : O_K \rightarrow N : \phi\left(a + b\frac{1+\sqrt{-3}}{2}\right) = \left(a + \frac{b}{2}\right)^2 + \left(\frac{\sqrt{-3}}{2}b\right)^2 = a^2 + ab + b^2,$$

çarpımsal norm özelliklerini taşımaktadır. $\alpha, \beta \in O_K$, $\beta \neq 0$ olmak üzere Örnek 3.6'dakine

benzer şekilde $\frac{\alpha}{\beta} = s + t\frac{1+\sqrt{-3}}{2} : s, t \in \mathbf{Z}$ yazabiliriz. m ve n sırasıyla s, t ye en yakın tam sayılar olarak alınırsa

$$|m-s| \leq \frac{1}{2}, |n-t| \leq \frac{1}{2} \text{ olur ve}$$

$$\phi\left(\frac{\alpha}{\beta} - \gamma\right) = (s-m)^2 - (s-m)(t-n) + (t-n)^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1 \text{ 'dir.}$$

(3.5) şartı da sağlanmaktadır. Dolayısıyla $\mathbf{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ bir Euclid bölgesidir. Bu iki örnekte

de tamlık halkası O_K 'yı EB yapan şey kompleks düzlemde herhangi bir noktanın O_K 'nın bir elemanına uzaklığının bir norm vasıtasıyla 1 birimden daha küçük olmasıdır.

Sanal kuadratik sayı cisimlerinden sadece 5 tanesi Euclidsel'dir. Bunlar

$d = -1, -2, -3, -7, -11$ için $\mathbb{Q}(\sqrt{d})$ 'lerdir. Reel kuadratik sayı cisimlerinden hangilerinin Euclidsel oldukları sorusu 20. yüzyılda değişik matematikçilerin çalışmalarıyla çözülmüştür. Dickson $d = 2, 3, 5, 13$ için $\mathbb{Q}(\sqrt{d})$ 'nin Euclidsel olduğunu ispatladı, Peron bunlara 6, 7, 11, 17, 21, 29 u ekledi, Oppenheimer, Remak ve Redei 19, 33, 37, 41, 55, 73 ü de kattı. Heilbronn 1934'te listenin sonlu olduğunu ispatladı. Hangi kuadratik sayı cisimlerinin EB olduğu son olarak Swinnerton-Dyer'ın çalışmasıyla 1952 yılında tamamlanmıştır. Özet olarak aşağıdaki teorem hangi kuadratik sayı cisimlerinin EB olduğunu açıklamaktadır.

Teorem 3.7. $d = -1, \pm 2, \pm 3, 5, 6, \pm 7, \pm 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$ için $K = \mathbb{Q}(\sqrt{d})$ norm-Euclidsel'dir.

Clark $\mathbb{Q}(\sqrt{69})$ kuadratik sayı cisminin norm-Euclidsel olmadığını fakat O_K 'nin EB olduğunu göstermiştir. Bu örnek norm-Euclidsel olmayan ama Euclidsel olan kuadratik sayı cismine ilk örnektir.

Daha önce değinildiği üzere, TÇAB olup EB olmayan kuadratik sayı cisimleri de mevcuttur. Sanal kuadratik sayı cisimlerinde sadece sonlu sayıda d için ($d = -19, -43, -67, -163$) $K = \mathbb{Q}(\sqrt{d})$, TÇAB olduğu halde EB değildir. Fakat reel kuadratik sayı cisimleri için aynı şey söylenemez. Bu tür reel kuadratik sayı cisimlerinin sayısının sonlu veya sonsuz olduğu henüz ispatlanmamıştır.

Euclid Bölgesi olan O_K 'larda Euclid algoritmasını tamsayılarda kullandığımız gibi bölme algoritmasında kullanabiliriz. Mesela onunla iki elemanın eleman'ın ebob'larını bulabiliriz.

Örnek 3.8. $\mathbb{Z}[\sqrt{2}]$ de Euclid algoritmasını kullanarak $\text{ebob}(5 + 4\sqrt{2}, 2 + \sqrt{2})$ yi hesaplayalım.

$$\frac{5 + 4\sqrt{2}}{2 + \sqrt{2}} = \frac{(5 + 4\sqrt{2})(2 - \sqrt{2})}{2} = \frac{10 - 5\sqrt{2} + 8\sqrt{2} - 8}{2} = \frac{2 + 3\sqrt{2}}{2} \notin O_K. \quad O_K \text{ 'da buna en yakın}$$

eleman olarak $1 + \sqrt{2}$ yi alabiliriz. O halde $\frac{5 + 4\sqrt{2}}{2 + \sqrt{2}} = (1 + \sqrt{2}) + \frac{1}{2}\sqrt{2}$. Böylelikle

$$5 + 4\sqrt{2} = (1 + \sqrt{2})(2 + \sqrt{2}) + \frac{1}{2}\sqrt{2}(2 + \sqrt{2}) = (1 + \sqrt{2})(2 + \sqrt{2}) + 1 + \sqrt{2}$$

Burada dikkat edilirse,

$$|N(1 + \sqrt{2})| = 1 < 2 = |N(2 + \sqrt{2})|.$$

Bölmede kalan 0 'dan farklı olduğundan bölmeye devam ediyoruz.

$$\frac{2 + \sqrt{2}}{1 + \sqrt{2}} = \frac{(2 + \sqrt{2})(1 - \sqrt{2})}{-1} = \frac{2 - 2\sqrt{2} + \sqrt{2} - 2}{-1} = -\frac{\sqrt{2}}{-1} = \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

$2 + \sqrt{2} = \sqrt{2}(1 + \sqrt{2}) + 0$, yani kalan $\delta = 0$. O halde burada bölme algoritmasını kesiyoruz. Tamsayılarda olduğu gibi sıfır olmayan en son bölen ebob olarak alınır. Yani $\text{ebob}(5 + 4\sqrt{2}, 2 + \sqrt{2}) = 1 + \sqrt{2}$.

Aslında $N(1 + \sqrt{2}) = -1$ olduğundan $1 + \sqrt{2}$ birimseldir. Dolayısıyla bu iki eleman aralarında asaldır. Öte yandan ebob olarak bulunan elemanla ilgili olan bütün elemanlar ebob olarak alınabilir.

Burada $O_K = \mathbb{Z}[\sqrt{2}]$ EB olduğu için bölme algoritmasını uygulayarak sonuca ulaşabildik. Fakat, eğer O_K EB değilse benzer algoritmayla sonuca varmamız mümkün değildir. Örneğin

$$\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{3}\right] \text{ tek TÇAB olmasına rağmen, EB değildir ve benzer bir bölme algoritması}$$

yoktur. Maple programı EB olan tamlık halkalarında aritmetiği oldukça kolaylaştıran kodlara sahiptir. Bunlar Bölüm 3.6'da tanıtılmıştır.

3.3 Kuadratik sayı Cisimlerinin İdealleri

O_K 'nın halka olduğunu Teorem 2.11 ile gösterdik. Dolayısıyla onun ideallerinden söz etmek mümkündür. O_K 'nın ideallerini $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cismindeki en genel tamsayılar olarak düşünebiliriz. İdeal toplam ve çarpımını kullanarak $\mathbb{Z}$ 'teki aritmetiğin benzerini O_K 'nın idealleri arasında inşa edebiliriz. O_K da her zaman tek türlü asal çarpanlara ayrılma özelliğinin olmayabileceğini daha önce belirttik. Kummer 1847 de ideal sayıları keşfetti ve bunların tamlık halkaları ile ilişkileri ve aritmetiği üzerinde çalıştı. Dedekind, Kummer'ın ideal sayılarını yaklaşık 40 yıl sonra daha da geliştirdi ve isim olarak ideal sayılar yerine ideal terimini kullandı. Bu çalışmalar O_K 'da ki tek türlü çarpanlara ayrılma özelliğinin eksikliğini O_K 'nın ideallerini kullanarak kapatmayı sonuç verdi. Bu bölümün sonunda herhangi bir O_K için bir idealin asal ideallere parçalanışının tek türlü olduğu görülecektir. Böylelikle O_K 'daki sayılar üzerindeki aritmetik yerine daha avantajlı olduğu için O_K 'nın idealleri üzerinde aritmetiği irdelleyeceğiz.

Tanım 3.12. Boştan farklı $\alpha \subseteq O_K$ aşağıdaki şartları sağlıyorsa α ya O_K 'nin *ideali* denir.

$$\text{i-)} \forall \alpha, \beta \in \alpha \text{ için } \alpha \pm \beta \in \alpha \quad (3.9)$$

$$\text{ii-)} \forall \alpha \in \alpha, \forall \gamma \in O_K \text{ için } \alpha \cdot \gamma \in \alpha \quad (3.10)$$

O_K 'nin ideallerini genel kullanıma uyarak $\alpha, \mathbf{b}, \mathbf{p}, \mathbf{q} \dots$ gibi Gothic karakterlerle göstereceğiz. $\{0\}$ ve $(1) = O_K$ idealleri O_K 'nin *aşıkâr idealleri* diye isimlendirilir. Bu iki ideal dışındaki ideallere öz idealler adı verilir.

Örnek 3.9. $K = \mathbb{Q}(\sqrt{-6})$ kuadratik sayı cismini ele alalım. $O_K = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$ halkasının bir ideali

$\alpha = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}, a = 2t, t \in \mathbb{Z}\} = \{2t + b\sqrt{-6} : t, b \in \mathbb{Z}\}$ dir. α 'nın O_K 'nin bir alt grubu olduğu açıktır, (3.9) sağlanmaktadır. Diğer taraftan,

$$\beta = 2t + b\sqrt{-6} \in \alpha, \gamma = m + n\sqrt{-6} \in O_K \text{ için}$$

$\gamma\beta = (m + n\sqrt{-6})(2t + b\sqrt{-6}) = 2(tm - 3nb) + (mb + 2tn)\sqrt{-6} \in \alpha$ dır. Dolayısıyla (3.10)' da sağlanmaktadır, böylece α , O_K 'nin bir idealidir. Bu ideal 2 ve $\sqrt{-6}$ tarafından üretilmiştir. Yani $\alpha = (2, \sqrt{-6})$ dır.

Eğer $\alpha_1, \alpha_2, \dots, \alpha_r \in O_K$ ise $\alpha_1, \alpha_2, \dots, \alpha_r$ tarafından üretilen $(\alpha_1, \alpha_2, \dots, \alpha_r)$ ideali α_i lerin O_K -lineer kombinasyonundan oluşan kümedir, yani;

$$(\alpha_1, \alpha_2, \dots, \alpha_r) = \{\alpha_1\beta_1 + \alpha_2\beta_2 + \dots + \alpha_r\beta_r : \beta_1, \beta_2, \dots, \beta_r \in O_K\}. \quad (3.11)$$

(3.11) ile verilen ideal $\alpha_1, \alpha_2, \dots, \alpha_r$ lerin en büyük ortak bölenleri olarak hesaba katılır.

Genel olarak K bir sayı cismi ve $|K : \mathbb{Q}| = n$ olmak üzere α idealinin $\{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq O_K$ ve $r \leq n$ olacak şekilde bir $\mathbb{Z}$ -tabanı vardır. Burada α_i 'lere α 'nın üreteçleri denir. Eğer değişmeli ve birimli bir halkada α idealinin sonlu sayıda üretici varsa α 'ya sonlu üretilmiş ideal denir, (Stewart ve Tall, 2002). O halde eğer K , kuadratik sayı cismi ise $|K : \mathbb{Q}| = 2$ olacağı için O_K 'nin idealleri en fazla iki eleman tarafından üretilir.

Tanım 3.13. Eğer O_K 'nin herhangi bir ideali bir tek eleman tarafından üretiliyorsa bu ideale *temel (esas) ideal* adı verilir.

$(\alpha) = \{\alpha\beta : \beta \in O_K\}$ ideali O_K 'nin α tarafından üretilen temel idealidir.

Bilindiği gibi tamsayıların her ideali bir temel idealdir. O_K 'nin idealleri için bu her zaman doğru değildir. İlk olarak Dedekind, birtakım ideallerin cisim genişlemelerinde temel ideal olduğunu fark etti.

Örnek 3.10. Örnek 3.9'da ele aldığımız $\alpha = (2, \sqrt{-6})$ ideali temel ideal değildir. Çünkü eğer α temel ideal olsaydı $\alpha = (\alpha)$ olacak şekilde $\alpha \in O_K$ bulunabilirdi.

$2 \in \alpha$ ve $\sqrt{-6} \in \alpha \Rightarrow \alpha | 2$ ve $\alpha | \sqrt{-6} \Rightarrow N(\alpha) | N(2) = 4$ ve $N(\alpha) | N(\sqrt{-6}) = 6$ 'dır. Bu ikisi birleştirilirse;

$$N(\alpha) = \mp 1, \mp 2 \quad (3.12)$$

elde edilir. $\alpha = a + b\sqrt{-6}$ biçiminde olduğu göz önüne alınırsa (3.1) yerine daha açık olan

$$\Rightarrow N(\alpha) = a^2 + 6b^2 = \mp 1, \mp 2 \quad (3.13)$$

denklemini yazılabilir. (3.13) denkleminin çözümleri $a = \mp 1, b = 0$ 'dır. Dolayısıyla $\alpha = \mp 1$ 'dir. Fakat bu da $\mp 1 \notin \alpha$ ile çelişir. Bu durumda $\alpha = (2, \sqrt{-6}) = (\alpha)$ şeklinde yazılamaz. Yani α temel ideal olamaz. Fakat $\alpha = (2, \sqrt{-5})$ ideali $O_K = \mathbb{Z}[\sqrt{-5}]$ e eşit olan bir temel idealdir. Çünkü, $1 = 2 \cdot 3 + \sqrt{-5}\sqrt{-5}$ olduğundan 2 ve $\sqrt{-5}$ in bir O_K - lineer kombinasyonudur. Diğer yandan idealin tanımından dolayı, idealler O_K çarpma işlemene göre de kapalı olduğundan ve O_K 'nin her bir elemanı 1 in bir katı olduğundan $(2, \sqrt{-5}) = (1) = O_K$.

Yine $\mathbb{Z}[\sqrt{-5}]$ 'te $(29, 13 - \sqrt{-5})$ ideali $(3 + 2\sqrt{-5})$ tarafından üretilen temel idealdir. Tanım 3.13'ten $(3 + 2\sqrt{-5})$ idealinin $3 + 2\sqrt{-5}$ in katlarından oluşan küme olduğu açıktır. $(29, 13 - \sqrt{-5}) \subseteq (3 + 2\sqrt{-5})$ olduğunu göstermek için $3 + 2\sqrt{-5}$ in hem 29 u hem de $13 - \sqrt{-5}$ i böldüğünü göstermemiz gerekir. Aşağıda (3.14) ile verilen eşitlikler bunu açıkça göstermektedir;

$$\begin{aligned} 29 &= (3 + 2\sqrt{-5})(3 - 2\sqrt{-5}), \\ 13 - \sqrt{-5} &= (3 + 2\sqrt{-5})(1 - \sqrt{-5}). \end{aligned} \quad (3.14)$$

Diğer yandan $(3 + 2\sqrt{-5}) \subseteq (29, 13 - \sqrt{-5})$ olduğunu göstermek için $3 + 2\sqrt{-5}$ 'in

29 ve $13 - \sqrt{-5}$ 'in lineer kombinasyonu olarak yazılıp yazılmayacağını kontrol etmek yeterlidir. Gerçekten $3 + 2\sqrt{-5} = 29.1 + (13 - \sqrt{-5})(-2)$ şeklinde lineer kombinasyonları olarak yazılabilmektedir. Buradan ayrıca 29 ile $13 - \sqrt{-5}$ 'in ebob'larının $3 + 2\sqrt{-5}$ olduğu da görülmektedir.

Sonuç olarak $(29, 13 - \sqrt{-5}) = (3 + 2\sqrt{-5})$ temel idealdir.

Tanım 3.14. $\mathfrak{a}$ ve $\mathfrak{b}$, O_K 'nin iki ideali olmak üzere bunların *toplamı* ve *çarpımı* sırasıyla aşağıdaki gibidir,

$$\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\},$$

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

Görüldüğü gibi ideallerin toplamı gerçekte ideallerin elemanlarının toplamıdır. Aslında $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_r)$, $\mathfrak{b} = (\beta_1, \beta_2, \dots, \beta_s)$ ise $\mathfrak{a} + \mathfrak{b} = (\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \beta_2, \dots, \beta_s)$ 'tir ve özel olarak $\mathfrak{a} = (\alpha)$, $\mathfrak{b} = (\beta)$ şeklinde her ikisi de temel ideal iseler $\mathfrak{a} + \mathfrak{b} = (\alpha, \beta)$ 'dir. Eğer $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha_r)$, $\mathfrak{b} = (\beta_1, \beta_2, \dots, \beta_s)$ ise $\mathfrak{a}\mathfrak{b}$, $1 \leq i \leq r$ ve $1 \leq j \leq s$ olmak üzere $\alpha_i \beta_j$ çarpımları tarafından üretilen idealdir. Özel olarak eğer, $\mathfrak{a} = (\alpha)$, $\mathfrak{b} = (\beta)$ ise $\mathfrak{a}\mathfrak{b} = (\alpha\beta)$ 'dir. Burada verilen ideallerin çarpma ve toplama işlemine göre, iki idealin çarpımı ve toplamının da yine bir ideal olduğu açıktır. Ayrıca ideallerin çarpımı değişme ve birleşme özelliklerine sahiptir.

Tanım 3.15. O_K 'nin *birim ideali* $(1) = (1, \omega) = O_K$ 'dir.

O_K 'nin her $\mathfrak{a}$ ideali için $(1)\mathfrak{a} = \mathfrak{a}(1) = \mathfrak{a}$ olduğu açıktır.

Tanım 3.16. $\mathfrak{a}$, O_K 'nin bir ideali olsun. $\mathfrak{a}' = \{\alpha' : \alpha \in \mathfrak{a}\}$ 'de bir idealdir ve bu ideale $\mathfrak{a}$ idealinin *eşleniği* adı verilir.

Örnek 3.11. $\mathfrak{a} = (11, 4 - \sqrt{-6})$ ise $\mathfrak{a}' = (11, 4 + \sqrt{-6})$ 'dir. Tanım 3.14'ü kullanırsak

$$\mathfrak{a}\mathfrak{a}' = (11, 4 - \sqrt{-6})(11, 4 + \sqrt{-6}) = (121, 11(4 + \sqrt{-6}), 11(4 - \sqrt{-6}), 22)$$

$= (11)(11, 4 + \sqrt{-6}, 4 - \sqrt{-6}, 2)$ 'dir. Diğer yandan $(11, 4 + \sqrt{-6}, 4 - \sqrt{-6}, 2) = (1) = O_K$.

Çünkü $1 = 11 - 5.2$ ve $\sqrt{-6} = 4 + \sqrt{-6} - 2.2$ 'dir.

Dolayısıyla $\mathfrak{a}\mathfrak{a}' = (11)$ 'dir.

Teorem 3.8. [Hurwitz Lemması]: $\alpha, \beta \in O_K$ ve $m \in N$ olsun. Eğer

$m|N(\alpha), m|N(\beta), m|Tr(\alpha\beta')$ şartları sağlanıyorsa $m|\alpha\beta'$ ve $m|\alpha'\beta$ 'dir.

İspat: $\gamma = \frac{\alpha\beta'}{m}$ alalım. $\gamma' = \frac{\alpha'\beta}{m}$ olur. Bu durumda;

$$\gamma + \gamma' = \frac{Tr(\alpha\beta')}{m} \in \mathbb{Z} \text{ ve } \gamma\gamma' = \frac{N(\alpha)}{m} \cdot \frac{N(\beta)}{m} \in \mathbb{Z} \quad (3.15)$$

tir. (3.15)'ten $N(\gamma), Tr(\gamma) \in \mathbb{Z}$ 'dir. γ 'nın normu ve iz'i tamsayı oldukları için

$\gamma = \frac{\alpha\beta'}{m} \in O_K$ 'dir. Yani $m|\alpha\beta'$. Benzer şekilde $\gamma' = \frac{\alpha'\beta}{m} \in O_K \Rightarrow m|\alpha'\beta$ 'dir.

Teorem 3.9. O_K 'nın sıfırdan farklı bir α ideali verilsin. Bu durumda $\alpha\alpha' = aO_K$ olacak şekilde $a \in \mathbb{Z}$ vardır.

İspat: O_K 'nın her bir ideali en fazla iki eleman tarafından üretildiği için $\alpha = (\alpha, \beta)$ olacak şekilde $\alpha, \beta \in O_K$ vardır. $\alpha' = (\alpha', \beta')$ olur. Bu durumda Tanım 3.14'ten $\alpha\alpha' = (\alpha\alpha', \alpha\beta', \alpha'\beta, \beta\beta') = (N(\alpha), N(\beta), \alpha\beta', \alpha'\beta)$ (3.16)

olur. Eğer $a = \text{ebob}(N(\alpha), N(\beta), Tr(\alpha\beta')) \in \mathbb{Z}$ alırsak Teorem 3.8'den $\frac{\alpha\beta'}{m}, \frac{\alpha'\beta}{m} \in O_K$ olduğu

için (3.16) yerine

$$\alpha\alpha' = (a) \left(\frac{N(\alpha)}{a}, \frac{N(\beta)}{a}, \frac{\alpha\beta'}{a}, \frac{\alpha'\beta}{a} \right) \quad (3.17)$$

yazabiliriz. Burada $\alpha\alpha' = (a)$ olduğunu göstermek için (3.17) nin sol tarafındaki ikinci

çarpanın 1'i içerdiğini yani $1 \in \left(\frac{N(\alpha)}{a}, \frac{N(\beta)}{a}, \frac{\alpha\beta'}{a}, \frac{\alpha'\beta}{a} \right)$ olduğunu göstermek gerekir.

$\text{ebob}\left(\frac{N(\alpha)}{a}, \frac{N(\beta)}{a}, \frac{Tr(\alpha\beta')}{a}\right) = 1$ olduğu için $1, \frac{N(\alpha)}{a}, \frac{N(\beta)}{a}$ ve $\frac{Tr(\alpha\beta')}{a}$, nin $\mathbb{Z}$ -lineer

kombinasyonu olarak yazılabilir. Dolayısıyla $\frac{N(\alpha)}{a}, \frac{N(\beta)}{a}$, ve $\frac{\alpha\beta'}{a} + \frac{\alpha'\beta}{a}$, yı 1'in O_K -lineer

kombinasyonu olarak yazabiliriz. Bu da $\alpha\alpha' = (a)(1) = (a)$ olduğunu gösterir.

Tanım 3.17. O_K 'nın sıfırdan farklı bir α idealinin *normu* $N(\alpha) = |O_K / \alpha|$ 'dir.

Teorem 3.10. (Stewart ve Tall, 2002)

d_K , K kuadratik sayı cisminin diskriminantı olmak üzere $\alpha \neq 0$ idealinin Z -tabanı $\{\alpha_1, \alpha_2\}$ ise

$$N(\alpha) = \left| \frac{\Delta[\alpha_1, \alpha_2]}{d_K} \right|^{\frac{1}{2}} \quad (3.18)$$

dir. Teorem 3.9’da elde ettiğimiz a doğal sayısı da α idealinin normuna eşittir.

Örnek 3.12. $K = \mathbb{Q}(\sqrt{-26})$, $O_K = \{1, \sqrt{-26}\}$, $\alpha = (5, 2 - \sqrt{-26})$ idealini ele alalım.

$$\begin{aligned} \alpha\alpha' &= (5, 2 - \sqrt{-26})(5, 2 + \sqrt{-26}) = (5.5, 5(2 + \sqrt{-26}), 5(2 - \sqrt{-26}), 30) \\ &= (5)(5, 2 + \sqrt{-26}, 2 - \sqrt{-26}, 6) \end{aligned}$$

Burada ikinci çarpan $(5, 2 + \sqrt{-26}, 2 - \sqrt{-26}, 6) = (1) = O_K$ ’dir, çünkü $1 = 6 - 5$, $\sqrt{-26} = 2 + \sqrt{-26} - 2(6 - 5)$ tir. O halde $\alpha\alpha' = (5)$ tir. Diğer yandan $\Delta[5, 2 - \sqrt{-26}] = 25 \cdot (-104)$, $d_K = -104$ olduğundan (3.18)’teki eşitlikten

$$N(\alpha) = \left| \frac{\Delta[5, 2 - \sqrt{-26}]}{-104} \right|^{\frac{1}{2}} = 5 \text{ ’tir.}$$

Teorem 3.11.

$$\text{i- } N(\alpha) = 1 \Leftrightarrow \alpha = (1), \quad N(\alpha) = 0 \Leftrightarrow \alpha = (0)$$

$$\text{ii- } 0 \neq \alpha \in O_K \text{ ise } N((\alpha)) = N(\alpha) \text{ (Temel idealin normu üreticinin normuna eşittir).}$$

$$\text{iii- } \alpha = (n, m(b + \omega)) \text{ ise } N(\alpha) = nm.$$

$$\text{iv- } N(\alpha\beta) = N(\alpha)N(\beta),$$

İspat: i, ii, iv açık. iii’ü gösterelim.

$$\text{iii- } \alpha = (n, m(b + \omega)) \Rightarrow \alpha\alpha' = (n, m(b + \omega))(n, m(b + \omega'))$$

$$= (n^2, mn(b + \omega), mn(b + \omega'), m^2 N(b + \omega))$$

$$= (mn) \left(c, b + \omega, b + \omega', \frac{1}{c} N(b + \omega) \right).$$

İkinci idealin birim ideal olduğunu göstermemiz gerek. $\alpha\alpha' = (a)$ olduğu için, bu ideal bir tamsayı tarafından üretilmiş olmalı. Fakat $b + \omega$ nun tamsayı bölenleri ∓ 1 den ibarettir. Dolayısıyla $\{1, \sqrt{d}\}$ tamlik bazıdır. Yani ikinci ideal O_K 'nın kendisidir.

Tanım 3.18. α ve $\mathfrak{b}$, O_K 'nın idealleri olmak üzere $\mathfrak{b} = \alpha.\mathfrak{c}$ olacak şekilde bir $\mathfrak{c}$ ideali varsa α ideal $\mathfrak{b}$ 'yi böler denir ve $\alpha \mid \mathfrak{b}$ biçiminde gösterilir.

Teorem 3.12. $\alpha \mid \mathfrak{b} \Leftrightarrow \mathfrak{b} \subseteq \alpha$ 'dır.

İspat: $\Rightarrow$: $\alpha \mid \mathfrak{b} \Rightarrow \mathfrak{b} = \alpha.\mathfrak{c}$ olacak şekilde bir $\mathfrak{c} \subseteq O_K = (1)$ ideali vardır. Buradan

$$\mathfrak{b} = \alpha.\mathfrak{c} \subseteq \alpha(1) = \alpha \text{ elde ederiz.}$$

$\Leftarrow$ $\mathfrak{b} \subseteq \alpha$ olduğunu varsayalım. $\alpha\alpha' = N(\alpha) = a$ olsun. Açıkça a , $\mathfrak{b}\alpha' \subseteq \alpha\alpha'$ 'nın her elemanını böler. Dolayısıyla,

$$I := \frac{1}{a}\alpha'\mathfrak{b} = \left\{ \frac{1}{a} \sum \alpha_i' \beta_i : \alpha_i \in \alpha, \beta_i \in \mathfrak{b} \right\} \subseteq \mathbb{Q}(\sqrt{d})$$

aslında O_K 'nın alt kümesidir. I aynı zamanda O_K 'nın bir idealidir. Buradan

$$I\alpha := \frac{1}{a}\alpha'\alpha\mathfrak{b} = \frac{1}{a}(a)\mathfrak{b} = (1)\mathfrak{b}. \text{ Böylelikle } \alpha \mid \mathfrak{b} \text{ 'dir.}$$

Tanım 3.19.

a-) $\mathfrak{p}$, O_K 'nın bir öz-ideali (sıfırdan ve birim idealden farklı) olmak üzere $\mathfrak{p}$ idealinin bütün bölenleri birim ideal ve kendisinden ibaretse, bu $\mathfrak{p}$ idealine *asal ideal* denir.

b-) Eğer α , O_K 'nın bir öz-ideali ve α ile O_K arasında başka bir ideali yoksa (yani; $\alpha \subseteq \mathfrak{b}$ ise $\alpha = \mathfrak{b}$ veya $\mathfrak{b} \subset O_K$ 'dır) bu α idealine *maksimal ideal* denir.

Teorem 3.13. (Mollin,1999) K bir sayı cismi ise O_K Dedekind bölgesidir (DB).

Tanım 3.20. O_K 'nın bütün idealleri temel idealse O_K 'ya *temel ideal bölgesi* denir ve kısaca TİB şeklinde gösterilir.

Teorem 3.14. (Mollin,1999) O_K , Dedekind bölgesi olduğu için O_K , TÇAB'dir $\Leftrightarrow O_K$, TİB dir.

Teorem 3.15. (Mollin,1999) O_K , EB $\Rightarrow O_K$, TİB'dir $\Rightarrow O_K$, TÇAB'dir.

Teorem 3.16. Eğer $\alpha, \mathbf{b}, \mathbf{c}$, O_K 'nin sıfırdan farklı idealleri ve $\alpha.\mathbf{b} = \alpha.\mathbf{c}$ ise $\mathbf{b} = \mathbf{c}$ 'dir.

İspat: $\alpha\mathbf{b} = \alpha\mathbf{c} \Rightarrow \alpha'\alpha\mathbf{b} = \alpha'\alpha\mathbf{c} \Rightarrow N(\alpha)\mathbf{b} = N(\alpha)\mathbf{c}$ 'dir, burada $N(\alpha)$ temel idealdir. O halde temel ideal için sadeleştirme yapabiliyorsak ispat tamamdır.

$(\alpha)\mathbf{b} = (\alpha)\mathbf{c}$ ise $\forall \beta \in \mathbf{b}$ için $\alpha\beta \in \alpha\mathbf{c}$ 'dir. Dolayısıyla $\alpha\beta = \alpha\gamma \Rightarrow \beta = \gamma \in \mathbf{c}$, böylece $\mathbf{b} \subseteq \mathbf{c}$ 'dir. Benzer şekilde $\mathbf{c} \subseteq \mathbf{b}$ 'dir. Bu sonuçlar birleştirilirse $\mathbf{b} = \mathbf{c}$ 'dir.

Teorem 3.17. $\alpha \subset O_K$ sıfırdan farklı bir ideal ise, α birtakım asal ideallerin çarpımı olarak tek türlü şekilde yazılabilir.

İspat: Eğer α indirgenemez ise ispat tamamlanmıştır. Eğer $\mathbf{b}$ ve $\mathbf{c}$ indirgenemez idealler olmak üzere $\alpha = \mathbf{b}.\mathbf{c}$ olarak yazılabiliyorsa yine ispat tamamlanmıştır. Yazılamıyorsa indirgenemez olmayan ideal, veya idealleri bu adımdaki gibi çarpanlara ayırmaya devam ederiz. $N(\alpha) = N(\mathbf{b}).N(\mathbf{c})$ ve $1 < N(\mathbf{b}), N(\mathbf{c}) < N(\alpha)$ dır. Normun doğal sayı olduğu ve çarpanlara ayırdıkça normların azaldığı hesaba katılırsa bu prosedür bir noktada sona erdiği görülür.

Şimdi $\mathbf{p}_1, \dots, \mathbf{p}_r, \mathbf{q}_1, \dots, \mathbf{q}_s$ asal idealler olmak üzere α idealinin,

$$\alpha = \mathbf{p}_1 \dots \mathbf{p}_r = \mathbf{q}_1 \dots \mathbf{q}_s \quad (3.19)$$

şeklinde iki farklı biçimde çarpanlara ayrıştığını varsayalım. $\mathbf{p}_1$ asal olduğundan $1 \leq i \leq s$ için

$\mathbf{p}_1 | \mathbf{q}_i$ 'dir. Yeniden numaralandırarak $\mathbf{p}_1 | \mathbf{q}_1$ olarak yazabiliriz. Fakat $\mathbf{q}_1$ indirgenemez olduğu

için $\mathbf{p}_1 = \mathbf{q}_1$ 'dir. (3.19)'daki eşitliğin her iki yanında ortak olan bu çarpanları sadeleştirsek

$\mathbf{p}_2 \dots \mathbf{p}_r = \mathbf{q}_2 \dots \mathbf{q}_s$ elde edilir. Bu süreç devam ettirilirse $r = s$ ve $\mathbf{p}_i = \mathbf{q}_i$ elde edilir. Yani

(3.19)'daki eşitliğin her iki yanı da aslında aynıdır.

α idealinin asal ideallerin çarpımı olarak yazılabilmesi O_K 'nin DB olmasından kaynaklanmaktadır. Çünkü DB'nde sıfırdan farklı her ideal bir kısım asal ideallerin çarpımı şeklinde tek türlü olarak yazılabilir. Teorem 3.17'de veirlen $\mathbf{p}_1, \mathbf{p}_2, \dots, \mathbf{p}_r$ asal idealleri arasında aynı olan idealleri gruplandırırsak α 'yı

$$\alpha = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \quad (3.20)$$

($r \geq 0$, p_i 'ler O_K 'nın farklı asal idealleri ve $e_i \geq 1$) şeklinde yazabiliriz.

İdeallerle TÇB olmayan O_K 'lardaki bu eksikliğin onarılabileceğini söylemiştik. Bunu bir örnekle açıklayalım.

Örnek 3.13. $K = \mathbb{Q}(\sqrt{-26})$ olmak üzere O_K da 27 'nin

$$27 = 3.3.3. = (1 + \sqrt{-26})(1 - \sqrt{-26}) \quad (3.21)$$

biçiminde iki farklı çarpanlara ayrılışını ele alalım. Burada çarpanlardan her birinin indirgenemez olduğu gösterilebilir. Dolayısıyla O_K , TÇAB değildir. Şimdi $\alpha = (3, 1 + \sqrt{-26})$ ve $\mathfrak{b} = (3, 1 - \sqrt{-26})$ ideallerini hesaba katalım.

$$(3) = \alpha \mathfrak{b}, \quad (1 + \sqrt{-26}) = \alpha^3, \quad (1 - \sqrt{-26}) = \mathfrak{b}^3 \quad (3.22)$$

olduğu yukarıdaki verdiğimiz özellikler kullanılarak kolayca gösterilebilir. Bu sonuçlar bize (3.21) ile verilen 27 'nin O_K 'da indirgenemezlerin çarpımı olarak farklı olan çarpanlara ayrılışının aslında O_K 'nın ideallerinin çarpımı olarak tek türlü olduğunu gösterir. Çünkü (3.22)'deki eşitliklerden $(27) = (3)^3 = (\alpha \mathfrak{b})^3 = \alpha^3 \mathfrak{b}^3 = (1 + \sqrt{-26})^3 (1 - \sqrt{-26})^3$

elde ederiz ki, eşitliğin her iki yanı da bu yeni çarpımda aynıdır. O halde O_K tamlık halkasında tek türlü çarpanlara ayrılma özelliğinin eksikliğini O_K 'nın idealleri üzerinde yeniden inşa edebiliriz.

O_K 'nın idealleri için ters eleman mevcut olmayabileceğinden O_K 'nın ideallerinin kümesinin bir grup oluşturmadığı açıktır. Fakat her bir idealin bir temel ideali böldüğünü gösterdik. O halde eğer temel idealleri birim ideal olarak hesaba katarsak ters ideallerden söz edebiliriz. Bu fikir yeni bir takım tanım ve teoremlerle birlikte önemli sonuçlar verecektir.

3.4 İdeal Sınıf Grubu

Tanım 3.21. $K = \mathbb{Q}(\sqrt{d})$ bir kuadratik sayı cismi olmak üzere eğer K 'nın boştan farklı bir α alt kümesi aşağıdaki özellikleri sağlıyorsa *kesirsel ideal ismi* verilir.

- $\forall \alpha, \beta \in \mathfrak{a}$ için $\alpha - \beta \in \mathfrak{a}$,
- $\forall \alpha \in \mathfrak{a}$ ve $\gamma \in O_K$ için $\alpha\gamma \in \mathfrak{a}$,
- $\exists 0 \neq \theta \in O_K$ için $\theta\mathfrak{a} \subset O_K$.

Tanım 3.22. $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cismi olsun. $\alpha \in K$ sıfırdan farklı bir eleman ve $\mathfrak{a}$, O_K 'nin sıfırdan farklı bir ideali olmak üzere K 'nin her bir kesirsel ideali $\alpha\mathfrak{a}$ şeklinde bir kümedir.

Burada dikkat edilirse $\alpha \in O_K$ olmayabilir. Özel olarak $\alpha \in O_K$ ise $\alpha O_K = (\alpha)$ 'dır ve bu tür kesirsel ideallere *temel kesirsel ideal* adı verilir. Kesirsel ideallerin toplam ve çarpımı da ideallerin toplam ve çarpımı gibi tanımlanmıştır.

Tanım 3.23. $\mathfrak{a}$ bir kesirsel ideal olmak üzere,

$$\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq O_K\}$$

idealine *ters kesirsel ideal* denir.

Teorem 3.18. (Murty, 1999)

$\mathfrak{p}$, O_K 'nin bir asal ideali ise $\mathfrak{p}^{-1}$ kesirsel idealdir ve $\mathfrak{p}\mathfrak{p}^{-1} = O_K$ 'dir.

K kuadratik sayı cisminin sıfırdan farklı kesirsel ideallerinin kümesini $\mathbf{F} = \mathbf{F}_K$ ile O_K 'nin temel kesirsel ideallerinin kümesini de $\mathbf{P} = \mathbf{P}_K$ ile göstereceğiz.

Teorem 3.19. (Mollin, 1999) $\mathbf{F}$, ideallerin çarpma işlemine göre, birim elemanı O_K olan değişmeli bir gruptur ve $\mathbf{P}$, $\mathbf{F}$ 'nin alt grubudur.

Tanım 3.24. $\mathbf{F}/\mathbf{P}$ bölüm grubuna K sayı cisminin *ideal sınıf grubu* adı verilir ve $\mathbf{Cl} = \mathbf{Cl}(O_K)$ biçiminde gösterilir.

Kesirsel idealler grubunu sınıflara ayırmış olduk. Aynı sınıfta bulunan ideallere *denk idealler* denir. Başka bir ifadeyle $\psi : \mathbf{F} \rightarrow \mathbf{F}/\mathbf{P}$ olmak üzere eğer $\psi(\mathfrak{a}) = \psi(\mathfrak{b})$ ise $\mathfrak{a}, \mathfrak{b}$ denktirler. İki kesirsel ideal $\mathfrak{a}$ ve $\mathfrak{b}$ 'nin denkliğini $\mathfrak{a} \sim \mathfrak{b}$ ile gösterirsek $\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \exists 0 \neq \alpha \in K : \mathfrak{a} = (\alpha)\mathfrak{b}$.

Kesirsel ideallerin sınıfında tam idealler de mevcuttur.

Tanım 3.25. Eğer $\alpha, \mathfrak{b}$ O_K 'nın tam idealleri ve $(\alpha)\alpha = (\beta)\mathfrak{b}$ olacak şekilde $\alpha, \beta \in O_K$ varsa α ile $\mathfrak{b}$ idealleri *denk ideallerdir* denir. İdealler arasında belirtilen bu şekilde bir bağıntı yansıma, simetri ve geçişme özelliklerini sağladığı açıktır, dolayısıyla bir denklik bağıntısıdır.

Bir α idealinin *denklik sınıfını* veya genel kullanımıyla *ideal sınıfını* $[\alpha]$ biçiminde göstereceğiz.

Örnek 3.14. $K = \mathbb{Q}(\sqrt{-5})$ alınırsa O_K da;

$$(7)(2, 3 + \sqrt{-5}) = (3 + \sqrt{-5})(7, 3 - \sqrt{-5})$$

eşitliği sağlandığı için $(2, 3 + \sqrt{-5}) \sim (7, 3 - \sqrt{-5})$ tir. Aslında $O_K = \mathbb{Z}[\sqrt{-5}]$ 'te iki ideal sınıfı mevcuttur. Bunlar temel ideal sınıfı ve temel ideal olmayanların ideallerin sınıfıdır.

Teorem 3.20. İdeallerin her bir denklik sınıfı bir tam ideal tarafından temsil edilir.

Dikkat edilirse O_K eğer TİB ise herhangi iki ideali birbirlerine denktirler.

Tanım 3.26. $\mathfrak{C} = \mathbf{F}/\mathfrak{P}$ bölüm grubunun mertebesine ($|\mathfrak{C}|$), K sayı cisminin *sınıf sayısı* adı verilir ve $h(K)$ veya h_K sembollerinden biriyle gösterilir. Eğer hangi sayı cismi K 'dan bahsedildiği biliniyorsa sadece h sembolü kullanılır.

O halde h_K 'nın büyüklüğü O_K 'nın TİB olmaktan ne kadar uzak olduğu hakkında bilgi verir. Bu sonuçları Teorem 3.14, 3.15 ile birleştirirsek; $\mathfrak{C}$ yalnız bir eleman içerir $\Leftrightarrow O_K$ TİB $\Leftrightarrow O_K$ TÇAB'dir.

Teorem 3.21. O_K da çarpanlara ayırma tek türdür (yani O_K , TÇAB'dir) ancak ve ancak $h_K = 1$.

İspat: O_K da çarpanlara ayırma tek türdür ancak ve ancak O_K 'nın her ideali temel ideal ise. Bu da her bir kesirsel idealin temel ideal olmasıyla mümkündür, yani $\mathbf{F} = \mathfrak{P}$ yada denk olarak $|\mathfrak{C}| = h_K = 1$ 'dir.

Teorem 3.22. α, O_K 'nın bir ideali ve h, K 'nın sınıf sayısı ise α^h her zaman temel idealdir .

Örnek 3.15. $K = \mathbb{Q}(\sqrt{-14})$ olmak üzere O_K da $\alpha = (3, 1 + \sqrt{-14})$ ideali için $\alpha, \alpha^2, \alpha^3$

idealleri temel ideal olmamasına rağmen α^4 ideali temel idealdir. Burada da $\mathbb{Z}[\sqrt{-14}]$ ün sınıf sayısı 4 tür. Bu örnekte de görüldüğü gibi temel ideal olmayan ideallerin bir kısım çarpımı temel ideal olmaktadır.

Teorem 3.23. K , bir sayı cismi ise $|\mathcal{C}(O_K)|$ sonludur.

Tanım 3.27. (Murty, 1999; Mollin, 1999)

[Minkowski Sınırı]: K sayı cismi r_1 ve r_2 parametreleriyle n . dereceden

$([K : \mathbb{Q}] = n = r_1 + 2r_2)$ bir sayı cismi olsun. $|\mathcal{C}(O_K)|$ 'nın her bir sınıfı normu aşağıdaki sınır şartını sağlayan bir α ideali içerir,

$$N(\alpha) \leq M_K = \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^{r_2} \sqrt{|d_K|} \quad (3.23)$$

Burada M_K değerine K için *Minkowski sınırı* adı verilir.

Teorem 2.8 in sonucu olarak belirtildiği gibi reel kuadratik sayı cisimlerinde $r_1 = 2, r_2 = 0$, sanal kuadratik sayı cisimlerinde ise $r_1 = 0, r_2 = 1$ 'dir. O halde (3.23)'ü kuadratik sayı cisimleri için yeniden düzenlediğimizde Minkowski sınırı;

- $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cismi ise $M_K = \frac{\sqrt{|d_K|}}{2}$,
- $K = \mathbb{Q}(\sqrt{d})$ sanal kuadratik sayı cismi ise $M_K = \frac{2}{\pi} \sqrt{|d_K|}$

biçimini alır.

Çizelge 3.2. $|d| \leq 70$ olan kare bağımsız d 'ler için $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisimlerine karşılık gelen Minkowski sınırlarının (M_K) değerleri

d	M_K	d	M_K	d	M_K	d	M_K	d	M_K	d	M_K	d	M_K	d	M_K
-	-	-1	1.273	17	2.062	-17	5.250	35	5.916	-35	3.766	55	7.416	-55	4.721
2	1.414	-2	1.800	19	4.359	-19	2.775	37	3.041	-37	7.745	57	3.775	-57	9.613
3	1.732	-3	1.103	21	2.291	-21	5.835	38	6.164	-38	7.849	58	7.616	-58	9.697
5	1.118	-5	2.847	22	4.690	-22	5.972	39	6.245	-39	3.975	59	7.681	-59	4.890
6	2.449	-6	3.119	23	4.796	-23	3.053	41	3.202	-41	8.153	61	3.905	-61	9.944
7	2.646	-7	1.684	26	5.099	-26	6.492	42	6.481	-42	8.251	62	7.874	-62	10.025
10	3.162	-10	4.026	29	2.693	-29	6.857	43	6.558	-43	4.175	65	4.031	-65	10.265
11	3.317	-11	2.111	30	5.478	-30	6.973	46	6.782	-46	8.636	66	8.124	-66	10.344
13	1.803	-13	4.591	31	5.567	-31	3.545	47	6.856	-47	4.364	67	8.185	-67	5.2110
14	3.741	-14	4.764	33	2.872	-33	7.314	51	7.141	-51	4.546	69	4.153	-69	10.576
15	3.873	-15	2.466	34	5.830	-34	7.424	53	3.640	-53	9.269	70	8.366	-70	10.652

Teorem 3.24. $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cismi olmak üzere $\mathfrak{C}$ 'nin her bir ideal sınıfı

$N(\mathfrak{a}) \leq M_K$ olan bir $\mathfrak{a}$ tam ideali tarafından temsil edilir.

Örnek 3.16. Teorem 3.27 ve Çizelge 3.2'den $K = \mathbb{Q}(\sqrt{-7})$ sanal kuadratik sayı cismi için Minkowski sınırının $M_K = \frac{2}{\pi} \sqrt{-7} = 1.684...$ olduğunu görüyoruz. Normu 1.684'ten küçük olan tek ideal aşık ideal O_K dir. Bu ideal de temel ideal olduğu için $h_K = 1$ 'dir. Benzer şekilde Çizelge 3.2'den $d = -3, -2, -1, 2, 3, 5, 13$ için M_K değerlerinin sırasıyla 1.102, 1.800, 1.273, 1.414, 1.732, 1.118, 1.803 yaklaşık değerlerini aldığı görülmektedir. Bu d değerlerine karşılık gelen her bir O_K da normu bu değerlerden küçük olan ideal sadece birim idealdir ki, o da temel idealdir. O halde $h_K = 1$ 'dir ve bunlara karşılık gelen tamlık halkası O_K 'lar TÇAB'dir.

Burada Minkowski sınırının 2'den küçük olması sınıf sayısının elde edilmesinde oldukça büyük bir kolaylık sağlamıştır. Fakat Çizelge 3.2'den de görüldüğü gibi Minkowski sınırları her zaman 2 den küçük olmayabilir. Bu da birim idealden başka normu bu şartı sağlayan ideallerin var olduğunu göstermektedir. Dolayısıyla bu tür tamlık halkalarında normları 2 ve 2'den büyük olan idealleri de hesaba katmak gerekmektedir. Bunu durumu sonraki bölümde verilen materyallerden sonra hesaba katacağız.

3.5 Asalların Parçalanışı

Teorem 3.25. $\mathfrak{p}$ asal bir ideal olmak üzere $\mathfrak{p} | (p)$ olacak şekilde mutlaka bir $p \in \mathbb{Z}$ asal sayısı vardır ve bu sayı tektir.

İspat: $\mathfrak{p} | \mathfrak{p}\mathfrak{p}' = N(\mathfrak{p})$ 'dir. $N(\mathfrak{p})$ 'yi $\mathbb{Z}$ 'de çarpanlarına ayırırsak ve $\mathfrak{p}$ 'nin asal olduğunu göz önüne alırsak $\exists p \in \mathbb{Z}$ asal sayısı vardır öyle ki $\mathfrak{p} | (p)$ 'dir. Şimdi $p \in \mathbb{Z}$ 'nin tek olduğunu gösterelim. p ve q 'lar farklı asallar olmak üzere $\mathfrak{p} | (p)(q)$ olacak şekilde (p) ve (q) idealleri varsa, p ve q aralarında asal olduğu için $\exists x, y \in \mathbb{Z} : px + qy = 1$ 'dir. Yani $\mathfrak{p}, 1$ 'i de içerir ki bu bir çelişkidir. Dolayısıyla $\mathfrak{p}$ birden fazla asal sayıyı bölemez.

Teorem 3.26. (Murty, 1999)

$O_K = \mathbb{Z}[\theta]$ olacak şekilde bir $\theta \in K$ olduğunu varsayalım. $f(x)$, θ 'nın $\mathbb{Z}[x]$ 'teki minimal polinomu olsun. $p \in \mathbb{Z}$ asal sayı ve $f_i(x) \in F_p[x]$ 'ler indirgenemez, $\mathfrak{p}_i = (p, f_i(\theta))$ öyleki $N(\mathfrak{p}_i) = p^{\text{der}(f_i)}$ olsun, Eğer

$$f(x) = f_1(x)^{e_1} f_2(x)^{e_2} \dots f_g(x)^{e_g} \pmod{p} \text{ ise } pO_K = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_g^{e_g} \quad (3.24)$$

dir.

$K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisminde her bir ideal bir kısım asal ideallerin çarpımı olarak $(p) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r}$ biçiminde yazılabileceğini Teorem 3.17 ile gösterdik. Diğer yandan $|K : \mathbb{Q}| = 2$ olduğundan $\text{der}(f_i) = 2$. O halde $p^2 = N(p) = N(\mathfrak{p}_1)^{e_1} N(\mathfrak{p}_2)^{e_2} \dots N(\mathfrak{p}_r)^{e_r}$ 'dir. Böylece $N(p) = p$ veya $N(p) = p^2$ 'dir.

O_K 'nin sıfırdan farklı her bir asal ideali $p \in \mathbb{Z}$ olmak üzere $pO_K = (p)$ biçiminde bir temel ideali böldüğünü Teorem 3.25'te ispatladık. O_K 'nin bütün asallarını bu pO_K ideallerinin asal çarpanlarını bularak elde edebiliriz.

Bunları elde edebilmek için $\mathbb{Z}[x]$ ve $F_p[x]$ 'teki polinomlarla çalışacağız. $\mathbb{Z}[x]$ 'teki polinomları $f(x)$ şeklinde, $F_p[x]$ teki polinomları $\text{mod } p$ 'ye göre indirgeyen $\bar{f}(x)$ polinomu ile ifade edeceğiz.

Teorem 2.10'un sonucu olarak $K = \mathbb{Q}(\sqrt{d})$ sayı cisminin tamlık halkası O_K 'nin $\mathbb{Z}[\omega]$ biçiminde olduğunu göstermiştik. Eğer $d \equiv 2,3 \pmod{4}$ ise $\omega = \sqrt{d}$ 'dir bu durumda ω 'nın minimal polinomu $f(x) = x^2 - d$ 'dir ve $d \equiv 1 \pmod{4}$ ise $\omega = \frac{1+\sqrt{d}}{2}$ dir, bu durumda da ω 'nın minimal polinomu $f(x) = x^2 - x + \frac{1-d}{4}$ tür, p bir asal sayı olmak üzere pO_K 'nin O_K 'daki parçalanışını elde etmek için $O_K \rightarrow O_K/pO_K$ dönüşümünü ele alalım. pO_K bu dönüşümün çekirdeğidir. Bu çekirdek için başka ikinci bir ifade bulacağız. Bunu yapabilmek için α 'yı x 'e taşıyan $O_K \cong \mathbb{Z}[x]/f(x)$ izomorfizmasını ele alacağız. Burada

$$O_K/pO_K \cong (\mathbb{Z}[x]/f(x))/p \cong \mathbb{Z}[x]/(p, f(x))$$

ve $\mathbb{Z}[x]/(p, f(x)) \cong F_p[x]/(\bar{f}(x))$ 'tir.

Şimdi pO_K 'nin O_K 'daki parçalanışı yerine $\bar{f}(x)$ 'in $F_p[x]$ 'teki parçalanışını inceleyeceğiz.

Burada, $\bar{f}(x)$ 2. dereceden bir polinom olduğuna göre üç farklı durum söz konusudur. Bunlar

i-) $\bar{f}(x)$ 'in indirgenemez olabileceği,

ii-) $\bar{f}(x)$ 'in $F_p[x]$ 'te birinci dereceden iki lineer monik polinomun çarpımı şeklinde yazılabileceği ve

iii-) $\bar{f}(x)$ 'in $F_p[x]$ 'te lineer bir monik polinomun karesi olması durumlarıdır. Şimdi daha ayrıntılı şekilde bu durumları inceleyelim.

i-) $\bar{f}(x)$ 'in indirgenemez olduğunu varsayalım. Böylece $F_p[x]/(\bar{f}(x))$ bir cisimdir. O halde O_K/pO_K bir cisimdir. O halde pO_K ideali O_K 'nın bir asal idealidir. Dolayısıyla artık çarpanlara ayrılamaz.

ii-) $\bar{f}(x)$ 'in $F_p[x]$ 'te $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ şeklinde birinci dereceden iki lineer monik polinomun çarpımı şeklinde yazılabildiğini varsayalım. Çinli kalan teoremi x 'i (x, x) 'e taşıyan

$$F_p[x]/(\bar{f}(x)) \cong F_p[x]/(\bar{g}(x)) \times F_p[x]/(\bar{h}(x))$$

izomorfizmasını verir. Burada, $\bar{g}(x)$ ve $\bar{h}(x)$ polinomları $F_p[x]$ 'te indirgenemez polinom

olduklarından $F_p[x]/(\bar{g}(x))$ ve $F_p[x]/(\bar{h}(x))$ in her ikisi de birer cisimdirler ve F_p 'ye izomorfturlar. Şimdi α 'yı (x, x) 'e taşıyan ve çekirdeği pO_K olan

$$O_K \rightarrow F_p[x]/(\bar{g}(x)) \times F_p[x]/(\bar{h}(x))$$

izomorfizmasını hesaba katalım. Birinci çarpanın çekirdeği pO_K 'nın $(p, g(\alpha))$ ideali ikinci çarpanın ise $(p, h(\alpha))$ idealidir. $(p, g(\alpha))$ ve $(p, h(\alpha))$ 'nın aralarında asal oldukları göz önüne alınırsa dönüşümün çekirdeğini,

$$(p, g(\alpha)) \cap (p, h(\alpha)) = (p, g(\alpha))(p, h(\alpha))$$

olarak elde ederiz. $O_K/(p, g(\alpha)) \cong F_p[x]/(\bar{g}(x))$ ve $O_K/(p, h(\alpha)) \cong F_p[x]/(\bar{h}(x))$ birer cisim olduklarından bu idelerin her ikisi de asal ideallerdir. Böylece pO_K 'nın asal çarpanlara ayrılışı $pO_K = (p, g(\alpha))(p, h(\alpha))$ şeklindedir.

iii-)Son olarak $\bar{f}(x) = \bar{g}(x)^2$ olacak şekilde $\bar{f}(x)$ 'in monik lineer bir $\bar{g}(x) \in F_p[x]$ polinomunun karesi şeklinde çarpanlara ayrıldığını varsayalım. Burada tek çarpan $\bar{g}(x)$ 'ler aralarında asal olmadığından Çinli kalan teoremini uygulayamayız, fakat ii' deki benzer bir yaklaşımla $pO_K = (p, g(\alpha))^2$ olduğu açıktır.

Tanım 3.28.

i-) $pO_K = \mathfrak{p}^2$ ise p , K 'da dallanmış (*ramified*) *asaldır* denir.

ii) $pO_K = \mathfrak{p}\mathfrak{p}'$ olacak şekilde $\mathfrak{p} \neq \mathfrak{p}'$ olacak şekilde farklı idealler varsa p , *tamamen parçalanmış* (*completely decomposed*) *asaldır* denir.

iii) $pO_K = \mathfrak{p}$ ise bu durumda p 'ye *asal* (*inert*) *kalır* denir.

Ayrıca $K = \mathbb{Q}(\sqrt{d})$ olmak üzere eğer $d \equiv 2,3 \pmod{4}$ ise $\omega = \sqrt{d}$ 'dir ve ω 'nun minimal polinomu $f(X) = X^2 - d$, eğer $d \equiv 1 \pmod{4}$ ise $\omega = \frac{1+\sqrt{d}}{2}$ 'dir, bu durumda da ω 'nun minimal polinomu $f(X) = X^2 - X + \frac{1-d}{4}$ 'dir.

Asal sayıların $K = \mathbb{Q}(\sqrt{d})$ sayı cisminde parçalanışı ile ilgili teoremleri vermeden önce bunlarla bağlantılı olacak bazı tanım ve teoremleri verelim.

Tanım 3.29. $p \neq 2$ bir asal sayı ve $a \neq 0$ bir tam sayı olsun.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & x^2 \equiv a \pmod{p} \text{ denklemi çözüme sahipse} \\ -1, & x^2 \equiv a \pmod{p} \text{ denklemi çözüme sahip değilse} \\ 0, & p|a \text{ ise} \end{cases}$$

şeklinde tanımlanan $\left(\frac{a}{p}\right)$ sembolüne *Legendre sembolü* adı verilir. Legendre sembolü aşağıdaki teoremden belirtilen özelliklere sahiptir.

Teorem 3.27. (Adams ve Goldstein, 1976) $p \neq 2$ bir asal sayı ve a ile b sıfırdan farklı birer tamsayı olmak üzere,

$$\text{i-)} \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p},$$

$$\text{ii-)} \text{Eğer } a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

$$\text{iii-)} \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right),$$

$$\text{iv-)} \left(\frac{a^2}{p}\right) = 1 \text{ dir. Özel olarak } \left(\frac{1}{p}\right) = 1,$$

$$\text{v-)} \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

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

Teorem 3.28. p ve q birbirinden farklı iki tek asal sayı olmak üzere,

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

dir.

Teorem 3.29. $p \in \mathbb{Z}$ tek asal sayı olsun. $K = \mathbb{Q}(\sqrt{d})$ bir kuadratik sayı cismi ve $d_K = \text{disk}(K)$ olmak üzere $(p) = pO_K$ 'nın parçalanışı aşağıdaki gibidir.

i-) $p|d_K$ ise $(p, \sqrt{d}) = \mathfrak{p}$ olmak üzere $pO_K = \mathfrak{p}^2$ 'dir.

$d_K \in \mathbb{Z}$ 'nin sadece sonlu sayıda asal çarpanı olduğu için K 'da dallanmış asalların sayısı sonludur.

ii) Eğer $\left(\frac{d_K}{p}\right) = 1$ ise $pO_K = \mathfrak{p}\mathfrak{p}'$ olacak şekilde $\mathfrak{p} \neq \mathfrak{p}'$ biçiminde farklı idealler vardır.

iii) Eğer $\left(\frac{d_K}{p}\right) = -1$ ise $pO_K = \mathfrak{p}$ 'dir.

İspat: i) $p|d_K$ olduğunu varsayalım. $p \neq 2$ olduğu için $(p, 4) = 1$ 'dir. Dolayısıyla

$p|d$ 'dir. $\Rightarrow (p, \sqrt{d})^2 = (p^2, p\sqrt{d}, d) = (p)(p, \sqrt{d}, \frac{d}{p})$. Burada $(p, \sqrt{d}, \frac{d}{p})$ ideali aralarında

asal olan p ve $\frac{d}{p}$ tamsayılarını içerdiği için $(p, \sqrt{d}, \frac{d}{p}) = (1)$. O halde $(p, \sqrt{d})^2 = (pO_K)$.

ii-) $\left(\frac{d_K}{p}\right) = 1$ olsun. Bu durumda $x^2 \equiv d_K \pmod{p}$ 'nin çözümü vardır. Yani

$\exists x \in \mathbb{Z} : d_K \equiv x^2 \pmod{p}$ 'dir. $\mathfrak{p} = (p, x + \sqrt{d})$ ise,

$$\mathfrak{p}\mathfrak{p}' = (p^2, p(x + \sqrt{d}), p(x - \sqrt{d}), x^2 - d) = (p)(p, (x + \sqrt{d}), (x - \sqrt{d}), \frac{x^2 - d}{p})$$

Burada $2\sqrt{d} = x + \sqrt{d} - (x - \sqrt{d})$ ve $4d = (2\sqrt{d})^2$, ayrıca $(p, 4d) = 1$ olduğundan

$(p, x + \sqrt{d}, x - \sqrt{d}, \frac{x^2 - d}{p}) = (1)$ 'dir. Bu da $\mathfrak{p}\mathfrak{p}' = pO_K$ olduğunu gösterir.

Eğer $\mathfrak{p} = \mathfrak{p}'$ olsaydı $4d \in \mathfrak{p}$ ve $\mathfrak{p} = (1)$ olurdu ki bu bir çelişkidir.

iii-) $\left(\frac{d_K}{p}\right) = -1$ olsun. Eğer normu p olan bir $\mathfrak{p}$ ideali olsaydı bu ideal $\mathfrak{p} = (p, b + w)$ ve

$p|N(b + w)$ biçiminde olurdu.

Eğer $\omega_d = \sqrt{d} \Rightarrow b^2 - d \equiv 0 \pmod{p} \Rightarrow \left(\frac{d}{p}\right) = \left(\frac{4d}{p}\right) = \left(\frac{d}{p}\right) = 1$ olurdu ki bu çelişkidir. Diğer

durumda yani $\omega_d = \frac{1}{2}(1 + \sqrt{d})$ ise $(2b+1)^2 \equiv d \pmod{p}$ olur, bu da yine kabul ile çelişir.

Teorem 3.30. $p = 2$ olsun. p 'nin K 'da parçalanışı aşağıdaki gibidir

i-) $2 \mid d_K \Rightarrow 2O_K = \mathfrak{p}^2$ öyle ki $\mathfrak{p}$ asaldir. Burada eğer $d \equiv 2 \pmod{4} \Rightarrow \mathfrak{p} = (2, \sqrt{d})$,

ve eğer $d \equiv 3 \pmod{4} \Rightarrow \mathfrak{p} = (2, 1 + \sqrt{d})$ 'dir.

Eğer $2, d_K$ 'nin böleni değilse $d \equiv 1 \pmod{4}$ olacağından iki durum söz konusudur.

ii-) $d \equiv 1 \pmod{8}$ olması durumunda $2O_K = \mathfrak{p}\mathfrak{p}'$ öyle ki $\mathfrak{p}$ ve $\mathfrak{p}'$ asaldir.

iii-) $d \equiv 5 \pmod{8}$ olduğunda ise $2O_K = \mathfrak{p}$ öyle ki $\mathfrak{p}$ asaldir.

İspat:

i-) $2 \mid d_K \Rightarrow d \equiv 2, 3 \pmod{4}$ 'tür.

$d \equiv 2 \pmod{4}$ ise $2 = (2, \sqrt{d})^2$ olduğunu iddia ediyoruz.

$(2, \sqrt{d})^2 = (4, 2\sqrt{d}, d) = (2)(2, \sqrt{d}, \frac{d}{2})$. d kare-bağımsız olduğu için 2 ve $\frac{d}{2}$ aralarında

asaldir. Dolayısıyla $(2, \sqrt{d}, d/2) = O_K = (1) \Rightarrow (2) = (2, \sqrt{d})^2$.

$d \equiv 3 \pmod{4} \Rightarrow (2) = (2, 1 + \sqrt{d})^2$ olduğunu iddia ediyoruz.

$(2, 1 + \sqrt{d})^2 = (4, 2 + 2\sqrt{d}, 1 + d + 2\sqrt{d}) = (2)(2, 1 + \sqrt{d}, \frac{1+d}{2} + \sqrt{d})$. Burada $1 + \sqrt{d}$ ve

$\frac{1+d}{2} + \sqrt{d}$ aralarında asal olduğu göz önüne alınırsa $(2, 1 + \sqrt{d}, \frac{1+d}{2} + \sqrt{d}) = (1) = O_K$ olduğu

anlaşılır. Yani $(2) = (2, 1 + \sqrt{d})^2$.

ii-) $d \equiv 1 \pmod{8} \Rightarrow (2O_K) = (2, (1 + \sqrt{d})/2)(2, (1 - \sqrt{d})/2)$ olduğunu iddia ediyoruz. Burada

$(2, \frac{1 + \sqrt{d}}{2})(2, \frac{1 - \sqrt{d}}{2}) = (2)(2, \frac{1 + \sqrt{d}}{2}, \frac{1 - \sqrt{d}}{2}, \frac{1 - d}{8})$ 'dir. Fakat

$1 = (1 + \sqrt{d})/2 + (1 - \sqrt{d})/2$. Dolayısıyla $(2, \frac{1 + \sqrt{d}}{2}, \frac{1 - \sqrt{d}}{2}, \frac{1 - d}{8}) = (1) = O_K$ 'dır. O halde

$$(2, \frac{1+\sqrt{d}}{2})(2, \frac{1-\sqrt{d}}{2}) = (2) \text{ 'dir.}$$

$$\text{iii-)} d \equiv 5(\text{mod } 8) \Rightarrow \exists n \in \mathbb{Z} : d = 8n + 5 \Rightarrow \frac{d-1}{4} = 2n + 1 \Rightarrow \frac{d-1}{4} \equiv 1(\text{mod } 2) .$$

$f(x) = x^2 + x + 1 \in F_2[x]$ indirgenemez olduğu için $d \equiv 5(\text{mod } 8)$ ise 2 inert asaldır.

Bu iki teoremden i, ii, iii te belirtilen iddialar ters yönde de doğrudur (Murty, 1999).

Örnek 3.17. $7O_K$ temel idealinin $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ ’de parçalanışını da minimal polinomu

kullanarak bulalım. $\frac{1+\sqrt{-3}}{2}$ ’nin minimal polinomu $x^2 - x + 1$ ’dir.

$$x^2 - x + 1 \equiv x^2 + 6x + 1 \equiv (x+2)(x+4)(\text{mod } 7) \Rightarrow 7 \text{ tamamen parçalanmıştır(decomposed).}$$

$$(7) = (7, \frac{5+\sqrt{-3}}{2})(7, \frac{9+\sqrt{-3}}{2}) \text{ elde ederiz.}$$

Örnek 3.18. (2730) idealinin $K = \mathbb{Q}(\sqrt{-6})$ olmak üzere O_K ’da asal ideallerin çarpımı olarak yazalım. Bu sayının $\mathbb{Z}$ ’de asal çarpanlara ayrılışı $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ ’tür. Teorem 3.29 ve Teorem 3.30 kullanılırsa $\mathfrak{p}_2 = (2, \sqrt{-6})$, $\mathfrak{p}_3 = (3, \sqrt{-6})$, $\mathfrak{p}_5 = (5, 2 + \sqrt{-6})$, $\mathfrak{p}_7 = (7, 1 + \sqrt{-6})$ ve $\mathfrak{p}_{13} = (13)$ olmak üzere $(2730) = \mathfrak{p}_2^2 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_5 \cdot \mathfrak{p}_5' \cdot \mathfrak{p}_7 \cdot \mathfrak{p}_7' \cdot \mathfrak{p}_{13}$

$$= (2, \sqrt{-6})^2 (3, \sqrt{-6})^2 (5, 2 + \sqrt{-6})(5, 2 - \sqrt{-6})(7, 1 + \sqrt{-6})(7, 1 - \sqrt{-6})(13) \quad (3.25)$$

olduğu görülür. (3.25)’teki sonuca varmak için Pari’de aşağıdaki komutu yazmak yeterlidir.

`nf=nfinit(x^2+6)`

`idealfactor(nf,2730)`

Şimdi de $K = \mathbb{Q}(\sqrt{-6})$ olmak üzere O_K ’da bütün asal ideallerin parçalanışını ele alalım. $d_K = -24$. d_K ’nin asal bölenleri 2 ve 3’ten ibarettir. Dolayısıyla K ’da dallanmış asallar sadece 2 ve 3’tür.

Teorem 3.27 kullanılırsa $p \neq 2, 3$ olmak üzere p ’nin tamamen parçalanmış olması için

$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) \left(\frac{3}{p}\right) = 1$ olması gerektiğini söyleyebiliriz. Yine Teorem 3.27 de v ve vi kullanılırsa;

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1(\bmod 4) \text{ ise} \\ -1, & p \equiv 3(\bmod 4) \text{ ise} \end{cases},$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1, 7(\bmod 8) \text{ ise} \\ -1, & p \equiv 3, 5(\bmod 8) \text{ ise} \end{cases},$$

yazabiliriz. Yine;

$$\left(\frac{p}{3}\right) = \begin{cases} 1, & p \equiv 1(\bmod 3) \text{ ise} \\ -1, & p \equiv 2(\bmod 3) \text{ ise} \end{cases}.$$

Diğer yandan $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} = \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2}}$ dir. O halde;

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 1, 11(\bmod 12) \text{ ise} \\ -1 & p \equiv 5, 7(\bmod 12) \text{ ise} \end{cases}$$

dir.

Şimdi $\left(\frac{-6}{p}\right) = 1$ olabilecek şekilde 4 farklı durumu inceleyip oluşan bu lineer kongrüans sistemlerini Çinli kalan teoremi vasıtasıyla çözelim.

i-) $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1 \Rightarrow p \equiv 1(\bmod 8), p \equiv 1(\bmod 12) \Rightarrow p \equiv 1(\bmod 24)$ elde edilir. Benzer şekilde;

$$\text{ii-)} \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1, \left(\frac{3}{p}\right) = 1 \Rightarrow p \equiv 3(\bmod 8), p \equiv 11(\bmod 12) \Rightarrow p \equiv 11(\bmod 24)$$

$$\text{iii-)} \left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = -1, \left(\frac{2}{p}\right) = 1 \Rightarrow p \equiv 7(\bmod 8), p \equiv 7(\bmod 12) \Rightarrow p \equiv 7(\bmod 24)$$

$$\text{iv-)} \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1, \left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 5(\bmod 8), p \equiv 5(\bmod 12) \Rightarrow p \equiv 5(\bmod 24)$$

Sonuç olarak O_K 'da

- 2 ve 3 dallanmış asal
- $p \equiv 1, 5, 7, 11 \pmod{24}$ ise p tamamen parçalanmış asaldır
- $p \equiv 13, 17, 19, 23 \pmod{24}$ ise p asal kalır.

Çizelge 5.2'de başka $|d| < 12$ için $K = \mathbb{Q}(\sqrt{d})$ 'lerde hangi asalların dallanmış, hangilerinin tamamen parçalanmış, hangilerinin asal kaldığını görebiliriz. Örneğin -6 'nın bulunduğu sütunda 2 ve 3'ün karşısında 0 değeri 1, 5, 7, 11 'in karşısında $+1$ değeri, ve 13, 17, 19, 23 karşısında ise -1 değeri bulunmaktadır. Bu da yukarıdaki elde ettiğimiz sonuçla aynı şeyi ifade etmektedir.

Örnek 3.19. Çizelge 3.2'den $d = -19, 21, 29$ için Minkowski sınırlarının sırasıyla 2.775, 2.291, 2.693 olduğu görülmektedir. Eğer $d \equiv 5 \pmod{8}$ ise Teorem 3.30'da görüleceği üzere $2O_K$ asaldır. Yani O_K 'da normu 2 olan idealler yoktur. Dolayısıyla bahsi geçen her bir kuadratik sayı cismi $\mathbb{Q}(\sqrt{d})$ 'de normu bu değerlerden küçük olan bir tek ideal vardır o da aşık ideal O_K 'dır. Böylelikle bu kuadratik sayı cisimlerinin her birinin sınıf sayıları 1 'dir.

Örnek 3.20. $K = \mathbb{Q}(\sqrt{-14})$ olmak üzere $O_K = \mathbb{Z}[\sqrt{-14}]$ ve $d_K = 4 \cdot (-14) = -56$ 'dır. Ayrıca K sanal kuadratik sayı cismi olduğundan $r_1 = 0, r_2 = 1$ 'dir. Bu durumda Minkowski sınırı

$$M_K = \frac{2}{\pi} \sqrt{56} \approx 4.764 < 5 \text{ olduğu açıktır.}$$

Dolayısıyla sınıf grubu, normu 4 veya 4'ten daha küçük olan idealler tarafından üretilmiştir.

$\theta = \sqrt{-14}$ olduğuna göre minimal polinom $f(x) = x^2 + 14$ 'tür. Şimdi normu 4'ten küçük olan ideallerin parçalanışına bakalım. Teorem 3.29 ve 3.30 kullanılırsa,

$$(2) = \mathfrak{p}_2^2 \text{ öyle ki } \mathfrak{p}_2 = (2, \sqrt{-14}) \text{ ve } N(\mathfrak{p}_2) = 2 \text{ 'dir}$$

$$(3) = \mathfrak{p}_3 \mathfrak{p}_3' \text{ öyle ki } \mathfrak{p}_3 = (3, 1 + \sqrt{-14}), \mathfrak{p}_3' = (3, 2 + \sqrt{-14}) \text{ ve } N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3 \text{ 'tür.}$$

Ayrıca normu 4 olan $\mathfrak{p}_2^2 = (2)$ ideali vardır.

Bu durumda O_K 'nın, normu 4 veya 4 ten küçük olan idealleri $O_K, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3', (2) = \mathfrak{p}_2^2$ 'den ibarettir. Bu da sınıf grubunun en fazla 5 elemanlı olabileceğini gösterir. Diğer yandan

$(2) = \mathfrak{p}_2^2$ temel idealdir ve $[(2)] = [O_K]$ denklik sınıfları eşittir. Bir elemanı daha çıkarabiliriz. O halde sınıf sayısı en fazla 4 elemanlıdır.

$N(a + b\sqrt{-6}) = a^2 + 14b^2 = 2$, veya 3 denklemlerinin çözümü olmadığından normu 2 ya da 3 olan bir ideal bulunamaz. Bu da $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3'$ ideallerinin hiçbirinin temel ideal olmadığını gösterir. Dolayısıyla bu ideallerden hiçbirisi $O_K = (1)$ idealine denk olamaz. Yine $a^2 + 14b^2 = 6$ denklemi çözümsüz olduğundan $\mathfrak{p}_2\mathfrak{p}_3'$ ve $\mathfrak{p}_2\mathfrak{p}_3 = \mathfrak{p}_2\mathfrak{p}_3''$ idealleri temel ideal olamaz.

$a^2 + 14b^2 = 9$ denkleminin tamsayı çözümleri $a = \pm 3, b = 0$ dan ibaret olduğundan O_K 'da normu 9 olan elemanlar sadece ± 3 tür. $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ normu 9 olan yegane temel idealdir. O halde normu 9 olan ve $\mathfrak{p}_3\mathfrak{p}_3'$ den farklı olan $\mathfrak{p}_3^2$ ideali temel ideal olamaz. $\mathfrak{p}_3\mathfrak{p}_3'' = \mathfrak{p}_3^2$ temel ideal değildir böylece $[\mathfrak{p}_3] \neq [\mathfrak{p}_3']$.

Böylece $O_K, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3'$ ideallerinin her biri birbirinden farklıdır ve bu durumda $h = |\mathbf{Cl}| = 4$ tür.

Şimdi sınıf grubunun yapısını belirleyelim. $[\mathfrak{p}_3]$ 'ün derecesi $|\mathbf{Cl}| = 4$ 'ü bölmesi gerekir. O halde 1,2,4'ten biri olmalıdır. Fakat $\mathfrak{p}_3^2$ ideali temel ideal olmadığından $[\mathfrak{p}_3] \neq O_K = (1)$ Buradan $[\mathfrak{p}_3]$ 'ün derecesi 2'den büyük olduğu anlaşılmaktadır, o halde 4'tür. Bu da $[\mathfrak{p}_3]$ 'ün, grubun üreteci olduğunu gösterir. Yani $\mathbf{Cl} = \langle [\mathfrak{p}_3] \rangle$ dir. O halde $\mathbf{Cl}(O_K) \cong \mathbb{Z}/4\mathbb{Z}$.

Çizelge 3.3, reel kuadratik sayı cisimlerinde O_K 'nın ideal sınıf gruplarının yapılarını, Çizelge 4.3 ise sanal kuadratik sayı cisimlerinde O_K 'nın ideal sınıf gruplarının yapılarını göstermektedir.

Tanım 3.30. (Adams ve Goldstein, 1976) n , 1 den büyük herhangi bir tek sayı, $\text{ebob}(a, n) = 1$ ve n tek sayısının asal çarpanlara ayrılışı $n = p_1 p_2 \dots p_t$ şeklinde verilsin. Buna göre $\left(\frac{a}{p_i}\right)$ ler Legendre anlamında olmak üzere *Jacobi sembolünü* aşağıdaki gibi tanımlarız,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_t}\right). \quad (3.26)$$

Tanım 3.31. (Kronecker Sembolü) $a \equiv 0,1(\text{mod } 4)$ için,

$$\left(\frac{a}{2}\right) = \left(\frac{a}{-2}\right) = \begin{cases} 0 & a \equiv 0(\text{mod } 8) \\ 1 & a \equiv 1(\text{mod } 8) \\ -1 & a \equiv 5(\text{mod } 8) \end{cases}$$

dir.

Genel olarak, eğer n_1 tek sayı ve $n = 2^c n_1$ olmak üzere

$$\left(\frac{a}{n}\right) = \left(\frac{a}{2}\right)^c \left(\frac{a}{n_1}\right) \quad (3.27)$$

Burada $\left(\frac{a}{n_1}\right)$ (3.26) ile verilen Jacobi sembolünü belirtmektedir.

Buna göre Teorem 3.29 ve 3.30'un sonucu olarak aşağıdaki teoremi yazabiliriz.

Teorem 3.31. $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisminin tamlık halkası O_K ve diskriminantı d_K olmak üzere

i-) Bir p tek asal sayısının parçalanışı Legendre ve Kronecker sembollerine bağlı olarak özetle aşağıdaki şekilde verilebilir

- $\left(\frac{d_K}{p}\right) = 1 \Leftrightarrow p$ ayrışır (Splits),
- $\left(\frac{d_K}{p}\right) = -1 \Leftrightarrow p$ asal kalır (Inert),
- $\left(\frac{d_K}{p}\right) = 0 \Leftrightarrow p$ dallanır (Ramified).

ii-) $p = 2$ asal sayısının ayrışımında aşağıdaki şekilde özetlemek mümkündür

- $\left(\frac{d_K}{2}\right) = 1 \Leftrightarrow 2$ ayrışır (Split),
- $\left(\frac{d_K}{2}\right) = -1 \Leftrightarrow 2$ asal kalır (Inert),

- $\left(\frac{d_K}{2}\right) = 0 \Leftrightarrow 2$ dallanır (Ramified).

Teorem 3.32. (Murty, 1999) d_K , $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisminin diskriminantı olmak üzere,

- eğer $n \equiv m \pmod{d_K}$ ise $\left(\frac{d_K}{n}\right) = \left(\frac{d_K}{m}\right)$ ve
- eğer $n \equiv -m \pmod{d_K}$ ise t , d_K 'nin işaretini belirtmek üzere $\left(\frac{d_K}{n}\right) = \left(\frac{d_K}{m}\right)t$

dir

İspat: Kronecker sembolünün özelliklerini kullanacağız.

$d_K = 2^a d'$, $n = 2^b n'$, $m = 2^c m'$ öyle ki d', n', m' tek sayılar olsun. Eğer $a > 0$ ise $b > 0$ durumu $c > 0$ olacağı için aşıkardır. Dolayısıyla $b = c = 0$ olduğunu varsayalım, (3.27) kullanılırsa;

$$\left(\frac{d_K}{n}\right) = \left(\frac{2^a d'}{n}\right) = \left(\frac{2}{n}\right)^a \left(\frac{d'}{n}\right) = (-1)^{a(n^2-1)/8} \left(\frac{n}{d'}\right) (-1)^{(n-1)(d'-1)/4} \quad (3.28)$$

ve benzer şekilde

$$\left(\frac{d_K}{m}\right) = \left(\frac{2^a d'}{m}\right) = \left(\frac{2}{m}\right)^a \left(\frac{d'}{m}\right) = (-1)^{a(m^2-1)/8} \left(\frac{m}{d'}\right) (-1)^{(m-1)(d'-1)/4}. \quad (3.29)$$

$4|d$ olduğundan m ve n için birinci çarpanlar aynıdır. Eğer $n \equiv m \pmod{d_K}$ ise (3.28) ve (3.29)'daki diğer çarpanlarda aynı olacağı için,

$$\left(\frac{d_K}{n}\right) = \left(\frac{d_K}{m}\right)$$

elde ederiz.

Eğer $n \equiv -m \pmod{d_K}$ ise bu durumda d_K 'nin dolayısıyla da d' 'nin işaretine göre durum değişir.

Eğer $a = 0$ ise $d_K \equiv 1 \pmod{4}$. Dolayısıyla, $\left(\frac{d_K}{2}\right) = \left(\frac{2}{d_K}\right)$ olacağından,

$$\left(\frac{d_K}{n}\right) = \left(\frac{d_K}{2^2 n'}\right) = \left(\frac{d_K}{2}\right)^b \left(\frac{d_K}{n'}\right) = \left(\frac{2}{d_K}\right)^b \left(\frac{d_K}{n'}\right)$$

Böylelikle ;

$$\left(\frac{d_K}{n}\right) = \left(\frac{n}{d_K}\right) \text{ ve } \left(\frac{-1}{d_K}\right) = t$$

dir. Böylece, eğer $m, n > 0$ ve $m \equiv n \pmod{d_K}$,

$$\left(\frac{d_K}{m}\right) = \left(\frac{d_K}{n}\right)$$

dir, ve eğer $m \equiv -n \pmod{d_K}$ ise,

$$\left(\frac{d_K}{n}\right) = \left(\frac{n}{d_K}\right) = \left(\frac{-m}{d_K}\right) = t \left(\frac{m}{d_K}\right) = t \left(\frac{d_K}{m}\right)$$

dir.

Çizelge 3.3 $d = 1, 2, \dots, 226$ için TİB olmayan reel kuadratik sayı cisimlerinde $K = \mathbb{Q}(\sqrt{d})$ 'nin ideal sınıf gruplarının yapıları

Bu tabloda $h = h_K$, $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisminin sınıf sayısını, $\mathbf{Cl}(O_K) \cong$ biçiminde verilen sütunlarda sınıf grubu $\mathbf{Cl}(O_K)$ 'nin izomorf olduğu grubu, idealler yazan sütundaki matrisler ise sınıf grubunun üretici olan idealleri belirtmektedir. Örneğin $d = 10$ alınırsa $K = \mathbb{Q}(\sqrt{10})$ un sınıf sayısının 2 olduğu O_K nin ideal sınıf grubunun $\mathbf{Cl}(O_K) \cong \mathbb{Z}/2\mathbb{Z}$ şeklinde $\mathbb{Z}/2\mathbb{Z}$ e izomorf olduğu ve bu grubun üretici olan idealin $\alpha_3 = (3 + 0, 1 + \omega) = (3, 1 + \sqrt{10})$ ideali olduğunu gösterir. Tabloda sınıf sayısı 1 olan kuadratik sayı cisimleri yer almamıştır, bunlar için bilindiği gibi $\mathbf{Cl}(O_K) \cong (1)$ olduğundan aşıkardır. Tablo pari programı kullanılarak elde edilmiştir.

d	h_K	$\mathbf{Cl}(O_K) \cong$	İdealler	d	h_K	$\mathbf{Cl}(O_K) \cong$	İdealler
10	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]	130	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	[7, 2; 0, 1], [3, 1; 0, 1]
15	2	$\mathbb{Z}/2\mathbb{Z}$	[2, 1; 0, 1]	138	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 0; 0, 1]
26	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 1; 0, 1]	142	3	$\mathbb{Z}/3\mathbb{Z}$	[3, 2; 0, 1]
30	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 0; 0, 1]	143	2	$\mathbb{Z}/2\mathbb{Z}$	[2, 1; 0, 1]
34	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]	145	4	$\mathbb{Z}/4\mathbb{Z}$	[2, 0; 0, 1]
35	2	$\mathbb{Z}/2\mathbb{Z}$	[2, 1; 0, 1]	146	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 1; 0, 1]
39	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 2; 0, 1]	154	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]
42	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 0; 0, 1]	155	2	$\mathbb{Z}/2\mathbb{Z}$	[7, 1; 0, 1]
51	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 1; 0, 1]	159	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 2; 0, 1]
55	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]	165	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 3; 0, 1]
58	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]	170	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	[11, 4; 0, 1], [7, 3; 0, 1]
65	2	$\mathbb{Z}/2\mathbb{Z}$	[2, 1; 0, 1]	174	2	$\mathbb{Z}/2\mathbb{Z}$	[11, 3; 0, 1]
66	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 1; 0, 1]	178	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]
70	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]	182	2	$\mathbb{Z}/2\mathbb{Z}$	[7, 0; 0, 1]
74	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 2; 0, 1]	183	2	$\mathbb{Z}/2\mathbb{Z}$	[7, 1; 0, 1]
78	2	$\mathbb{Z}/2\mathbb{Z}$	[7, 1; 0, 1]	185	2	$\mathbb{Z}/2\mathbb{Z}$	[2, 0; 0, 1]
79	3	$\mathbb{Z}/3\mathbb{Z}$	[3, 2; 0, 1]	186	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 1; 0, 1]
82	4	$\mathbb{Z}/4\mathbb{Z}$	[3, 2; 0, 1]	187	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]
85	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]	190	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]
87	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 0; 0, 1]	194	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 2; 0, 1]
91	2	$\mathbb{Z}/2\mathbb{Z}$	[5, 1; 0, 1]	195	4	$\mathbb{Z}/2\mathbb{Z}$	[6, 3; 0, 1], [10, 5; 0, 1]
95	2	$\mathbb{Z}/2\mathbb{Z}$	[7, 2; 0, 1]	202	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]
102	2	$\mathbb{Z}/2\mathbb{Z}$	[7, 2; 0, 1]	203	2	$\mathbb{Z}/2\mathbb{Z}$	[11, 4; 0, 1]
105	2	$\mathbb{Z}/2\mathbb{Z}$	[2, 0; 0, 1]	205	2	$\mathbb{Z}/2\mathbb{Z}$	[3, 1; 0, 1]

106	2	$\mathbb{Z}/2\mathbb{Z}$	$[3, 1; 0, 1]$	210	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$[7, 0; 0, 1], [11, 1; 0, 1]$
110	2	$\mathbb{Z}/2\mathbb{Z}$	$[5, 0; 0, 1]$	215	2	$\mathbb{Z}/2\mathbb{Z}$	$[5, 0; 0, 1]$
111	2	$\mathbb{Z}/2\mathbb{Z}$	$[5, 1; 0, 1]$	218	2	$\mathbb{Z}/2\mathbb{Z}$	$[11, 3; 0, 1]$
114	2	$\mathbb{Z}/2\mathbb{Z}$	$[5, 2; 0, 1]$	219	4	$\mathbb{Z}/4\mathbb{Z}$	$[5, 3; 0, 1]$
115	2	$\mathbb{Z}/2\mathbb{Z}$	$[3, 1; 0, 1]$	221	2	$\mathbb{Z}/2\mathbb{Z}$	$[5, 1; 0, 1]$
119	2	$\mathbb{Z}/2\mathbb{Z}$	$[5, 2; 0, 1]$	222	2	$\mathbb{Z}/2\mathbb{Z}$	$[13, 1; 0, 1]$
122	2	$\mathbb{Z}/2\mathbb{Z}$	$[11, 1; 0, 1]$	223	3	$\mathbb{Z}/3\mathbb{Z}$	$[3, 2; 0, 1]$
123	2	$\mathbb{Z}/2\mathbb{Z}$	$[7, 2; 0, 1]$	226	8	$\mathbb{Z}/8\mathbb{Z}$	$[3, 2; 0, 1]$

Çizelge 3.4 Kare-bağımsız d ($d < 870$) değerleri için $K = Q(\sqrt{d})$ reel kuadratik sayı cisimlerinin sınıf sayıları ($h = h_K$)

d	h	d	h	d	h	d	h	d	h	d	h	d	h	d	h	d	h	d	h	d	h	d	h
2	1	73	1	145	4	217	1	290	4	366	2	435	4	505	4	581	1	653	1	719	1	794	2
3	1	74	2	146	2	218	2	291	4	367	1	437	1	506	6	582	4	654	2	721	1	795	4
5	1	77	1	149	1	219	4	293	1	370	4	438	4	509	1	583	2	655	2	723	4	797	1
6	1	78	2	151	1	221	2	295	2	371	2	439	5	510	4	586	2	658	4	727	5	798	4
7	1	79	3	154	2	222	2	298	2	373	1	442	8	511	2	587	1	659	3	730	12	799	8
10	2	82	4	155	2	223	3	299	2	374	2	443	3	514	4	589	1	661	1	731	4	802	2
11	1	83	1	157	1	226	8	301	1	377	2	445	4	515	2	590	2	662	1	733	3	803	2
13	1	85	2	158	1	227	1	302	1	379	1	446	1	517	1	591	2	663	4	734	1	805	2
14	1	86	1	159	2	229	3	303	2	381	1	447	2	518	2	593	1	665	2	737	1	806	2
15	2	87	2	161	1	230	2	305	2	382	1	449	1	519	2	595	4	667	2	739	1	807	2
17	1	89	1	163	1	231	4	307	1	383	1	451	2	521	1	597	1	669	1	741	2	809	1
19	1	91	2	165	2	233	1	309	1	385	2	453	1	523	1	598	2	670	2	742	2	811	1
21	1	93	1	166	1	235	6	310	2	386	2	454	1	526	1	599	1	671	2	743	1	813	1
22	1	94	1	167	1	237	1	311	1	389	1	455	4	527	2	601	1	673	1	745	2	814	2
23	1	95	2	170	4	238	2	313	1	390	4	457	1	530	4	602	2	674	4	746	2	815	2
26	2	97	1	173	1	239	1	314	2	391	2	458	2	533	2	606	2	677	1	749	1	817	5
29	1	101	1	174	2	241	1	317	1	393	1	461	1	534	2	607	1	678	2	751	1	818	4
30	2	102	2	177	1	246	2	318	2	394	2	462	4	535	2	609	2	679	2	753	1	821	1
31	1	103	1	178	2	247	2	319	2	395	2	463	1	537	1	610	4	681	1	754	4	822	2
33	1	105	2	179	1	249	1	321	3	397	1	465	2	538	2	611	2	682	2	755	2	823	1
34	2	106	2	181	1	251	1	322	4	398	1	466	2	541	1	613	1	683	1	757	1	826	2
35	2	107	1	182	2	253	1	323	4	399	8	467	1	542	1	614	1	685	2	758	1	827	1
37	1	109	1	183	2	254	3	326	3	401	5	469	3	543	2	615	4	687	2	759	4	829	1
38	1	110	2	185	2	255	4	327	2	402	2	470	2	545	2	617	1	689	4	761	3	830	2
39	2	111	2	186	2	257	3	329	1	403	2	471	2	546	4	618	2	690	4	762	2	831	2
41	1	113	1	187	2	258	2	330	4	406	2	473	3	547	1	619	1	691	1	763	2	834	2
42	2	114	2	190	2	259	2	331	1	407	2	474	2	551	2	622	1	694	1	766	1	835	2
43	1	115	2	191	1	262	1	334	1	409	1	478	1	553	1	623	2	695	2	767	2	838	1
46	1	118	1	193	1	263	1	335	2	410	4	479	1	554	2	626	4	697	6	769	1	839	3
47	1	119	2	194	2	265	2	337	1	411	2	481	2	555	4	627	4	698	2	770	4	842	6
51	2	122	2	195	4	266	2	339	2	413	1	482	2	557	1	629	2	699	2	771	2	843	2
53	1	123	2	197	1	267	2	341	1	415	2	483	4	559	2	631	1	701	1	773	1	849	1
55	2	127	1	199	1	269	1	345	2	417	1	485	2	561	2	633	1	703	2	777	4	851	2
57	1	129	1	201	1	271	1	346	6	418	2	487	1	562	2	634	2	705	2	778	2	853	1
58	2	130	4	202	2	273	2	347	1	419	1	489	1	563	1	635	2	706	4	779	2	854	2
59	1	131	1	203	2	274	4	349	1	421	1	491	1	565	2	638	2	707	2	781	1	857	1
61	1	133	1	205	2	277	1	353	1	422	1	493	2	566	1	641	1	709	1	782	2	858	4
62	1	134	1	206	1	278	1	354	2	426	2	494	2	569	1	642	2	710	2	785	6	859	1
65	2	137	1	209	1	281	1	355	2	427	6	497	1	570	4	643	1	713	1	786	6	861	2
66	2	138	2	210	4	282	2	357	2	429	2	498	2	571	1	645	2	714	4	787	1	862	1
67	1	139	1	211	1	283	1	358	1	430	2	499	5	573	1	646	8	715	4	789	1	863	1
69	1	141	1	213	1	285	2	359	3	431	1	501	1	574	6	647	1	717	1	790	2	865	2
70	2	142	3	214	1	286	2	362	2	433	1	502	1	577	7	649	1	718	1	791	4	866	2
71	1	143	2	215	2	287	2	365	2	434	4	503	1	579	4	651	4	719	1	793	4	869	1

Çizelge 3.5 Kare-bağımsız $d = -1, -2, \dots, -718$ değerleri için $K = Q(\sqrt{d})$ sanal kuadratik sayı cisimlerinin sınıf sayıları ($h = h_K$)

d	h	d	h	d	h	d	h	d	h	d	h	d	h	d	h	d	h	d	h
-1	1	-71	7	-143	10	-215	14	-287	14	-365	20	-434	24	-503	21	-579	8	-651	8
-2	1	-73	4	-145	8	-217	8	-290	20	-366	12	-435	4	-505	8	-581	28	-653	14
-3	1	-74	10	-146	16	-218	10	-291	4	-367	9	-437	20	-506	28	-582	16	-654	28
-5	2	-77	8	-149	14	-219	4	-293	18	-370	12	-438	8	-509	30	-583	8	-655	12
-6	2	-78	4	-151	7	-221	16	-295	8	-371	8	-439	15	-510	16	-586	18	-658	8
-7	1	-79	5	-154	8	-222	12	-298	6	-373	10	-442	8	-511	14	-587	7	-659	11
-10	2	-82	4	-155	4	-223	7	-299	8	-374	28	-443	5	-514	16	-589	16	-661	18
-11	1	-83	3	-157	6	-226	8	-301	8	-377	16	-445	8	-515	6	-590	20	-662	22
-13	2	-85	4	-158	8	-227	5	-302	12	-379	3	-446	32	-517	12	-591	22	-663	16
-14	4	-86	10	-159	10	-229	10	-303	10	-381	20	-447	14	-518	16	-593	24	-665	24
-15	2	-87	6	-161	16	-230	20	-305	16	-382	8	-449	20	-519	18	-595	4	-667	4
-17	4	-89	12	-163	1	-231	12	-307	3	-383	17	-451	6	-521	32	-597	12	-669	12
-19	1	-91	2	-165	8	-233	12	-309	12	-385	8	-453	12	-523	5	-598	8	-670	12
-21	4	-93	4	-166	10	-235	2	-310	8	-386	20	-454	14	-526	12	-599	25	-671	30
-22	2	-94	8	-167	11	-237	12	-311	19	-389	22	-455	20	-527	18	-601	20	-673	12
-23	3	-95	8	-170	12	-238	8	-313	8	-390	16	-457	8	-530	28	-602	24	-674	24
-26	6	-97	4	-173	14	-239	15	-314	26	-391	14	-458	26	-533	12	-606	12	-677	30
-29	6	-101	14	-174	12	-241	12	-317	10	-393	12	-461	30	-534	20	-607	13	-678	20
-30	4	-102	4	-177	4	-246	12	-318	12	-394	10	-462	8	-535	14	-609	16	-679	18
-31	3	-103	5	-178	8	-247	6	-319	10	-395	8	-463	7	-537	12	-610	12	-681	20
-33	4	-105	8	-179	5	-249	12	-321	20	-397	6	-465	16	-538	10	-611	10	-682	12
-34	4	-106	6	-181	10	-251	7	-322	8	-398	20	-466	8	-541	10	-613	10	-683	5
-35	2	-107	3	-182	12	-253	4	-323	4	-399	16	-467	7	-542	24	-614	34	-685	12
-37	2	-109	6	-183	8	-254	16	-326	22	-401	20	-469	16	-543	12	-615	20	-687	12
-38	6	-110	12	-185	16	-255	12	-327	12	-402	16	-470	20	-545	32	-617	12	-689	40
-39	4	-111	8	-186	12	-257	16	-329	24	-403	2	-471	16	-546	24	-618	12	-690	16
-41	8	-113	8	-187	2	-258	8	-330	8	-406	16	-473	12	-547	3	-619	5	-691	5
-42	4	-114	8	-190	4	-259	4	-331	3	-407	16	-474	20	-551	26	-622	12	-694	10
-43	1	-115	2	-191	13	-262	6	-334	12	-409	16	-478	8	-553	8	-623	22	-695	24
-46	4	-118	6	-193	4	-263	13	-335	18	-410	16	-479	25	-554	22	-626	36	-697	8
-47	5	-119	10	-194	20	-265	8	-337	8	-411	6	-481	16	-555	4	-627	4	-698	26
-51	2	-122	10	-195	4	-266	20	-339	6	-413	20	-482	20	-557	18	-629	36	-699	10
-53	6	-123	2	-197	10	-267	2	-341	28	-415	10	-483	4	-559	16	-631	13	-701	34
-55	4	-127	5	-199	9	-269	22	-345	8	-417	12	-485	20	-561	16	-633	20	-703	14
-57	4	-129	12	-201	12	-271	11	-346	10	-418	8	-487	7	-562	8	-634	14	-705	24
-58	2	-130	4	-202	6	-273	8	-347	5	-419	9	-489	20	-563	9	-635	10	-706	24
-59	3	-131	5	-203	4	-274	12	-349	14	-421	10	-491	9	-565	12	-638	20	-707	6
-61	6	-133	4	-205	8	-277	6	-353	16	-422	10	-493	12	-566	30	-641	28	-709	10
-62	8	-134	14	-206	20	-278	14	-354	16	-426	24	-494	28	-569	32	-642	16	-710	32
-65	8	-137	8	-209	20	-281	20	-355	4	-427	2	-497	24	-570	16	-643	3	-713	24
-66	8	-138	8	-210	8	-282	8	-357	8	-429	16	-498	8	-571	5	-645	16	-714	24
-67	1	-139	3	-211	3	-283	3	-358	6	-430	12	-499	3	-573	16	-646	16	-715	4
-69	8	-141	8	-213	8	-285	16	-359	19	-431	21	-501	16	-574	16	-647	23	-717	16
-70	4	-142	4	-214	6	-286	12	-362	18	-433	12	-502	14	-577	8	-649	20	-718	12

3.5.1 Bölümle İlgili Pari Komut ve Programları

kronecker(x,y): Kronecker sembolü (x/y) yi hesaplar.

quadclassunit(dK): d_K diskriminantlı kuadratik cisminin sırasıyla sınıf grubunun mertebesini(sınıf sayısı), yapısını, üretici olan kuadratik formu(ya da formları) ve $d_K > 0$ olduğunda da regülatörünü verir. $d_K < 0$ ise çıktı matrisinin son hanesinde 1 yer alır.

Örnek 3.21. $d_K = -1311.4$ diskriminantlı kuadratik cisimde bunu uygulamak için quadclassunit(-1311*4) yazarız. Sonuç olarak ta [28, [14, 2], [Qfb(5, 4, 263), Qfb(3, 0, 437)], 1] biçiminde bir matris elde ederiz. Bu matriste birinci bileşen 28, kuadratik formun sınıf grubunun mertebesini dolayısıyla da buna karşılık gelen kuadratik sayı cisminin sınıf sayısını, [14, 2], grubun $\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ e izomorf olduğunu, [Qfb(5, 4, 263), Qfb(3, 0, 437)] grubun üretici olan kuadratik formu gösterir.

nf: Sayı cismini tanımlamak için kullanılır. nf=nfinit(pol) biçiminde kullanılır. Burada pol'dan kasıt sayı cismine karşılık gelen indirgenemez minimal polinom'dur. Eğer sayı cismine karşılık gelen indirgenemez polinom bilinmiyorsa, d_K sayı cisminin diskriminantını göstermek üzere nf=nfinit(quadpoly(dk)) biçiminde, hatta diskriminant ta bilinmiyorsa sadece d değeri kullanılarak nf=nfinit(quadpoly(quaddiscdisc(d))) biçiminde sayı cismi tanımlanabilir. Bu şekilde yazılan bir komutla kuadratik sayı cismi hakkında birçok gerekli bilgi elde edilebilir. Örneğin, onun sınıf sayısı, diskriminantı, regülatörü, tamlık tabanı vs. Cismnin hakkında bütün bilgileri bu şekilde elde edebileceğimiz gibi sadece istediğimiz bilgileri aşağıda tanımlanan komutlar vasıtasıyla elde edebiliriz. Örneğin, sayı cismine karşılık gelen diskriminantı belirlemek için nf.disc yazmak yeterlidir.

nf.pol: sayı cismini tanımlayan minimal polinomu,

nf.sign: sırasıyla r_1, r_2 değerlerini,

nf.disc: sayı cisminin diskriminantı,

nf.index: sayı cisminin indeks'ini yani θ indirgenemez bir polinomun kökü olmak üzere $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ 'yı,

nf.roots: indirgenemez polinomun köklerini,

nf.zk: O_K 'nın tamlık tabanını verir.

bnf: nf ile elde ettiğimiz bilgilere ek olarak sayı cismi hakkında başka bilgiler verir. Kullanımı da nf'nin kullanımıyla aynıdır yani öncelikle sayı cismini yine $\text{bnf}=\text{bnfinit}(\text{pol})$ biçiminde tanımlarız. Ayrıca kuadratik sayı cisimlerinde sadece d değeri biliniyorsa bile $\text{bnf}=\text{bnfinit}(\text{quadpoly}(\text{quaddisc}(\text{disc}(d))))$ komutu kullanılarak istenen bilgiler elde edilebilir. Aşağıdaki biçimde kullanılarak sadece istenen bilgilerde elde edilebilir.

bnf.nf : nf nin verdiği sonucun aynısını,

bnf.clgp : sayı cisminin ideal sınıf grubunun yapısını,

bnf.reg : regülatörü,

bnf.fu : temel birimi verir.

Örnek 3.22. $\mathbb{Q}(\sqrt{2006})$ kuadratik sayı cismine ait bilgileri öğrenmek için $\text{nf}=\text{nfinit}(\text{x}^2-2006)$ veya $\text{nf}=\text{nfinit}(\text{quadpoly}(\text{quaddisc}(2006)))$ yazmak gerekir. Bu sayı cisminin diskriminantı için nf.disc , minimal polinomu için nf.pol yazmak yeterlidir. Sınıf grubunun yapısı için $\text{bnf}=\text{bnfinit}(\text{x}^2-2006)$; bnf.clgp yazmak gereklidir.

Çizelge 6.daki tablonun ilk dört sütunu,

```
for(d=1,100,\
```

```
if(issquarefree(-d),if(qfbclassno(quaddisc(-d))<>1,\
```

```
write("sinifgrubusanal.doc",-d,bnfclgp(quadpoly(quaddisc(-d))))))
```

biçiminde bir programla elde edilmiştir. Burada sadece sınıf sayısı 1'den farklı olan sanal kuadratik sayı cisimleri için sonuç istenmiştir. Çizelge.5 için ise,

```
for(d=2,500,if(issquarefree(d),\
```

```
if(qfbclassno(quaddisc(d))<>1,\
```

```
write("sinifgrubureel.doc",d,bnfclgp(quadpoly(quaddisc(d))))))
```

kodları kullanılmıştır.

$\text{idealadd}(\text{nf},I,J)$: Sayı cisminde I ve J ideallerinin toplamını hesaplar.

$\text{idealcoprime}(\text{nf},I,J)$: Verilen I ve J tam idealleri için cismin öyle bir α elemanını bulur ki αI ideali J ile aralarında asal olan bir idealdir.

`idealdiv(nf,I,J)`: Sayı cisminde verilen I ve J için IJ^{-1} bölüm idealini hesaplar.

`idealfactor(nf,I)`: I idealini, verilen sayı cisminde (nf) asal ideallerin kuvvetlerinin çarpımı olarak çarpanlarına ayırır.

Örnek 3.23. $K = \mathbb{Q}(\sqrt{12345})$ reel kuadratik sayı cisminde $16452O_K$ temel idealinin asal ideal çarpanlarını bulmak için `p=quadpoly(12345); nf=nfinit(p); idealfactor(nf,16452)` komutları kullanılabilir. Sonucun nasıl yorumlanması gerektiği Örnek 3.18’le açıklanmıştır.

`idealintersect(nf,I,J)`: I ve J tam ideallerinin arakesitini verir.

`idealinv(nf,I)`: I idealinin tersi olan ideali bulur.

`ideallist(nf,M)`: Sayı cisminde normu M ’den küçük veya eşit olan ideallerin listesini verir.

Örnek 3.24. $K = \mathbb{Q}(\sqrt{-393})$ sanal kuadratik sayı cisminde normu 100’den küçük bütün ideallerin listesi `d=quaddisc(-393); p=quadpoly(d); nf=nfinit(p); ideallist(nf,100)` komutlarıyla elde edilebilir.

`idealmul(nf,I,J)`: Sayı cisminde I ve J ideallerinin çarpımını hesaplar.

`idealpow(nf,I,k)`: Sayı cisminde (nf) I idealinin k . kuvvetini hesaplar. Burada k , pozitif tamsayı veya negatif olabilir. Sonuçta verilen ideal indirgenmiş değildir.

`idealprimedec(nf,p)`: p asal sayısının verilen sayı cisminde (nf) asal ideallerin çarpımı olarak yazılışını verir. Öncelikle tabi ki sayı cismini tanımlamak gerekir.

Örnek 3.25. 7 asal sayısının $K = \mathbb{Q}(\sqrt{-213})$ sayı cisminde asal ideallerin çarpımı olarak yazılışını için `p=x^2+213; nf=nfinit(p); idealprimedec(nf,7)`,

yazmak gereklidir.

`idealprincipal(nf,x)`: x cebirsel sayısının sayı cisminde (nf) ürettiği temel ideali verir.

3.5.2 Bölümle İlgili Maple Komut ve Programları

Maple programında çok fazla olmasa da kuadratik sayı cisimlerinde aritmetiğe imkan tanıyan bir kısım komutları vardır. Örneğin `FactorEQ` komutu, O_K bir Euclid Bölgesi ise verilen bir elemanın O_K ’da çarpanlara ayrılışını bulmaktadır. Özel olarak `sq2factor` komutu $\mathbb{Z}[\sqrt{2}]$ ’de verilen sayının parçalanışını hesaplayabilmektedir.

Gaussian Integers paketi Gauss tamsayılarında ($\mathbb{Z}[i]$ 'de)aritmetiğe imkan tanıyan birçok kod içermektedir. Bunlardan bazıları Gfbasis(Verilen iki elemanın baz oluşturup oluşturmadığını verir), Gfactors(Verilen Gauss sayısının parçalanışı), Gfgcd(Girilen iki Gauss sayısının ebobunu), Gfissqr(Verilen bir Gauss sayısının başka bir Gauss sayısının karesi olup olmadığını), Gf lcm(iki Gauss sayısının ekoklarını), Gfnorm(Gauss sayısının normunu), Gfprime(Verilen sayının Gauss asal sayısı olup olmadığı), Gfrem(Bir sayının diğer biriyle bölümünden kalanı) vs. Aşağıdada bu kodlar ve diğer bazı kodların kullanımına dair kısa örnekler verilmiştir.

Örnek 3.26. $K = \mathbb{Q}(\sqrt{-3})$ olmak üzere O_K 'da $21-14\sqrt{-3}$ 'ün parçalanışını önce Maple kullanarak bulalım. Öncelikle `> with(numtheory);` yazarak sayılar teorisi paketini işlek hale getirmek gerekir.

`> with(numtheory);`

`> factorEQ(21-14*sqrt(-3),-3);`

$$-(2 + I\sqrt{3})^2 (2 - I\sqrt{3})(I\sqrt{3})$$

Yani $21-14\sqrt{-3} = -(2 + \sqrt{-3})^2 (2 - \sqrt{-3})(\sqrt{-3})$ tür.

Gerçekten $21-14\sqrt{-3} = 7(3-2\sqrt{-3})$ tür. Ayrıca $N(3-2\sqrt{-3})=21$ olacağı için $\alpha|3-2\sqrt{-3}$ ise $N(\alpha)|21$ 'dir. $\alpha \in \mathbb{Z}[\sqrt{-3}]$ olduğu için $\alpha = a + b\sqrt{-3}$ biçimindedir ve $N(\alpha)=1, 3, 7, 21$ olabilir. $N(\alpha)=1$, birimsel bir α değeri verir.

$N(a + b\sqrt{-3}) = a^2 + 3b^2 = 3 \Rightarrow a = 0, b = \pm 1$ çözümdür. Dolayısıyla $\pm\sqrt{-3}$ bölendir. Bunun normu asal sayı olduğundan kendisi de indirgenemezdir.

$N(a + b\sqrt{-3}) = a^2 + 3b^2 = 7 \Rightarrow a = \pm 2, b = \pm 1$. Yani $\pm 2 \pm \sqrt{-3}$ bölendir. Bunların normu da asal olduğundan kendisi indirgenemezdir. Gerçekten $(3-2\sqrt{-3}) = (-2-\sqrt{-3})\sqrt{-3}$ tür

Şimdi 7'nin çarpanlarını bulalım. Yine α bir bölense $N(\alpha)=1, 7, 49$. $N(\alpha)=1$ birimsel verir. $N(\alpha)=7$ 'nin çözümünü yukarıda bulduk. Bir çarpan olarak $2 + \sqrt{-3}$ alabiliriz. Bu

eleman da indirgenemezdir. Diğer çarpanı da $\frac{7}{2 + \sqrt{-3}} = 2 - \sqrt{-3}$ olarak elde ederiz.

Yani $21 - 14\sqrt{-3} = (2 + \sqrt{-3})(-2 - \sqrt{-3})(2 - \sqrt{-3})(\sqrt{-3}) = -(2 + \sqrt{-3})^2(2 - \sqrt{-3})(\sqrt{-3})$ tür.

Şimdide sq2factor komutu ile $\mathbb{Z}[\sqrt{2}]$ 'de $1240 - 982\sqrt{2}$ 'nin çarpanlarını bulalım.

>sq2factor(1240-982*sqrt(2)); yazıldığında sonucun $-(\sqrt{2})^3 \cdot (-1 + \sqrt{2}) \cdot (1 - 2\sqrt{2}) \cdot (85 - 11\sqrt{2})$ olduğunu görürüz.

Maple programında Gauss sayılarıyla çalışmak için de with(GaussInt); yazarak Gauss halkası paketini işlek hale getirmek gerekir.

> with(GaussInt);

> Glbasis(3+4*I,1+I);

> Glbasis(3-4*I,18+8*I);

kodları yazıldığında çıkan sonuç bize $\{3 + 4i, 1 + i\}$ 'nin $\mathbb{Z}[i]$ için bir baz olduğunu fakat $\{3 - 4i, 18 + 8i\}$ 'nin bir baz oluşturmadığını belirtmektedir.

> Gldivisor(73+12*I);

ile $73 + 12i$ nin bölenlerinin $1, 73 + 12i, 15 + 14i, 2 + 3i$ olduğunu anlarız. Bundan biraz farklı olarak,

> GIfactor(128+48*I);

ile $128 + 48i$ 'nin $\mathbb{Z}[i]$ 'de çarpanlara ayrılışının $128 + 48i = (i) \cdot (1 + i)^8 \cdot (-3 + 8i)$ biçiminde olduğunu görürüz.

> Glgcd(1249-185*I,540-138*I);

ile $\text{ebob}(1249 - 185i, 540 - 138i) = 1 + i$ olduğunu görebiliriz. Eğer

> Glgcdex(1249-185*I,540-138*I,'x','y');

yazdıktan sonra sırasıyla x; ve y; yazarsak;

$(1249 - 185i)x + (540 - 138i)y = \text{ebob}(1249 - 185i, 540 - 138i)$ denklemini sağlayan x ve y değerlerinin sırasıyla $178 + 6i$ ve $-385 - 197i$ olduğu görülebilir. Bu şekilde x ve y 'ler elde edildikten sonra eğer sol tarafta ebob'un katı olan bir değer varsa bu denklem de rahatlıkla çözülebilir.

> Gllcm(184+13*I,28-6*I);

komutu ile de $\text{ekok}(184 + 13i, 28 - 6i) = 740 + 5230i$ olduğunu anlarız.

> Glissqr(-297-304*I);

ile $-297 - 304i$ Gauss sayısının, başka bir Gauss sayısının karesi olduğunu doğrulayabiliriz.

Gerçekten $-297 - 304i$ sayısı $8 - 19i$ 'nin karesidir.

> GInearest((5+7*I)/2);

Komutu ile $\frac{5+7i}{2}$ sayısına en yakın Gauss sayısının $3+4i$ olduğunu görmekteyiz.

> GInorm(256-17*I);

yazarak $256 - 17i$ sayısının normunun 65825 olduğunu görürüz.

> GInormal(-13+21*I);

ile $-13 + 21i$ 'nin kompleks düzlemin 1. bölgesinde yer alan eşleniğinin $13 + 21i$ olduğunu görürüz.

> GInodiv(971+38*I);

yazıldığında sonuç olarak çıkan 4 bize $971 + 38i$ nin birbirinin eşlenikleri olmayan 4 tane böleninin olduğunu belirtir.

> GIprime(36+19*I);

ile $36 + 19i$ 'nin bir Gauss asal sayısı olduğunu anlarız.

> GIquo(81-27*I,5+2*I,'r');

> r;

ile $81 - 27i$ nin $5 + 2i$ ile bölümünde sırasıyla bölüm ve kalanın $12 - 10i$ ve $1 - i$ olduğunu görürüz. Eğer sadece kalanı bulmak istersek > GRem(81-27*I,5+2*I) komutunu kullanabiliriz.

4. İKİLİ KUADRATİK FORMLAR ve KUADRATİK SAYI CİSİMLERİYLE BAĞLANTISI

4.1 İkili Kuadratik Formlar

Tanım 4.1. $a, b, c \in \mathbb{Z}$ olmak üzere $Q(x, y) = ax^2 + bxy + cy^2$ şeklinde iki değişkenli ikinci dereceden homojen polinoma tamsayı katsayılı *ikili kuadratik form* (İKF) adı verilir. Katsayıları sırasıyla a, b, c olan İKF bazen basitçe (a, b, c) biçiminde gösterilir.

Tanım 4.2. Eğer $Q(x, y) = n$ olacak şekilde $x, y \in \mathbb{Z}$ tamsayıları varsa $Q(x, y)$ ikili kuadratik formu n sayısını temsil eder denir.

Örnek 4.1. $Q(x, y) = x^2 + y^2$ ikili kuadratik formunun hangi sayıları temsil ettiği temel sayılar teorisinde verilmektedir. Buna göre eğer $n = s^2 p_1 p_2 \dots p_t$ şeklinde çarpanlara ayrılıyorsa ve $p_i (i = 1, 2, \dots, t)$ 'lerin her biri birbirinden farklı asal sayılar ise (kare olanları s 'de topla), n ' nin bu form tarafından temsil edilebilmesi için p_i 'lerin $p_i = 2$ ya da $p_i \equiv 1 \pmod{4}$ şartını sağlaması gerekir.

Değişken sayısı ikiden fazla olduğunda kuadratik form ikili diye isimlendirilmez. Kuadratik formlar üzerinde çalışılarak sayılar teorisinde birçok problem çözülmüştür. Örneğin Lagrange(1736-1855), $x^2 + y^2 + z^2 + w^2$ kuadratik formunun bütün pozitif sayıları temsil ettiği sonucuna varmıştır. Kuadratik formlarda en temel problem hangi sayıların bir kuadratik form tarafından temsil edilip edilmediğinin tespiti ve bu temsilin kaç farklı türde olduğunun bulunmasıdır.

Tanım 4.3. $Q = (a, b, c)$ ikili kuadratik formuna karşılık gelen matris $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ şeklinde tanımlanır.

Teorem 4.1. $v = \begin{pmatrix} x \\ y \end{pmatrix}$ olmak üzere $Q(x, y) = v^T Q v$ dir.

İspat: $ax^2 + bxy + cy^2 = ax^2 + \frac{b}{2}xy + \frac{b}{2}yx + cy^2$ eşitliğinden dolayı açıktır.

Eğer M matrisi tersi tamsayı bileşenli bir matris ise Q ile $M^T Q M$ matrisleri her zaman aynı sayıları temsil ederler. Eğer M matrisinin tamsayı bileşenli tersi M' matrisi ise

$\det M.M' = \det M \det M' = 1$ olacağından $\det M = \pm 1$ olmalıdır. Yine tersine, eğer $\det M = \pm 1$ ise M matrisinin tersi de tamsayı bileşenlidir. Bu yüzden Lagrange $M^T Q M = Q'$ (4.1)

şartlarını sağlayan ve determinantı ± 1 olan bir M matrisi varsa Q ve Q' matrislerini *denk matrisler* olarak tanımlamıştır. Gauss ise (4.1) şartını sağlayan ve determinantı 1 olan bir matris varsa gerçek denklik vardır diye sınırlandırmıştır, bu denkliğe *öz denklik* adı verilir. Bu tanım aşağıdaki biçimde verilebilir.

Tanım 4.4. $Q(x, y) = ax^2 + bxy + cy^2$ ve $Q'(x, y) = a'x^2 + b'xy + c'y^2$ formları verilsin. Eğer $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = M^T \begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix} M$ eşitliğini sağlayan $M \in SL_2(\mathbb{Z})$ matrisi varsa tamsayı katsayılı $Q(x, y)$ ve $Q'(x, y)$ kuadratik formları *denktir* denir ve $Q(x, y) \sim Q'(x, y)$ biçiminde gösterilir. Eğer $\det(M) = 1$ ise $Q(x, y)$ ve $Q'(x, y)$ kuadratik formları *öz denktirler* denir ve $Q(x, y) \approx Q'(x, y)$ biçiminde gösterilir.

Örnek 4.2: (a, b, c) kuadratik formu ile $(c, -b, a)$ kuadratik formu birbirlerine denktirler.

Çünkü $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$ matrisi için $\begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix} = M^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M$ eşitliği sağlanır. Burada eşitliğin sol tarafındaki matrisin temsil ettiği formun Tanım 4.3'ten dolayı $(c, -b, a)$ kuadratik formu olduğu açıktır.

Kolayca gösterilebilir ki;

$$Q(x, y) \sim Q(y, x) \sim Q(-x, y) \sim Q(y, -x) \sim Q(-x, -y) \sim Q(x, -y) \sim Q(-y, x) \sim Q(-y, -x)$$

ve

$$Q(x, y) \approx Q(y, -x) \approx Q(-y, x) \approx Q(-x, -y)$$

dir.

İKF'lar için Tanım 4.4 ile verilen bu bağıntı yansıma, simetri ve geçişme özelliklerini sağladığından dolayı bir denklik bağıntısıdır. İlk olarak Gauss, Disquisitiones Arithmeticae adlı çalışmasında kuadratik formların denkliği üzerine geniş çaplı çalışma yapmıştır. Dedekind'e kadar da kuadratik formların kuadratik sayı cisimlerinin idealleri ile bağlantısı üzerine bir çalışma yapılmamıştır.

Dikkat edilirse eğer Q ve Q' denk iseler $\det Q' = \det M^T \det Q \det M = \det Q$ 'dur.

Bu da bize, katsayıları farklı fakat determinantları aynı olan ve aynı değerleri taşıyan formlar elde etmenin mümkün olduğunu göstermektedir.

Tanım 4.5. $Q(x, y)$ formunun *diskriminantı* $d_Q = -4 \det Q = b^2 - 4ac$ 'dir.

O halde bu tanım yukarıda verilen sonuçla birleştirilirse denk kuadratik formların diskriminantlarının da eşit olduğu sonucuna varılır. Fakat bu ifadenin tersi doğru değildir. Yani diskriminantları aynı olan formların denk olması gerekmez. Örneğin; $(1, 0, 10)$ ve $(2, 0, 5)$ formlarının diskriminantları aynıdır fakat bu iki form denk değildir. Buna örnek olarak $x^2 + 10y^2$ formunun 1'i temsil ettiği aşıkardır ama $2x^2 + 5y^2$ formu 1'i temsil etmez.

Teorem 4.2. İkili kuadratik formların diskriminantlarının kümesi tam olarak $d \equiv 0, 1 \pmod{4}$ şartını sağlayan d tamsayılarından oluşmaktadır.

İspat: Dikkat edilirse $d_Q = b^2 - 4ac \equiv b^2 \equiv 0, 1 \pmod{4}$. Çünkü bir b tamsayısının karesi 4'le bölündüğünde ya 0 veya 1 kalanını verir. Tersine eğer $d \equiv 0 \pmod{4}$ ise

$$Q\left(1, 0, \frac{-d}{4}\right) \quad (4.2)$$

formunun diskriminantı $d_Q = d$ 'dir, eğer $d \equiv 1 \pmod{4}$ olduğunda ise

$$Q\left(1, 1, -\frac{(d-1)}{4}\right) \quad (4.3)$$

yine $d_Q = d$ dir. Eğer d_Q tam-kare ise Q ikili kuadratik formu iki lineer formun çarpımı şeklinde yazılabileceği için bu durumda teori açıktır, bu yüzden sadece diskriminantı tam kare olmayan kuadratik formlar hesaba katılacaktır.

Yani bundan böyle sadece $d = d_Q$ tam-kare olmayan ve $d \equiv 0, 1 \pmod{4}$ biçiminde sayılardan ibaret olacaktır.

Tanım 4.6. Teorem 4.2 ile elde edilen ve (4.2), (4.3) denklemleriyle belirtilen d diskriminantlı bu iki kuadratik forma d *diskriminantlı temel form* adı verilir. Bu formların özelliği 1'i temsil eden d diskriminantlı yegane indirgenmiş form olmalarıdır.

Örnek 4.3. Diskriminantları $-12, -7, 13, 28$ olan temel formların (4.2) ve (4.3) kullanıldığında sırasıyla $x^2 + 3y^2, x^2 + xy + 2y^2, x^2 + xy - 3y^2, x^2 - 7y^2$ olduğu görülür.

Teorem 4.3. Eğer $d > 0$ ise Q hem pozitif hem de negatif sayıları temsil eder. Eğer $d < 0$ ve $a > 0$ ise Q sadece negatif olmayan sayıları temsil eder. Eğer $d < 0$ ve $a < 0$ ise Q sadece pozitif olmayan sayıları temsil eder.

İspat: Eğer $d > 0$ ise $Q(1, 0) = a$ ve $Q(b, -2a) = -da$ iki zıt işaretli sayı olduklarından Q 'nın hem pozitif hem de negatif sayıları temsil ettiği açıktır. Eğer $d < 0$ ise $4aQ(x, y) = 4a(ax^2 + bxy + cy^2) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 - dy^2 \geq 0$

olacağından $Q(x, y) = \frac{(2ax + by)^2 - dy^2}{4a}$ nın alacağı değer doğrudan a 'nın işaretiyle ilgilidir.

Eğer $a > 0$ ise Q sadece negatif olmayan sayıları, $a < 0$ ise Q sadece pozitif olmayan sayıları temsil eder.

Tanım 4.7. Eğer $d_Q > 0$ ise Q 'ya *belirsiz form*, $d_Q < 0$ ve $a > 0$ ise Q 'ya *pozitif belirli*, $d_Q < 0$ ve $a < 0$ olduğunda ise Q 'ya *negatif belirli* form adı verilir.

Ramanujan(1887-1920) denkliği de göz önünde bulundurarak 54 tane pozitif tanımlı diyagonal kuadratik formun bütün pozitif tamsayıları temsil ettiğini ispatlamıştır. Dickson daha sonra diyagonal olmayanlar için de ispatı geliştirmiştir.

Pozitif ve negatif formlar basitçe birbirlerinin negatifleri olduğundan negatif belirli formları göz ardı edip sadece pozitif belirli formlarla çalışmak yeterlidir.

Tanım 4.8. Eğer $\text{ebob}(a, b, c) = 1$ ise $Q(x, y) = ax^2 + bxy + cy^2$ ikili kuadratik formu *ilkeldir* denir.

Kuadratik formlar için verilen bağıntının bir denklik bağıntısı olduğunu belirtmiştik. Dolayısıyla formların denklik sınıfları mevcuttur. Her bir sınıf için katsayıları küçük sayılar olan temsilciler elde edilebilir.

Teorem 4.4. Her bir sınıf $|b| \leq |a| \leq c$ şartını sağlayan bir form içermektedir.

İspat: Sözü edilen sınıftan (a_0, b_0, c_0) formunu ele alalım. m 'nin de (a_0, b_0, c_0) İKF'ü tarafından minimal mutlak değerle temsil edildiğini varsayalım. Böylece

$$m = a_0 r^2 + b_0 r t + c_0 t^2$$

Dir.

Burada $ebob(r, t) = 1$ olmalıdır aksi halde $\frac{m}{ebob(r, t)}$ minimal temsille çelişir. O halde $ru - st = 1$ olan u ve t tamsayıları bulunabilir.

$\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ matrisi (a_0, b_0, c_0) formunu bir kısım b' ve c' sayıları için (a, b', c') formuna dönüştürür. $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ dönüşümü de (a, b', c') formunu $(a_0, 2ah + b', c(h))$ formuna dönüştürür.

Dolayısıyla uygun seçilen bir h değeri için ikinci bileşen b , $(-|a|, |a|)$ aralığına düşürülebilir. Böylece (a, b, c) formunun sınıfından $|b| \leq |a|$ şartını sağlayan bir eleman elde ettik. $c \neq 0$, Q tarafından temsil edilebileceği için beklenildiği gibi $|a| \leq |c|$ elde ederiz.

O halde verilen şartı sağlayan bir form mutlaka bulunabilir. Bu şartı veya denk olan şartları sağlayan formlar özel bir öneme sahiptir.

Tanım 4.9.

$Q(x, y) = ax^2 + bxy + cy^2$ İKF'nun diskriminantı tam-kare olmasın. Eğer

$$-a < b \leq a; \quad a \leq c, \quad \text{ve} \quad a = c \quad \text{ise} \quad b \geq 0 \quad (4.4)$$

şartları sağlanıyorsa $Q(x, y) = ax^2 + bxy + cy^2$ İKF'una *indirgenmiş form* adı verilir.

Bu tanımın geometrik karşılığı $ax^2 + bx + c$ 'nin kökü olan ve kompleks üst yarı düzlemde yer

alan $\tau = \frac{-b + \sqrt{d}}{2a}$ 'nın $SL_2(\mathbb{Z})$ dönüşümü için standart temel bölgede bulunması demektir.

İndirgenmiş formlar elde etmek için basit bir prosedür:

1- Eğer $|b| > a$ ise $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dönüşümünü uygulayarak b 'yi $-a \leq b \leq a$ aralığında bırakacak şekilde a 'ya dönüştürmek.

2- Eğer $a > c$ ise $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ dönüşümünü uygulayarak a ve c 'yi birbirlerine

dönüştüreceğiz. Eğer $a = c$ ise $b \geq 0$ olduğundan emin olunur ya da aynı dönüşüm yeniden uygulanır.

3- Eğer yine $|b| > a$ ise birinci adım tekrar uygulanarak sürece devam edilir.

İndirgenmiş formlar elde etmek için uygulanabilecek bu yöntemdeki koşullara işlemleri biraz daha da kolaylaştıracak ek bir koşul ekleyebiliriz. Şöyle ki;

$$|d| = 4ac - b^2 \geq 4a^2 - b^2 \geq 3a^2 \geq 3b^2$$

dir.

Yani daha çok

$$|b| \leq \sqrt{\frac{d}{3}} \quad (4.5)$$

şartını sağlayan kuadratik formlarla uğraşmak yeterli olacaktır. Bu da bize kuadratik formları temsil eden sadece sonlu sayıda (a, b, c) üçlülerini hesaba katma kolaylığı getirecektir. Böylelikle formları sayma şansına sahip olmuş oluruz.

Sonuç olarak d tam-kare olmayan bir tamsayı olmak üzere, d diskriminantlı her kuadratik form indirgenmiş bir kuadratik forma denktir.

Tanım 4.10. d tam-kare olmasın. d diskriminantlı ilkel kuadratik formların denklik sınıfları sayısına d nin sınıf sayısı denir ve $h(d)$ ile gösterilir.

Örnek 4.4. $K = \mathbb{Q}(\sqrt{-119})$ sanal kuadratik sayı cismini hesaba katalım. Burada, Tanım 4.9'un sonunda elde edilen koşuldan dolayı sadece $|b| \leq \sqrt{\frac{d}{3}} \approx 6.29$ şartını sağlayan b 'leri hesaba katmamız yeterlidir. -119 tek sayı olduğundan b 'de tek'tir ve bu biçimde b 'ler de $b = \pm 1, \pm 3, \pm 5$ ten ibarettir. Aşağıdaki tabloda (4.4) ve (4.5)'i sağlayan bütün (a, b, c) üçlülerini yani indirgenmiş formlar hesaplanmıştır. Bu tablodan da anlaşılacağı üzere diskriminantı -119 olan indirgenmiş formların sayısı 8 'dir. Böylece $h(\mathbb{Q}(\sqrt{-119})) = 10$ elde ettik.

Çizelge 4.1 $K = \mathbb{Q}(\sqrt{-119})$ sanal kuadratik sayı cismi için indirgenmiş kuadratik formlar

b	$ac = \frac{119 + b^2}{4}$	(a, b, c)
1	30	(1, 1, 30), (2, 1, 15), (3, 1, 10), (5, 1, 6)
-1	30	(2, -1, 15), (3, -1, 10), (5, -1, 6)
3	32	(4, 3, 8)
-3	32	(4, -3, 8)
5	36	(6, 5, 6)
-5	36	-

4.2 İkili Kuadratik Formlar ve Kuadratik Sayı Cisimlerinin İdealleri Arasındaki Bağlantı

Bu kısımda kuadratik formlar ile kuadratik sayı cisimlerinin idealleri arasındaki ilişki kısaca sanal kuadratik sayı cisimlerini ele alarak açıklanacak. Yine kuadratik formlar arasında tanımlanan bir bileşke işleminin O_K 'nin idealleri arasında tanımlanan çarpma işlemine karşılık geldiği görülecektir.

$K = \mathbb{Q}(\sqrt{d})$ diskriminantı $d = d_K < 0$ olan sanal kuadratik sayı cismi olsun. K 'nin $\alpha = (\alpha, \beta)$ ideali verilsin. Bu ideale karşılık gelen kuadratik form aşağıdaki şekildedir.

$$Q_\alpha(x, y) = \frac{1}{N(\alpha)} N(\alpha x + \beta y) = \frac{1}{N(\alpha)} (\alpha x + \beta y)(\alpha'x + \beta'y) = ax^2 + bxy + cy^2. \quad (4.6)$$

Norm form diye isimlendirilen (4.6) denklemindeki form pozitif tanımlıdır ve diskriminantı $d = d_K$ 'dir. $Q_\alpha(x, y)$ 'nin denklik sınıfı α 'nın tamlık tabanının seçiminden bağımsızdır. Bundan ayrı α ile aynı ideal sınıfında bulunan bir $\mathbf{b}$ ideali için $Q_\alpha(x, y) \sim Q_{\mathbf{b}}(x, y)$ 'dir.

Tersine bir eşleme için tamsayı katsayılı pozitif tanımlı $d < 0$ diskriminantlı $Q(x, y) = ax^2 + bxy + cy^2$ kuadratik formuyla başlayalım. $K = \mathbb{Q}(\sqrt{d})$ de buna karşılık gelen ideali bulmak istiyoruz. $Q(x, y)$ yi çarpanlarına ayırırsak $\theta = \frac{b + \sqrt{d}}{2a}$, $Q(x, 1)$ 'in eksi bir kökü olmak üzere $Q(x, y) = a(x + \theta y)(x + \theta'y)$ 'dir ve burada θ kompleks üst yarı düzlemde. $a\theta \in O_K$ olduğu açıktır, ayrıca $(a, a\theta)$ ideali tam idealdir.

İki denk form'da aynı ideal sınıfında bulunan ideallere denk gelir. Bununla birlikte $Q(x, y) = ax^2 + bxy + cy^2$ ve θ daha önce verildiği gibi, $\alpha = (a, a\theta)$ olmak üzere ve $Q_\alpha(x, y)$

formu $Q(x, y)$ 'ye eşit form olmak üzere aşağıdaki eşleme verilebilir.

Teorem 4.5. (Mastropietro, 2000) $K = \mathbb{Q}(\sqrt{d})$, diskriminantı $d = d_K < 0$ olan sanal kuadratik sayı cismi olsun. K 'nın ideal sınıfları ile d diskriminantlı pozitif tanımlı formlar arasında birebir bir eşleme vardır ve bu eşleme

$$\mathfrak{a} = (\alpha, \beta) \rightarrow \frac{1}{N(\mathfrak{a})} N(\alpha x + \beta y),$$

$$ax^2 + bxy + cy^2 \rightarrow \left(a, \frac{b + \sqrt{b^2 - 4ac}}{2} \right)$$

şeklinde verilir.

Son olarak kuadratik sayı cisimlerinde O_K 'nin ideallerinin çarpımına karşılık gelen formların bileşke işlemini tanımlayalım.

Tanım 4.11. $Q_1(x, y) = a_1x^2 + b_1xy + c_1y^2$ ve $Q_2(x, y) = a_2x^2 + b_2xy + c_2y^2$ aynı

diskriminantlı iki kuadratik form olmak üzere

$$s = (b_1 + b_2)/2, n = (b_1 - b_2)/2 \text{ ve } u, v, w \text{ ve } d$$

$$u = a_1 + va_2 + ws = d = \text{ebob}(a_1, a_2, s) \text{ ve} \quad (4.7)$$

$d_0 = \text{ebob}(d, c_1, c_2, n)$ olarak verilsin.

$Q_1(x, y)$ ve $Q_2(x, y)$ kuadratik formlarının denklik sınıflarının bileşkesi katsayıları (a_3, b_3, c_3) aşağıdaki gibi verilen $Q_3(x, y)$ kuadratik formunun denklik sınıfı olarak verilir.

$$a_3 = d_0 \frac{a_1 a_2}{d_2}, b_3 = b_2 + 2 \frac{a_2}{d} (v(s - b_2) - wc_2), c_3 = \frac{b_3^3 - D}{4a_3} \quad (4.8)$$

Bu bileşke işlemini ve ideallerdeki çarpma işlemiyle bağlantısını bir örnekle açıklayalım.

Örnek 4.5. $K = \mathbb{Q}(\sqrt{-71})$ sanal kuadratik sayı cisminde $|b| \leq \sqrt{\frac{71}{3}} \leq 4$ şartını sağlayan b 'leri yani $b = \pm 1, \pm 3$ 'ü hesaba katmamız gerekir. Aşağıdaki tabloda bu biçimde ve denklem (4.5)'i sağlayan bütün (a, b, c) üçlülere gösterilmiştir.

Çizelge 4.2 $K = \mathbb{Q}(\sqrt{-71})$ sanal kuadratik sayı cismi için indirgenmiş kuadratik formlar

b	$ac = \frac{71+b^2}{4}$	(a, b, c)
1	18	(1, 1, 18), (2, 1, 9), (3, 1, 6)
-1	18	(2, -1, 9), (3, -1, 6)
3	20	(4, 3, 5)
-3	20	(4, -3, 5)

Burada görünmeyen fakat diskriminantı -71 olan her bir kuadratik formun Tanım 4.9'un sonunda verilen dönüşümler kullanılarak indirgeme işlemi yapıldığında aşağıda gösterildiği gibi başka bir indirgenmiş forma karşılık geldiği görülür.

$$\begin{array}{ll}
 [1, 1, 18] \rightarrow [1, 1, 18] & [5, 3, 4] \rightarrow [4, -3, 5] \\
 [1, 3, 20] \rightarrow [1, 1, 18] & [6, 1, 3] \rightarrow [3, -1, 6] \\
 [2, 1, 9] \rightarrow [2, 1, 9] & [9, 1, 2] \rightarrow [2, -1, 9] \\
 [2, 3, 10] \rightarrow [2, -1, 9] & [10, 3, 2] \rightarrow [2, 1, 9] \\
 [3, 1, 6] \rightarrow [3, 1, 6] & [18, 1, 1] \rightarrow [1, 1, 18] \\
 [4, 3, 5] \rightarrow [4, 3, 5] & [20, 3, 1] \rightarrow [1, 1, 18]
 \end{array}$$

Sonuç olarak $h(\mathbb{Q}(\sqrt{-71})) = 7$ elde ettik. Bu kuadratik formlara karşılık gelen idealleri $Q(x, y) \rightarrow (a, a\theta)$ eşlemesini kullanarak bulabiliriz. Ayrıca

$$2O_K = \mathfrak{p}_2 \mathfrak{p}_2'$$

$$3O_K = \mathfrak{p}_3 \mathfrak{p}_3'$$

olduğu açıktır. Burada $2x^2 \pm xy + 9y^2$ formları $\mathfrak{p}_2, \mathfrak{p}_2'$ ideallerine $3x^2 \pm xy + 6y^2$ formları ise $\mathfrak{p}_3, \mathfrak{p}_3'$ ideallerine karşılık gelir. Aslında $Q_1(x, y) = ax^2 + bxy + cy^2$ ve $Q_2(x, y) = ax^2 - bxy + cy^2$ formları her zaman birbirinin eşleniği olan ideallere karşılık gelirler. Bunu $\theta_2 = -\theta_1$ eşitliğinden görebiliriz. Dolayısıyla $Q_2(x, y)$ formunun eşleniği olan $Q_1(x, y)$ formuna karşılık gelen ideal $(a, -a\theta_1') = (a, -a\theta_1')$ dir. O halde sadece normu 4 olan idealler kaldı. Bunlar da $2O_K, \mathfrak{p}_2^2, \mathfrak{p}_2'^2$ olmak üzere üç tanedir. $2O_K$ temel idealdir ve temel sınıf $x^2 + xy + 18y^2$ formuna karşılık geldiğinden son iki form $\mathfrak{p}_2^2$ ile $\mathfrak{p}_2'^2$ ideallerine karşılık gelirler. Burada ideal sınıf grubu devirseldir ve $\mathfrak{p}_2$ ideali tarafından üretilir. Tanım 4.11'i kullanarak bunu kolayca görebiliriz. (2, 1, 9) formunun kendisiyle bileşkesi (4.7) ve (4.8) denklem takımları kullanıldığında (4, -3, 5) formunu verir, ve sırasıyla bu formun 3., 4., 5.,

6.,7., kuvvetleri de $(3, 1, 6), (3, -1, 6), (4, 3, 5), (2, -1, 9), (1, 1, 18)$ formlarını vermektedir. 8 kez kendisiyle bileşkesi ise yine kendisini vermektedir. Bunun böyle olacağı sınıf sayısının 7 olmasından açıktır. Aşağıdaki pari kodu da bunu yapabilir. Bunu Çizelge 4.3'teki $d = -71$ olan satırdan görmek mümkündür. Burada grubun üretici olan ideal $[2, 0; 0, 1]$ yani tablonun başında açıklandığı gibi $\mathfrak{p}_2 = \left(2, \frac{1 + \sqrt{-71}}{2}\right)$, yi belirtmektedir. Yine kuadratik formlara göre düşünersek son sütundan $(2, 1, 9)$ formunun üreteç olduğu görülmektedir.

```
kuvvet(s)=for(i=1,qfbclassno(s),print(i," ",qfbprimeform(s,2)^i))
kuvvet(-71)
```

Ayrıca formların bileşkesini kullandığımızda sonuç olarak $(1, 1, 18)$ kuadratik formunun da etkisiz eleman olduğunu görmekteyiz. Her bir elemanla bileşkesi kendisini vermektedir.

Çizelge 4.3 $d = -1, -2, \dots, -100$ için, TİB olmayan sanal kuadratik sayı cisimleri $K = \mathbb{Q}(\sqrt{d})$ 'lerde ideal sınıf gruplarının yapıları.

Bu tabloda 2. sütundaki $h = h_K$, $K = \mathbb{Q}(\sqrt{d})$ sanal kuadratik sayı cisminin sınıf sayısını, üçüncü sütunda verilen grup, sınıf grubu $\mathfrak{Cl}(O_K)$ 'nin izomorf olduğu grubu belirtmektedir. Dördüncü sütundaki matrisler ise sınıf grubunun üretici olan idealleri belirtmektedir. Örneğin $d = -5$ alınırsa $K = \mathbb{Q}(\sqrt{-5})$ in sınıf sayısının 5 olduğu O_K 'nin ideal sınıf grubunun $\mathfrak{Cl}(O_K) \cong \mathbb{Z}/2\mathbb{Z}$ şeklinde $\mathbb{Z}/2\mathbb{Z}$ e izomorf olduğu ve bu grubun üretici olan idealin $\alpha_2 = (2 + 0, 1 + \omega_K) = (2, 1 + \sqrt{-5})$ ideali olduğunu gösterir. Tabloda sınıf sayısı 1 olan kuadratik sayı cisimleri yer almamıştır, bunlar için bilindiği gibi $\mathfrak{Cl}(O_K) \cong (1)$ dir. Tablo pari programı kullanılarak elde edilmiştir. Beşinci sütun ise sınıf grubunun üretici olan formu belirtmektedir. Örneğin $\text{Qfb}(3, -2, 2)$, diskriminantı $(-2)^2 - 4.3.2 = -20$ olan $Q(x, y) = x^2 - 2xy + 3y^2$ kuadratik formunu temsil etmektedir.

d	h	$\mathfrak{Cl}(O_K) \cong$	Sınıf grubunun üretici olan ideal ya da idealler	Sınıf grubunun üretici olan form ya da formlar
-5	2	$\mathbb{Z}/2\mathbb{Z}$	$[2, 1; 0, 1]$	$[\text{Qfb}(3, -2, 2)]$
-6	2	$\mathbb{Z}/2\mathbb{Z}$	$[2, 0; 0, 1]$	$[\text{Qfb}(5, -4, 2)]$
-10	2	$\mathbb{Z}/2\mathbb{Z}$	$[2, 0; 0, 1]$	$[\text{Qfb}(7, -4, 2)]$
-13	2	$\mathbb{Z}/2\mathbb{Z}$	$[2, 1; 0, 1]$	$[\text{Qfb}(7, -2, 2)]$
-14	4	$\mathbb{Z}/4\mathbb{Z}$	$[3, 2; 0, 1]$	$[\text{Qfb}(3, 2, 5)]$
-15	2	$\mathbb{Z}/2\mathbb{Z}$	$[2, 0; 0, 1]$	$[\text{Qfb}(2, 1, 2)]$
-17	4	$\mathbb{Z}/4\mathbb{Z}$	$[3, 2; 0, 1]$	$[\text{Qfb}(3, 2, 6)]$
-21	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$[2, 1; 0, 1], [5, 2; 0, 1]$	$[\text{Qfb}(2, 2, 11), \text{Qfb}(5, 4, 5)]$
-22	2	$\mathbb{Z}/2\mathbb{Z}$	$[2, 0; 0, 1]$	$[\text{Qfb}(13, -4, 2)]$
-23	3	$\mathbb{Z}/3\mathbb{Z}$	$[2, 0; 0, 1]$	$[\text{Qfb}(2, 1, 3)]$
-26	6	$\mathbb{Z}/6\mathbb{Z}$	$[5, 2; 0, 1]$	$[\text{Qfb}(5, -4, 6)]$
-29	6	$\mathbb{Z}/6\mathbb{Z}$	$[3, 2; 0, 1]$	$[\text{Qfb}(3, 2, 10)]$
-30	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$[3, 0; 0, 1], [5, 0; 0, 1]$	$[\text{Qfb}(3, 0, 10), \text{Qfb}(5, 0, 6)]$
-31	3	$\mathbb{Z}/3\mathbb{Z}$	$[2, 1; 0, 1]$	$[\text{Qfb}(2, 1, 4)]$
-33	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$[2, 1; 0, 1], [6, 3; 0, 1]$	$[\text{Qfb}(2, 2, 17), \text{Qfb}(6, 6, 7)]$
-34	4	$\mathbb{Z}/4\mathbb{Z}$	$[5, 4; 0, 1]$	$[\text{Qfb}(5, 2, 7)]$
-35	2	$\mathbb{Z}/2\mathbb{Z}$	$[3, 0; 0, 1]$	$[\text{Qfb}(3, 1, 3)]$
-37	2	$\mathbb{Z}/2\mathbb{Z}$	$[2, 1; 0, 1]$	$[\text{Qfb}(19, -2, 2)]$
-38	6	$\mathbb{Z}/6\mathbb{Z}$	$[3, 2; 0, 1]$	$[\text{Qfb}(3, 2, 13)]$

-39	4	$Z/4Z$	$[2, 0; 0, 1]$	$[Qfb(2, 1, 5)]$
-41	8	$Z/8Z$	$[3, 2; 0, 1]$	$[Qfb(3, 2, 14)]$
-42	4	$Z/2Z \oplus Z/2Z$	$[3, 0; 0, 1], [6, 0; 0, 1]$	$[Qfb(3, 0, 14), Qfb(6, 0, 7)]$
-46	4	$Z/4Z$	$[5, 3; 0, 1]$	$[Qfb(5, 4, 10)]$
-47	5	$Z/5Z$	$[2, 1; 0, 1]$	$[Qfb(2, 1, 6)]$
-51	2	$Z/2Z$	$[3, 1; 0, 1]$	$[Qfb(5, -3, 3)]$
-53	6	$Z/6Z$	$[3, 2; 0, 1]$	$[Qfb(3, 2, 18)]$
-55	4	$Z/4Z$	$[2, 0; 0, 1]$	$[Qfb(2, 1, 7)]$
-57	4	$Z/2Z \oplus Z/2Z$	$[2, 1; 0, 1], [6, 3; 0, 1]$	$[Qfb(2, 2, 29), Qfb(6, 6, 11)]$
-58	2	$Z/2Z$	$[2, 0; 0, 1]$	$[Qfb(31, -4, 2)]$
-59	3	$Z/3Z$	$[3, 2; 0, 1]$	$[Qfb(3, 1, 5)]$
-61	6	$Z/6Z$	$[7, 3; 0, 1]$	$[Qfb(7, -6, 10)]$
-62	8	$Z/8Z$	$[3, 2; 0, 1]$	$[Qfb(3, 2, 21)]$
-65	8	$Z/4Z \oplus Z/2Z$	$[3, 2; 0, 1], [2, 1; 0, 1]$	$[Qfb(3, 2, 22), Qfb(2, 2, 33)]$
-66	8	$Z/4Z \oplus Z/2Z$	$[5, 3; 0, 1], [2, 0; 0, 1]$	$[Qfb(5, 4, 14), Qfb(2, 0, 33)]$
-69	8	$Z/4Z \oplus Z/2Z$	$[5, 4; 0, 1], [2, 1; 0, 1]$	$[Qfb(5, 2, 14), Qfb(2, 2, 35)]$
-70	4	$Z/2Z \oplus Z/2Z$	$[5, 0; 0, 1], [7, 0; 0, 1]$	$[Qfb(5, 0, 14), Qfb(7, 0, 10)]$
-71	7	$Z/7Z$	$[2, 0; 0, 1]$	$[Qfb(2, 1, 9)]$
-73	4	$Z/4Z$	$[7, 5; 0, 1]$	$[Qfb(7, 4, 11)]$
-74	10	$Z/10Z$	$[5, 1; 0, 1]$	$[Qfb(5, -2, 15)]$
-77	8	$Z/4Z \oplus Z/2Z$	$[3, 2; 0, 1], [2, 1; 0, 1]$	$[Qfb(3, 2, 26), Qfb(2, 2, 39)]$
-78	4	$Z/2Z \oplus Z/2Z$	$[3, 0; 0, 1], [6, 0; 0, 1]$	$[Qfb(3, 0, 26), Qfb(6, 0, 13)]$
-79	5	$Z/5Z$	$[2, 1; 0, 1]$	$[Qfb(2, 1, 10)]$
-82	4	$Z/4Z$	$[7, 4; 0, 1]$	$[Qfb(7, 6, 13)]$
-83	3	$Z/3Z$	$[3, 2; 0, 1]$	$[Qfb(3, 1, 7)]$
-85	4	$Z/2Z \oplus Z/2Z$	$[5, 0; 0, 1], [10, 5; 0, 1]$	$[Qfb(2, 2, 43), Qfb(10, 10, 11)]$
-86	10	$Z/10Z$	$[3, 2; 0, 1]$	$[Qfb(3, 2, 29)]$
-87	6	$Z/6Z$	$[2, 0; 0, 1]$	$[Qfb(2, 1, 11)]$
-89	12	$Z/12Z$	$[3, 2; 0, 1]$	$[Qfb(3, 2, 30)]$
-91	2	$Z/2Z$	$[5, 1; 0, 1]$	$[Qfb(5, 3, 5)]$
-93	4	$Z/2Z \oplus Z/2Z$	$[3, 0; 0, 1], [6, 3; 0, 1]$	$[Qfb(2, 2, 47), Qfb(6, 6, 17)]$
-94	8	$Z/8Z$	$[5, 4; 0, 1]$	$[Qfb(5, 2, 19)]$
-95	8	$Z/8Z$	$[2, 1; 0, 1]$	$[Qfb(2, 1, 12)]$
-97	4	$Z/4Z$	$[7, 6; 0, 1]$	$[Qfb(7, 2, 14)]$

4.3 Bölümle İlgili Pari Komut ve Programları

$\text{Qfb}(a,b,c)$: $ax^2 + bxy + cy^2$ ikili kuadratik formunu oluşturur.

Örnek 4.6. $2x^2 + xy + 15y^2$ İKF'ünü oluşturmak için $\text{Qfb}(2,1,15)$ yazmak gereklidir.

$\text{qfbclassno}(\text{dk}, \{\text{flag}(=0)\})$: Shank algoritmasını kullanarak d_K diskriminantlı kuadratik forma karşılık gelen sınıf sayısını verir. Eğer geçerli flag değeri 0 yerine 1 kullanılırsa Euler çarpımını kullanarak sonucu bulur.

Örnek 4.7. Çizelge.3.4 için,

```
for(d=2,870,if(issquarefree(d),\
write("sinifsayisireel.doc",d,"",qfbclassno(quaddisc(d))))))
```

kodlarını kullandım. Çizelge.3.5 için ise aşağıdaki kodları kullandım.

```
for(d=1,720,if(issquarefree(-d),\
write("sinifsayisisanal.doc",-d,"",qfbclassno(quaddisc(-d))))))
```

Sonuçlar sırasıyla “sinifsayisireel.doc” ve “sinifsayisisanal.doc” isimli dokümanlara aktarıldı.

$\text{qfbcompraw}(Q1,Q2)$: $Q1$ ve $Q2$ İKF'lerinin bileşkesini verir. Fakat sonuçta verilen form indirgenmiş bir İKF olmayabilir(indirgemediği için).

$\text{qfbnucomp}(Q1,Q2,l)$: $Q1$ ve $Q2$ ilkel pozitif tanımlı İKF'lerinin bileşkesini verir. l olarak herhangi bir pozitif sabit alınabilir, fakat en uygun hız için, d_Q değeri $Q1$ ve $Q2$ formlarının ortak diskriminantı olmak üzere $l = |d_Q|^{1/4}$ alınmalıdır.

$\text{qfbnupow}(Q,n)$: Q ilkel pozitif tanımlı ikili kuadratik formunun n . kuvvetini alır.

Örnek 4.8. Aşağıda açıklanacak olan $\text{quadclassunit}(\text{quaddisc}(-143))$ ile -143 diskriminantlı kuadratik formların sınıf grubunun mertebesinin, 10 olduğunu ve grubun üreticinin $(2, 1, 18)$ olduğunu görmekteyiz. $Q=\text{Qfb}(2,1,18)$; $\text{for}(i=1,11,\text{print}(\text{"Qfb}(2,1,18)^\wedge",i,"=",\text{qfbnupow}(Q,i)))$ komutu da $(2,1,18)$ İKF'ünün ilk 11 kuvvetini almaktadır. Burada görüldüğü gibi 11. kuvveti grubun üretici olan $(2,1,18)$ İKF'ünü vermektedir.

$\text{qfbpowraw}(Q,n)$: Q ilkel pozitif tanımlı ikili kuadratik formun n . kuvvetini alıp indirgeme

yapmadan sonucu verir. Yani qfbcompraw kullanarak sonucu bulur. Burada n 'nin pozitif ve 2^{31} 'den küçük olması gerekir.

qfbprimeform(dQ,p): d_Q diskriminantlı, baş katsayısı p olan asal İKF' u verir.

qfbred(Qfb(a,b,c)): (a, b, c) ikili kuadratik formunu indirger.

qfbsolve(Q,p): p asal sayısının Q sanal İKF' u tarafından temsil edilip edilmeyeceğini bulur.

Örnek 4.9. 1' den 1000'e kadar hangi asalların $x^2 + 3y^2$, İKF' u tarafından temsil edildiğini ve hangi x, y değerlerinin bunu sağladığını görmek için forprime(i=1,1000,print(i," ",qfbsolve(Qfb(1,0,3),i))) yazmak yeterlidir.

$Q=(a,b,c)$ pozitif tanımlı ikili kuadratik formlar olmak üzere olmak üzere Bölüm 4.1' deki tanım ve teoremler ışığında, $Q=(a,b,c)$ pozitif tanımlı ikili kuadratik formunun indirgenmiş olup olmadığını araştırmak için Pari Programı

```
{indirgenmis(a,b,c) =
local(dQ);
dQ= b^2-4*a*c;
if(dQ>=0 || a<0,
error("Q(a,b,c) Pozitif Tanimli Olmali!"));
if(!(abs(b)<=a && a<=c), return(0));
if(abs(b)==a || a==c, return(b>=0));
return(1);
}
```

Örnek 4.10. indirgenmis(3,4,6), yazılırsa $3x^2 + 4xy + 6y^2$ kuadratik formunun indirgenmiş olmadığı anlaşılır.

Q Pozitif tanımlı ikili kuadratik formunu indirgemek için Pari Programı

```
{indirge(q)=
local(dQ, k, t, a,b,c);
```

```

a=q[1]; b=q[2]; c=q[3]; dQ=b^2-4*a*c;
if(dQ>=0 || a<0, error("Verilen Kuadratik Form Pozitif Tanimli Olmalidir!"));
while(!indirgenmis(a,b,c),
if(c<a, b=-b; t=a; a=c; c=t,
if(abs(b)>a || -b==a, k= floor((a-b)/(2*a));
b=b+2*k*a;c=(b^2-dQ)/(4*a);
)
)
);
return([a,b,c])
}

```

Örnek 4.11. indirge([3,4,6]) yazıldığında $3x^2 + 4xy + 6y^2$ İKF'unun denk olduğu indirgenmiş formun $3x^2 - 2xy + 5y^2$ olduğu görülür.

d_Q diskriminantlı indirgenmiş formları elde etmek için Pari Programı

```

{indirgenmisformlar(dQ)=
local(sinir, Formlar, b,ind);
if (dQ>0, error("Girdiginiz Deger Negatif Degil!"));
if (dQ%4 ==2 || dQ%4==3, error("Bu Bir Kuadratik Formun Diskriminanti Degildir"));
sinir = floor(-dQ/3) ;
Formlar =[];
for(a= 1, sinir,
for(c = 1, sinir,
if(3*a*c<=-dQ && issquare(4*a*c+dQ),
b= floor(sqrt(4*a*c+dQ));

```

```

ind=indirge( [a,b,c] );

print1( [a,b,c] , "---> ", ind) ;

if (gcd(ind[1],gcd(ind[2],ind[3]))==1,

Formlar = setunion(Formlar, [ind]); print(""),

print (" \t(ilkel degil)")

)

)

)

);

return(eval(Formlar));

}

```

Örnek 4.12. indirgenmisformlar(-2003) yazıldığında -251 diskriminantlı indirgenmiş ikili kuadratik formların $(1,1,501), (13,-5,39), (13,5,39), (19,-7,27), (19,7,27), (3,-1,167), (3,1,167), (9,-7,57), (9,7,57)$ 'lerden ibaret olduğu anlaşılır. Ayrıca diskriminantı -2003 olan diğer formların da hangi indirgenmiş forma denk olduğu da sonuçlardan görülebilir. Örneğin sonuçtaki $[657, 25, 1] \rightarrow [1, 1, 501]$ ten $657x^2 + 25xy + 1y^2$ formunun aynı diskriminantlı indirgenmiş $x^2 + xy + 501y^2$ formuna denk olduğu anlaşılır.

Tanım 4.3 kullanarak Q_1 ve Q_2 ikili kuadratik formlarının bileşkesini bulmak için Pari Programı

```

{bileske(q1, q2)=

local(dQ,dQ2,s,n,b0,b1,u,v,w,a,b,c,bileskeF);

dQ=q1[2]^2-4*q1[1]*q1[3]; dQ2= q2[2]^2-4*q2[1]*q2[3];

if(dQ2!=dQ, error("Diskriminantlari Ayni Olan Formlar Girmeniz Gerekir!"));

s=(q1[2]+q2[2])/2; n=(q1[2]-q2[2])/2;

b0=bezout(q1[1],q2[1]);

```

```

b1=bezout(b0[3],s);

u=b1[1]*b0[1];

v=b1[1]*b0[2];

w=b1[2];

d=b1[3];

d0=gcd(gcd(gcd(d,q1[3]),q2[3]),n);

a=d0*q1[1]*q2[1]/d^2;

b=q2[2]+2*q2[1]*(v*(s-q2[2])-w*q2[3])/d;

c=(b^2-dQ)/(4*a);

bileskeF = indirge( [a,b,c] );

return(bileskeF);

}

```

Örnek 4.13. $\text{bileske}([5,3,13],[7,-1,9])$ yazarak $5x^2 + 3xy + 13y^2$ ile $7x^2 - xy + 9y^2$ formlarının bileşkesi olan formun $3x^2 - xy + 21y^2$ formu olduğunu görebiliriz. Eğer $\text{bileske}([5,3,13],[7,-1,9])$ yazarsak bu iki formun diskriminantları aynı olmadığından dolayı hata mesajı ile karşılaşırız.

5. ZETA ve L-FONKSİYONLARI

5.1 Dirichlet Karakterleri

Tanım 5.1. G bir grup olsun. Eğer G üzerinde tanımlı kompleks-değerli bir f fonksiyonu $\forall a, b \in G$ için $f(ab) = f(a)f(b)$, ve $\exists c \in G : f(c) \neq 0$ özelliklerini taşıyorsa f 'ye G 'nin bir karakteri adı verilir.

Teorem 5.1. (Apostol, 1976) f , etkisiz elemanı e olan sonlu bir G grubunun karakteri ise $f(e) = 1$ 'dir ve her bir $f(a)$ değeri 1'in bir köküdür. Eğer $a^n = e$ ise $f(a)^n = 1$ 'dir.

İspat: $c \in G$ için $f(c) \neq 0$ olsun. $ce = c$ olduğundan $f(ce) = f(c)$ 'dir. Dolayısıyla $f(e) = 1$. Eğer $a^n = e \Rightarrow f(a)^n = f(a^n) = f(e) = 1$ 'dir.

Tanım 5.2. G üzerinde her bir elemanı 1'e taşıyan karaktere *temel (principal) karakter* adı verilir. Her grupta en azından temel karakter mevcuttur.

Teorem 5.2. Sonlu, değişmeli bir G grubunun mertebesi n ise, G tam olarak n -farklı karaktere sahiptir.

G grubu olarak $\text{mod } k$ indirgenmiş temsilciler sistemi (İTS) alalım. Bilindiği gibi İTS $\{a_1, a_2, \dots, a_{\varphi(n)}\}$ (5.1)

biçiminde $\text{mod } k$ 'ya göre birbirlerine denk olmayan ve her biri k ile aralarında asal olan $\varphi(n)$ tane tamsayıdan oluşur.

Bu sistemdeki her bir a 'ya karşılık gelen $\bar{a}$ temsilci sınıfı $\bar{a} = \{x : x \equiv a(\text{mod } k)\}$ şeklindedir.

Bu temsilci sınıflarının çarpımı $\bar{a}\bar{b} = \overline{ab}$ şeklinde tanımlanmıştır.

Bu biçimde tanımlanan çarpmaya göre (5.1) ile verilen $\text{mod } k$ İTS, mertebesi $\varphi(n)$ olan sonlu ve değişmeli bir gruptur. Bu grubun etkisiz elemanı $\bar{1}$ temsilci sınıfı ve $\bar{a}$ temsilci sınıfının ters elemanı $\bar{a}\bar{b} \equiv \bar{1}(\text{mod } k)$ şartını sağlayan $\bar{b}$ temsilci sınıfıdır (Ters elemanın varlığı açıktır).

Tanım 5.3. $G, \text{mod } k$, İTS grubu olsun. G 'nin her bir karakteri f için $\chi = \chi_f$ aritmetik fonksiyonunu,

$$\chi(n) = \begin{cases} f(\bar{n}), & (n, k) = 1 \text{ ise} \\ 0, & (n, k) > 1 \text{ ise} \end{cases} \quad (5.2)$$

biçiminde tanımlarız.

Bu şekilde tanımlanan χ fonksiyonuna, mod k Dirichlet karakteri adı verilir. Temel karakter

$$\chi_1(n) = \begin{cases} 1, & (n, k) = 1 \text{ ise} \\ 0, & (n, k) > 1 \text{ ise} \end{cases}$$

Özelliklerini taşıyan karakterdir.

Teorem 5.3. Her biri aşağıdaki iki şartı sağlayan $\phi(k)$ tane birbirinden farklı mod k Dirichlet karakteri mevcuttur. $\forall m, n \in \mathbb{Z}$ için,

$$\begin{aligned} \chi(mn) &= \chi(m)\chi(n) \\ \chi(n+k) &= \chi(n) \end{aligned} \quad (5.3)$$

dir. Yani tamamen çarpımsal ve periyodik olan karakterlerdir.

İspat: G grubu, mod k İTS grubu olduğuna göre ve İTS'nin eleman sayısı $\phi(k)$ olduğuna göre $\phi(k)$ tane χ_f Dirichlet karakteri olduğu açıktır.

Diğer yandan $(m, k) = (n, k) = 1$ ise $\chi(mn) = f(\overline{mn}) = f(\overline{m}\overline{n}) = f(\overline{m})f(\overline{n}) = \chi(m)\chi(n)$ 'dir. Eğer m, n den birisi k ile aralarında asal değilse $\chi(mn) = \chi(m)\chi(n) = 0$ olduğu açıktır.

(5.3)'teki ikinci özellik, yani periyodik olma özelliği ise $\chi_f(n) = f(\bar{n})$ ve $a \equiv b \pmod{k} \Rightarrow \text{ebob}(a, k) = \text{ebob}(b, k)$ olmasından kaynaklanmaktadır.

O halde mod n , Dirichlet karakterleri $U(\mathbb{Z}/n\mathbb{Z})$ 'ten (yani $(\mathbb{Z}/n\mathbb{Z})$ halkasında tersi olan elemanların çarpımsal grubundan) sıfırdan farklı kompleks sayılar kümesinin çarpımsal grubuna tanımlanan, $\chi : U(\mathbb{Z}/n\mathbb{Z}) \rightarrow C^\times$ homomorfizmasıdır.

Örnek 5.1. $\chi(n) = \begin{cases} (-1)^{(n-1)/2}, & \text{ebob}(n, 4) = 1 \text{ ise (yani } n \text{ tek ise)}, \\ 0, & \text{ebob}(n, 4) > 1 \text{ ise (yani } n \text{ çift ise)} \end{cases}$

karakteri, periyodu dört olan bir Dirichlet karakteridir. Yine p bir tek asal sayı olmak üzere

$\chi(p) = \left(\frac{n}{p}\right)$ biçiminde verilen ve Tanım 3.29 ile tanımlanan Legendre sembolü periyodu p

olan bir Dirichlet karakteridir.

Aşağıdaki teoremler ilkel köklerin Dirichlet karakterlerinin belirlenmesinde nasıl kullanılabileceğini göstermektedir.

Teorem 5.4. (Apostol, 1976) p , bir tek asal sayı ve g , hem $\text{mod } p$ hem de $\text{mod } p^\beta$, $\beta \geq 1$ bir ilkel kök olsun (Böyle bir ilkel kök her zaman mevcuttur). Ayrıca $(n, p) = 1$ olmak üzere $b(n)$ sayısı

$$g^{b(n)} \equiv n \pmod{p^\alpha}, \quad 0 \leq b(n) \leq \varphi(p^\alpha). \quad (5.4)$$

şartını sağlayan yegane tamsayı olsun,

$h = 0, 1, 2, \dots, \varphi(p^\alpha) - 1$ olmak üzere eğer χ_h aşağıdaki şekilde tanımlanırsa her bir χ_h bir Dirichlet karakteridir.

$$\chi_h(n) = \begin{cases} e^{2\pi i h b(n) / \varphi(p^\alpha)}, & p, n \text{ nin böleni değilse} \\ 0, & p | n \text{ ise} \end{cases} \quad (5.5)$$

dir.

Örnek 5.2. $p = 5$ alalım. $2, 2^2 \equiv 4 \pmod{5}, 2^3 \equiv 3 \pmod{5}, 2^4 \equiv 1 \pmod{5}$ ve

$\varphi(5) = 4$ olduğundan $2 \pmod{5}$ 'e göre bir ilkel köktür. Ayrıca bu hesaplamalardan $b(1) = 0, b(2) = 1, b(3) = 3, b(4) = 2$, olduğu da görülmektedir. O halde $\text{mod } 5$ bütün Dirichlet karakterlerini artık hesaplayabiliriz. (5.5)'i kullanarak

$$\chi_h(n) = \begin{cases} \left(e^{2\pi i b(n) / 4}\right)^h & p, 5 \text{ i bölmez ise} \\ 0 & p | 5 \text{ ise} \end{cases}$$

elde ederiz. Buradaki değerler yerine yazıldığında aşağıdaki çizelge ile bütün Dirichlet karakterlerini belirtebiliriz.

Çizelge 5.1 mod5 Dirichlet karakterleri

n	1	2	3	4	5
$b(n)$	0	1	3	2	0
$\chi_1(n)$	$e^0 = 1$	$e^{\pi/2} = i$	$e^{3\pi/2} = -i$	$e^{\pi} = -1$	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	-i	i	-1	0
$\chi_4(n)$	1	1	1	1	0

(5.3) ile verilen ikinci özellikten dolayı Dirichlet karakterinin periyodik oldukları göz önüne alınırsa mod5, istenen diğer $\chi(m)$ değeri de rahatlıkla hesaplanabilir. Örneğin; $123 \equiv 3(\text{mod } 5)$ olduğundan $\chi_1(123) = \chi_1(3) = -i$ olduğu açıktır.

Teorem 5.5. $m, n \in \mathbb{Z}$ ve $(m, n) = 1$ olsun. Eğer χ_1 , mod m Dirichlet karakteri ve χ_2 , mod n Dirichlet karakter ise $\chi(k) = \chi_1(k)\chi_2(k)$, mod mn Dirichlet karakterdirler.

Genel olarak; $p_1, p_2, \dots, p_r$ farklı tek asal sayılar olmak üzere eğer, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, n doğal sayısının asal çarpanlara ayrılışı ve χ_i , mod $p_i^{\alpha_i}$ Dirichlet karakterleri ise $\chi = \chi_1 \chi_2 \dots \chi_r$ mod n de Dirichlet karakteridir.

$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_r^{\alpha_r})$ olduğundan mod n , $\varphi(n)$ tane Dirichlet karakter olduğu buradan da görülmektedir.

Bilindiği üzere $\alpha \geq 3$ ise mod 2^α ilkel kök yoktur. Dolayısıyla mod 2^α için Dirichlet karakterlerini belirlemek için Teorem 5.4'ü kullanamayız. Aşağıdaki teorem bu boşluğu doldurabilecek bir sayı ve $b(n)$ değerinin var olduğunu belirtmektedir.

Teorem 5.6. (Apostol, 1976) $\alpha \geq 3$ olsun. Bu durumda n tek tamsayısı için tek türlü bir $b(n)$ bunun değeri,

$$n \equiv (-1)^{(n-1)/2} 5^{b(n)} (\text{mod } 2^\alpha), \quad 1 \leq b(n) \leq \varphi(2^\alpha)/2$$

şeklindedir.

Burada belirtilen $b(n)$ değerini kullanarak $\alpha \geq 3$ için mod 2^α , Dirichlet karakterleri

$$\chi_{a,c}(n) = f(n)^a g(n)^a : \quad a = 1, 2, c = 1, 2, \dots, \varphi(2^\alpha)/2, \text{ öyle ki;}$$

$$f(n) = \begin{cases} (-1)^{(n-1)/2} & n \text{ tek ise} \\ 0 & n \text{ çift ise} \end{cases}, \quad g(n) = \begin{cases} e^{2\pi i b(n)/2^{\alpha-2}} & n \text{ tek ise} \\ 0 & n \text{ çift ise} \end{cases}$$

Bu bölümde; ilerde kullanılacağı için özetle Dirichlet karakterleri hakkında bilgi verildi. Bizim daha çok üzerinde duracağımız Dirichlet karakterleri, $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisimleriyle bağlantılı olan $\text{mod}|d_K|$ Dirichlet karakterleridir. p asal sayısının $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cismindeki ayrışımını Legendre ve Kronecker sembolleriyle bağlantılı olarak Bölüm 3.5'te Teorem 3.31 ile elde etmiştik. Buna göre bir $K = \mathbb{Q}(\sqrt{d})$ sayı cisminin Dirichlet karakteri için aşağıdaki tanımı verebiliriz.

Tanım 5.4 $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisminin diskriminantı d_K olmak üzere bu sayı cismine karşılık gelen $\text{mod}|d_K|$ Dirichlet karakteri aşağıdaki gibi tanımlanır

$$\chi_K(p) = \begin{cases} \left(\frac{d_K}{p}\right) & p \neq 2, p \nmid d_K \\ (-1)^{\frac{d^2-1}{8}} & p = 2, 2 \nmid d \\ 0 & p \mid d_K \end{cases} \quad (5.6)$$

Daha geniş biçimde Dirichlet sembollerinin özellikleri burada da geçerli olacağı için, asal olmayan n 'ler için de $\chi(n)$ 'ler elde edilebilir. Ayrıca hangi kuadratik sayı cismi üzerinde çalışıldığı biliniyorsa $\chi(n)$ yerine genellikle sadece $\chi(n)$ sembolü de kullanılır.

Örnek 5.3 $K = \mathbb{Q}(\sqrt{-10})$ olmak üzere $d = -10, d_K = -40$ 'tır. Bu durumda (5.6) eşitliği kullanılırsa;

$$\chi(a) = \begin{cases} 1 & a \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40} \\ -1 & a \equiv 3, 17, 21, 27, 29, 31, 33, 39 \pmod{40} \\ 0 & \text{ebob}(a, 40) \neq 1 \end{cases}$$

olduğu görülür. Çizelge 5.2'de $|d| < 12$ ve $1 \leq n \leq 45$ için $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisimlerinin $\chi(n)$ Dirichlet karakterlerinin aldığı değerler verilmiştir.

Çizelge 5.2 $|d| < 12$ ve $1 \leq n \leq 45$ için $\chi(n)$ 'nin değerleri. Eğer $d \equiv 1(\text{mod } 4)$ ise χ , $\text{mod } |d|$ Dirichlet karakteri, $d \equiv 2,3(\text{mod } 4)$ ise χ , $\text{mod } |4d|$ Dirichlet karakteridir.

$n \cdot d$	2	3	5	6	7	10	11	-1	-2	-3	-5	-6	-7	-10	-11
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	0	-1	0	0	0	0	0	0	-1	0	0	1	0	-1
3	-1	0	-1	0	1	1	-1	-1	1	0	1	0	-1	-1	1
4	0	0	1	0	0	0	0	0	0	1	0	0	1	0	1
5	-1	-1	0	1	-1	0	1	1	-1	-1	0	1	-1	0	1
6	0	0	1	0	0	0	0	0	0	0	0	0	-1	0	-1
7	1	-1	-1	-1	0	-1	1	-1	-1	1	1	1	0	1	-1
8	0	0	-1	0	0	0	0	0	0	-1	0	0	1	0	-1
9	1	0	1	0	1	1	1	1	1	0	1	0	1	1	1
10	0	0	0	0	0	0	0	0	0	1	0	0	-1	0	-1
11	-1	1	1	-1	-1	-1	0	-1	1	-1	-1	1	1	1	0
12	0	0	-1	0	0	0	0	0	0	0	0	0	-1	0	1
13	-1	1	-1	-1	-1	1	-1	1	-1	1	-1	-1	-1	1	-1
14	0	0	1	0	0	0	0	0	0	-1	0	0	0	0	1
15	1	0	0	0	-1	0	-1	-1	-1	0	0	0	1	0	1
16	0	0	1	0	0	0	0	0	0	1	0	0	1	0	1
17	1	-1	-1	-1	-1	-1	-1	1	1	-1	-1	-1	-1	-1	-1
18	0	0	-1	0	0	0	0	0	0	0	0	0	1	0	-1
19	-1	-1	1	1	1	-1	1	-1	1	1	-1	-1	-1	1	-1
20	0	0	0	0	0	0	0	0	0	-1	0	0	-1	0	1
21	-1	0	1	0	0	-1	-1	1	-1	0	1	0	0	-1	-1
22	0	0	-1	0	0	0	0	0	0	1	0	0	1	0	0
23	1	1	-1	1	-1	-1	-1	-1	-1	-1	1	-1	1	1	1
24	0	0	1	0	0	0	0	0	0	0	0	0	-1	0	-1
25	1	1	0	1	1	0	1	1	1	1	0	1	1	0	1
26	0	0	1	0	0	0	0	0	0	-1	0	0	-1	0	1
27	-1	0	-1	0	1	1	-1	-1	1	0	1	0	-1	-1	1
28	0	0	-1	0	0	0	0	0	0	1	0	0	0	0	-1
29	-1	-1	1	1	1	-1	-1	1	-1	-1	1	1	1	-1	-1
30	0	0	0	0	0	0	0	0	0	0	0	0	1	0	-1
31	1	-1	1	-1	1	1	-1	-1	-1	1	-1	1	-1	-1	1
32	0	0	-1	0	0	0	0	0	0	-1	0	0	1	0	-1
33	1	0	-1	0	-1	-1	0	1	1	0	-1	0	-1	-1	0
34	0	0	1	0	0	0	0	0	0	1	0	0	-1	0	1
35	-1	1	0	-1	0	0	1	-1	1	-1	0	1	0	0	-1
36	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1
37	-1	1	-1	-1	1	1	1	1	-1	1	-1	-1	1	1	1
38	0	0	-1	0	0	0	0	0	0	-1	0	0	-1	0	1
39	1	0	1	0	-1	1	1	-1	-1	0	-1	0	1	-1	-1
40	0	0	0	0	0	0	0	0	0	1	0	0	-1	0	-1
41	1	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1
42	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	1
43	-1	-1	-1	1	-1	1	1	-1	1	1	1	-1	1	-1	-1
44	0	0	1	0	0	0	0	0	0	-1	0	0	1	0	0

5.2 Zeta ve L-Fonksiyonları

Tanım 5.5. f aritmetik bir fonksiyon olmak üzere $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ sonsuz toplamına *Dirichlet serileri* adı verilir.

Tanım 5.6. *Riemann zeta fonksiyonu,*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} \dots \quad (5.7)$$

biçiminde tanımlanmıştır. Riemann'ın 19. yüzyılda bu fonksiyon üzerinde öncü çalışmalarından ötürü fonksiyon onun ismiyle anılmaktadır.

Görüldüğü gibi Dirichlet serilerinde, $n = 1, 2, 3, \dots$ olmak üzere $f(n) = 1$ özel hali Riemann zeta fonksiyonunu vermektedir.

Örnek 5.4. $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = \frac{\pi^2}{6}$ formülü Euler tarafından 1735 yılında elde edilmiştir.

Euler bu formülün sol tarafını hesaplamak için yıllarca uğraşmış ve sonuç olarak onun π ile bağlantılı çıkması onu şaşırtmıştır. O halde;

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = \frac{\pi^2}{6},$$

yazabiliriz, yine

$$\zeta(4) = \sum_{n=1}^{\infty} \frac{1}{n^4} = 1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \dots = \frac{\pi^4}{90}$$

olduğu bilinmektedir.

Tanım 5.7. χ bir Dirichlet karakteri olmak üzere $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ fonksiyonu (χ 'ye göre)

Dirichlet L fonksiyonu olarak adlandırılır.

Örnek 5.5. $\chi(\mathbb{Z}/4\mathbb{Z})^\times = \{1 \bmod 4, 3 \bmod 4\} \rightarrow \mathbb{C}^\times$ Dirichlet karakteri,

$\chi(1 \bmod 4) = 1, \chi(3 \bmod 4) = -1$, biçiminde verilsin. Bu karaktere göre,

$$L(1, \chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \frac{1}{15} + \dots \quad (5.8)$$

Leibniz bu toplam üzerinde epeyce çalışmış ve 1673 yılında

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \frac{1}{15} + \dots = \frac{\pi}{4}$$

eşitliğini elde etmiştir ve o zaman doğanın gizemini çözdüğüne inanmıştır. Hatta bu buluşundan sonra avukat ve bir diplomat olma hevesini bir yana bırakıp matematikle uğraşmaya karar verdiği söylenir.

Tanım 5.8. $f(s)$, $s > r$ için tanımlı bir fonksiyon ve $\lim_{s \rightarrow r^+} f(s) = \infty$ olmak üzere eğer $\lim_{s \rightarrow r^+} (s - r) f(s)$ limiti mevcut ve sıfırdan farklı ise $f(s)$, $s = r$ ’de *basit bir kutuba* sahiptir denir ve bu limite de $f(s)$ ’nin $s = r$ de *rezidüsü* adı verilir.

Teorem 5.7. $s > 1$ olmak üzere $\zeta(s)$ yakınsaktır ve $\lim_{s \rightarrow 1^+} (s - 1)\zeta(s) = 1$ ’dir.

İspat: Yakınsaklığı göstermek için integral testini kullanacağız.

$$\begin{aligned} \int_1^\infty \frac{1}{x^s} dx &\leq \zeta(s) \leq 1 + \int_1^\infty \frac{1}{x^s} dx \\ \Rightarrow \lim_{s \rightarrow 1^+} (s - 1)\zeta(s) &= \lim_{s \rightarrow 1^+} (s - 1) \int_1^\infty \frac{1}{x^s} dx = \lim_{s \rightarrow 1^+} (s - 1) \frac{1}{s - 1} = 1 \end{aligned}$$

elde edilir. Bunun sonucu olarak Riemann zeta fonksiyonunun $s = 1$ ’de 1 rezidüsü ile basit bir kutuba sahiptir diyebiliriz.

Euler 1737 yılında Zeta fonksiyonunu ilginç bir biçimde asal sayılarla ilişkilendiren aşağıdaki teoremden verilen formülü elde etmiştir.

Teorem 5.8. (Euler Çarpımı) Eğer $s > 1$ ise;

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{(1 - p^{-s})} \quad (5.9)$$

dir, öyle ki bu son çarpım bütün asal sayılar üzerindedir.

İspat: p , bir asal sayı ve $s > 0$ olmak üzere $p^{-s} < 1$ olduğu açıktır, dolayısıyla;

$$(1 - p^{-s})^{-1} = 1 + p^{-s} + p^{-2s} + p^{-3s} + \dots \quad (5.10)$$

yazabiliriz. Eğer $p = 2$ ve $p = 3$ hesaba katarak bu değerleri (5.10)'da yerine yazıp çarpımlarını alırsak,

$$\begin{aligned} (1 - 2^{-s})^{-1}(1 - 3^{-s})^{-1} &= (1 + 2^{-s} + 4^{-s} + 8^{-s} + \dots)(1 + 3^{-s} + 9^{-s} + 27^{-s} + \dots) \\ &= 1 + 2^{-s} + 3^{-s} + 4^{-s} + 6^{-s} + 8^{-s} + 9^{-s} + 12^{-s} + 16^{-s} + \dots \end{aligned} \quad (5.11)$$

elde ederiz.

Görüldüğü gibi (5.11) eksik terimlerine rağmen (5.7)'deki sonsuz toplama oldukça benzemektedir. Dikkat edilirse (5.11)'de iki ve üç ile bölünebilen bütün pozitif n 'ler için n^{-s} 'ler mevcuttur. Eğer $(1 - 2^{-s})^{-1}(1 - 3^{-s})^{-1}(1 - 5^{-s})^{-1}$ çarpımını hesaba katarsak o zaman beş ile bölünebilen bütün pozitif n 'ler için de n^{-s} terimleri toplamda yer alacaktır. Fakat yine de (5.7)'deki sonsuz toplamdan eksik terimler olacaktır. Örneğin $7^{-s}, 11^{-s}, 13^{-s}, 14^{-s}$ gibi terimler hala toplamda yer almamaktadır. Fakat bu prosedürü bütün asal sayılar için işletirsek hiçbir terimi atlamamış oluruz ki;

$$\prod_p \frac{1}{(1 - p^{-s})} = \frac{1}{(1 - 2^{-s})} \cdot \frac{1}{(1 - 3^{-s})} \cdot \frac{1}{(1 - 5^{-s})} \dots = 1 + 2^{-s} + 3^{-s} + 4^{-s} + 5^{-s} \dots = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

elde ederiz.

Asal sayıları $p = 2$, $p \equiv 1(\text{mod } 4)$, $p \equiv 3(\text{mod } 4)$ biçiminde üç gruba ayırırsak Euler çarpımı olarak adlandırılan bu çarpımı;

$$\zeta(s) = \prod (1 - p^{-s})^{-1} = (1 - 2^{-s}) \prod_{p \equiv 1(\text{mod } 4)} (1 - p^{-s})^{-1} \prod_{p \equiv 3(\text{mod } 4)} (1 - p^{-s})^{-1}$$

biçiminde de yazabiliriz.

Tanım 5.9. $B_0 = 1$ olmak üzere *Bernoulli sayılarının* dizisi $(m+1)B_m = -\sum_{k=0}^{m-1} \binom{m+1}{k} B_k$

şeklinde tanımlanmıştır. Aşağıdaki çizelgede Bernoulli sayılarının bir listesi verilmiştir.

Çizelge 5.3 $n = 0,1,2,...,50$ için Bernoulli sayıları

n	B_n	n	B_n	n	B_n
0	1	16	-3617/510	34	2577687858367/6
1	-1/2	18	43867/798	36	-26315271553053477373/1919190
2	1/6	20	-174611/330	38	2929993913841559/6
4	-1/30	22	854513/138	40	-261082718496449122051/13530
6	1/42	24	-236364091/2730	42	1520097643918070802691/1806
8	-1/30	26	8553103/6	44	-27833269579301024235023/690
10	5/66	28	-23749461029/870	46	596451111593912163277961/282
12	-691/2730	30	8615841276005/14322	48	-5609403368997817686249127547/46410
14	7/6	32	-7709321041217/510	50	495057205241079648212477525/66

Tanım 5.10. Bernoulli polinomu $B_m(x)$, $(m = 0, 1, 2, \dots)$ için $B_m(x) = \sum_{k=0}^m \binom{m}{k} B_k x^{m-k}$ olarak

tanımlanmıştır. Burada $\binom{m}{k}$, m 'nin k 'lı kombinasyonunu belirtmektedir.

Örnek 5.6. $B_0(x) = 1$, $B_1(x) = x - \frac{1}{2}$, $B_2(x) = x^2 - x + \frac{1}{6}$, $B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x, \dots$

$n = 2k$ çift sayı ve B_n , n . Bernoulli sayısını göstermek üzere Bernoulli sayıları ve Zeta

fonksiyonu arasında $\zeta(n) = \frac{2^{n-1} |B_n| \pi^n}{n!}$ eşitliği elde edilmiştir. Başka bir bağlantı da

$B_n = (-1)^{n+1} n \zeta(1-n)$ biçimindedir. Bu son formül $n \geq 1$ için $B_n = -n \zeta(1-n)$ şeklinde yazılabilir.

Bernoulli sayılarını ve birinci formülü kullanarak zeta fonksiyonunun

$\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, $\zeta(6) = \frac{\pi^6}{945}$, $\zeta(8) = \frac{\pi^8}{9450}$, $\zeta(10) = \frac{\pi^{10}}{93555}$, gibi değerlerini elde

edebiliriz. Çizelge 5.4 zeta fonksiyonunun $n = 2, \dots, 50$ için aldığı yaklaşık değerleri göstermektedir.

Çizelge 5.4 Zeta fonksiyonunun bazı tamsayı değerleri

n	$\zeta(n)$	n	$\zeta(n)$	n	$\zeta(n)$
2	1.64493406684822644	15	1.00003058823630702	28	1.000000000372533402
3	1.20205690315959429	16	1.00001528225940865	29	1.000000000186265972
4	1.08232323371113819	17	1.00000763719763790	30	1.000000000093132743
5	1.03692775514336993	18	1.00000381729326500	31	1.000000000046566291
6	1.01734306198444914	19	1.00000190821271655	32	1.000000000023283118
7	1.00834927738192283	20	1.00000095396203387	33	1.000000000011641550
8	1.00407735619794434	21	1.00000047693298679	34	1.000000000005820772
9	1.00200839282608221	22	1.00000023845050273	35	1.000000000002910385
10	1.00099457512781809	23	1.00000011921992596	36	1.000000000001455192
11	1.00049418860411946	24	1.00000005960818905	37	1.000000000000727596
12	1.00024608655330805	25	1.00000002980350351	38	1.000000000000363798
13	1.00012271334757849	26	1.00000001490155483	39	1.000000000000181899
14	1.00006124813505870	27	1.00000000745071179	40	1.000000000000090949

5.3 Kuadratik Sayı Cisimlerinin Zeta ve L-Fonksiyonları

Tanım 5.11. K , bir sayı cismi ve O_K 'da onun tamlık halkası olsun.

$$\zeta_K(s) = \sum_{m=1}^{\infty} \frac{1}{N(\mathfrak{a})^s} \quad (5.12)$$

şeklinde tanımlanan fonksiyona K sayı cisminin zeta fonksiyonu denir. (5.12)'de belirtilen toplam $\mathfrak{a} \subset O_K$ olan bütün idealler üzerindedir.

Örnek 5.7. Özel olarak eğer $K = \mathbb{Q}$ olarak alınırsa Tanım 5.6. ile verilen Riemann zeta fonksiyonunu elde ederiz.

$$\textbf{Teorem 5.9.} \quad \zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} \quad (5.13)$$

tir. (Burada çarpım $\mathfrak{p} \subset O_K$ olan bütün asal idealler üzerindedir).

$$\textbf{İspat:} \quad \zeta_K(s) = \sum_{m=1}^{\infty} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \sum_{n=0}^{\infty} \frac{1}{N(\mathfrak{p})^{ns}} = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

$f(x)$, α 'nın minimal polinomu olmak üzere $f(x)$ polinomunun mod p 'ye göre indirgenemez polinomların çarpımı olarak yazılışı ile (p) idealinin asal ideallerin çarpımı olarak yazılımı arasındaki bağlantının Teorem 3.26'nın sonucu olarak aşağıdaki gibi olduğunu belirtmiştik.

Eğer $f(x) = \prod_{i=1}^r f_i(x)^{e_i} \pmod{p}$ ise $(p) = \prod_{i=1}^r (p, f_i(x))^{e_i}$

dir.

Tanım 5.12. $f(x) = \prod_{i=1}^r f_i(x)^{e_i} \pmod{p}$, $f(x) \in \mathbb{Z}[x]$ 'in modulo p 'ye göre indirgenemez polinomların çarpımı olarak yazılışı olsun. f 'nin mod p 'ye göre Euler çarpımı

$$A_{f,p}(t) = \prod_{i=1}^r (1 - t^{\deg(f_i)})$$

polinomu olarak tanımlanmıştır.

Tanım 5.13. $f(x) \in \mathbb{Z}[x]$ polinomunun zeta fonksiyonu,

$$\zeta_f(s) = \prod_p A_{f,p}(p^{-s})^{-1}$$

şeklinde verilir.

Teorem 5.10. K bir sayı cismi ve $O_K = \mathbb{Z}[\alpha]$, K 'nin tamlık halkası olsun. $f(x)$ polinomu α 'nın minimal polinomu olmak üzere;

$$\zeta_K(s) = \zeta_f(s)$$

tir.

İspat: (5.13) eşitliği kullanılarak $\zeta_K(s) = \sum_{m=1}^{\infty} \frac{1}{N(\alpha)^s} = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \prod_{p \in \mathbb{Z}} \prod_{\mathfrak{p} | (p)} \frac{1}{1 - N(\mathfrak{p})^{-s}}$

elde ederiz. $f(x) = \prod_{i=1}^r f_i(x)^{e_i} \pmod{p} \Rightarrow \prod_{\mathfrak{p} | (p)} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \prod_{i=1}^r \frac{1}{1 - (p^{\deg f_i})^{-s}} = \frac{1}{A_{f,p}(p^{-s})}$

$$\Rightarrow \zeta_K(s) = \prod_{p \in \mathbb{Z}} \frac{1}{A_{f,p}(p^{-s})} = \zeta_f(s).$$

Teorem 5.11. $s > 1$ olmak üzere $\zeta_K(s) = \zeta(s)L(s, \chi)$ 'dir.

İspat:

$$\begin{aligned}
\zeta_K(s) &= \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \prod_{\left(\frac{d_K}{p}\right)=1} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=-1} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p|d_K} \left(1 - \frac{1}{p^s}\right)^{-1} \\
&= \prod_{\left(\frac{d_K}{p}\right)=1} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=-1} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p|d_K} \left(1 - \frac{1}{p^s}\right)^{-1} \\
&= \left[\prod_{\left(\frac{d_K}{p}\right)=1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=-1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p|d_K} \left(1 - \frac{1}{p^s}\right)^{-1} \right] \left[\prod_{\left(\frac{d_K}{p}\right)=1} \left(1 + \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=-1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p|d_K} 1 \right]
\end{aligned}$$

Bu son çarpımda birinci parantezle belirtilen çarpanı $\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ biçiminde tek bir çarpanla ifade edebiliriz. O halde;

$$= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \left[\prod_{\left(\frac{d_K}{p}\right)=1} \left(1 + \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=-1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p|d_K} 1 \right]$$

dir.

Burada iki çarptandan birincisi (5.9) eşitliğinden ötürü tam olarak $\zeta(s)$ 'tir. O halde

$$\zeta_K(s) = \zeta(s) \prod_p \left(1 - \frac{\left(\frac{d_K}{p}\right)}{p^s}\right)^{-1} = \zeta(s) \sum_{n=1}^{\infty} \frac{\left(\frac{d_K}{p}\right)}{n^s} = \zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \zeta(s) L(s, \chi)$$

Burada $\left(\frac{d_K}{p}\right)$ ile belirtilen Kronecker sembolüdür. $\chi(n)$ Tanım 5.4 ile verildiği gibi ilgili K kuadratik sayı cisminin Dirichlet karakterini belirtmektedir.

Teorem 5.12. $\lim_{s \rightarrow 1^+} (s-1) \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = L(1, \chi)$ 'dir.

İspat: $\chi(n), \text{mod } |d_K|$ Dirichlet karakteri olmak üzere $s > 0$ için $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ serisi koşullu yakınsaktır ve $s > 0$ için s 'nin bir fonksiyonunu belirtir. Dolayısıyla Teorem 5.7 ile ispatlanan $\lim_{s \rightarrow 1^+} (s-1) \zeta(s) = 1$ eşitliği göz önüne alınırsa;

$\lim_{s \rightarrow 1^+} (s-1) \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \lim_{s \rightarrow 1^+} (s-1) \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \lim_{s \rightarrow 1^+} (s-1) \zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = L(1, \chi)$ elde edilir.

Aşağıdaki teoremlerde de görüleceği üzere $L(1, \chi)$ fonksiyonlarının değerlerinin hesaplanması, sınıf sayılarıyla olan bağlantısından ötürü oldukça önemlidir. Bu fonksiyonun değerlerinin hesaplanması için çok değişik formüller ortaya konmuştur.

Örnek 5.8. $d = -3 \Rightarrow d_K = -3$, $\text{mod}|d_K|$ Dirichlet karakteri χ 'yi göz önüne aldığımızda;

$$\begin{aligned} L(1, \chi) &= 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \dots = \sum_{k=0}^{\infty} \left(\frac{1}{3k+1} - \frac{1}{3k+2} \right) \\ &= \int_0^1 ((1-x) + (x^3 - x^4) + (x^6 - x^7) + \dots) dx = \int_0^1 (1-x)(1+x^3+x^6+x^9+\dots) dx \\ &= \int_0^1 \frac{1-x}{1-x^3} dx = \int_0^1 \frac{dx}{1+x+x^2} = \int_0^1 \frac{dx}{x^2+x+1} = \int_0^1 \frac{dx}{x^2+x+\frac{1}{4}+\frac{3}{4}} = \int_0^1 \frac{dx}{\left(x+\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} \\ &= \frac{2}{\sqrt{3}} \arctan \left(\left(x+\frac{1}{2}\right) / \frac{\sqrt{3}}{2} \right) \Big|_0^1 = \frac{2}{\sqrt{3}} \left[\arctan \sqrt{3} - \arctan \frac{1}{\sqrt{3}} \right] = \frac{\pi}{3\sqrt{3}} = 0.604599... \end{aligned}$$

Örnek 5.9. $d = 21 \Rightarrow d_K = 21$, $\text{mod}|d_K|$ Dirichlet karakteri χ 'yi göz önüne aldığımızda;

$$\begin{aligned} L(1, \chi) &= 1 - \frac{1}{2} + \frac{1}{4} + \frac{1}{5} - \frac{1}{8} - \frac{1}{10} - \frac{1}{11} - \frac{1}{13} + \frac{1}{16} + \frac{1}{17} - \frac{1}{19} + \frac{1}{20} + \dots \\ &= \sum_{k=0}^{\infty} \left(\frac{1}{21k+1} - \frac{1}{21k+2} + \frac{1}{21k+4} + \frac{1}{21k+5} - \frac{1}{21k+8} - \frac{1}{21k+10} - \frac{1}{21k+11} - \frac{1}{21k+13} \right. \\ &\quad \left. + \frac{1}{21k+16} + \frac{1}{21k+17} - \frac{1}{21k+19} + \frac{1}{21k+20} \right) \\ &= \int_0^1 (1-x+x^3+x^4-x^7-x^9-x^{10}-x^{12}+x^{15}+x^{16}-x^{18}+x^{19}+\dots) dx \\ &= \int_0^1 (1-x+x^3+x^4-x^7-x^9-x^{10}-x^{12}+x^{15}+x^{16}-x^{18}+x^{19})(1+x^{21}+x^{42}+\dots) dx \\ &= \int_0^1 \frac{(1-x+x^3+x^4-x^7-x^9-x^{10}-x^{12}+x^{15}+x^{16}-x^{18}+x^{19}) dx}{1-x^{21}} \\ &= \int_0^1 \frac{(x^2-1)(x^8-2x^7+2x^6+2x^2-2x+1)}{x^{12}-x^{11}+x^9-x^8+x^6-x^4+x^3-x+1} dx = 0.683807... \end{aligned}$$

$L(1, \chi)$ ile sonraki integral arasındaki bu bağlantıyı genelleştirmek mümkündür. Dirichlet karakterlerinin periyodik olduklarını göz önünde bulundurduğumuzda $L(1, \chi)$ 'deki terimleri $\text{mod}(\varphi(|d_K|))$ 'ya göre gruplandırmak mümkündür. Şöyle ki; bu integralin içinde her zaman iki çarpan bulunacaktır. Bunlardan birinci çarpan;

$$f_{d_K}(x) = 1 + x^1 \left(\frac{d_K}{1} \right) + x^1 \left(\frac{d_K}{2} \right) + \dots + x^{d_K-1} \left(\frac{d_K}{|d_K|} \right) = \sum_{t=1}^{|d_K|} x^{t-1} \left(\frac{d_K}{t} \right) \quad (5.14)$$

biçimindedir.

İkinci çarpan ise her zaman,

$$1 + x^{|d_K|} + x^{2|d_K|} + x^{3|d_K|} + \dots \quad (5.15)$$

sonsuz toplama eşit olacağı için (5.15)'i $\frac{1}{1 - x^{|d_K|}}$ olarak yazmak mümkündür.

O halde bu sonucu (5.14) ile birleştirdiğimizde aşağıdaki teoremi yazabiliriz.

Teorem 5.13. $f_{d_K}(x) = \sum_{t=1}^{|d_K|} x^{t-1} \left(\frac{d_K}{t} \right)$ olmak üzere,

$$L(1, \chi) = \int_0^1 \frac{f_{d_K}(x) dx}{1 - x^{|d_K|}} \quad (5.16)$$

dır.

Burada f_{d_K} fonksiyonu için Örnek 5.11 ile verilen Pari kodları kullanılabilir. (5.16) ile verilen formülü kullanarak (5.8)'de verilen Leibniz formülünü elde edelim.

Örnek 5.10. $K = \mathbb{Q}(\sqrt{-1})$ kuadratik sayı cismi için $d = -1, d_K = -4$ tür.

$$f_{-4}(x) = \sum_{t=1}^{|d_K|} x^{t-1} \left(\frac{d_K}{t} \right) = \sum_{t=1}^4 x^{t-1} \left(\frac{d_K}{t} \right) = 1.x^0 + 0.x^1 + (-1).x^2 + 0.x^3 = 1 - x^2$$

$$L(1, \chi) = \int_0^1 \frac{f_{d_K}(x) dx}{1 - x^{|d_K|}} = \int_0^1 \frac{1 - x^2}{1 - x^4} = \int_0^1 \frac{dx}{1 + x^2} = \arctan(1) - \arctan(0) = \frac{\pi}{4}$$

$$L(1, \chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \frac{1}{15} + \dots = \frac{\pi}{4}$$

Bu integralin içindeki rasyonel fonksiyon aşağıdaki Pari kodları ile elde edilebilir.

Örnek 5.11.

```
{fon(d)=
local(dk,s,i);
dk=quaddisc(d);
s=sum(i=1,abs(dk),(x^(i-1))*kronecker(dk,i));
return(s);
}

{int(d)=
local(dk,intm);
dk=quaddisc(d);
intm=fon(d)/(1-x^abs(dk));
return(intm);
}
```

Burada int(d) içinde d değerinin yerine çalıştığımız kuadratik sayı cismi $K = \mathbb{Q}(\sqrt{d})$ 'deki d 'nin değerinin girilmesi gerekir. Örnek 5.8'deki rasyonel fonksiyon için yukarıdaki kodlardan sonra int(-3) yazmak yeterlidir. Sonuç olarak $-1/(-x^2 - x - 1)$ elde edilecektir. İntegralin sonucunu da intnum(x=0,1, $-1/(-x^2 - x - 1)$) ile hesaplayabiliriz. Bu değer $\text{Pi}/3 * \text{sqrt}(3)$ yazarak çıkacak sonuçla karşılaştırılabilir.

Şimdi $L(1, \chi)$ ile sınıf sayısı arasındaki bağlantı üzerinde duralım.

Teorem 5.14. $K = \mathbb{Q}(\sqrt{d})$ bir sanal kuadratik sayı cismi ve $d \equiv 2,3 \pmod{4}$ olsun. Bu durumda;

$$L(1, \chi) = \frac{h\pi}{2\sqrt{|d|}} \quad (5.17)$$

dir.

İspat: α idealinin herhangi iki denklik sınıfı üzerinde $\sum \frac{1}{N(\alpha)^s}$ 'ların toplamaları aynıdır.

Buna göre farklı denklik sınıflarının sayısını daha önce gösterdiğimiz gibi h olarak alırsak

$$\lim_{s \rightarrow 1^+} (s-1) \sum_{\alpha} \frac{1}{N(\alpha)^s} = h \lim_{s \rightarrow 1^+} (s-1) \sum_{\alpha \text{ temel ideal}} \frac{1}{N(\alpha)^s}$$

elde ederiz. Teorem 2.15'te $d = -1$ için O_K 'nın birimsellerinin $\pm 1, \pm i$ ve $d < 0$ ve $d \equiv 2, 3 \pmod{4}$ ise birimsellerin ± 1 'den ibaret olduğunu ispatladık. Bu durumda genel kullanıma uyarak birimsellerin sayısını w ile gösterirsek

$$\sum_{\alpha \text{ temel ideal}} \frac{1}{N(\alpha)^s} = \frac{1}{w} \sum_{(m,n) \neq (0,0)} (x^2 - dy^2)$$

elde ederiz. $s \rightarrow 1^+$ iken $\sum_{(m,n) \neq (0,0)} (x^2 - dy^2)$ toplamı $\iint_{x^2 - dy^2 \geq 1} (x^2 - dy^2)^{-s} dx dy$ integrali ile aynı

şekilde sonsuza yaklaşır. Bu ikisi arasındaki fark $s \rightarrow 1^+$ iken sınırlı kalır. Bu integrali değişken değiştirme yöntemiyle hesaplamak mümkündür.

$$\begin{aligned} \iint_{x^2 - dy^2 \geq 1} (x^2 - dy^2)^{-s} dx dy &= \iint_{-dz^2 - dy^2 \geq 1} (-dz^2 - dy^2)^{-s} d(\sqrt{-d} z) dy \\ &= |d|^{-s} |d|^{1/2} \iint_{z^2 + y^2 \geq |d|^{-1}} (z^2 + y^2)^{-s} dz dy \\ &= |d|^{(1-2s)/2} \iint_{r^2 \geq |d|^{-1}} r^{-2s} r dr d\theta \\ &= |d|^{(1-2s)/2} 2\pi \frac{r^{2-2s}}{2-2s} \Big|_{|d|^{-1/2}}^{\infty} \\ &= \frac{\pi}{s-1} |d|^{(1-2s)/2} |d|^{s-1}. \end{aligned}$$

Bunu yukarıdaki denklemde yerine koyarsak,

$$\lim_{s \rightarrow 1^+} (s-1) \sum_{\alpha} \frac{1}{N(\alpha)^s} = h \frac{1}{w} \lim_{s \rightarrow 1^+} \pi |d|^{(1-2s)/2} |d|^{s-1} = h \frac{1}{w} \pi |d|^{-1/2} = \frac{h\pi}{w\sqrt{|d|}}$$

elde ederiz. Özetlersek,

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \frac{h\pi}{w\sqrt{|d|}}$$

dir. Burada sadece $d < 0, d \equiv 1(\text{mod } 4)$ durumunu hesaba kattık. Diğer kare-bağımsız d değerleri için de benzer formüller vardır. Aşağıda Teorem 5.15 ile diğer durumları ispatsız olarak vereceğimiz Dirichlet sınıf sayı formülünün sonucu olarak O_K 'nin sınıf sayısını biliyorsak O_K 'ya karşılık gelen Dirichlet karakteri $\chi(n)$ için $L(1, \chi)$ 'yi rahatlıkla hesaplayabiliriz. Yine tersine, eğer $L(1, \chi)$ 'yi biliyorsak O_K 'nin sınıf sayısı h 'ı bu formülle hesaplayabiliriz. Sınıf sayılarıyla olan bu bağlantısından dolayı L -fonksiyonlarının ve özellikle de $L(1, \chi)$ değerlerinin hesaplanması cebirsel sayılar teorisinde önemli bir yere sahiptir.

Örnek 5.12. $K = \mathbb{Q}(\sqrt{-13})$ 'yi göz önüne alalım. Bilindiği üzere $O_K = \mathbb{Z}[\sqrt{-13}]$,

$h = 2$, $w = 2$ ve $|d_K| = 52$ 'dir. Dolayısıyla $\frac{2\pi}{2\sqrt{|-13|}} = \frac{\pi}{\sqrt{13}} = L(1, \chi)$ 'dir. Dirichlet

karakterlerini mod 52 göre hesapladığımızda bunların sırasıyla,

1, 0, -1, 0, -1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, -1, 0, -1, 0, 1, 0, -1, 0, 1, 0, 1, 0, -1, 0, 1, 0, -1, 0, 0, 0, -1, 0, -1, 0, -1, 0, 1, 0, 1, 0, -1, 0

olduğunu görürüz. Bunun sonucu olarak,

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \left(\frac{-52}{n} \right) \frac{1}{n} =$$

$$1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \frac{1}{11} + \frac{1}{15} + \frac{1}{17} + \frac{1}{19} - \frac{1}{21} - \frac{1}{23} + \frac{1}{25} - \frac{1}{27} + \frac{1}{29} + \frac{1}{31} - \frac{1}{33} - \frac{1}{35} - \frac{1}{37}$$

$$- \frac{1}{41} - \frac{1}{43} - \frac{1}{45} + \frac{1}{47} + \frac{1}{49} - \frac{1}{51} + \dots = \frac{\pi}{\sqrt{13}} = 0.871321\dots$$

elde ederiz.

Teorem 5.15. (Murty, 1999)

[Dirichlet Sınıf Sayı Formülü] $K = \mathbb{Q}(\sqrt{d})$, diskriminantı d_K olan bir kuadratik sayı cismi olsun. Bu durumda h , K 'nin sınıf sayısını, ε_K , $R = \log \varepsilon_K$ sırasıyla K reel kuadratik sayı cismi olduğunda temel birimini ve regülatörü, w , K sanal kuadratik sayı cismi olduğunda birimsellerin sayısını belirtmek üzere;

$$L(1, \chi) = \begin{cases} \frac{2\pi h}{w\sqrt{|d_K|}} & d < 0 \\ \frac{2hR}{\sqrt{d_K}} & d > 0 \end{cases} \quad (5.18)$$

eşitliği vardır.

Dikkat edilirse özel hal olarak $d \equiv 2,3 \pmod{4}$ ise $\sqrt{|d_K|} = \sqrt{|4d|} = 2\sqrt{|d|}$ olacağı için $d < 0$ ve $d \equiv 2,3 \pmod{4}$ durumu Teorem 5.14'ü belirtmektedir.

Örnek 5.13. $K = \mathbb{Q}(\sqrt{57})$ 'yi göz önüne alalım. Bu durumda $O_K = \mathbb{Z}\left[\frac{1+\sqrt{57}}{2}\right]$,

$|d_K| = 57$ 'dir. Çizelge 2.3 ve 2.5'ten $R = \log \varepsilon_K = \log(131 + 40\omega) = 5.710416$ olduğunu görüyoruz. Yine Çizelge 3.4'ten $h = 1$ olduğu anlaşılmaktadır. Dolayısıyla (5.18)

kullanıldığında $L(1, \chi) = \frac{2 \log(131 + 40\omega)}{\sqrt{57}} = \frac{2(5.710416)}{\sqrt{57}} = 1.512726...$ 'dir. Dirichlet

karakterlerini mod 57 göre hesaplırsak bunların sırasıyla 1, 1, 0, 1, -1, 0, 1, 1, 0, -1, -1, 0, -1, 1, 0, 1, -1, 0, 0, -1, 0, -1, -1, 0, 1, -1, 0, 1, 1, 0, -1, 1, 0, -1, -1, 0, -1, 0, 0, -1, 1, 0, 1, -1, 0, -1, -1, 0, 1, 1, 0, -1, 1, 0, 1, 1, 0, ... olduğunu görürüz. Bunun sonucu olarak mod 57 Dirichlet karakterine göre;

$$\begin{aligned} L(1, \chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \left(\frac{57}{n} \right) \frac{1}{n} \\ &= 1 + \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} + \frac{1}{8} - \frac{1}{10} - \frac{1}{11} - \frac{1}{13} + \frac{1}{14} + \frac{1}{16} - \frac{1}{17} - \frac{1}{20} - \frac{1}{22} - \frac{1}{23} + \frac{1}{25} - \frac{1}{26} + \frac{1}{28} + \frac{1}{29} \\ &\quad - \frac{1}{31} + \frac{1}{32} - \frac{1}{34} - \frac{1}{35} - \frac{1}{37} - \frac{1}{40} + \frac{1}{41} + \frac{1}{43} - \frac{1}{44} - \frac{1}{46} - \frac{1}{47} + \frac{1}{49} + \frac{1}{50} - \frac{1}{52} + \frac{1}{53} + \frac{1}{55} + \frac{1}{56} \dots \\ &= \frac{2 \log(151 + 20\sqrt{57})}{\sqrt{57}} = 1.512726... \end{aligned}$$

elde ederiz. Örnek 5.12 ve 5.13'te K sayı cisminde sınıf sayısının değerini kullanarak mod d_K Dirichlet karakterine göre $L(1, \chi)$ fonksiyonunun değerini hesapladık. Daha önce de belirttiğimiz gibi tersini yapmak ta mümkündür. Eğer (5.16) ve (5.18) denklemlerini tek bir denklemde birleştirek aşağıdaki teoremi yazabiliriz.

Teorem 5.16. $K = \mathbb{Q}(\sqrt{d})$ bir kuadratik sayı cismi olsun, d_K cismin diskriminantını, w sayı cismi sanal olduğunda birimlerin sayısını, ε_K da K reel sayı cismi olduğunda onun

temel birimini ve $f_{d_K}(x)$ (5.14) ile belirtilen fonksiyon olmak üzere,

$$h = \begin{cases} \frac{w\sqrt{|d_K|}}{2\pi} \int_0^1 \frac{f_{d_K}(x)dx}{1-x^{|d_K|}} & d < 0 \\ \frac{\sqrt{d_K}}{2\log \varepsilon_K} \int_0^1 \frac{f_{d_K}(x)dx}{1-x^{d_K}} & d > 0 \end{cases} \quad (5.19)$$

dır.

İspat: (5.16) ve (5.18) denklemleri birleştirildiğinde (5.19) açıkça görülmektedir.

Fakat daha önce kullandığımız metotla (5.16) denklemi yardımıyla $L(1, \chi)$ 'nin değerinin hesaplanması d değeri büyüdükçe oldukça zor ve karmaşık hale gelebileceği görülmektedir. Aşağıdaki teorem $L(1, \chi)$ fonksiyonunun değerlerinin bulunmasında oldukça kolay bir yol vermektedir.

Teorem 5.17. (Edwards, 1977)

- $d < 0$ kare-bağımsız olmak üzere d_K , $K = \mathbb{Q}(\sqrt{d})$ sanal kuadratik sayı cisminin diskriminantını ve χ , mod d_K Dirichlet karakterini göstermek üzere;

$$L(1, \chi) = -\frac{\pi}{d_K \sqrt{|d_K|}} \sum_{a=1}^{|d_K|} |a\chi(a)| = -\frac{\pi}{d_K \sqrt{|d_K|}} |1 + \chi(2).2 + \chi(3).3 + \dots + |d_K| \chi(|d_K|)| \quad (5.20)$$

- Şimdi $d > 0$ kare-bağımsız bir tamsayı χ , mod d_K Dirichlet karakteri olsun. Bu durumda;

$$L(1, \chi) = \frac{-1}{\sqrt{d_K}} \sum_{a=1}^{d_K} \chi(a) \log \sin(a\pi / d_K) \quad (5.21)$$

dır.

Örnek 5.14. $d = -33 \Rightarrow d_K = -132$ 'dir.

1, 7, 17, 19, 23, 25, 29, 37, 41, 43, 47, 49, 59, 65, 71, 79, 97, 101, 119, 127 için $\chi(a \bmod 132) = 1$,
5, 13, 31, 35, 53, 61, 67, 73, 83, 85, 89, 91, 95, 103, 107, 109, 113, 115, 125, 131 için $\chi(a \bmod 132) = -1$
ve $\text{ebob}(a, 75) = 1$ ise $\chi(a \bmod 132) = -0$ dır. O halde (5.20) kullanılırsa;

$$L(1, \chi) = \frac{\pi}{132\sqrt{132}} |1 - 5 + 7 - 13 + 17 + 19 + 23 + 25 \dots - 125 + 127 - 131| = \frac{\pi}{132\sqrt{132}} |-528| = \frac{2\pi}{\sqrt{33}} \approx 1.093762$$

Dolayısıyla;

$$L(1, \chi) = \sum_{n=1}^{\infty} \left(\frac{-68}{n} \right) \frac{1}{n} = 1 - \frac{1}{5} + \frac{1}{7} - \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{23} + \frac{1}{25} + \frac{1}{29} - \frac{1}{31} - \frac{1}{35} + \frac{1}{37} + \frac{1}{41} + \frac{1}{43} + \frac{1}{47} + \frac{1}{49} - \frac{1}{53} + \frac{1}{59} - \frac{1}{61} + \frac{1}{65} - \frac{1}{67} + \frac{1}{71} - \frac{1}{73} + \frac{1}{79} - \frac{1}{83} - \frac{1}{85} - \frac{1}{89} - \frac{1}{91} - \frac{1}{95} + \frac{1}{97} + \frac{1}{101} - \frac{1}{103} - \frac{1}{107} - \frac{1}{109} - \frac{1}{113} - \frac{1}{115} + \frac{1}{119} - \frac{1}{125} + \frac{1}{127} - \frac{1}{131} \dots = \frac{2\pi}{\sqrt{33}} = 1.093762$$

χ , mod d_K Dirichlet karakteri olmak üzere kare-bağımsız $d = -1 \dots -200$ için $L(1, \chi)$ fonksiyonlarının aldığı değerler Çizelge 5.6 ile verilmiştir. Çizelge hazırlanırken (5.20) denklemi göz önüne alınarak oluşturulan ve Bölüm 5.3'te verilen Pari programı kullanılmıştır.

Örnek 5.15. $d = 3$ alınırsa buna karşılık gelen mod12 Dirichlet karakterleri sırasıyla $\chi(1) = 1, \chi(5) = -1, \chi(7) = -1, \chi(11) = 1$ 'dir. Bu durumda (5.21) kullanılırsa;

$$L(1, \chi) = \frac{-1}{\sqrt{12}} \sum_{a=1}^{12} \chi(a) \log \sin(a\pi / d_K) = \frac{-1}{2\sqrt{3}} \log \left[\frac{\sin\left(\frac{\pi}{12}\right) \sin\left(\frac{11\pi}{12}\right)}{\sin\left(\frac{5\pi}{12}\right) \sin\left(\frac{7\pi}{12}\right)} \right] = \frac{-1}{2\sqrt{3}} \log \frac{1 - \frac{\sqrt{3}}{2}}{1 + \frac{\sqrt{3}}{2}}$$

$$= \frac{1}{2\sqrt{3}} \log \frac{1 + \frac{\sqrt{3}}{2}}{1 - \frac{\sqrt{3}}{2}} = \frac{1}{2\sqrt{3}} \log(2 + \sqrt{3})^2 = \frac{2}{2\sqrt{3}} \log(2 + \sqrt{3}) = \frac{\log(2 + \sqrt{3})}{\sqrt{3}} \approx 0.760345$$

elde edilir.

χ , mod d_K Dirichlet karakteri olmak üzere kare-bağımsız $d = 1 \dots 150$ için $L(1, \chi)$ aldığı değerler Çizelge 5.5 ile verilmiştir. Çizelge hazırlanırken (5.21) denklemi göz önüne alınarak oluşturulan ve Bölüm 5.3'te verilen Pari programı kullanılmıştır.

Bu formül ve metodlar kullanılarak $L(1, \chi)$ 'lerin değerlerini artık daha kolayca belirleyebiliriz Şimdi de (5.18)'deki sınıf sayısı ve $L(1, \chi)$ değerleri arasındaki ilişkiyi göz

önüne alarak (5.20) ve (5.21) denklemlerini kullanarak bazı kuadratik sayı cisimlerinin sınıf sayılarını bu yolla hesaplayalım. Öncelikle $L(1, \chi)$ için yazılmış olan (5.18) i h için yeniden düzenlersek,

$$h = \begin{cases} \frac{w\sqrt{|d_K|}}{2\pi} L(1, \chi) & d < 0 \\ \frac{\sqrt{d_K}}{2\log \varepsilon_K} L(1, \chi) & d > 0 \end{cases} \quad (5.22)$$

Bununla birlikte (5.20) ve (5.21)'i göz önünde bulundurduğumuzda sonuç olarak aşağıdaki teoremi yazabiliriz.

Teorem 5.18. $K = \mathbb{Q}(\sqrt{d})$ bir kuadratik sayı cismi ve $d_K, w, \varepsilon_K, \chi$ daha önce belirtildiği gibi olmak üzere

$$h = \begin{cases} -\frac{w}{2d_K} \sum_{a=1}^{|d_K|} a\chi(a) & d < 0 \\ -\frac{1}{2\log \varepsilon_K} \sum_{a=1}^{d_K} \chi(a) \log \sin(a\pi/d_K) & d > 0 \end{cases} \quad (5.23)$$

dır.

Örnek 5.16. $K = \mathbb{Q}(\sqrt{-47})$ alınırsa $d_K = -47, w_K = 2$ dir. Diğer yandan,

$1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42$ için $\chi(a \bmod d_K) = 1$ ve $5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45, 46$ için $\chi(a \bmod d_K) = -1$

olduğu karakterin özelliklerinden açıktır. $\sum_{a=1}^{|d_K|} a\chi(a) = \sum_{a=1}^{47} a\chi(a) = -235$. O halde (5.23)

kullanılırsa;

$$h = -\frac{2}{2 \cdot (-57)} |-235| = 5.$$

Benzer şekilde $K = \mathbb{Q}(\sqrt{-33})$ alınırsa $d_K = -132, \omega_K = 2$ dir. Diğer yandan

$a = 1, 7, 17, 19, 23, 25, 29, 37, 41, 43, 47, 49, 59, 65, 71, 79, 97, 101, 119, 127$ için $\chi(a \bmod d_K) = 1$ ve

$a = 5, 13, 31, 35, 53, 61, 67, 73, 83, 85, 89, 91, 95, 103, 107, 109, 113, 115, 125, 131$ için

$\chi(a \bmod d_K) = -1$ ve $ebob(a, 132) = 1$ olan a 'lar içinse $\chi(a \bmod d_K) = 0$ dir. Bu durumda

$$\sum_{a=1}^{|d_K|} a\chi(a) = \sum_{a=1}^{132} a\chi(a) = -528.$$

O halde $h_K = -\frac{2}{2 \cdot (132)}(-528) = 4$ elde ederiz.

Örnek 5.17. $K = \mathbb{Q}(\sqrt{85})$ reel kuadratik sayı cismini ele alalım. $d_K = 85$,

$$\varepsilon_K = 4 + \omega = \frac{9 + \sqrt{85}}{2}, R = \log \varepsilon_K = 2.209347 \text{ 'dir.}$$

Bu durumda, $h = -\frac{1}{2 \log \frac{9 + \sqrt{85}}{2}} \sum_{a=1}^{85} \chi(a) \log \sin(a\pi/85)$ 'dir. Hesaplamalar yapıldığında;

$$\sum_{a=1}^{85} \chi(a) \log \sin(a\pi/85) = 8.837390...$$

olduğu görülür. O halde;

$$h = -\frac{1}{2 \log \frac{9 + \sqrt{85}}{2}} 8.837390 = 2$$

elde edilir.

Çizelge 5.5 $d = 2...443$ için $K = Q(\sqrt{d})$ 'lere karşılık gelen $L(1, \chi)$ fonksiyonlarının değerleri

d	$L(1, \chi)$	d	$L(1, \chi)$	d	$L(1, \chi)$	d	$L(1, \chi)$	d	$L(1, \chi)$	d	$L(1, \chi)$
2	0.623225	74	1.035646	149	0.673596	221	0.727449	298	1.577505	374	0.911556
3	0.760346	77	0.497927	151	1.787361	222	0.764726	299	0.777420	377	1.265766
5	0.430409	78	1.056041	154	1.717914	223	1.226421	301	1.156481	379	1.941262
6	0.935881	79	1.712992	155	0.997694	226	1.810545	302	0.918500	381	0.780338
7	1.046455	82	1.278110	157	0.855759	227	0.405779	303	0.979697	382	1.357001
10	1.150087	83	0.559779	158	0.767529	229	1.075469	305	1.577052	383	0.538214
11	0.902491	85	0.958550	159	1.250097	230	0.686280	307	1.083930	385	2.479635
13	0.662735	86	1.072202	161	1.586763	231	1.322177	309	0.970072	386	1.253677
14	0.908711	87	0.863058	163	1.462253	233	1.407615	310	1.629441	389	0.795953
15	1.065554	89	1.464441	165	0.796865	235	1.769768	311	0.982979	390	1.025410
17	1.016085	91	1.688687	166	1.703462	237	0.564299	313	2.187652	391	1.669065
19	1.337250	93	0.698098	167	0.450141	238	1.303839	314	0.765993	393	1.850943
21	0.683807	94	1.575084	170	0.999991	239	1.056456	317	0.504228	394	2.064301
22	1.274161	95	0.893944	173	0.390911	241	2.418356	318	0.601815	395	0.579840
23	0.807111	97	1.893495	174	1.208887	246	1.541322	319	1.911028	397	0.817598
26	0.907013	101	0.596669	177	1.764089	247	1.533062	321	2.030683	398	0.334944
29	0.611766	102	1.051189	178	1.209974	249	2.110940	322	1.442414	399	1.477149
30	1.127932	103	1.283704	179	1.191517	251	0.997930	323	0.797397	401	1.842450
31	1.440365	105	1.720149	181	1.066472	253	0.946672	326	1.076179	402	0.667045
33	1.332797	106	1.746070	182	0.591316	254	1.173544	327	0.671680	403	1.405539
34	1.457152	107	0.731062	183	1.017377	255	0.867886	329	1.695220	406	1.845619
35	0.837679	109	1.065972	185	1.444758	257	1.297485	330	1.185622	407	0.850625
37	0.819292	110	0.712637	186	1.410150	258	0.777247	331	1.992831	409	2.584507
38	0.698182	111	1.211148	187	1.187716	259	1.782445	334	1.777226	410	1.005026
39	1.252722	113	1.382352	190	1.676220	262	1.183859	335	0.775471	411	1.135247
41	1.299093	114	1.428405	191	1.208747	263	0.773021	337	2.334964	413	0.404539
42	1.005013	115	1.439708	193	2.170434	265	2.310878	339	1.323658	415	1.710396
43	1.349385	118	1.226894	194	0.856688	266	0.885688	341	0.609114	417	1.856470
46	1.591314	119	1.004816	195	0.954130	267	1.037593	345	2.048451	418	1.088092
47	0.665763	122	0.560073	197	0.475001	269	0.621893	346	1.685637	419	0.982327
51	1.289678	123	0.991323	199	1.715883	271	1.589701	347	0.755042	421	1.267717
53	0.540025	127	1.425335	201	1.953138	273	1.762924	349	1.051433	422	0.801152
55	1.397415	129	1.835837	202	1.230655	274	1.919263	353	1.263265	426	1.171209
57	1.512726	130	1.661595	203	0.664821	277	0.945515	354	1.398267	427	1.399600
58	1.388774	131	0.870445	205	1.050623	278	0.510851	355	1.535170	429	0.961107
59	0.906899	133	0.893688	206	0.814304	281	1.738377	357	0.622756	430	1.500765
61	0.938310	134	1.087092	209	1.582843	282	1.007064	358	1.405335	431	0.940710
62	0.614200	137	1.393813	210	1.120707	283	1.155463	359	1.041718	433	2.248559
65	1.377516	138	0.773483	211	1.861876	285	0.670476	362	0.382447	434	1.060151
66	1.198290	139	1.599663	213	0.587929	286	1.647646	365	0.617054	435	1.088716
67	1.403665	141	0.883754	214	1.911364	287	0.750378	366	1.506661	437	0.291061
69	0.774628	142	1.423918	215	0.610686	290	0.828503	367	1.271681	438	1.218115
70	1.486529	143	0.531233	217	2.152641	291	1.492029	370	1.348163	439	1.617940
71	1.050057	145	2.112534	218	0.842354	293	0.331438	371	0.844030	442	1.422478
73	1.794636	146	0.938483	219	1.350709	295	1.771613	373	0.956202	443	0.967018

Çizelge 5.6 $d = -1 \dots -443$ için $K = Q(\sqrt{d})$ sanal kuadratik sayı cisimlerine karşılık gelen $L(1, \chi)$ fonksiyonlarının değerleri

d	$L(1, \chi)$	d	$L(1, \chi)$	d	$L(1, \chi)$	d	$L(1, \chi)$	d	$L(1, \chi)$	d	$L(1, \chi)$
-1	0.785398	-73	0.735391	-146	2.080000	-219	0.849157	-295	1.463285	-373	0.813328
-2	1.110721	-74	1.826014	-149	1.801585	-221	1.690611	-298	0.545963	-374	2.274270
-3	0.604599	-77	1.432071	-151	1.789614	-222	1.265099	-299	1.453464	-377	1.294402
-5	1.404963	-78	0.711431	-154	1.012627	-223	1.472636	-301	0.724314	-379	0.484118
-6	1.282550	-79	1.767284	-155	1.009355	-226	0.835903	-302	1.084670	-381	1.609487
-7	1.187410	-82	0.693862	-157	0.752179	-227	1.042574	-303	1.804798	-382	0.642952
-10	0.993459	-83	1.034504	-158	0.999727	-229	1.038011	-305	1.439097	-383	2.728974
-11	0.947226	-85	0.681507	-159	2.491445	-230	2.071505	-307	0.537901	-385	0.640442
-13	0.871321	-86	1.693833	-161	1.980737	-231	2.480419	-309	1.072314	-386	1.599029
-14	1.679252	-87	2.020885	-163	0.246069	-233	1.234875	-310	0.713722	-389	1.752136
-15	1.622311	-89	1.998049	-165	0.978291	-235	0.409870	-311	3.384724	-390	1.272646
-17	1.523896	-91	0.658657	-166	1.219174	-237	1.224410	-313	0.710293	-391	2.224280
-19	0.720731	-93	0.651536	-167	2.674141	-238	0.814557	-314	2.304774	-393	0.950834
-21	1.371103	-94	1.296122	-170	1.445695	-239	3.048191	-317	0.882247	-394	0.791356
-22	0.669790	-95	2.578565	-173	1.671956	-241	1.214207	-318	1.057031	-395	1.264565
-23	1.965202	-97	0.637961	-174	1.428981	-246	1.201804	-319	1.758954	-397	0.473016
-26	1.848351	-101	2.188201	-177	0.472273	-247	1.199369	-321	1.753466	-398	1.574738
-29	1.750137	-102	0.622128	-178	0.941889	-249	1.194542	-322	0.700297	-399	2.516422
-30	1.147147	-103	1.547752	-179	1.174068	-251	1.388069	-323	0.699212	-401	1.568837
-31	1.692740	-105	1.226352	-181	1.167564	-253	0.395021	-326	1.913964	-402	1.253507
-33	1.093762	-106	0.915415	-182	1.397222	-254	1.576968	-327	2.084766	-403	0.312988
-34	1.077557	-107	0.911128	-183	1.857866	-255	2.360810	-329	2.078419	-406	1.247317
-35	1.062052	-109	0.902730	-185	1.847796	-257	1.567737	-330	0.691756	-407	2.491567
-37	0.516475	-110	1.797235	-186	1.382116	-258	0.782348	-331	0.518033	-409	1.242734
-38	1.528901	-111	2.385494	-187	0.459472	-259	0.780836	-334	1.031402	-410	1.241218
-39	2.01223	-113	1.182145	-190	0.455830	-262	0.582265	-335	3.089584	-411	0.929780
-41	1.962537	-114	1.176948	-191	2.955130	-263	2.518346	-337	0.684534	-413	1.545877
-42	0.969517	-115	0.585910	-193	0.452274	-265	0.771946	-339	1.023767	-415	1.542147
-43	0.479088	-118	0.867621	-194	2.255532	-266	1.926234	-341	2.381775	-417	0.923067
-46	0.926405	-119	2.879893	-195	0.899897	-267	0.384525	-345	0.676551	-418	0.614641
-47	2.291242	-122	1.422132	-197	1.119146	-269	2.107009	-346	0.844465	-419	1.381292
-51	0.879822	-123	0.566536	-199	2.004314	-271	2.099220	-347	0.843248	-421	0.765559
-53	1.294593	-127	1.393856	-201	1.329545	-273	0.760551	-349	1.177159	-422	0.764652
-55	1.694449	-129	1.659611	-202	0.663125	-274	1.138743	-353	1.337681	-426	1.826528
-57	0.832228	-130	0.551072	-203	0.881986	-277	0.566280	-354	1.335790	-427	0.304065
-58	0.412511	-131	1.372411	-205	0.877673	-278	1.318941	-355	0.666957	-429	1.213420
-59	1.227002	-133	0.544821	-206	2.188851	-281	1.874117	-357	0.665083	-430	0.909006
-61	1.206719	-134	1.899746	-209	2.173085	-282	0.748317	-358	0.498115	-431	3.177829
-62	1.595931	-137	1.073617	-210	0.867162	-283	0.560245	-359	3.150331	-433	0.905852
-65	1.558666	-138	1.069721	-211	0.648829	-285	1.488735	-362	1.486066	-434	1.809615
-66	1.546813	-139	0.799399	-213	0.861034	-286	1.114598	-365	1.644385	-435	0.602511
-67	0.383807	-141	1.058279	-214	0.644265	-287	2.596193	-366	0.985282	-437	1.502828
-69	1.512813	-142	0.527273	-215	2.999568	-290	1.844807	-367	1.475908	-438	0.600444
-70	0.750984	-143	2.627132	-217	0.853061	-291	0.736654	-370	0.979942	-439	2.249101
-71	2.609869	-145	1.043580	-218	1.063878	-293	1.651804	-371	1.304827	-442	0.597721

5.4 Bölümle İlgili Pari Komut ve Programları

d_K , $K = \mathbb{Q}(\sqrt{d})$ kuadratik sayı cisminin diskriminantı olmak üzere buna karşılık gelen $\chi(j) \pmod{d_K}$ Dirichlet karakterlerini hesaplamak için aşağıdaki kodları yazarak kullandım.

```
{chi(j,d)=
local(c);
if(issquarefree(d)<>1,
error("d kare-bagimsiz olmalı."));
c=kronecker(quaddisc(d),j);
return(c);
}
```

Örnek 5.18. $K = \mathbb{Q}(\sqrt{21})$ kuadratik sayı cisminin diskriminantı $d_K = 21$ olduğundan $\pmod{21}$ Dirichlet karakterleri $n = 1, 2, 3, \dots, 21$ için sırasıyla $1, -1, 0, 1, 1, 0, 0, -1, 0, -1, -1, 0, -1, 0, 0, 1, 1, 0, -1, 1, 0$ dir. Bunu `for(i=1,21,print(i," ",chi(i,21)))` ile elde edebiliriz.

`zeta(x)`: Riemann ζ fonksiyonunun x -kompleks veya p -adik sayısına karşılık aldığı değeri verir.

`zetakinit(P)`: P polinomu ile belirlenen bir sayı cisminde Dedekind ζ fonksiyonu ve λ fonksiyonları değerlerini (`zetak(x)`, `zetak(x,1)`) bulabilmemiz için bazı gerekli sayı cismi verilerini hesaplar. `znf=zetakinit(pol)` biçiminde kullanılabilir.

`zetak(znf,x)`: Sayı cisminde Dedekind ζ fonksiyonunun x -kompleks sayısında aldığı değeri hesaplar.

Örnek 5.19. $K = \mathbb{Q}(\sqrt{37})$ kuadratik sayı cismi için $\zeta_K(3)$ değerini hesaplatmak için,

`znf=zetakinit(quadpoly(quaddisc(37)))`; `zetak(znf,3)` kodlarını yazarız. Bundan sonra örneğin $\zeta_K(1+3i)$ değeri için `zetak(znf,1+3*I)` yazmak yeterlidir.

Aşağıdaki programı reel kuadratik sayı cisimlerine karşılık gelen $L(1, \lambda_d)$ değerlerini

hesaplatmak için yaptım. Herhangi bir $K = \mathbb{Q}(\sqrt{d})$ reel kuadratik sayı cismine karşılık gelen $L(1, \chi_d)$ 'yi hesaplatmak için bu kodları Pari'de yazdıktan sonra $Lr(d)$ yazmak yeterlidir. Burada d 'nin kare-bağımsız tamsayı olması gerekmektedir. Diğer durumda zaten program hata verecektir.

```
{Lr(d)=
local(s,m,j);
if(issquarefree(d)<>1,
error("d kare bagimsiz olmalı."));
s=1;\
for(j=1,abs(quaddisc(d)),\
s=((sin(Pi*j/quaddisc(d)))^(kronecker(quaddisc(d),j))))*s);\
m=-log(s)/sqrt(quaddisc(d));
return(m)
}
```

Örnek 5.20. $K = \mathbb{Q}(\sqrt{38765})$ kuadratik sayı cismine karşılık gelen χ Dirichlet karakteri için $L(1, \chi)$ 'yi hesalarırken $Lr(38765)$ yazmak gerekir. Sonuç 0.483542... çıkacaktır.

Bu kodlar kopyalanıp Pari'ye aktarıldıktan sonra Çizelge 5.5'in benzeri aşağıdaki kodlarla elde edilebilir. "L(1,chi_reel).doc" isimli Microsoft Word dokümanı oluşturularak sonuçlar oraya kaydedilecektir.

```
\p 6;
for(d=2,443,\
if(issquarefree(d)==1,\
write("L(1,chi_reel).doc", d, " ",Lr(d))))
```

Sanal kuadratik sayı cisimlerine karşılık gelen $L(1, \chi_d)$ değerleri içinse aşağıdaki pari programı kullanılabilir. $Ls(d)$ 'nin kullanımı $Lr(d)$ ile aynıdır.

```

{Ls(d)=
local(s,m);
if(issquarefree(d)<>1,
error("d kare bagimsiz olmalı."));
s=0;\
for(j=1,abs(quaddisc(-d)),\
s=s+j*kroncker(quaddisc(-d),j));\
m=(abs(s)*Pi)/(abs(quaddisc(-d)*sqrt(abs(quaddisc(-d)))));
return(m)
}

```

Örnek 5.21. $K = \mathbb{Q}(\sqrt{-95357})$ sanal kuadratik sayı cismine karşılık gelen χ Dirichlet karakteri için $L(1, \chi)$ 'yi hesaplariken $Ls(95357)$ yazmak gerekir. Sonuç 1.607424... çıkacaktır.

Çizelge 5.6'nın benzeri aşağıdaki kodlarla elde edildi. Sonuçlar "L(1,chi_sanal).doc" isimli dokümana aktarılacaktır.

```

\p 6;
for(d=1,443,\
if(issquarefree(d)==1,\
write("L(1,chi_sanal).doc", -d, " ", Ls(-d))))

```

Aşağıdaki kodları ve (5.22)'yi kullanarak reel ve sanal kuadratik sayı cisimlerinin sınıf sayıları hesaplanabilir.

```

{h(d)=
local(w,sinsay);
if(issquarefree(d)<>1,
error("d kare bagimsiz olmalı."));

```

```

if(d<0,
if(d==-1,w=4,
if(d==-3,w=6,w=2));
sinsay=((w*sqrt(abs(quaddisc(d)))/(2*Pi))*Ls(-d));
if(d>0,
sinsay=(sqrt(quaddisc(d))/(2* log(quadunit(quaddisc(d))))) *Lr(d));
return(sinsay);
}

```

Bu kodlar ve $L_r(d)$, $L_s(d)$ 'yi hesaplayan kodlar girildikten sonra $K = \mathbb{Q}(\sqrt{d})$ 'nin sınıf sayısını hesaplamak için $h(d)$ yazmak yeterlidir.

Örnek 5.22. $K = \mathbb{Q}(\sqrt{37187})$ reel kuadratik sayı cisminin sınıf sayısı için $h(37187)$ yazarız. Bu sonucu Parinin kendi kodu olan `qfbclassno(quaddisc(37187))` ile karşılaştırırsak aynı sonucu yani 4'ü elde ederiz. Benzer şekilde $K = \mathbb{Q}(\sqrt{-147083})$ sanal kuadratik sayı cismi için $h(-147083)$ yazdığımızda sonucun 153 olduğunu görürüz.

6. SONUÇLAR

Bu çalışmada $\mathbb{Q}(\sqrt{d})$ kuadratik sayı cisimlerinde çarpanlara ayırma, idealler, ideal sınıf grupları ve sınıf sayıları çalışılmıştır. Ayrıca bu sayı cisimleriyle bağlantılı kuadratik formlar, zeta ve L-fonksiyonları bir bütün olarak ele alınmış bütün bunların birbirleriyle bağlantılarına dair sonuçlar elde edilmiştir.

Bazı kuadratik sayı cisimlerinin Dirichlet karakterleri hesaplanmış ve bunlara karşılık gelen $L(1, \chi)$ değerleri ile bunların sınıf sayılarıyla bağlantılarına dair sonuçlar elde edilmiştir. Pari programı vasıtasıyla, elde edilen sonuçlar desteklenmiş ve her bir bölümle ilgili Pari ile elde edilen tablolar ilgili kısımlara eklenmiştir.

KAYNAKLAR

- Adams, W.W. ve Goldstein, L.J., (1976), Introduction to Number Theory, Prentice-Hall Inc, Englewood Cliffs, New Jersey.
- Apostol, T.M., (1976), Introduction to Analytic Number Theory, Springer-Verlag New York Inc., New York.
- Çallıalp, F., (1999), Sayılar Teorisi, İstanbul.
- Dodd, F.W., (1983), Number Theory in the Quadratic Field with Golden Section Unit, Polygonal Publishing House, New Jersey.
- Edwards, H.M., (1977), Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory, Springer-Verlag, New York.
- Frleigh, J.B. ve Katz, V., (2003), A first Course in Abstract Algebra, Pearson Education Inc., Mexico.
- Jacobson, M.J., (1995), "Computational Techniques in Quadratic Fields", Ms Thesis in Computer Science, University of Manitoba, Manitoba.
- Jones, B.W., (1950), "The Arithmetic Theory of Quadratic Forms", John Wiley and Sons Inc., Maryland.
- Kato, K., Kurokawa, N. ve Saito T., (2000), Number Theory 1-Fermat's Dream, Translations of Mathematical Monographs, Vol. 186 (İng. Çev., M. Kuwata), American Mathematical Society, United States of America.
- Köklüce, B., (2000), "Quadratic Fields in Number Theory", Ms Thesis, Fatih Üniversitesi, İstanbul.
- Marcus, D.A., (1977), Number Fields, Springer-Verlag New York Inc., New York.
- Mastropietro, M.W., (2000), "Quadratic Forms and Relative Quadratic Extensions", PhD Thesis in Mathematics, University of California, San Diego.
- Mollin, R.A., (1996), Quadratics, CRC Press, New York.
- Mollin, R.A., (1999), Algebraic Number Theory, CRC Press LLC, New York.
- Murty, M.R., (1999), Problems in Algebraic Number Theory, Springer Verlag New York Inc, New York.
- Silverman, J.H., (2001), A Friendly Introduction to Number Theory, Pearson Education, New Jersey.
- Stewart, I. ve Tall, D., (2002), Algebraic Number Theory and Fermat's Last Theorem, A. K Peters, Ltd, Natick, Massachusetts.
- Swinerton-Dyer, H.P.F, (2001), A Brief Guide to Algebraic Number theory, Cambridge University Press, Cambridge.

INTERNET KAYNAKLARI

- [1] <http://pari.math.u-bordeaux.fr/>

- [2] www.ma.utexas.edu/users/villegas/cnt/cnt-frames.html
- [3] www.math.uga.edu/~mbaker/math8400.html
- [4] <http://modular.fas.harvard.edu:9000/>
- [5] <http://maths.dur.ac.uk/~dma0td/computel/>
- [6] www.maths.dur.ac.uk/~dma0smjw/nt/
- [7] www.math.umn.edu/~garrett/students/reu/zaki.pdf

ÖZGEÇMİŞ

Doğum tarihi 25.12.1975

Doğum yeri Bayburt

Lise 1989-1991 Bayburt Lisesi (1. ve 2. sınıflar)
1991-1992 İstanbul Bahçelievler Kocasınan Lisesi (Son sınıf)

Lisans 1992-1996 Karadeniz Teknik Üniversitesi Fatih Eği. Fak.
Matematik Öğretmenliği Bölümü

Yüksek Lisans 1997-2000 Fatih Üniversitesi Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Doktora 2000-2005 Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Çalıştığı Kurum

1997-1999 Fatih Üniversitesi. Fen Bil. Enst. Matematik Bölümü
Araştırma Görevlisi
1999-2001 Fatih Üniversitesi Enformatik Bölümü Okutmanı
2001-Devam Ediyor Fatih Üniversitesi Fen-Edeb. Fak.
Matematik Bölümü Öğretim Görevlisi