T.C.
BALIKESİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

REZİDÜ TEORİLERİ

YÜKSEK LİSANS TEZİ

AYŞE GÖZDE YAMAN

BALIKESİR, ŞUBAT - 2014

T.C.
BALIKESİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

REZİDÜ TEORİLERİ

YÜKSEK LİSANS TEZİ

AYŞE GÖZDE YAMAN

BALIKESİR, ŞUBAT - 2014

KABUL VE ONAY SAYFASI

AYŞE GÖZDE YAMAN tarafından hazırlanan "**REZİDÜ TEORİLERİ**" adlı tez çalışmasının savunma sınavı 13.02.2014 tarihinde yapılmış olup aşağıda verilen jüri tarafından oy birliği / ~~oy çokluğu~~ ile Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri	İmza
Danışman Yrd.Doc.Dr.Dilek NAMLI	.....
Üye Prof.Dr.Recep ŞAHİN	.....
Üye Doc.Dr.Özden KORUOĞLU	.....

Jüri üyeleri tarafından kabul edilmiş olan bu tez BAÜ Fen Bilimleri Enstitüsü Yönetim Kurulunca onanmıştır.

Fen Bilimleri Enstitüsü Müdürü

Prof.Dr.Cihan ÖZGÜR .....

ÖZET

REZİDÜ TEORİLERİ
YÜKSEK LİSANS TEZİ
AYŞE GÖZDE YAMAN
BALIKESİR ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

(TEZ DANIŞMANI: YRD. DOÇ. DR. DİLEK NAMLI)

BALIKESİR, ŞUBAT - 2014

REZİDÜ TEORİLERİ

Bu tezin amacı kuadratik, kübik ve kuartik rezidüler için literatürde yer alan sonuçları biraraya getirmektir.

Bu çalışma beş bölümden oluşmaktadır. İkinci bölümde daha sonraki bölümlerde gerekli olacak bazı önbilgiler hatırlatılmıştır.

Üçüncü bölümde kuadratik rezidüler ile ilgili sonuçlar bir araya getirilmiş ve Legendre sembolü yardımı ile kuadratik rezidüler belirlenmiştir.

Dördüncü bölümde ise kübik rezidüler ele alınmış, bu bölümde kübik rezidü karakterinin nasıl hesaplandığı belirtilmiş, Kübik İndirgeme Yasası verilmiştir.

Beşinci bölümde de kuartik rezidülerin tanım ve teoremlerine yer verilmiştir.

ANAHTAR KELİMELER: kuadratik rezidü, kübik rezidü, kuartik rezidü, indeks, kompleks asal, rasyonel asal, legendre sembolü.

ABSTRACT

THE RESIDUE THEORYS
MSC THESIS
AYŞE GÖZDE YAMAN
BALIKESIR UNIVERSITY INSTITUTE OF SCIENCE
MATHEMATICS
(SUPERVISOR: ASSIST. PROF. DR. DİLEK NAMLI)

BALIKESİR, FEBRUARY 2014

The aim of this thesis is combine the results in of the quadratic , cubic and quartic residues in literatur chapters.

This study consists of five parts.In the second chapter some information that will be mentioned later are reminded.

In the third chapter , the results of residues have been combined and with the help of Legendre symbol ,quadratic residues have been identified.

In the fourt chapter , cubic residues have been deal with and calculation of cubic residue character established and cubic reduction have been provided.

And finally , in the fifth chapter the definations of residues have been mentioned and the theorems were used.

KEYWORDS: quadratic residue, cubic residue, quartik residue, index, complex prime, rational prime, legendre symbol.

İÇİNDEKİLER

Sayfa

SEMBOL LİSTESİ

Simge	**Adı**
$\mathbb{Z}$	Tamsayılar kümesi
$\mathbb{C}$	Karmaşık sayılar kümesi
$\mathbb{R}$	Reel sayılar kümesi
$\mathbf{N}$	Doğal sayılar kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\mathbb{Z}[x]$	Kat sayıları tam sayılar olan x'in polinomlarının halkası
$\mathbb{Z}_n$	n modunda kalan sınıflarının kümesi
$\mathbb{Z}_p$	p asal modundaki tam sayılar cismi
U_n	Birimlerin kümesi
Q_n	İkinci dereceden kalanların kümesi
$\chi(a)$	α'nın *p* asal modunda Legendre sembolü
$\left(\frac{a}{p}\right)$	α'nın *p* asal modunda Legendre sembolü
$\chi_3(\alpha)$	α'nın *p* asal modunda üçüncü dereceden kalanlar kümesi
$\left(\frac{a}{p}\right)_3$	α'nın *p* asal modunda üçüncü dereceden kalanlar kümesi
$\varphi(m)$	m modülüne göre asal kalan sınıflarının sayısı

ÖNSÖZ

Bu tezde Rezidü teorileri incelendi. Genel teori verildikten sonra bu konudaki literatürü oluşturan çalışmalardan bazı önemli teoremler seçilerek bunların ispatları anlaşılır biçimde verildi. Tez beş bölümden oluşmaktadır.

Tez çalışmamın başından sonuna kadar bana tüm desteğini veren, fazlasıyla sabır gösterip, bilgilerini bana aktaran çok kıymetli hocam, sevgili danışmanım Yrd. Doc. Dr. Dilek NAMLI'ya

Bana gösterdikleri destek için sayın Prof. Dr. Abdullah SOYKAN ve Prof. Dr. Turgut KILIÇ'a,

Her koşulda yanımda olan, bugüne gelmemi sağlayan canım annem ve babama,

Hayatıma neşe katan canım kardeşlerim; İlayda ve Hüseyin'e,

Sonsuz teşekkürlerimi sunarım

1. GİRİŞ

Denklemler konusunda ilk önemli adımların Babilliler tarafından atıldığı bilinmektedir. Bu konudaki en eski yazılı belge ise M.Ö. 1700' den önce yaşadığı sanılan Mısırlı Ahnes'in çalışmalarını içeren Rhind Papirüsü'dür. Rhind Papirüsü'nde çeşitli birinci dereceden denklemlerin çözümü yer alır. Sonraki yüzyıllarda, önce Yunan ve Mısır, daha sonra da İslam ve Hint matematikçileri denklemlere ilgi duymuşlardır. Bu dönemlerin en ilgi çekici yapıtları arasında İskenderiyeli Diophantos'un Aritmetike'si (y.200), Hintli Brahmugupta (y.630) ve Bhaskara'nın (y.1150) yapıtları ve Arap matematikçi Harizmi'nin Hisabü'l-cebr ve İtalyan Leonardo Pisano 'nun Liber abaci (1202; Abaküs kitabı) adlı kitabıyla Hristiyan Batı'da tanınmaya başlayan denklemlerin genel bir kurama dayandırılmasını sağlayacak ilk önemli adımlar 15. ve 16. yüzyılda İtalyan matematikçiler tarafından atıldı. 17. yüzyıl matematikçilerinden Pierre de Fermat kendi adını verdiği teoremiyle bazı sonuçlar elde etmiştir.18.yüzyılda da önemli matematikçilerden Leonhard Euler bu konuda bazı teoremler ileri sürmüştür.

Kübik denklemlerin çözülebilmesi problemi ile ilgili çalışmalar yaklaşık 4000 yılı bulmaktadır. Scipione dal Ferro, Nicol Tartaglia, Cardano, Viete, Lodovico Ferrari Ars manga (1545; Büyük Sanat) adlı yapıtında Ferro'nun üçüncü dereceden denklemlere ilişkin buluşlarının yanı sıra Ferrari'nin dördüncü dereceden denklemlere ilişkin buluşlarının yanı sıra Ferrari'nin dördüncü dereceden denklemlerin çözümüne ilişkin çalışmalarından da yararlanan Gerolamo Cardano sözü geçen dönemin en önemli matematikçileri arasındadır.Kübik rezidü kavramı Gauss tarafından da ele alınmış olup G.Eiseinstein tarafından bazı sonuçlar elde edilmiştir.

2. ÖN BİLGİLER

2.1 Kongrüanslar

2.1.1.Tanım: a, b, m $\in \mathbb{Z}$; m >0 verilsin eğer $m|(a-b)$ ise a ile b ye m modülüne göre denktir denir ve $a \equiv b \pmod m$ şeklinde gösterilir [2] .

2.1.2.Teorem: Sabit bir m modülüne göre kongrüans bağıntısı tam sayılar kümesi üstünde bir denklik bağıntısıdır [2].

İspat: 1) $m|(a-a)=0$ olduğu için $a \equiv a \pmod m$ sağlanır, yani " $\equiv$ " bağıntısı yansıyandır.

2) $a \equiv b \pmod m$ ise $m|(a-b), m|-(a-b)$. O halde $b \equiv a \pmod m$ olup "$\equiv$" bağıntısı simetriktir.

3) $a \equiv b \pmod m$, $b \equiv c \pmod m$ olsun, o halde $m|(a-b)$, $m|(b-c)$ dir. Buradan $m|(a-b)+(b-c)$, yani $m|(a-c)$ olduğundan $a \equiv c \pmod m$ dir. Bu durumda , "$\equiv$" bağıntısı geçişme özelliğine sahiptir. 1), 2) ve 3)'ten " $\equiv$ " bağıntısı bir denklik bağıntısıdır.

2.1.3 Teorem: m > 0 bir tam sayı ve a, b, c, d keyfi tam sayılar olsun. Bu durumda aşağıdaki özellikler geçerlidir. $a \equiv b \pmod m$, $c \equiv d \pmod m$ olduğunda,

a) $a \equiv b \pmod m$, $c \equiv d \pmod m$ ise, $a+c \equiv b+d \pmod m$, $ac \equiv bd \pmod m$,

b) $a \equiv b \pmod m$ ise $a+c \equiv b+c \pmod m$ ve $ac \equiv bc \pmod m$,

c) $a \equiv b \pmod m$ ise k herhangi bir pozitif tam sayı olmak üzere $a^k \equiv b^k \pmod m$ dir [1].

2.1.4 Teorem: k, a, b, m $\in \mathbb{Z}$; m>0, $k \not\equiv 0 \pmod m$, (k,m)=d ve $ka \equiv kb \pmod m$ olsun. Bu durumda, $a \equiv b \pmod{\frac{m}{d}}$'dir [4].

2.1.5 Sonuç: $ka \equiv kb \pmod m$, $(k,m)=1$ ise $a \equiv b \pmod m$'dir [4]

2.1.6 Sonuç: $a \equiv b \pmod m$, $n \in N$, $c \in \mathbb{Z}$ olmak üzere

a) $a^n \equiv b^n \pmod m$

b) $a \mp c \equiv b \mp c \pmod m$

c) $ac \equiv bc \pmod m$'dir [4].

2.1.7 Teorem: $a \equiv b \pmod m$ ve P(x) tam sayı katsayılı bir polinom fonksiyon olsun. Bu taktirde

$P(a) \equiv P(b) \pmod m$

dir [4].

İspat: $P(x)=\sum_{j=0}^{n} c_j x^j$ olsun. 2.1.3. Teorem'den $a \equiv b \pmod m$ ise

$a^j \equiv b^j \pmod m$ $(j=0, 1, \ldots, n)$ olur. O halde $c_j a^j \equiv c_j b^j \pmod m$ $(j=1,\ldots, n)$ ve buradan

$\sum_{j=0}^{n} c_j a^j \equiv \sum_{j=0}^{n} c_j b^j \pmod m$ elde edilir. Yani $P(a) \equiv P(b) \pmod m$ bulunur.

2.1.8 Önerme: $a, b \in \mathbb{Z}$, $d, m \in \mathbb{Z}^+$ ve $a \equiv b \pmod m$, $d \mid m$ ise $a \equiv b \pmod d$ dir [4].

Çözüm: $a \equiv b \pmod m$ ise $m \mid (a-b)$'dir.

$\left.\begin{matrix} d \mid m \\ m \mid (a-b) \end{matrix}\right\}$ ise $d \mid (a-b)$, yani $a \equiv b \pmod d$'dir.

2.1.9 Önerme: $a, b \in \mathbb{Z}$ ve $m>0$ bir pozitif tamsayı olmak üzere $a \equiv b \pmod m$ olması için gerek ve yeter şart a ile b'nin m ile bölündüğünde aynı kalanı vermesidir [4].

2.1.10 Örnek: $x, y \in \mathbb{Z}$ olmak üzere $x \equiv y \pmod{m_i}$, $i=1,2,3,\ldots,k$ ise $x \equiv y \pmod{[m_1, m_2, m_{3,\ldots,} m_k]}$'dır [4].

Çözüm: $x \equiv y \pmod{m_1}$ ise $m_1 \mid (x-y)$

$x \equiv y \pmod{m_2}$ ise $m_2 \mid (x-y)$,

$x \equiv y \pmod{m_2}$ ise $m_k \mid (x-y)$ 'dir.

E.K.O.K. tanımından , $[m_1, m_2, m_3, ..., m_k] \mid (x-y)$ ise

$x \equiv y \pmod{[m_1, m_2, m_{3,\ldots,} m_k]}$ bulunur.

2.2 Kalan Sistemleri

m>0 bir tam sayı ve $a \in \mathbb{Z}$ olsun. Bölme algoritmasına göre a=mq+r, $0 \leq r<m$ olacak şekilde q ve r tam sayıları vardır .Böylece a-r=mq olduğundan $m \mid (a-r)$;

Yani $a \equiv r \pmod{m}$'dir. Burada r = 0, 1, 2,…, m-1'dir ve bunlardan herhangi ikisi m modülüne göre birbirine denk değildir.

2.2.1 Tanım: Elemanları m ile aralarında asal olan bir kalan sınıfına m modülüne göre asal kalan sınıfı denir [4] .

2.2.2 Uyarı: Eğer bir kalan sınıfında m ile aralarında asal olan bir sayı varsa, bu kalan sınıfının bütün sayıları m ile aralarında asaldır. Çünkü: $\bar{a} \equiv \{\ldots, e, f, \ldots\}$, (e,m)=1 olsun. Bu taktirde, $e \equiv f \pmod{m}$ ise (e,m)=(f,m)=1 olacaktır [4].

2.2.3 Tanım: Her m>0 tamsayısını, m'yi geçmeyen ve m ile aralarında asal olan tam sayıların sayısına eşleyen fonksiyona Euler-φ fonksiyonu adı verilir. Bu tanıma göre,

$\varphi(1)=1$; {1}

$\varphi(4)=2$; {1,3}

$\varphi(5)=4$; {1,2,3,4},

$\varphi(17)=16$; {1,2,…,15,16}

$\varphi(p)=p-1$; {1,2,3,…,p-1} dir.

Yukarıdaki verilenlerden görüldüğü gibi verilen bir asal sayının görüntüsü o asal sayının bir eksiğidir [4].

2.2.4 Teorem: m modülüne göre asal kalan sınıflarının sayısı $\varphi(m)$'dir [4].

İspat: {1,2,…,m} kümesi bir kalan sistemi olup, bunlar arasında m ile aralarında asal olan $\varphi(m)$ tane tamsayı vardır. Böylece m modülüne göre asal kalan sınıflarının sayısı $\varphi(m)$'dir.

2.2.5 Tanım: $a_1, a_2, a_3, ..., a_{\varphi(m)}$ tam sayıları aşağıdaki koşulları sağlıyorsa, "bu sayılar m modülüne göre indirgenmiş kalan sistemi oluşturuyor." denir.

i) $\forall$ i için $(a_i,m)=1$, $i \in 1,2,\ldots,\varphi(m)$

ii) $i \neq j$ için $a_j \not\equiv a_j \pmod m$,

iii) (a,m)=1 koşulunu sağlayan $\forall a \in \mathbb{Z}$ için $1 \leq i \leq \varphi(m)$ olmak üzere $a \equiv a_i \pmod m$ olacak şekilde bir i tamsayısı vardır. Böylece asal kalan sınıflarının her birinden bir sayı alarak indirgenmiş kalan sistemi oluşturulabilir [4].

2.2.6 Teorem: n>0, m>0 iki tamsayı ve (m, n)=1 ise $\varphi(m.n) = \varphi(m).\varphi(n)$ dir [1].

2.2.7 Teorem: φ (1)=1 ve n>1 bir pozitif tamsayı olmak üzere

$\varphi(n)=n.\prod_{p|n}\left(1-\frac{1}{p}\right)$'dir [2]. Burada $\prod_{p|n}$ 'de çarpım n tamsayısının bütün p asal bölenlerinin üzerinden alınmaktadır. Şu halde n tamsayısının kanonik formu

$n= p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$ ise $\prod_{p|n}\left(1-\frac{1}{p}\right)=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)=\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right)$ olur.

2.2.8 Örnek: n=174 için $\varphi(n)$'yi bulalım.

Çözüm: 174=2.3.29'dur, çarpanlarının hepsi asaldır. O halde

$\varphi(174) = \varphi(2.3.29)$

$=2.3.29.(1-1/2).(1-1/3).(1-1/29)$

$=2.3.29.1/2.2/3.28/29$

$=56$ bulunur.

2.2.9 Teorem: $a_1, a_2, a_3, ..., a_{\varphi(m)}$ tam sayıları m modülüne göre bir asal kalan sistemi oluşturuyor ve (k, m) =1 ise bu taktirde $ka_1, ka_2, ka_3, ..., ka_{\varphi(m)}$ tamsayıları da m modülüne göre bir asal kalan sistemi oluşturur [3].

2.2.10 Teorem (Euler): $m \in N$, m>1, $a \in \mathbb{Z}$ ve (a, m) =1 olsun. Bu taktirde, $a^{\varphi(m)} \equiv 1 \pmod{m}$'dir [2].

2.2.11 Teorem (Fermat): p bir asal sayı ve p∤a olsun. Bu taktirde, $a^{p-1} \equiv 1 \pmod{p}$'dir [1].

2.2.12 Sonuç: Eğer p bir asal sayı ise $\forall a \in \mathbb{Z}$ için $a^p \equiv a \pmod{p}$'dir. Çünkü Fermat teoremine göre p∤a ise $a^{p-1} \equiv 1 \pmod{p}$ olduğundan her iki tarafı a ile çarparsak istenen durum elde edilir, eğer $p \mid a$ ise $a \equiv 0 \pmod{p}$ ve böylece $a^p \equiv 0 \pmod{p}$ ise $a^p \equiv a \pmod{p}$'dir [4].

2.2.13 Örnek: $126^{\varphi(143)} \equiv 1 \pmod{143}$ denkliğini sağlayan x tam sayılarını bulalım.

Çözüm: 143=11.13, 126=$2.3^2.7$ ve (126,143)=1 olduğundan Euler teoreminden $126^{\varphi(143)} \equiv 1 \pmod{143}$ buluruz.

$\varphi(143) = \varphi(11).\varphi(13) = (11-1).(13-1)=120$ olduğundan

$126^{120} \equiv 1 \pmod{143}$ ve

$126^{7007} \equiv \left(126^{120}\right)^{58}.126^{47} \equiv (-17)^{47} \equiv -3^{23}.17$

$\equiv -42^3.9.7 \equiv -48.42.9.7$

$\equiv -140 \equiv 3 \pmod{143}$ elde edilir.

2.3 Lineer Kongrüanslar

2.3.1 Tanım: a, b, m $\in \mathbb{Z}$, m>0 ve a$\not\equiv$0 (mod m) olmak üzere, $ax \equiv b \pmod{m}$ şeklindeki bir ifadeye "bir bilinmeyenli bir lineer kongrüans denklemi" denir.

2.3.2 Teorem: $ax \equiv b \pmod{m}$ kongrüansının bir çözümünün olabilmesi için gerek ve yeter şart $(a,m) \mid b$ olmasıdır [1] .

2.3.3 Tanım: $ax \equiv b \pmod{m}$ kongrüansının çözümlerinden aynı kalan sınıfına ait olan çözümlere denk çözümler, aynı kalan sınıfına ait olmayan herhangi iki çözüme ise denk olmayan çözümler denilir [4].

2.3.4 Örnek: $2x \equiv 6 \pmod{8}$ kongrüansının çözümlerinin $\bar{3}$, $\bar{7}$ sınıflarındaki x=3 için: $2.3 \equiv 6 \pmod{8}$, x=7 için: $2.7 \equiv 6 \pmod{8}$ olduğundan 3 ve 7 kongrüansın iki denk olmayan çözümüdür.

2.3.5 Teorem: $ax \equiv b \pmod{m}$ kongrüansında (a,m)=d ve $d \mid b$ ise kongrüansın, mod m tam d tane denk olmayan çözümü vardır. Bu çözümler x_0 herhangi bir çözüm ve $m' = \frac{m}{d}$ olmak üzere,

$x_0 + m'$, $x_0 + 2m'$,…, $x_0 + (d-1)\, m'$ şeklindedir [1].

2.3.6 Sonuç: (a,m) =1 ise $ax \equiv b \pmod{m}$ kongrüansının bir tek çözümü vardır [4].

2.3.7 Sonuç: p bir asal sayı ve a$\not\equiv$ 0 (mod p), yani (p,a)=1 ise $ax \equiv b \pmod{p}$ kongrüansı bir ve yalnız bir çözüme sahiptir [4].

2.3.8 Teorem: (a, m)=1 olmak üzere $ax \equiv b \pmod{m}$ lineer kongrüansının çözümü $x \equiv a^{\varphi(m)-1}.b(m)$ dir [1].

İspat: (a,m) =1 olduğundan Euler toremine göre $a^{\varphi(m)} \equiv 1 \pmod{m}$ dir. Eğer $ax \equiv b \pmod{m}$ kongrüansının her iki tarafını $a^{\varphi(m)-1}$ ile çarparsak

$a^{\varphi(m)-1} ax \equiv a^{\varphi(m)-1} b \pmod{m}$

$a^{\varphi(m)-1} x \equiv a^{\varphi(m)-1} b \pmod{m}$

$x \equiv a^{\varphi(m)-1} b \pmod{m}$ buluruz.

2.3.9 Örnek: $3x \equiv 1 \pmod{7}$ kongrüansının çözüm kümesini bulalım.

(3,7) =1 olduğu için

$x \equiv 3^{6-1} .1 \pmod{7}$

$\equiv 3^{6-1} .1 \pmod{7}$

$\equiv 3^5\ 1 \pmod{7}$

$\equiv 243 \pmod{7} \equiv 5 \pmod{7}$ bulunur.

2.3.10 Uyarı: $ax \equiv c \pmod{b}$ lineer kongrüansının çözümlerinin bulunması ax+by=c Lineer Diophant denkleminin çözümlerinin bulunmasına denktir.ax+by=c denkleminin tüm çözümleri, (x_0, y_0) bir özel çözüm ve t bir tam sayı olmak üzere $x=x_0+\frac{b}{d}$ t, $y= y_0 -\frac{a}{d}$ t şeklindeydi. Yani $ax \equiv c \pmod{b}$ kongrüansının genel çözümü $x=x_0+\frac{b}{d}$ t şeklindedir [2].

2.3.11 Örnek: 48x+7y=17 lineer Diophant denkleminin çözümlerini bulalım. $(48,7) = 1 \mid 17$ olduğundan çözümü vardır. Öncelikle bir özel çözümünü bulalım:

$48x \equiv 17 \pmod{7}$ kongrüansını göz önüne alırsak;

$-x \equiv 3 \pmod{7}$ ve buradan

$x \equiv 4 \pmod{7}$ elde edilir. Verilen denklemde x=4 yazılarak

48.4+7y=17 olur. Buradan y=-25 bulunur. Böylece (4,-25) ikilisi,

48x+7y=17 denkleminin bir özel çözümü olur [2].

2.3.12 Teorem (Çin Kalan Teoremi): $m_1, m_2, m_3, ..., m_r$ pozitif tamsayılar ve her $i \neq j$ için $(m_i, m_j) = 1$ olsun. $a_1, a_2, a_3, \ldots, a_r$ tamsayıları verildiğinde

$x \equiv a_i \pmod{m_i}$, (i=1,2,3,…,r) kongrüansının ortak çözümleri vardır ve herhangi iki ortak çözüm $\mathrm{mod}(m_1.m_2.m_3...m_r)$ denktir [4].

2.3.13 Örnek: $\left.\begin{array}{l} x \equiv 1(\mathrm{mod}\ 3) \\ x \equiv 2(\mathrm{mod}\ 4) \\ x \equiv 3(\mathrm{mod}\ 5) \end{array}\right\}$ kongrüans sisteminin çözümünü bulalım.

(3, 4)=(3,5)=(4,5)=1 olduğundan, kongrüansın mod (3.4.5)'te bir tek çözümü vardır.m_1=3 , m_2=4 , m_3 =5 , a_1=1, a_2=2, a_3=3 tür.

Buradan, m=3.4.5=60, $\frac{m}{m_1}$=20, $\frac{m}{m_2}$=15, $\frac{m}{m_3}$=12 bulunur.

$20b_1 \equiv 1 \pmod 3$ ise $b_1 \equiv -1 \pmod 3$,

$15b_2 \equiv 1 \pmod 4$ ise $b_2 \equiv -1 \pmod 4$,

$12b_3 \equiv 1 \pmod 5$ ise $b_3 \equiv 3 \pmod 5$

elde edilir. Şu halde sistemin çözüm $x \equiv 20.(-1).1+15.(-1).2+12.3.3 \equiv 58 \pmod{60}$ bulunur [4].

3. İKİNCİ DERECEDEN KALANLAR

Lineer kongrüans, en basit anlamda verilen bir sayının mod denilen verilen büyüklüğü aşmayacak şekilde değerinin yeniden belirlenmesidir. Benzer olarak lineer kongrüans denklemiyle kastedilen ise denklemdeki katsayılara verilen modda yeniden değer verilmesinden sonra istenilen değişkenlerin değerlerinin yine bu modda elde edilmesidir.

Kongrüans kavramı, sadece lineer kongrüanslarla sınırlı değildir. Benzer şekilde verilen bir sayının karesini, küpünü ya da daha yüksek kuvvetlerini verilen modda indirgediğimizde ikinci, üçüncü ya da daha yüksek mertebeden kalanını bulmuş oluruz.

Amacımız ikinci dereceden kongrüans denklemlerinin belirli modlarda ki çözümlerini aramaktır. Aslında bunu yaparken bir sayının verilen bir modda kareköklerini bulmuş oluruz. Tam sayılar kümesinde bir sayının eğer varsa sadece bir tane karekökü olduğunu biliyoruz. Ancak verilen bir modda bir sayının birden fazla karekökü olabilir.

Örneğin; 15 modunda karesi 1 eden 4 tane sayı mevcuttur: Bunlar 1, 4, 11ve14 tür. Daha büyük p asal ise ab≡0 (p) iken a≡0 veya b≡0 (p) dir. Yani, $\mathbb{Z}_p$ nin de aritmetiği $\mathbb{Z}$'nin kine benzerlik gösterir(ab≡0 iken a=0 veya b=0 dır.) Ancak bu özellik mod birleşik sayı olduğunda geçerli olmaz. Eğer n=ab,1<a<n ve 1<b<n ise ab≡0(n) olması durumunda ab≠0 olabilir. Bu gibi problemler sebebiyle asal moddan birleşik moda geçerken dikkatli olmak gereklidir. Daha büyük modlara geçildiğinde bu sayının daha da artacağı görülebilir.

3.1 $\mathbb{Z}_n$ Halkasında Birimler

Şimdi $\mathbb{Z}_n$ 'deki dört işlemi düşünelim: Bölme yaparken böleceğimiz sayının mod ile aralarında asal olması önemlidir.

3.1.1 Örnek: n birleşik sayı ise $\bar{0}$ olmayan bir denklik sınıfı ile bölme yapabiliriz. $\mathbb{Z}_4$ 'de $\bar{1}/\bar{2}$ tanımsızdır. Çünkü $\overline{2x} = \bar{1}$ olacak şekilde bir x∈ $\mathbb{Z}_4$

yoktur.Şimdi hangi $\bar{a}$ lar için aynı zamanda $\bar{1}/\bar{a}$ sınıfında da Z_n de olduğunu belirleyeceğiz [1].

3.1.2 Tanım: $\bar{a} \in \mathbb{Z}_n$ elemanın çarpmaya göre bir tersi, $\overline{ab}=1$ olacak şekilde bir $\bar{b} \in \mathbb{Z}_n$ elemanıdır. $\mathbb{Z}_n$'de çarpmaya göre tersi olan bir elemana birim denir [1].

3.1.3 Yardımcı Teorem: $\bar{a} \in \mathbb{Z}_n$ elemanın bir birim olması için gerek ve yeter şart (a,n)=1 olmasıdır. Yani sadece mod ile aralarında asal olan elemanlar birer birim olur [1].

İspat: $\bar{a}$, n modunda bir birimse, $\overline{ab}=1$ yani ab≡1 (n) olacak şekilde $\bar{b} \in \mathbb{Z}_n$ elemanı bulunabilmelidir. O halde, q∈ ℤ olmak üzere ab=1+qn yazabiliriz. Bu durumda a ve n sayılarını aynı anda bölen bir sayı bunların bir lineer birleşimi olan 1'i de bölecektir. O halde (a, n) =1 olmalıdır.(a,n) =1 ise 1=ax+ny olacak şekilde x ve y tam sayıları vardır. O halde $ax \equiv 1$ (n) yazabileceğimizden $\bar{x}$, $\bar{a}$ elemanının çarpmaya göre tersidir.

3.1.4 Örnek: $\mathbb{Z}_8$ de birimler $\bar{1},\bar{3},\bar{5},\bar{7}$ dir. Çünkü $\bar{7}.\bar{7}=1$, $\bar{5}.\bar{5}=1$, $\bar{5}.\bar{5}=1$, $\bar{7}.\bar{7}=1$ dir. Yani her bir elemanın tersi kendisidir.$\mathbb{Z}_9$ halkasında birimler $\bar{1},\bar{2},\bar{4},\bar{5},\bar{7}$ ve $\bar{8}$ dir. $\bar{2}.\bar{5}=\bar{1}$ olup $\bar{2}$ ile $\bar{5}$ birbirinin tersidir. Bundan böyle $\mathbb{Z}_n$ halkasındaki birimlerin kümesini U_n ile göstereceğiz [1].

3.1.5 Örnek: $U_8=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$ ve $U_9=\{\bar{1},\bar{2},\bar{4},\bar{5},\bar{7},\bar{8}\}$ dir.

3.1.6 Sonuç: $|U_n| = \varphi(n)$ dir. Yani $\mathbb{Z}_n$ halkasında birimlerin sayısı n ile aralarında asal ve n den küçük olan sayıların sayısı kadardır [1].

3.2 İkinci Dereceden Denklikler

İkinci derece kongrüansların çözümünde de köklerin bulunması, ikinci dereceden denklem çözümlerinde olduğu gibi önemlidir. a, b, c $\in \mathbb{R}$ veya $\mathbb{C}$ olmak üzere $ax^2+bx+c=0$ denkleminin köklerini veren $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ bağıntısını ele alalım. Bunu katsayıların $\mathbb{Z}_n$ halkasından alınması durumuna uygularsak $\overline{2a}$ ile bölünmeyi garantilememiz gerekir. Bu durumda $\overline{2a}$, n modunda bir birim olmalıdır.

O zaman $1/\overline{2a} \in \mathbb{Z}_n$ olur.Şimdi n tek ve $\bar{a} \in U_n$ olsun. O halde $\overline{4a} \in U_n$ olduğundan, $ax^2+bx+c=0$ denkleminin her iki tarafı 4a ile çarpılırsa $4a^2x^2+4abx+4ac\equiv 0$ (n) elde edilir. Böylece $(2ax+b)^2=b^2-4ac$ olur. O halde b^2-4ac sayısının $\mathbb{Z}_n$ halkasındaki tüm kare köklerini bulabilirsek, 2ax+b=s veya denk olarak x= $\frac{-b+s}{2a}$ olacak şekildeki tüm $\mathbb{Z}_n$ çözümlerini de bulabiliriz. Dikkat edilirse, $\mathbb{Z}_{15}$ halkasının $\bar{1}$ ve $\bar{4}$ elemanlarının herbirinin dörder tane karekökü vardır. 1 in karekökleri ±1 ve ±4 ve $\bar{4}$ nin kareköklerinin ± 2 ve ± 7 olduğu görülür.

3.3 İkinci Dereceden Kalanlar Grubu

3.3.1 Tanım: $\bar{a}=\bar{s}^2$ olacak şekilde bir $\left(\frac{g^i}{p}\right)=(-1)^i$ varsa $\bar{a}$ elemanına n modunda ikinci dereceden kalan denir. n modunda ikinci dereceden kalanların kümesi $\mathbb{Q}_n$ ile gösterilir [1].

3.3.2 Yardımcı Teorem: k, n sayısını bölen farklı asalların sayısı olsun. $\bar{a} \in \varphi_n$ ise $\bar{t}^2=\bar{a}$ olacak şekildeki $\bar{t} \in U_n$ elemanlarının sayısı

$$N=\begin{cases} 2^{k+1} & ,n\equiv 0(8) \\ 2^{k-1} & ,n\equiv 2(4) \\ 2^k & ,\text{aksi halde} \end{cases}$$ dir [3].

3.3.3 Teorem: $|\mathbb{Q}_n| = \varphi_n / N$ dir [3].

3.4 Legendre Sembolü

Bu bölümde verilen bir $\bar{a} \in U_n$ biriminin ikinci dereceden bir kalan olup olmadığını belirleyeceğiz. Modun asal olması durumu kolaydır. n =2 ise $\mathbb{Q}_2 = \{1\}$ dir ve ikinci dereceden bir kalandır. O halde n=p nin tek asal olması durumunu inceleyelim:

3.4.1 Tanım: p tek asal sayısı için bir a tam sayısının Legendre sembolü

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p|a \\ 1 & a \in \mathbb{Q}_p \\ -1 & a \notin \mathbb{Q}_p \end{cases}$$ olarak tanımlanır [10].

3.4.2 Tanım: U_n 'in bir g elemanının mertebesi $\varphi(n)$ ise g ye n modunda bir ilkel kök denir [1].

3.4.3 Teorem: n>2 olsun. U_n'de ilkel kök olması için gerek ve yeter şart n nin asal olmasıdır [1].

3.4.4 Sonuç: p tek asal ve g, p modunda bir ilkel kök ise , $\left(\frac{g^i}{p}\right) = (-1)^i$

dir [3].

3.4.5 Teorem: p tek asal ise her a, b tamsayı çifti için $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

dir [10].

3.4.6 Örnek: p=13 olsun $\left(\frac{1}{13}\right) = +1$ dir. Çünkü $\bar{1} = \bar{1}^2$ dir.O halde her $\bar{a} \in U_p$ için $\left(\frac{a}{13}\right) = \left(\frac{-a}{13}\right)$, yani $a \in \varphi_{13} \Leftrightarrow -a \in \varphi_{13}$ dir [1].

3.4.7 Uyarı: Yukarıda bir sayının Legendre sembolünü hesaplamak istediğimizde işareti önemsemeyebiliriz. Genelde ise $\left(\frac{-a}{p}\right)$ ile -$\left(\frac{a}{p}\right)$ farklı olabilir.

Örneğin , $\left(-\frac{1}{13}\right)$ =+1, -$\left(-\frac{1}{13}\right)$=-1 dir [1].

3.4.8 Sonuç: $a_1, a_2, a_3, \ldots, a_k \in \mathbb{Z}$ için

$\left(\frac{a_1a_2a_3\ldots a_k}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\left(\frac{a_3}{p}\right)\ldots\left(\frac{a_k}{p}\right)$ dir [3].

3.4.9 Teorem: $a \equiv b$ (p) olması için gerek ve yeter şart $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ olmasıdır [10].

3.4.10 Teorem (Euler Kriteri): p tek asal ise her $a \in \mathbb{Z}$ için $\left(\frac{a}{p}\right)=a^{(p-1)/2}$ (p) dir [10].

3.4.11 Sonuç: p tek asal olsun.$-1 \in \varphi_p$ olması için gerek ve yeter şart $p \equiv 1$ olmasıdır [1].

3.4.12 Sonuç: $p \equiv 1(4)$ olacak şekilde sonsuz çoklukta asal sayı vardır [1].

3.4.13 Teorem: p modundaki kuadratik rezidülerin sayısı kuadrik rezidü olmayanların sayısına eşittir [1].

3.4.14 Sonuç: p tek asal ise $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$ dir [10].

3.5 Kuadratik İndirgeme Kuralı

Bir a tamsayısının bir p modunda kuadratik rezidü olup olmadığını belirleyebilmek için $\left(\frac{a}{p}\right)$ sayısını hesaplamak yerine yukarıdaki sonuçlar gereği sadece üç özel durumu incelemek yeterli olacaktır.

3.5.1 Teorem (Gauss'un kuadratik indirgeme kuralı):

p ve q farklı tek asal sayılar ise $(-1)^{(p-1)(q-1)/4} = \begin{cases} -\left(\frac{q}{p}\right) & p \equiv q \equiv 3(4) \\ \left(\frac{p}{q}\right) & \text{aksi halde} \end{cases}$

dir. Uygulamada genellikle, yukarıdaki ifadeye denk olan $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$ eşitliği kullanılır [10].

3.5.2 Örnek: 219, 383 modunda bir ikinci dereceden kalan mıdır? Burada 383 asaldır, ancak 219=3.73 olduğundan $\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right).\left(\frac{73}{383}\right)$ yazılabilir [1].

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right).(-1)^{382.2/4}$$

$$= (-1).\left(\frac{2}{3}\right) = +1 \text{ bulunur ve}$$

$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right).(-1)^{382.72/4}$$

$$= (+1).\left(\frac{383}{73}\right) = \left(\frac{18}{73}\right)$$

$$= \left(\frac{2}{73}\right).\left(\frac{3}{73}\right)^2$$

= +1 bulunur. Böylece $\left(\frac{219}{383}\right) = +1$ dir. Yani 219, 383 modunda bir ikinci dereceden kalandır.

4. KÜBİK REZİDÜLER

Bu bölümde $x^3 \equiv a(p)$ denkliğinin çözülebilme koşullarını inceleyeceğiz. Bunun için, birimin 3.dereceden köklerinden biri (yani $x^3 = 1$ denkleminin çözümlerinden biri) olan $\omega = \frac{-1+\sqrt{-3}}{2}$ kullanılacaktır.

4.1 Giriş

4.1.1 Tanım: $\omega = \frac{-1+\sqrt{-3}}{2}$ olmak üzere $\mathbb{Z} = a + b\omega$ sayılarına "Eiseinstein sayıları"denir. $\mathbb{Z}[\omega] = \{a+b\omega \mid a,b \in Z\}$ halkası genellikle D ile gösterilir [1].

4.1.2 Tanım: $\alpha = a+b\omega$ sayısının normu $\alpha.\bar{\alpha}$ şeklinde tanımlanır ve $N\alpha$ ile gösterilir [1].

4.1.3 Teorem: $\alpha = a+b\omega$'nin normu $N\alpha = a^2-ab+b^2$ şeklindedir [1].

İspat: $N\alpha = \alpha.\bar{\alpha}$ olduğu için

$$N\alpha = (a+b\omega)\overline{(a+b\omega)}$$

$$= (a+b\omega)(a+b\bar{\omega})$$

$$= a^2+ab\bar{\omega}+ab\omega+b^2\omega\bar{\omega}$$

$$= a^2+ab(\omega+\bar{\omega})+b^2.1$$

$$= a^2+ab(2\mathrm{Re}\,\omega)+b^2$$

$$= a^2+(2.-\frac{1}{2})+b^2$$

$=a^2-ab+b^2$ bulunur.

4.1.4 Teorem: $\alpha \in D$ 'nin birim olması için gerek ve yeter şart $N\alpha = 1$ olmasıdır. D deki birimler: $\pm 1, \pm\omega, \pm\omega^2$ dir [1].

4.1.5 Tanım: $u \in D$ birim olmak üzere $\alpha = ß.u$ olacak biçimdeki α ve ß sayılarına denktir denir ve $\alpha \sim ß$ ile gösterilir [1].

4.1.6 Teorem: $p \equiv 1$ (3) asal olsun $\omega = \frac{-1+\sqrt{-3}}{2}$ sayısı $\mathbb{Z}_p$'nin bir elemanıdır [1].

İspat: $\sqrt{-3} \in \mathbb{Z}_p$ olduğunu gösterelim.Yani $-3 \equiv k^2(p)$ olacak biçimde bir k tamsayısının varlığını gösterelim. $\left(\frac{-3}{p}\right)=1$ olduğunu göstermemiz gerekir.

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{3}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{p}{3}\right).(-1)^{(p-1).2/4}$$

$$=(-1)^{(p-1)/2}\cdot\left(\frac{p}{3}\right)\cdot(-1)^{(p-1)/2}=(-1)^{p-1}\cdot\left(\frac{p}{3}\right)=1 \text{ bulunur.}$$

p asal olduğu için p-1 çifttir ve $p \equiv 1$ (3) olduğu için $\left(\frac{p}{3}\right)=1$dir.Ayrıca (2,p) =1 ise 2 nin mod p de çarpmaya göre bir t tersi vardır.Öyle ise $\sqrt{-3} \in \mathbb{Z}_p$ olduğu için $-1+\sqrt{-3} \in Zp$ olur.O zaman $\frac{1}{2}(-1+\sqrt{-3})$ yapabiliriz. $\sqrt{-3} \in Zp$ ise $1+\sqrt{-3} \in \mathbb{Z}_p$ olur. $\frac{-1+\sqrt{-3}}{2} \equiv t\,(-1+\sqrt{-3}) \in Z_p$ olur.

4.1.7 Sonuç: $p \equiv 1$ (3) asal iken $\omega^2 \in \mathbb{Z}_p$ dir [5].

4.1.8 Örnek: 13 modunda, $\omega=\frac{-1+\sqrt{-3}}{2}=\frac{5}{2}\equiv\frac{18}{2}\equiv 9 \in \mathbb{Z}_{13}$ ve $\omega^2=-1-9=-10\equiv 3 \in \mathbb{Z}_{13}$ elde edilir.

4.1.9 Tanım: $\pi=a+b\omega \in D$ olsun. $c+d\omega$, $e+f\omega$ birimden farklı olmak üzere $\pi=(c+d\omega)(e+f\omega)$ olacak şekilde c, d, e, f tam sayıları bulunamıyorsa π'ye D'de asaldır denir. Aksi halde D'de bileşik sayı denir [1].

4.1.10 Teorem: p rasyonel asal ise $Np=p.p=p^2$ dir [1].

4.1.11 Teorem: p rasyonel asalı D de asal değilse, birimden farklı tam iki çarpanı vardır, üstelik bu çarpanlardan her birinin normu p dir [1].

İspat: p rasyonel asalı D de asal değilse en az iki çarpanı vardır. Bu çarpanlara $a_1, a_2, \ldots, a_n$ denirse, $p=a_1, a_2, \ldots, a_n$ olduğunda $Np= N(a_1, a_2, \ldots, a_n)$ ve $Np=p^2$ olduğu hatırlanırsa $p^2=Na_1 Na_2 \ldots Na_n$ bulunur.Bu durumda yukarıda elde edilen sayılardan sayılardan sadece biri p^2 olup diğerleri 1 e eşit olur veya ikisi p ye eşit olup diğerleri 1'e eşit olur. İlk durumda normu 1 olmayan(yani birimden farklı) bir çarpan olduğundan p nin asal olduğu çıkar ki, bu bir çelişkidir.O halde iki çarpan olmalıdır.Bu çarpanların normu p dir.

4.1.12 Teorem: $p\equiv 1\ (3)$ rasyonel asal ise p, D de asal değildir [1].

4.1.13 Teorem: p rasyonel asal olsun.p'nin D'de asal olması için gerek ve yeter şart $p\equiv 2\ (3)$ olmasıdır [1].

4.1.14 Teorem: Normu 3 olan tüm π sayıları D'de asaldır [1].

4.1.15 Teorem: D'de normu $N\pi \equiv 2\ (3)$ olan hiçbir π asalı yoktur [1].

4.1.16 Teorem: k>1 olsun.D'de normu 3k olan hiçbir asal yoktur [1].

İspat: $\pi=a+b\omega$ 'nın normu 3 modunda 0'a denk ise üç ihtimal vardır.

1) $a\equiv 0, b\equiv 0\ (3)$
2) $a\equiv 2, b\equiv 1\ (3)$
3) $a\equiv 1, b\equiv 0\ (3)$

1. $a\equiv 0, b\equiv 0\ (3)$ ise π 3 ün katı olacağından asal değildir.

2. $a\equiv 2, b\equiv 1 (3)$ ise $k,t \epsilon Z$ olmak üzere $a=3k+2$, $b=3t+1$

$N\pi = a^2-ab+b^2$ olduğu için

$N\pi = 9k^2+6k+4+9t^2+6t+1 -9kt-3k-6t-2$

$=9k^2 + 9t^2-9kt+9k+3$

$=3(3k^2+3t^2-3kt+3k+1)$ olur.

D'de normu 3 olan asalların varlığını biliyoruz. Şimdi de normu $3k^2+3t^2-3kt+3k+1$ olan bir elemanın varlığını göstermeliyiz. D'de a^2 biçimindeki elemanların 6 modunda 1'e denk olduğunu biliyoruz. Bu durumda $3(k^2+t^2-kt+k)+1$ ifadesinde k^2+t^2-kt+k nın çift sayı olduğunu göstermeliyiz. Bu şekilde $a+b\omega$ 'nın iki elemanın çarpımı şeklinde yazılabildiğini, yani asal olmadığını göstermiş olacağız.

k, t tek olduğunda $k^2 +t^2-kt+k$ çift olur.

k, t çift olduğunda k^2+t^2-kt+k çift olur.

k tek, t çift olduğunda $k^2 +t^2-kt+k$ çift olur.

k çift, t tek olduğunda $a=3k+2$ çift ve $b=3t+1$ çift olur. $2|\pi$ olur, ki bu durumda π asal olamaz.

3. $a\equiv 1$, $b\equiv 2 (3)$ içinde benzer şekilde gösterilebilir.O halde D de normu 3 ün katı olan hiçbir sayı yoktur.

4.1.17 Teorem: p rasyonel asal ise $N\pi = p\equiv 1$ (3) özelliğindeki $\pi \in D$ ler D'de asaldır [1].

4.1.18 Uyarı: Böylece D'de üç tip asal olduğu görülür [1].

1) $p\equiv 1(3)$ rasyonel asal olmak üzere, $N\pi = p$ olan tüm $\pi = a+b\omega \in D$ sayıları
2) $\pi = q\equiv 2$ (3) tipindeki tüm rasyonel asallar
3) $\pi = 1-\omega$ 'nın , D'deki tüm denkleri asaldır.

4.1.19 Tanım: 1) 1 ve 2 deki asallara 1.tip asallar denir.

2) 1 deki asallardan 1.tip olmayanlar

$a\equiv 1$ (3), $b\equiv 0$ (3)

$a\equiv 1$ (3), $b\equiv 1$ (3)

$a\equiv 0$ (3), $b\equiv 1$ (3)

$a \equiv 2\ (3),\ b \equiv 2\ (3)$

$a \equiv 0\ (3),\ b \equiv 2\ (3)$ tür. Bunlara da 2.tip asallar denir.

3)1-ω 'nin denklerine de 3.tip asallar denir [1].

Örneğin;2,5,11,17 gibi rasyonel asallar da D de 1.Tip asallardır.Normu 7 olan 1+3ω,normu 13 olan 3+4ω ve normu 19 olan 2+5ω 2.tip asallardır.3.Tip asallar toplam 6 tanedir ve bunlar 1-ω,-1+ω,1+2ω,-1-2ω,2+ω,2-ω dır.

4.1.20 Teorem: π, D de asal ise p rasyonel asal olmak üzere $N\pi = p$ ve $N\pi = p^2$ dir [1].

4.1.21 Teorem: p rasyonel asal ise $\pi \in D$ olmak üzere $N\pi = p$ ise π, D'de asaldır. Yani normu asal olan her eleman D'de asaldır [1].

İspat: π'nin D de asal olmadığını varsayalım. O halde $N\alpha > 1, N\beta > 1$ ise $\pi = \alpha\beta$ yazabiliriz. $p = N\pi = N\alpha\ N\beta$ 'dır. Ancak p, $\mathbb{Z}$ 'de asal olduğundan çarpanlarından birinin 1 olması gerekir. Bu çelişkiden dolayı p, D'de asaldır.Bu teoremin tersi doğru değildir.Örneğin;a=0,b≡2(3) şeklindeki $\pi = a+b\omega$ elemanları D'de 2. Tip asallar olup $N\pi = b^2$ bir rasyonel asal değildir.Yani D de normu asal olmayan asallar da vardır.

4.1.22 Teorem: π, D'de asal ise denkleri de D de asaldır ve $N\pi = p$ ise denklerinin normları da p ye eşittir [1].

4.1.23 Teorem: p≡1 (3) rasyonel asal olsun. Eğer p-1=6k=n(n+1) ise $\pi = n+(n+1)\omega$ ve $\lambda = 1+(n+1)\omega$'nin denkleri D'de asaldır [1].

4.1.24 Örnek: p≡13≡1 (6) olsun.p-1≡12=3.4 olduğundan $\pi = 3+4\omega$, $\lambda = 1+4\omega$ ve denkleri asaldır.

4.2 Kübik Rezidü Karakteri

4.2.1 Tanım: π, D'de asal ve $\pi \nmid 1-\omega$ ise (yani $N\omega \neq 3$) α'nın mod π deki kübik karakteri $\left(\frac{\alpha}{\pi}\right)_3$ ile gösterilir ve

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & \pi, \alpha \text{ yı bölüyor ise} \\ \alpha^{(N\pi-1)/3} & \pi, \alpha \text{ yı bölmüyor ise} \end{cases}$$

şeklinde tanımlanır.Burada $\alpha^{(N\pi-1)/3}$, π modunda $1, \omega$ veya ω^2'ye denktir.Bu karakter, Legendre sembolünün kuadratik rezidü teorisindeki yerini tutar. $\left(\frac{\alpha}{\pi}\right)_3$ gösterimi yerine bazen $\chi_\pi(\alpha)$ sembolü de kullanılır [1].

4.2.2 Tanım: $\left(\frac{\alpha}{\pi}\right)_3 = 1$ ise α ya π modunda bir kübik rezidü, aksi halde kübik rezidü olmayan (non-rezidü) denir. $p \equiv 1 \pmod 3$ iken $\frac{p+1}{3}$ tane birbirinden farklı kübik rezidü ve $\frac{2p-1}{3}$ tane kübik rezidü olmayan, $q \equiv 2 \pmod 3$ iken tam q tane birbirinden farklı kübik rezidü vardır [9] .

4.2.3 Sonuç: İki kübik rezidünün ve farklı türdeki kübik rezidü olmayan (ω, ω^2) iki elemanın çarpımı bir kübik rezidüdür.Ayrıca bir kübik rezidü ile bir kübik rezidü olmayanın (ω veya ω^2) çarpımı ve aynı tipteki iki kübik rezidü olmayanın (ω ve ω, ω^2 ve ω^2) çarpımı bir kübik rezidü olmayandır [1].

4.2.4 Teorem: π, D'de asal ve $N\pi = p$ olsun. $x^3 \equiv a \pmod p$ çözülebilirdir [1].

İspat : $p = \pi\bar{\pi}$ oluşundan görülür.

4.2.5 Örnek: $\left(\frac{2+4\omega}{3+4\omega}\right)_3 = ?$

$N(2+4\omega)=4-8+16=12$, $N(3+4\omega)=9-12+16=13$ olduğundan

$\left(\frac{2+4\omega}{3+4\omega}\right)_3 \equiv 12^{\frac{13-1}{3}}\ (13) \equiv 12^4 (13) \equiv (-1)^4\ (13) \equiv 1\ (13)$ elde edilir. O halde $2+4\omega$, $3+4\omega$ modunda bir kübik rezidü dür.

4.2.6 Örnek: $\alpha = 5+8\omega$ ve $\pi = 1+3\omega$ alınırsa, $N\alpha$ =25-40+64=49 ve $N\pi = 1-3+9 = 7$ bulunur. $7 \mid 49$ olduğu için $\left(\frac{\alpha}{\pi}\right)_3$ =0 dır [1]. Gerçekten;

$$\left(\frac{5+8\omega}{1+3\omega}\right) = 49^{\frac{7-1}{3}}\ (7)$$

$$\equiv 49^2\ (7)$$

$$\equiv 0^2\ (7)$$

$\equiv 0\ (7)$ elde edilir .

4.2.7 Önerme: $x^3 \equiv \alpha(\pi)$ çözülebilir ise yani α bir kübik rezidü ise

a) $\alpha^{(N\pi-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \quad (\pi)$

b) $\left(\frac{\alpha.\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 . \left(\frac{\beta}{\pi}\right)_3$

c) $\alpha \equiv \beta$ ise $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$ dir [1].

İspat: a)Tanımdan açıkça görülür.

b) $(\alpha\beta/\pi) \equiv (\alpha\beta)^{\frac{N\pi-1}{3}} \equiv \alpha^{(N\pi-1)/3}\beta^{(N\pi-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 . \left(\frac{\beta}{\pi}\right)_3$ sonucu bulunur.

c) $\alpha \equiv \beta(\pi)$ ise $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{(N\pi-1)/3} \equiv \beta^{(N\pi-1)/3} \equiv \left(\frac{\beta}{\pi}\right)_3$ olur.Buradan $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$ elde edilir.

4.2.8 Teorem: π, D'de asal ve $N\pi \neq 3$ olsun.O zaman $\left(\frac{-1}{\pi}\right)_3 = 1$ dir [1].

İspat: π asal ise, $p \equiv 1(3)$ rasyonel asal olmak üzere $N\pi = p$ dir.$p \equiv 1\ (3)$ ise

$k \in Z$ olmak üzere p=3k+1 dir ve p asal olduğundan k çift sayıdır. O zaman $\left(\frac{-1}{\pi}\right)_3 = (-1)^{(N\pi-1)/3}$ olduğu için, $N\pi-1$ =p-1=3k+1-1=3k olduğundan $\left(\frac{-1}{\pi}\right)_3 = (-1)^{3k/3} = (-1)^k$ olur ,k çift sayı olduğu için $\left(\frac{-1}{\pi}\right)_3 = 1$ olur. Eğer $q \equiv 2$ (3) ve asal olduğundan q tek sayı olur.O halde Nq-1 çift sayıdır. Yani $\frac{Nq-1}{3}$ bir çift sayıdır.O halde $\left(\frac{-1}{q}\right)_3 = (-1)^{(Nq-1)/3} = 1$ olur.

4.2.9 Uyarı: -1 in her π modundaki kübik karakterinin 1 olacağı, $(-1)^3 = -1$ den görülür [1].

4.2.10 Teorem: π_1, π_2 1.tip asal, $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$ ve $N\pi_1 \neq N\pi_2$ olsun Bu durumda $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$ olur [1].

4.2.11 Teorem: π 1.tip asal ise $\chi_\pi(2) = 1$, buradan $\pi = q > 2$ olur.1.tip rasyonel asal olmak üzere 2 her q modunda bir kübik rezidü olur [1].

4.2.12 Teorem: $\pi = a + b\omega$, 1.tip kompleks asal iken $x^3 \equiv 2(\pi)$ 'nin çözülebilmesi için gerek ve yeter şart $\pi \equiv 1(2)$ olmasıdır.Bu ise $b \equiv 0(2)$ olması anlamına gelir [1].

İspat: $\pi \equiv 1 + 0\omega(2)$ çözülebilir olsun, bu durumda $\chi_\pi(2) = 1$ dir.2 ve π 1.tip asal olduğu için kübik indirgeme kuralından $\chi_\pi(2) = \chi_2(\pi)$ yazılabilir. Buradan $\chi_2(\pi) \equiv \pi^{(N(2)-1)/3}(2)$, $N(2) = 2^2 = 4$ olduğundan $\chi_2(\pi) \equiv \pi(2)$ dir.Dolayısıyla $\chi_2(\pi) = 1$ olması için $\chi_2(\pi) \equiv \pi \equiv 1(2)$ olması gerekir.Tersi de benzer olarak gösterilir.

4.2.13 Teorem: $x^3 \equiv 2(5+6\omega)$ denkliği çözülebilir midir? $\pi = (5+6\omega)$, $\pi \equiv 2(3)$ olduğu için 1.Tip asaldır . Ayrıca $\pi \equiv 1(2)$ olduğu için $\left(\frac{2}{5+6\omega}\right)_3 = 1$ ve bu durumda $x^3 \equiv 2(5+6\omega)$ denkliği çözülebilirdir [1].

$\left(\frac{2}{5+6\omega}\right)_3 = \left(\frac{5+6\omega}{2}\right)_3 = (5+6\omega)^{\frac{N(2)-1}{3}} = 5+6\omega(2) \equiv 1+0\omega(2) \equiv 1(2)$ bulunur.

4.2.14 Sonuç: $p \equiv 2(\mathrm{mod}\,3)$ asal ise p modunda birbirinden farklı tam p tane üçüncü dereceden kalan vardır. Yani $\mathbb{Z}_p$'nin tüm elemanları üçüncü dereceden bir kalandır [11].

4.2.15 Tanım: $x^3 \equiv a(p)$ olacak şekilde bir $x \in \mathbb{Z}$ varsa $a \in \mathbb{Z}$ ye p modunda bir kübik rezidü denir [11].

4.2.16 Teorem: p rasyonel asal ve $p \equiv 1(3)$ olsun. $x^3 \equiv a(p)$ denkliğinin çözülebilmesi için gerek ve yeter şart $a^{(p-1)/3} \equiv 1(p)$ olmasıdır [5].

İspat: Euler kıriterinin k=3 için özel halidir.

4.2.17 Teorem: p rasyonel asal ve $a \in \mathbb{Z}$ olmak üzere $\left(\frac{a^3}{p}\right)_3 = 1$ dir [1].

İspat: $\left(\frac{a^3}{p}\right)_3 = \left(\frac{a}{b}\right)_3^3$ yazılabilir $\left(\frac{a}{p}\right)_3$ 1, ω ya da ω^2 ye eşit olacağından $\left(\frac{a^3}{p}\right)_3 = \left(\frac{a}{b}\right)_3^3 = 1$ olur.

4.2.18 Örnek: $x^3 \equiv 2(7)$ çözülebilir midir?

$\left(\frac{2}{7}\right)_3 = 2^{\frac{7-1}{3}} = 2^2 = 4(7)$, $\omega \equiv 4(7)$ olduğu için $\left(\frac{2}{7}\right)_3 = \omega$ 'dir.

Bu durumda $x^3 \equiv 2(7)$ çözülebilir değildir [5].

4.2.19 Örnek: $x^3 \equiv 1(7)$ çözülebilir midir?

$\left(\frac{1}{7}\right)_3 = 1^{\frac{7-1}{3}} = 1^2 = 1(7)$ olduğu için çözülebilirdir. $x^3 \equiv 1(7)$ 'nin kökleri ise $x = 1, \quad x = \omega, \quad x = \omega^2$ dir. $\omega = \frac{-1+\sqrt{-3}}{2} \equiv 4(\mathrm{mod}\,7)$ ve $\omega^2 \equiv 2(\mathrm{mod}\,7)$ olduğu için bu denkliğin kökleri $x \equiv 1(\mathrm{mod}\,7)$, $x \equiv 4(\mathrm{mod}\,7), x \equiv 2(\mathrm{mod}\,7)$ dir.

4.2.20 Teorem: $q \equiv 2(3)$ asal ve a, (a,q)=1 olacak şekilde pozitif bir tam sayı ise a mod q da bir kübik rezidüdür [1].

İspat: $q \equiv 2(3)$ asal ve (a,q)=1 olacak şekilde $a \in \mathbb{Z}^+$ olsun. $q \equiv 2(3)$ ise q=3k+2($k \in \mathbb{Z}$)olur. Bu durumda; $Nq = q.\bar{q} = (3k+2)(3k+2) = 9k^2 + 12k + 4$ ve $\frac{Nq-1}{3} = 3k^2 + 4k + 1$ dir. $(a,q) = 1$ olmak üzere $a^{(Nq-1)/3} = a^{3k^2+4k+1}$ dir.Fermat'ın Küçük teoreminden $\left(a^{3k+1}\right)^{k+1} \equiv 1^{k+1} \equiv 1(q)$ olduğu için, $a^{q-1} = a^{3k+2-1} = a^{3k+1} \equiv 1(q)$ olur. $a^{(Nq-1)/3} = a^{3k^2+4k+1} = a^{(3k+1)(k+1)} = \left(a^{3k+1}\right)^{k+1} \equiv 1^{k+1} \equiv 1(q)$ olur.

4.2.21 Sonuç: $p \equiv 2(\mathrm{mod}\,3)$ asal ise p modunda birbirinden farklı tam p tane üçüncü dereceden kalan vardır. Yani $\mathbb{Z}_p$'nin tüm elemanları üçüncü dereceden bir kalandır [1].

4.2.22 Örnek: p=17 olsun, mod17 de

$0^3 \equiv 0, \quad 1^3 \equiv 1, \quad 2^3 \equiv 8, \quad 3^3 \equiv 10, \quad 4^3 \equiv 13, 5^3 \equiv 6, \quad 6^3 \equiv 12, \quad 7^3 \equiv 3, \quad 8^3 \equiv 2, \quad 9^3 \equiv 15,$
$10^3 \equiv 14, \quad 11^3 \equiv 5, \quad 12^3 \equiv 11, \quad 13^3 \equiv 4, \quad 14^3 \equiv 7, 15^3 \equiv 9, \quad 16^3 \equiv 16$ 'dır [1].

4.2.23 Teorem: $p \equiv 1(\mathrm{mod}\,3)$ asal ise p modundaki farklı kübik rezidülerin sayısı $\frac{p+2}{3}$ dir [5].

5. KUARTİK REZİDÜLER

4.dereceden kalanlar teoremi Gauss tarafından 1832'de ispatsız olarak verilmiştir. Daha sonra1844'de Eisenstein, Jacobi ve Gauss toplamlarını kullanarak pek çok ispat yaptı.3.Dereceden kalanlar ile benzer olmasına rağmen daha zordur. İlk olarak Gauss,2.Dereceden kalanlar teoreminin altıncı ispatında Gauss toplamlarını kullanmıştır.(Ireland ve Rosen 1990). $\mathbb{Z}[i]$ de bölme algoritması geçerli oldugundan $\mathbb{Z}[i]$ bir Öklit halkasıdır.

5.1 $\mathbb{Z}[i]$ Halkasının Özellikleri

5.1.1 Tanım: Herhangi $a,b \in \mathbb{Z}$ ve $i = \sqrt{-1}$ olmak üzere a+bi biçimindeki bütün sayılara Gauss Tamsayıları denir.Bu tür sayıların kümesi $\mathbb{Z}[i]$ ile gösterilir.Yani, $i = \sqrt{-1}$ olmak üzere, $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$ dir [6].

5.1.2 Tanım: $a,b \in \mathbb{Z}$ olmak üzere $\alpha = a+bi \in \mathbb{Z}[i]$ sayısının eşleniği a-bi şeklinde tanımlanır ve $\overline{\alpha}$ şeklinde gösterilir. Bir $\alpha = a+bi \in \mathbb{Z}[i]$ sayısının normu ise $N(a+bi) = \alpha.\overline{\alpha} = a^2+b^2 \in \mathbb{Z}$ dir [6] .

5.1.3 Önerme: Norm fonksiyonu aşağıdaki özelliklere sahiptir [6]:

1) $\forall \alpha \in \mathbb{Z}[i]$ için $N(\alpha) \geq 0$
2) $N(\alpha) = 0 \Leftrightarrow \alpha = 0$
3) $\forall \alpha,\beta \in \mathbb{Z}[i]$ için $N(\alpha.\beta) = N(\alpha).N(\beta)$ dır.
4) $\alpha = a+bi \in \mathbb{Z}[i]$, $\beta = c+di (a,b,c,d \in \mathbb{Z})$ olmak üzere
   a) $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$
   b) $\overline{(\alpha+\beta)} = \overline{\alpha}+\overline{\beta}$ dır.

5.1.4 Tanım: $\forall \alpha \in \mathbb{Z}[i]$ için $u|\alpha$ olacak şekilde bir u tamsayısı varsa bu α sayısına $\mathbb{Z}[i]$ 'nin bir tersinir elemanı denir [6] .

5.1.5 Önerme: $\forall \alpha \in \mathbb{Z}[i]$ 'nin tersinir olması için gerek ve yeter şart $N(\alpha)=1$ olmasıdır. Bu durumda tersinir elemanlar $\mp 1, \mp i$ dir [7].

İspat: $\forall \alpha \in \mathbb{Z}[i]$ tersinir $\Leftrightarrow \frac{1}{\alpha} \in \mathbb{Z}[i]$ demektir.

$1=\alpha.\frac{1}{\alpha}$ ise $N(1)=N\left(\frac{1}{\alpha}\right)$ ve $N(\alpha)\in\mathbb{Z}$, $N(\alpha)\geq 0$ olduğundan eğer α tersinir eleman ise $N(\alpha)=1$ olmalıdır.

Tersine olarak $\alpha = a+bi \in \mathbb{Z}[i]$ için $N(\alpha)=1=\alpha.\bar{\alpha}$ ise $\frac{1}{\alpha}=\bar{\alpha}=a-bi\in\mathbb{Z}[i]$ bulunur. $N(\alpha)=a^2+b^2=1$ olması için gerek ve yeter şart $a=\pm 1$ ve $b=0$ veya $b=\pm 1$ ve $a=0$ olmasıdır. Böylece tersinir elemanların $\mp 1, \mp i$ olduğu anlaşılır.

5.1.6 Tanım: u, $\mathbb{Z}[i]$ 'nin herhangi bir tersinir elemanı olmak üzere, herhangi $\alpha,\beta\in\mathbb{Z}[i]$ için $\alpha = u.\beta$ olacak şekildeki α ve β sayılarına denktir, denir ve $\alpha \approx \beta$ ile gösterilir [6].

5.1.7 Tanım: $\alpha \in \mathbb{Z}[i]$ elemanına eğer α nın $\mathbb{Z}[i]$ deki her böleni ya kendisinin bir tersinir eleman ise indirgenemez denir [6].

5.1.8 Uyarı: Bu bölümde 3.bölümde olduğu gibi rasyonel $\mathbb{Z}$'de ki asallara rasyonel asal diyeceğiz [6] .

5.1.9 Teorem ($\mathbb{Z}[i]$de kalanlı bölme teoremi): $\forall \alpha,\beta\in\mathbb{Z}[i]$ ve $\beta\neq 0$ için, $\alpha=\beta\gamma+\delta$ olacak şekilde $\exists\gamma,\delta\in\mathbb{Z}[i]$ ve $N(\alpha)<N(\beta)$ dır [6].

5.1.10 Yardımcı Teorem: π indirgenemez ise, $\pi \mid p$ olacak şekilde $p \in \mathbb{Z}$ rasyonel asalı vardır [8].

İspat: $p_i \in \mathbb{Z}$ asal olmak üzere, $N(\pi) = \pi.\bar{\pi} = n = p_1 p_2 ... p_s$ olduğundan, en az bir i için $\pi \mid p_i$ sağlanır.

5.1.11 Teorem: $\alpha \in \mathbb{Z}[i]$ ve $N(\alpha)$ asal ise α indirgenemezdir [6] .

İspat: Eğer $\alpha = \mu\lambda$ ise $N(\alpha) = N(\mu)N(\lambda)$ dir. $N(\alpha)$ asal olduğundan $N(\mu) = 1$ veya $N(\lambda) = 1$ dir. Böylece μ ya da λ tersinirdir. Böylece α indirgenemezdir.

5.1.12 Teorem: 1+i indirgenemezdir ve $2 = -1(1+i)^2$, 2'nin $\mathbb{Z}[i]$'de asal çarpanlarına ayrılmış şeklidir [6].

İspat: $N(1+i) = 2$ dir ve 2 asaldır o halde 1+i indirgenemezdir.

5.1.13 Teorem: Eğer $q \equiv 3 (\mathrm{mod}\, 4)$, $\mathbb{Z}$ 'de bir asal ise, q, $\mathbb{Z}[i]$ 'nin bir indirgenemez elemanıdır [6].

5.1.14 Teorem: Eğer p bir asal ve $p \equiv 1 (\mathrm{mod}\, 4)$ ise, $p = \pi\bar{\pi}$ olacak şekilde bir π indiregenemez elemanı vardır ve $(\pi) \neq (\bar{\pi})$ dir [6].

İspat: $p \equiv 1 \pmod 4$ olduğundan, $a^2 \equiv -1 (\mathrm{mod}\, p)$ olacak şekilde bir a tam sayısı vardır. Böylece $p \mid a^2 + 1 = (a+i)(a-i)$ olur.Eğer p indirgenemez olsaydı, $p \mid a+1$ olurdu.

Böylece $p=\alpha\beta, N(\alpha)>1, N(\beta)>1$ dir.Norm alarak $p=N(\alpha)$ sonucuna varırız. $N(\alpha)$ asal olduğundan α indirgenemezdir. Buradan $(\alpha)\neq(\overline{\alpha})$ olduğu açıktır.

5.1.15 Tanım: Tersinir olmayan bir $\alpha\in\mathbb{Z}[i]$ için, eğer $\alpha\equiv 1\left(\mathrm{mod}(1+i)^3\right)$ ise α ya $\mathbb{Z}[i]$ 'nin birinci tip elemanı denir. Eğer α, $\mathbb{Z}[i]$ 'de birinci tip ise, $\alpha\equiv 1(\mathrm{mod}\,2+2i)$ olduğuna dikkat çekilmelidir [6] .

5.1.16 Teorem: $\mathbb{Z}[i]$ 'de tersinir olmayan bir $\alpha=a+bi(a,b\in\mathbb{Z})$ elemanı birincil ise $a\equiv 1(\mathrm{mod}\,4), b\equiv 0(\mathrm{mod}\,4)$ veya $a\equiv 3(\mathrm{mod}\,4), b\equiv 2(\mathrm{mod}\,4)$ dir [6].

5.1.17 Teorem: $\alpha\in\mathbb{Z}[i]$ tersinir olmayan bir eleman ve $(1+i)\nmid\alpha$ olsun.
O halde $u\alpha$ birincil olacak şekilde u tersinir elemanı vardır [6].

5.1.18 Teorem: $\mathbb{Z}[i]$ 'nin birincil elemanı , birincil indirgenemezlerin çarpımı şeklinde yazılabilir [6] .

İspat: $\alpha\in\mathbb{Z}[i]$ birincil olsun, O halde, $q_i\equiv 3(\mathrm{mod}\,4)$ rasyonel asalları, π_i birincil indirgenemezleri $N(\pi_i)=1(\mathrm{mod}\,4)$ ve $\alpha=u\pi_1...\pi_t(-q_1)...(-q_s)$ olacak şekilde bir ise u tersinir elemanı vardır. İndirgenmiş modül $(1+i)^3$ bize, $1\equiv u\left(\mathrm{mod}(1+i)^3\right)$ olduğunu gösterir.Bu u=1 demektir,dolayısıyla u tersinir elemandir.

5.1.19 Teorem : Eğer $\pi\in\mathbb{Z}[i]$ bir birincil asal ise,ya $\pi\equiv 1(\mathrm{mod}\,4)$ yada $\pi\equiv 3+2i(\mathrm{mod}\,4)$ tür [6].

5.2 Dördüncü Dereceden Kalan Sembolü

5.2.1 Önerme: Eğer $\pi \nmid \alpha$ ise $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$ dir [6].

5.2.2 Uyarı: Eğer π'nin normu 2 den farklı ise, o zaman $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$de 1,-1, -i, +i 'nin kalan sınıfları birbirinden farklıdır. $i \equiv 1 \pmod{\pi}$ olsun. i-1 asal olduğundan π ve 1-i bağlantılı olurlar. Buradan $N(\pi) = N(1-i) = 2$ olur ki, bu durum π'nin normunun 2 den farklı olmasıyla çelişir [6].

5.2.3 Önerme: Eğer $\pi \nmid \alpha$ ise, $(\pi) \neq (1+i)$ ise, $0 \leq j \leq 3$ olacak şekilde bir tek j tamsayısı vardır.Yani, $\alpha^{N(\pi)-1/4} \equiv i^j \pmod{\pi}$ dir [6].

5.2.4 Uyarı: Bu önermede $(\pi) \neq (1+i)$ hipotezi önemlidir. Gerçekten $\pi = 1+i$ olsaydı, bunların normları aynı olacağından 1+i indirgenemez olup $N(1+i) = 2 = -i(1+i)^2$ asal çarpanlarına ayrılacaktı. Ancak π asal olduğundan bu durum çelişki olacaktı [6] .

5.2.5 Uyarı: $x^4 \equiv 1 \pmod{\pi}$ olduğunu göz önüne alalım: $x^4 - 1 \equiv 0 \pmod{\pi}$

$x^4 - 1 = (x^2 - 1)(x^2 + 1) \equiv 0 \pmod{\pi}$

$x^4 - 1 = (x-1)(x+1)(x-i)(x+i) \equiv 0 \pmod{\pi}$ dir [6].

Buradan denklemin köklerinin Lagrange teoremine göre,+1,-1,+i,-i olduğu ortaya çıkar. Öte yandan,{+1,-1,+i,-i} mertebesi 4 olan devirli bir grup olduğundan, $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ çarpımsal alt grubunun mertebesini böler. Bu grubun mertebesi $N(\pi)-1$ olup , $4 \mid (N(\pi)-1)$'dir.

Buradan, $\alpha^{(N(\pi)-1)/4}$'ün aynı zamanda $x^4 \equiv 1 \pmod{\pi}$ kongrüansının bir çözümü olduğu ortaya çıkar. Bu bir çözüm ise,+1,-1,+i,-i birbirlerine denk değildirler, yani kalan sınıfları farklıdır. O halde, $\alpha^{N(\pi)-1/4} \equiv i^j \pmod{\pi}$ dir.

5.2.6 Tanım: Eğer π bir indirgenemez ise , $N(\pi) \neq 2$ olmak üzere, α nın 4.dereceden kalanı $\pi \nmid \alpha$ için $\chi_\pi(\alpha) = i^j (0 \leq j \leq 3)$ olarak tanımlanır. Bu Legendre sembolünün 4.dereceden kalanlara bir genişlemesidir.Özel olarak, $\pi | a$ ise $\chi_\pi(\alpha) = 0$ dır.Bu durum

$$\left(\frac{\alpha}{\pi}\right)_4 = \begin{cases} 1 \ , & \text{Eğer} \quad x^4 \equiv \alpha \pmod{\pi} \quad \text{çözülebilirse} \\ -1, \ i, \ -i & \text{Aksi halde} \end{cases}$$

şeklinde de ifade edilebilir [6].

5.2.7 Önerme: Eğer $\pi \nmid \alpha$ ise,

1) $\chi_\pi = 1 \Leftrightarrow x^4 \equiv \alpha \pmod{\pi}$ dir.Yani $\mathbb{Z}[i]$'de bir çözümü vardır.

2) $\left(\frac{\alpha\beta}{\pi}\right) = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4$,

3) $\overline{\chi_\pi(\alpha)} = \chi_{\bar{\pi}}(\bar{\alpha})$,

4) Eğer $\pi = a + bi$ olmak üzere, birinci tip bir indirgenemez ise, $\left(\frac{-1}{\pi}\right)_4 = (-1)^{(a-1)/2}$

5) Eğer $\alpha \equiv \beta \pmod{\pi}$ ise, $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$ [6] dir.

5.2.8 Önerme: $q \equiv 3 \pmod 4$ olacak şekilde q bir asal olsun. O halde

$\alpha \in \mathbb{Z}, q \nmid a$ için $\left(\frac{a}{q}\right)_4 = 1$ dir [6].

İspat: $q \equiv 3 \pmod 4$ biçiminde bir asal ise, $N(q) = q^2$ dir. Böylece,

$\left(\frac{a}{q}\right)_4 = a^{(q^2-1)/4} = \left(a^{(q-1)}\right)^{(q+1)/4}$ bulunur. Fermat'ın Küçük teoreminden, q asal ve $q \nmid a$ olduğu için $a^{q-1} \equiv 1 \pmod q$ elde edilir.

5.2.9 Önerme: $\alpha \in \mathbb{Z}, \alpha \neq 0$ve $\alpha \in \mathbb{Z}$ tersinir olmayan bir tek sayı olsun.Eğer $(a,\alpha)=1$ ise, $\left(\frac{\alpha}{a}\right)_4 = 1$dir [6].

5.2.10 Önerme: Eğer $n \neq 1$bir tam sayı ve $n \equiv 1 \pmod 4$ ise,$\left(\frac{i}{n}\right)_4 = (-1)^{(n-1)/4}$ dir [6].

5.2.11 Teorem (4.Dereceden Kalanlar Teoremi): Eğer π, θ ; $\mathbb{Z}[i]$de farklı birinci tip asallar ise,$\left(\frac{\pi}{\theta}\right)_4 = \left(\frac{\theta}{\pi}\right)_4 (-1)^{(N(\pi)-1)(N(\theta)-1)/16}$ dir [6].

5.2.12 Uyarı : Eğer π, θ birinci tip asal ise, $\pi = a+bi$ ve $\theta = c+di$ olmak üzere $(N(\pi)-1)(N(\theta)-1)/16$ ile $(a-1)(b-1)/4$ aynı işarete sahiptir.Bu durumda $\left(\frac{\pi}{\theta}\right)_4 = \left(\frac{\theta}{\pi}\right)_4 (-1)^{(a-1)(b-1)/4}$ yazabiliriz [6].

5.2.13 Yardımcı Teorem: Eğer $\pi, \theta \in \mathbb{Z}[i]$ farklı birinci tip asallar ise, $\pi = a+bi$ ve $\theta = c+di$ olmak üzere, π veya θ 'dan biri 4 modülüne göre 1 e denk ise, $\left(\frac{\pi}{\theta}\right)_4 = \left(\frac{\theta}{\pi}\right)_4$ dir [6].

5.2.14 Yardımcı Teorem: $p \equiv 1 \pmod 4$ olmak üzere, $p = a^2 + b^2$ şeklinde yazılır.Ayrıca a bir tek sayı ise,

1) $\left(\frac{a}{p}\right) = 1$,

2) $(a+b)^2 \equiv 2ab \pmod m$

3) $(a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} \pmod p$ [6] dir.

6. SONUÇ VE ÖNERİLER

Tezimde kalan sınıfları incelendi.İkinci bölümde kongrüans kavramı verildi, Fermat'ın küçük teoremi ve Euler'in genelleştirilmesi verildi. Bu teoremlerin bazı büyük sayıların verilen bazı sayılara bölümünden elde edilecek kalanları bulmada nasıl kullanılacağı belirtildi. İki değişkenli lineer kongrüansların oluşturduğu sistemleri ve bunun sonrasında da farklı modlarda verilmiş olan iki değişkenli lineer kongrüansların oluşturduğu sistemler ele alındı.

Konrüans kavramının sadece lineer kongrüanslarla sınırlı olmadığını benzer şekilde verilen bir sayının karesini , küpünü ya da daha yüksek kuvvetlerini verilen moda indirgediğimizde ikinci, üçüncü ya da daha yüksek mertebeden kalanını bulmuş olacağımız görüldü. Diğer bölümlerimizde ikinci dereceden, üçüncü dereceden ve dördüncü dereceden kalanlar incelendi.

Tezim daha yüksek mertebeden kalan bulmada bir fikir verebilir ve n.dereceden kalanlar araştırılabilir.

7. KAYNAKLAR

[1] Namlı, D., "*Kübik Rezidüler*", Doktora Tezi, Balıkesir Üniversitesi Fen Bilimleri Enstitüsü , Matematik Ana Bilim Dalı, Balıkesir, (2001),

[2] Bayraktar, M., *"Soyut Cebir Ve Sayılar Teorisi"* , Gazi Yayınevi, Ankara, (2006).

[3] Jones, G.A. , Jones, J.M. , "*Elementary Number Theory"* , Springer-Verlag New York, Inc: 37-62,83-96, (1998).

[4] Erdoğan, M. and Yılmaz, G., *"Soyut Cebir ve Sayılar Teorisi"*, Beykent Üniversitesi, İstanbul, (2008).

[5] Yıldız İkikardeş, N.," Sonlu Cisimler Üzerinde Frey Eliptik Eğrileri" , Doktora Tezi, Balıkesir Üniversitesi Fen Bilimleri Enstitüsü, Matematik Ana Bilim Dalı , Balıkesir, (2006).

[6] Aktaş, K.," *On The Solutıons Of Congruence Equatıons In The Gaussıan İntegers Rıng and Bıquadratıc Resıdues"*, Yüksek Lisans Tezi, Selçuk Üniversitesi, Konya, (2008).

[7] Çallıalp, F.*,"Sayılar Teorisi"*, Marmara Üniversitesi, Atatürk Egitim Fakültesi, Birsen Yayınevi, İstanbul, (2009).

[8] Ireland, K. Rosen, M. A.," *Classical Introduction to Modern Number Theory"*, Springer-Verlag, New York, Berlin, Heidelberg, (1990),

[9] Lemmeyer, F., "Reciprocity *Laws From Euler to Eiseinstein"*, Stringer, (1991).

[10] LeVeque, W.J., "Fundamentals of Number Theory", Dover Publications, INC: New York, 97-113 , (1996).

[11] Mollin, R.A., “Algebraic Number Theory” , Chapman&Hall/CRC, United States of America, (1999).